Program Fundusz Inicjatyw Obywatelskich na lata 2014–2020 FIO

KONFEDERACJA INICJATYW POZARZĄDOWYCH RZECZYPOSPOLITEJ

NIW Narodowy Instytut Wolności Centrum Rozwoju Społeczeństwa Obywatelskiego

Konfederacja Inicjatyw Pozarządowych Rzeczypospolitej

KODEKS POSTĘPOWANIA

w zakresie przetwarzania danych osobowych w organizacjach pozarządowych

Kodeks został opracowany przez adw. dr Klaudię Gawlik-Bugańską, radcę prawnego Dagmarę Knagę oraz radcę prawnego Krystiana Owczarka, pod nadzorem dr Tymoteusza Zycha.

SPIS TREŚCI

WSTĘP

Kodeks dobrych praktyk adresowany jest do krajowych organizacji społecznych działających na obszarze Rzeczypospolitej Polskiej. W szczególności należą do nich: fundacje, stowarzyszenia, organizacje młodzieżowe, organizacje z obszarów wiejskich i małych miejscowości, organizacje eksperckie typu *think-tank*, organizacje seniorów, organizacje osób niepełnosprawnych oraz organizacje mniejszości narodowych i etnicznych.

Celem kodeksu jest stworzenie spójnych wytycznych pomocnych we wdrożeniu w każdej organizacji pozarządowej podstawowych zasad ochrony danych osobowych, m.in. zasady rozliczalności, zasady zgodności z prawem, rzetelności i przejrzystości, jak również spełnienia obowiązku informacyjnego wobec poszczególnych osób, których dane osobowe organizacja pozarządowa przetwarza jako ich administrator lub podmiot przetwarzający. Kodeks zawiera projekty klauzul informacyjnych dostosowanych do poszczególnych procesów przetwarzania najczęściej występujących w organizacjach. Określa również procedury zbierania danych osobowych. W kodeksie zaproponowano środki zabezpieczenia gromadzonych danych osobowych i wiele innych.

Wśród podstaw prawnych przetwarzania danych osobowych opisano przede wszystkim uzasadniony interes administratora danych (art. 6 ust. 1 lit. f RODO) pod kątem celów statutowych organizacji pozarządowych, przypadki konieczne do pozyskiwania zgody na przetwarzanie danych osobowych (art. 6 ust. 1 lit. a RODO) a także podstawy prawne przetwarzania w procesie zbierania funduszy (fundrisingu). Podstawy prawne przetwarzania danych osobowych opisujące w szczególności uzasadniony interes administratora danych (art. 6 ust. 1 lit. f RODO) pod kątem celów statutowych organizacji pozarządowych, przypadków koniecznych do pozyskiwania zgody na przetwarzanie danych osobowych.

Kodeks opisuje również typowe, najczęściej stosowane w działalności organizacji pozarządowych, procesy przetwarzania, jak np. wpłaty od darczyńców, działania na rzecz podopiecznych, beneficjentów, współpraca z wolontariuszami.

ROZDZIAŁ I. DEFINICJE i SKRÓTY

RODO (ogólne rozporządzenie o ochronie danych) - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Ustawa o ochronie danych osobowych - ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.2019.123 t.j. z późn. zm.).

Ustawa o świadczeniu usług drogą elektroniczną - ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.2019.123 t.j. z późn. zm.).

Prawo telekomunikacyjne - ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U.2018.1954 t.j. z późn. zm.).

Prawo autorskie - ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2019 r. poz. 1231 z późn. zm.).

Ustawa o działalności pożytku publicznego i o wolontariacie - ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (Dz.U. z 2019 r. poz. 688).

Ustawa o rachunkowości - ustawa z dnia 29 września 1994r. o rachunkowości (t.j. Dz. U. z 2019 r.351).

Ustawa o podatku dochodowym od osób fizycznych - ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (t.j. Dz.U.2019.1387).

Dekret – dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim, wydany na podstawie kan. 455 Kodeksu Prawa Kanonicznego przez Konferencję Episkopatu Polski w dniu 13 marca 2018 r.

Kodeks dobrych praktyk (Kodeks) - niniejszy kodeks.

Organizacja (organizacja pozarządowa, organizacja społeczna, NGO) - *niebędące jednostkami sektora finansów publicznych, w rozumieniu przepisów o finansach publicznych, i niedziałające w celu osiągnięcia zysku, osoby prawne lub jednostki nieposiadające osobowości prawnej utworzone na podstawie przepisów ustaw, w tym fundacje i stowarzyszenia*, przy czym niektórych przepisów ustawy nie stosuje się do fundacji publicznych i fundacji partii politycznych (art. 3 ust. 2 ustawy o działalności pożytku publicznego i o wolontariacie (Dz.U. z 2019 r. poz. 688). Do przykładowych organizacji pozarządowych należą: fundacje, stowarzyszenia, organizacje młodzieżowe, organizacje z obszarów wiejskich i małych miejscowości, organizacje eksperckie typu think-tank, organizacje seniorów, organizacje osób niepełnosprawnych, organizacje mniejszości narodowych i etnicznych, jak również stowarzyszenia zwykłe a także pozostałe NGO's działające na obszarze Polski.

UODO - Urząd Ochrony Danych Osobowych.

ROZDZIAŁ II.
PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH W ORGANIZACJACH SPOŁECZNYCH

Organizacja społeczna planując przetwarzanie danych osobowych w toku swojej działalności, powinna określić odpowiednią podstawę prawną przetwarzania. Podstawy prawne przetwarzania danych zostały określone w art. 6 i 9 RODO.

Typowymi przesłankami legalizującymi przetwarzanie zwykłych danych osobowych w organizacjach społecznych są:

1. Prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO),
2. Umowa (art. 6 ust. 1 lit. b RODO)
3. Zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a RODO).

Odnośnie danych wrażliwych RODO przewiduje, że organizacja może przetwarzać dane osobowe:

1. członków oraz byłych członków fundacji, stowarzyszeń lub innych niezarobkowych podmiotów o celach politycznych, światopoglądowych, religijnych lub związkowych (art. 9 ust. 2 lit. d RODO). Więcej informacji o przetwarzaniu danych członków i byłych członków znajduje się w rozdziale IV pkt 13,
2. na podstawie wyraźnej zgody osoby, której dane dotyczą (art. 9 ust. 2 lit. a RODO).

Organizacja jest zobowiązana do wyboru właściwej podstawy prawnej przetwarzania danych.

I. Przesłanki legalizujące przetwarzanie danych zwykłych

1. Prawnie uzasadniony interes administratora

Zgodnie z motywem 47 preambuły RODO podstawą prawną przetwarzania mogą być prawnie uzasadnione interesy administratora, w tym administratora, któremu mogą zostać ujawnione dane osobowe lub strony trzeciej, o ile w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z administratorem nadrzędne nie są interesy lub podstawowe prawa i wolności osoby, której dane dotyczą. Taki prawnie uzasadniony interes może istnieć na przykład w przypadkach, gdy zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą a administratorem, na przykład gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz. Aby stwierdzić istnienie prawnie uzasadnionego interesu, należałoby w każdym przypadku przeprowadzić dokładną ocenę, w tym ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w tym celu. Interesy i prawa podstawowe osoby, której dane dotyczą, mogą być nadrzędne wobec interesu administratora danych w szczególności w przypadkach, gdy dane osobowe są przetwarzane w sytuacji, w której osoby, których dane dotyczą, nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania. (…) Prawnie uzasadnionym interesem administratora, którego sprawa dotyczy, jest również przetwarzanie danych osobowych bezwzględnie niezbędne do zapobiegania oszustwom. Za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego.

Prawnie uzasadniony interes administratora będzie główną podstawą prawną przetwarzania danych osobowych w organizacjach społecznych. Nie oznacza to jednak, że podstawa ta będzie zawsze właściwa dla wszystkich procesów przetwarzania w organizacji. W celu oceny, czy będzie to odpowiednia przesłanka legalizująca przetwarzanie danych, organizacja przed rozpoczęciem czynności przetwarzania powinna przeprowadzić test uzasadnionego interesu, o którym mowa w art. 6 ust. 1 lit. f RODO.

Jeżeli w efekcie przeprowadzenia testu uzasadnionego interesu organizacja dojdzie do wniosku, że interes administratora danych w przetwarzaniu danych osobowych jest co najmniej równoważny wobec praw, wolności i interesów osób, których dane dotyczą, wówczas przetwarzanie danych na podstawie prawnie uzasadnionego interesu administratora będzie dopuszczalne.

Natomiast jeśli w wyniku testu okaże się, że interesy osoby, której dane dotyczą, mają charakter nadrzędny wobec interesów organizacji jako administratora danych, wówczas nie może ona oprzeć przetwarzania na prawnie uzasadnionym interesie administratora, lecz powinna poszukiwać innej przesłanki legalizującej przetwarzanie danych osobowych.

Na test uzasadnionego interesu składa się**:**

1) **ocena celowości przetwarzania** – w ramach której należy określić na czym polega uzasadniony interes administratora na przetwarzanie danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach.

   W ramach oceny celowości przetwarzania należy uwzględnić następujące zagadnienia:
   - dlaczego organizacja chce przetwarzać dane osobowe?
   - jakich korzyści spodziewa się po realizacji procesu przetwarzania danych?
   - jak istotne są one dla organizacji?
   - czy z przetwarzania danych korzystają osoby trzecie?
   - czy przetwarzanie danych przynosi szersze korzyści dla społeczeństwa?
   - jakie byłyby skutki, gdyby nie mogła kontynuować przetwarzania danych?
   - czy organizacja przestrzega regulacji szczególnych w zakresie przetwarzania danych osobowych, np. przepisów branżowych, kodeksów postępowania, innych szczególnych zasad ochrony danych, które mają zastosowanie do przetwarzania danych np. wymogów w zakresie profilowania?
   - czy istnieją inne kwestie etyczne związane z przetwarzaniem danych?

2) **ocena niezbędności przetwarzania** – w ramach, której należy zbadać, czy przetwarzanie danych jest niezbędne do osiągnięcia określonego celu przetwarzania.

   W ramach oceny niezbędności należy uwzględnić następujące zagadnienia:
   - czy to przetwarzanie rzeczywiście pomoże organizacji osiągnąć cel, w którym zamierza przetwarzać dane osobowe?
   - czy przetwarzanie danych jest proporcjonalne do tego celu?
   - czy można osiągnąć ten sam cel bez przetwarzania danych osobowych?

- czy ten sam cel można osiągnąć, przetwarzając mniej danych lub przetwarzając dane w inny, prostszy lub mniej inwazyjny, sposób?
- z jakich przyczyn inne, mniej inwazyjne, sposoby przetwarzania danych osobowych nie stanowią alternatywy godnej rozważenia?

3) **test równowagi interesów administratora i podmiotu danych** – w ramach którego należy dokonać weryfikacji, czy nadrzędny charakter wobec interesów administratora mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem (art. 6 ust. 1 lit. f) RODO).

   W ramach testu równowagi należy uwzględnić:

   a) **naturę (kategorię) przetwarzanych danych**, w tym w szczególności:
      - czy są to dane szczególnych kategorii, czy dane dotyczące wyroków skazujących i czynów zabronionych?
      - czy są to dane, które w ocenie przeciętnego człowieka mogą być uznane za szczególnie chronione?
      - czy organizacja przetwarza dane dzieci bądź osób wymagających specjalnej troski?

   b) **uzasadnione oczekiwania podmiotów danych** - czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w określonym celu.

      W tym zakresie należy rozważyć w szczególności:
      - jaki jest charakter relacji zachodzącej pomiędzy organizacją a osobą, której dane dotyczą?
      - w jaki sposób organizacja wykorzystywała dane osobowe w przeszłości?
      - czy dane zostały zebrane bezpośrednio od tej osoby czy z innego źródła?
      - jaki był sposób komunikacji celów przetwarzania danych w momencie zbierania danych?
      - czy i w jaki sposób podmiot ten spełnił obowiązek informacyjny, jeżeli dane zostały pozyskane z innego źródła niż osoba, której dotyczą, np. od brokera danych?
      - jak dawno dane zostały pozyskane i czy od tego czasu nastąpiły zmiany technologiczne lub kontekst, który powodowałaby, że wykorzystanie danych mogłoby być zaskakujące dla osoby, której dane dotyczą?
      - czy zamierzony cel i metoda wykorzystania danych osobowych nie jest ujmowana przez organizację zbyt szeroko?
      - czy organizacja zamierza wprowadzać nowości bądź innowacje w wykorzystaniu danych osoby, której dane dotyczą?
      - czy organizacja dysponuje wynikami badań osób, których dane dotyczą, w zakresie oczekiwań co do wykorzystania ich danych przez organizację, wynikami z badań rynkowych, grup fokusowych bądź wynikami innych form konsultacji?
      - czy w danych okolicznościach istnieją inne czynniki wpływające na oczekiwanie podmiotów danych odnośnie przetwarzania ich danych osobowych?
      - czy zgoda nie jest bardziej odpowiednią przesłanką mając na względzie, że wymaga ona świadomości i dobrowolności ze strony podmiotu danych?

c) **potencjalny wpływ na osoby, których dane dotyczą -** w tym zakresie należy rozważyć m.in.:
   - jaki jest możliwy wpływ przetwarzania na osoby, których dane dotyczą?
   - czy przetwarzania danych nie przyczyni się do powstania barier utrudniających osobom fizycznym dostęp do usług?
   - czy przetwarzania danych nie przyczyni się do powstania barier utrudniających osobom fizycznym korzystania z przysługujących im praw?
   - czy osoby, których dane dotyczą, mogłyby utracić kontrolę nad swoimi danymi wykorzystywanymi przez organizację?
   - czy przetwarzania danych nie przyczyni się do powstania szkód fizycznych, strat finansowych, szkód moralnych, kradzieży tożsamości etc.?
   - jakie jest prawdopodobieństwo wystąpienia jakiegokolwiek potencjalnego wpływu i jego dotkliwość?
   - czy wyjaśnienie osobom fizycznym konieczności przetwarzania ich danych nie byłoby zbyt problematyczne dla organizacji?
   - czy osoby, których dane dotyczą, mogłyby sprzeciwić się wobec przetwarzania ich danych bądź uznać je za zbyt uciążliwe?
   - jakie dodatkowe zabezpieczenia może zapewnić organizacja w celu zminimalizowania negatywnego wpływu na osobę, których dane dotyczą, takich jak, minimalizacja danych, technologie służące zwiększeniu ochrony prywatności; zwiększona przejrzystość, ogólne i ułatwienia w realizacji prawa do zgłoszenia sprzeciwu wobec przetwarzania danych oraz możliwość przenoszenia danych?

Po obiektywnym rozważeniu wszystkich czynników zidentyfikowanych podczas badania uzasadnionego interesu, organizacja powinna dokonać oceny, czy interesy organizacji mogą mieć pierwszeństwo przed interesami lub podstawowymi prawami i wolności osoby, której dane dotyczą.

Organizacja powinna umieć wykazać, dlaczego korzyści płynące z przetwarzania danych uzasadniają przetwarzanie danych, pomimo zidentyfikowanego w trakcie badania ryzyka dla osoby, której dane dotyczą. Im większe jest to ryzyko, tym bardziej przekonujące musi być uzasadnienie przetwarzania danych.

Przykład:

Organizacja planuje wysłać materiały informujące o działalności organizacji oraz możliwości wsparcia finansowego za pośrednictwem poczty tradycyjnej do osób, które wpłaciły darowiznę na cele statutowe organizacji. Wysyłka materiałów kierowana jest wyłącznie do darczyńców, którzy wcześniej nie sprzeciwiali się otrzymywaniu od organizacji materiałów w celu pozyskania funduszy.

Odpowiedź na pytanie, czy przetwarzanie danych jest zgodne z prawem na podstawie prawnie uzasadnionego interesu administratora zależy od konkretnych okoliczności i wymaga badania pod kątem niezbędności, celowości przetwarzania a także równowagi interesów organizacji i darczyńcy.

W ramach testu uzasadnionego interesu należy wziąć pod uwagę w szczególności, czy adresaci informacji mogą oczekiwać, że organizacja wykorzysta ich dane w ten sposób. W tym zakresie organizacja powinna zwrócić uwagę na to, czy dane odbiorców informacji zostały zebrane bezpośrednio od nich, czy też od osób, których dane nie dotyczą (pośrednio).

Organizacja powinna również ocenić możliwe niedogodności dla odbiorców w związku z potencjalnie niepożądanym komunikatem ze strony organizacji, w szczególności czy wybrana metoda komunikacji lub jej częstotliwość może być odebrana jako istotna niedogodność dla bardziej wrażliwego odbiorcy.

Osoby, których dane dotyczą, posiadają bezwzględne prawo do zgłoszenia sprzeciwu wobec komunikacji ze strony organizacji pozarządowej. O prawie tym osoba, której dane dotyczą, powinna być poinformowana przy zbieraniu danych bądź przy pierwszej komunikacji, jeżeli dane zostały zebrane w sposób inny niż od osoby, której dane dotyczą.

Dla oceny, czy wystarczającą podstawę prawną przetwarzania danych darczyńców w celu wysyłki powyższych materiałów stanowi uzasadniony interes administratora organizacji, powinna rozważyć:

1) czy wysyłka materiałów jest konieczna dla celów fundraisingowych?	po analizie organizacja stwierdza, że istnieje taka konieczność
2) jakiego rodzaju dane osobowe mogą być wykorzystane w wysyłce materiałów, biorąc pod uwagę racjonalne oczekiwania odbiorców ze względu na charakter komunikacji?	po analizie organizacja stwierdza, że może wykorzystać jedynie imię, nazwisko, adres korespondencyjny odbiorców

3) czy wysyłka materiałów pocztą tradycyjną stanowi proporcjonalny sposób zwracania się do darczyńców z prośbą o dalsze wsparcie oraz informowania o realizacji celów statutowych organizacji?	po analizie organizacja określa, że wpływ na darczyńców może być minimalny; jednocześnie w wysyłanych materiałach organizacja zamieszcza informację o możliwości złożenia sprzeciwu i rezygnacji z otrzymywania tego typu materiałów w przyszłości; zgodnie z art. 21 RODO osobie, której dane dotyczą, przysługuje prawo do wniesienia sprzeciwu wobec przetwarzanie jej danych osobowych, o czym należy ją uprzednio poinformować; w takim przypadku organizacja powinna zaprzestać przetwarzania jej danych do celów wysłania materiałów informujących o działalności organizacji oraz możliwości wsparcia finansowego organizacji.

Po wykonaniu powyższego testu należy zapisać jego wynik, niezależnie od tego, czy odpowiedzi na poszczególne zagadnienia wspierają stanowisko organizacji odnośnie dopuszczalności przetwarzania danych na podstawie uzasadnionego interesu administratora. Pozwali to organizacji na wykazanie przed organem nadzoru, że wszystkie czynniki zostały wzięte pod uwagę przed podjęciem ostatecznej decyzji o przetwarzaniu danych na podstawie prawnie uzasadnionego interesu administratora.

2. Umowa

Zgodnie z art. 6 ust. 1 lit. b RODO oraz motywem 44 RODO przetwarzanie powinno być zgodne z prawem, jeżeli jest ono niezbędne w związku z zawarciem umowy lub zamiarem zawarcia umowy na żądanie osoby, której dane dotyczą.

W organizacjach społecznych ta podstawa prawna przetwarzania danych ma zastosowanie w szczególności w następujących przypadkach:

- wpłat dokonywanych przez darczyńców na rzecz organizacji (wykonywanie umów darowizny),
- zawierania umów ze zleceniobiorcami, z dostawcami towarów i usług na rzecz organizacji,
- nawiązywania umów cywilnoprawnych, np. z wolontariuszami,
- realizacji zamówienia na bezpłatną publikację.

3. Zgoda osoby, której dane dotyczą

Zgoda jako przesłanka legalizująca przetwarzania danych osobowych

Organizacje społeczne powinny opierać się na zgodzie osoby, której dane dotyczą, dopiero gdy nie znajdą innych przesłanek legalizujących przetwarzanie danych określonych w art. 6 lub art. 9 RODO.

Przetwarzanie danych osobowych na podstawie zgody może wystąpić w następujących przypadkach:

1) gdy organizacja planuje przekazanie osobie obdarowanej danych osobowych darczyńcy, który przekazuje 1% podatku na rzecz organizacji pożytku publicznego,
2) gdy organizacja planuje rozpowszechnianie wizerunku uczestnika konkursu organizowanego przez organizację bądź planuje upublicznić dane osobowe laureata konkursu,
3) gdy organizacja zamierza rozpowszechnić wizerunek prelegenta lub uczestnika wydarzenia publicznego,
4) gdy organizacja zamierza korzystać z dokumentów aplikacyjnych przesłanych przez kandydatów do pracy w przyszłych rekrutacjach,
5) gdy organizacja społeczna prowadząca działalność gospodarczą, planuje wysłanie informacji handlowych w rozumieniu z art. 10 ust. 2 ustawy o świadczeniu usług drogą elektroniczną lub kierowanie treści marketingowych na telekomunikacyjne urządzenia końcowe na podstawie art. 172 prawa telekomunikacyjnego.

Formy wyrażenia zgody

W przypadku, gdy podstawą przetwarzania danych osobowych ma być zgoda osoby, której dane dotyczą, zgoda może zostać wyrażona poprzez:
1) złożenie oświadczenia woli w formie ustnej, dokumentowej lub w formie pisemnego oświadczenia podpisanego przez osobę, której dane dotyczą,
2) wyraźne działanie potwierdzające, w tym poprzez:
   a) wypełnienie formularza elektronicznego,
   b) zaznaczenie okienka wyboru na formularzu lub w systemie informatycznym, przy którym są wskazane treści zgód,
   c) zaznaczenie pola wyboru 'TAK' pod tekstem „Niniejszym wyrażam zgodę na przetwarzania danych osobowych" zamieszczonym w wiadomości e-mail,
   d) weryfikację dwuetapową via e-mail lub SMS – w celu potwierdzenia wyraźnej zgody osoby, której dane dotyczą, otrzymuje:
      i. wiadomość e-mail z prośbą o odpowiedź w formie wiadomości e-mail zawierającej oświadczenie „Wyrażam zgodę" bądź
      ii. wiadomość e-mail z linkiem weryfikacyjnym, który należy kliknąć, bądź
      iii. wiadomość SMS z kodem weryfikacyjnym.
   e) wybór przez osobę, której dane dotyczą, określonych ustawień technicznych w systemie informatycznym,
   f) przekazanie danych osobowych przez osobę, której dane dotyczą, w celu uzyskania odpowiedzi na zapytanie,
   g) oświadczenie o wyrażeniu zgody przesłane drogą elektroniczną, np. e-mailem,
   h) wrzucenie wizytówki do wyznaczonego pojemnika w celu wzięcia udziału w losowaniu, np. w loterii z nagrodami,
   i) przesłanie dokumentów aplikacyjnych zawierających zdjęcie kandydata do pracy.

Nieważność zgody

Zgoda nie może być uznawana za wyrażoną świadomie i dobrowolnie w następujących przypadkach:
1) milczenia osoby, niepodjęcia przez nią działań, bądź braku sprzeciwu z jej strony, zaznaczenia domyślnie okienek wyboru w systemie informatycznym (motyw 32 RODO),

2) zapytanie o zgodę nie zostało przedstawione w sposób pozwalający wyraźnie odróżnić go od pozostałych kwestii, w przypadku gdy treść zgody na przetwarzanie danych zawarta jest w pisemnym oświadczeniu, które zawiera również inne treści (art. 7 ust. 2 RODO),
3) jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji (motyw 42 RODO),
4) jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne (motyw 43 RODO),
5) jeżeli od zgody uzależnione jest wykonanie umowy - w tym świadczenie usługi - mimo że do jej wykonania zgoda nie jest niezbędna (motyw 43 RODO).

Okres ważności zgody

Ramy czasowe, w których zgoda jest ważna, zależy od kontekstu, zakresu pierwotnej zgody i oczekiwań osoby, której dane dotyczą. Jeżeli operacje przetwarzania zmienią się lub ewoluują w sposób znaczący, wówczas pierwotna zgoda nie będzie już ważna. W takim wypadku organizacja powinna uzyskać nową zgodę.

Aktualizacja zgody

Dobrą praktyką jest, aby zgoda była aktualizowana we właściwych odstępach czasu. Ponowne przekazanie wszystkich informacji pomaga zapewnić, by osoba, której dane dotyczą, w dalszym ciągu była dobrze poinformowana, w jaki sposób wykorzystywane są jej dane i jak może korzystać ze swoich praw.

Wykazanie zgody przez organizację

Administrator jest odpowiedzialny za uzyskanie ważnej zgody od osób, które dane dotyczą i wdrożone mechanizmy pozyskiwania zgód. Zgodnie z art. 7 ust. 1 RODO oraz motywem 42 RODO na administratorze spoczywa obowiązek wykazania, że osoba, której dane dotyczą, wyraziła zgodę (ciężar dowodu).

Obowiązek wykazania, że administrator uzyskał ważną zgodę, nie powinien jednak sam w sobie prowadzić do nadmiernego przetwarzania dodatkowych danych.

Dowód na wyrażenie zgody nie powinien być przechowywany dłużej niż jest to bezwzględnie konieczne do wywiązania się z prawnego obowiązku lub do ustalenia, dochodzenia lub obrony roszczeń zgodnie z art. 17 ust. 3 lit. b) i e) RODO.

Administrator musi być również w stanie wykazać, że osoba, której dane dotyczą, została poinformowana a procedura zastosowana przez administratora spełniała wszystkie właściwe kryteria uzyskania ważnej zgody.

Przykład:

Zgoda zostaje uzyskana w trakcie rozmowy telefonicznej przez nagranie ustnego oświadczenia

osoby, której dane dotyczą, w którym osoba ta potwierdza, że zgadza się na wykorzystanie swoich danych do rejestracji na konferencję naukową.

Prawa osób, które wyraziły zgodę na przetwarzanie danych

Jeżeli przetwarzanie danych odbywa się w oparciu o przesłankę zgody, osoba, których dane dotyczą, posiada prawo do:

1) wycofania zgody,
2) usunięcia danych, jeżeli zgoda została wycofana,
3) ograniczenia przetwarzania,
4) sprostowania danych
5) dostępu do danych oraz uzyskania kopii danych.

Więcej informacji o wyżej wymienionych uprawnieniach znajduje się w Rozdziale III poświęconym realizacji praw jednostki.

Zgoda udzielana przez dzieci

W przypadku gdy przetwarzanie dotyczy usług społeczeństwa informacyjnego (usługi w trybie online) oferowanych bezpośrednio dziecku, a przetwarzanie to jest oparte na zgodzie, administrator może przetwarzać dane dziecka, pod warunkiem, że ukończyło ono 16 lat.

Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zatwierdziła osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody (art. 8 ust. 1 RODO). Zgodnie z motywem 38 RODO zgoda rodzica lub opiekuna nie jest wymagana w przypadku usług profilaktycznych lub doradczych, oferowanych za pośrednictwem Internetu bezpośrednio dziecku.

Świadcząc dzieciom usługi społeczeństwa informacyjnego na podstawie zgody, administrator powinien podjąć rozsądne starania, by zweryfikować:

1) czy użytkownik osiągnął wiek uprawniający do wyrażenia zgody drogą elektroniczną,
2) czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała.

Powyższe starania powinny uwzględniać dostępną technologię oraz być proporcjonalne do charakteru czynności przetwarzania i związanego z nimi ryzyka, tak aby nie prowadzić do nadmiernego przetwarzania danych.

W sytuacjach niskiego ryzyka związanego z przetwarzaniem wystarczająca będzie weryfikacja za pośrednictwem poczty elektronicznej.

W przypadku wysokiego ryzyka, administrator powinien zwrócić się o dostarczenie innych dowodów , np. poprosić rodzica lub opiekuna, aby dokonał przelewu symbolicznej kwoty, np. 1 gr na rachunek bankowy administratora a w opisie transakcji wskazał, że sprawuje władzę rodzicielską lub opiekę nad użytkownikiem.

Ważność zgód na przetwarzanie danych udzielonych przed rozpoczęciem obowiązywania RODO

Zgodnie z motywem 171 RODO osoba, której dane dotyczą, nie musi ponownie wyrażać zgody, jeżeli pierwotny sposób jej wyrażenia odpowiada warunkom RODO.

Nie jest wymagane, automatycznie, przeprowadzenie całkowitego odświeżenia zgód na przetwarzanie danych osobowych pozyskanych zgodnie z krajowym prawem w dziedzinie ochrony danych przed rozpoczęciem obowiązywania RODO, tj. przed 25 maja 2018r.

Zgoda, którą uzyskano do tego czasu, pozostaje ważna w zakresie, w jakim jest ona zgodna z warunkami określonymi w RODO. Na ciągłość zgody wyrażonej przed rozpoczęciem obowiązywania RODO nie ma wpływu rozszerzony obowiązek informacyjny przewidziany w art. 13 i 14 RODO.

Zgodnie z motywem 42 RODO „aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych."

Mając na uwadze, że RODO podnosi standardy w zakresie zgód na przetwarzanie danych, zgody będą wymagają odnowienia w przypadku gdy administrator uzyskał zgodę w sposób domniemamy, np. w formie domyślnie zaznaczonego okienka wyboru w formularzu internetowym albo, gdy zgoda była 'ukryta' w ogólnych warunkach umowy.

Administrator powinien zaprzestać czynności przetwarzania danych osobowych, co do których:

1) nie jest w stanie odnowić zgody w sposób zgodny z RODO,
2) nie jest w stanie zapewnić przestrzegania zasad zgodnego z prawem, uczciwego i przejrzystego przetwarzania danych
3) nie może powołać na inną podstawę przetwarzania danych.

4. Wypełnienie obowiązku prawnego ciążącego na administratorze.

Zgodnie z art. 6 ust.1 lit. c RODO przetwarzanie jest zgodne z prawem w przypadkach, gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

Przepis ten nie stanowi samodzielnej przesłanki do legalizacji przetwarzania danych, ale może zaistnieć jedynie w połączeniu z odpowiednim przepisem prawa obowiązującego w państwie, któremu podlega administrator lub też w połączeniu z odpowiednim przepisem unijnym. Podstawami prawnymi muszą być przepisy prawne o charakterze powszechnie obowiązującym, które mogą być zastosowane bezpośrednio.

Administrator może być zarówno podmiotem prawa prywatnego, jak, i prawa publicznego, przepis ten bowiem znajduje zastosowanie tak do organów publicznych, jak i do organizacji prywatnych Nie ma także znaczenia, z jakiej gałęzi prawa pochodzą normy prawne kreujące obowiązek prawny. Dla organizacji społecznych podlegających prawu polskiemu będą ustawy, rozporządzenia, ratyfikowane

umowy międzynarodowe. Ewentualną kolizję pomiędzy przepisami prawa krajowego i prawa Unii rozstrzyga zasada pierwszeństwa prawa europejskiego.

Przetwarzanie danych osobowych wynikające z przepisu prawa musi być do tego celu niezbędne. Niezbędność przetwarzania danych oznacza, iż konkretny przepis prawa określać będzie zakres przetwarzania wyznaczający ramy niezbędności, np. poprzez wskazanie zakresu danych.

Ze względu na cel przetwarzania danych legalizacja przetwarzania danych na podstawie przesłanki z art. 6 ust. 1 lit. c RODO wyłącza, zgodnie z art. 17 ust. 3 lit. b RODO, uprawnienie podmiotu danych do skorzystania z prawa do usunięcia danych (prawa do bycia zapomnianym) w zakresie, w jakim przetwarzanie jest niezbędne w szczególności do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, oraz wyłącza także prawo podmiotów danych do przenoszenia danych, które to prawo uregulowano w art. 20 RODO.

Przy omawianiu przesłanki legalizacyjnej z art. 6 ust. 1 lit. c należy także wspomnieć, iż zgodnie z art. 6 ust. 2 RODO państwa członkowskie mogą zachować lub wprowadzić bardziej szczegółowe przepisy, aby dostosować stosowanie przepisów rozporządzenia w odniesieniu do przetwarzania służącego wypełnieniu obowiązku prawnego ciążącego na administratorze. Nie upoważnia to państw członkowskich do rozszerzania katalogu podstaw legalizacyjnych przetwarzania danych.

Osobną kwestią związaną z interpretacją art. 6 ust. 1 lit. c RODO jest przetwarzanie danych wynikające z treści wyroku sądu powszechnego przekazanego administratorowi do wykonania (dotyczyć to może np. sytuacji w której osoba skazana prawomocnym wyrokiem sądu jest zobowiązana do wykonania prac społecznych na rzecz jakiegoś podmiotu lub do zapłaty nawiązki na wskazany cel społeczny, np. na fundację zajmującą się ochroną zdrowia, i te podmioty stają się administratorami danych osoby skazanej).

W tym miejscu należy wskazać, iż orzeczenia sądów powszechnych są elementami porządku prawnego każdego państwa, zatem wykonanie tych orzeczeń także musi mieć oparcie w konkretnych przepisach prawa, przy czym na administratora danych nakładany jest obowiązek prawny współdziałania w wykonaniu orzeczeń – innymi słowy, przetwarzanie danych w sytuacji, gdy jest ono wynikiem orzeczenia sądu, odpowiada przesłance legalizacji wynikającej z treści art. 6 ust. 1 lit. c RODO.

5. Niezbędność przetwarzania dla wykonania zadania realizowanego w interesie publicznym.

Zgodnie z art. 6 ust. 1 lit. e RODO przetwarzanie jest zgodne z prawem, gdy jest ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

W tym przypadku przewidziane są dwie rozłączne przesłanki legalizujące przetwarzanie:
- przetwarzanie może być niezbędne do wykonania zadania realizowanego w interesie publicznym lub
- niezbędne w ramach sprawowania władzy publicznej powierzonej administratorowi.

W obu przypadkach zarówno zadanie, jak i sprawowanie władzy publicznej muszą zostać sprecyzowane w innych przepisach prawa krajowego lub unijnego.

RODO w motywie 45 wskazuje, że prawo Unii lub prawo państwa członkowskiego powinno określać, czy administratorem wykonującym zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powinien być organ publiczny, czy inna osoba fizyczna lub prawna podlegająca prawu publicznemu lub prawu prywatnemu, np. zrzeszenie zawodowe, jeżeli uzasadnia to interes publiczny, w tym cele zdrowotne, takie jak zdrowie publiczne, ochrona socjalna oraz zarządzanie usługami opieki zdrowotnej.

Przetwarzanie danych osobowych do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi musi być do tego celu niezbędne.

W przypadku korzystania przez administratora z przesłanki legalizacyjnej z art. 6 ust. 1 lit. e osobie, której dane dotyczą, przysługuje zgodnie z art. 21 ust. 1 RODO prawo wniesienia sprzeciwu wobec przetwarzania z przyczyn związanych z jej szczególną sytuacją. W takiej sytuacji administrator musi zaprzestać przetwarzania, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Uprawnienie do wniesienia sprzeciwu wyłączone będzie w stosunku do przetwarzania do celów badań naukowych lub historycznych lub do celów statystycznych, jeśli następuje ono na podstawie przesłanki niezbędności do wykonania zadania realizowanego w interesie publicznym.

6. Niezbędność przetwarzania z uwagi na ochronę żywotnych interesów osoby.

W przepisie art. 6 ust. 1 lit. d RODO ustawodawca przewidział przesłankę legalizującą przetwarzanie danych osobowych w postaci niezbędności przetwarzania do ochrony żywotnych interesów podmiotu danych lub innej osoby fizycznej.

Jak wynika z powyższego, przetwarzanie danych osobowych na podstawie art. 6 ust. 1 lit. d RODO jest możliwe, gdy brak jest możliwości oparcia przetwarzania danych na innej przesłance legalizującej przetwarzanie danych osobowych, gdyż na taką wolę prawodawcy unijnego wskazuje motyw 46 RODO.

Dla możliwości oparcia przetwarzania danych osobowych na przepisie art. 6 ust. 1 lit. d niezbędne jest występowanie żywotnych interesów. Autorzy RODO w motywie 46 wskazują, że chodzi tu o interesy, które mają znaczenie dla życia podmiotu danych lub innej osoby fizycznej, jednakże nie należy przy tym rozumieć tych interesów jako tych, od których zależy życie człowieka. Przykładami żywotnych interesów mogą być: cele humanitarne, monitorowanie epidemii i ich rozprzestrzeniania się, nadzwyczajne sytuacje humanitarne, a w szczególności klęski żywiołowe i katastrofy spowodowane przez człowieka, przypadki ratowania życia, zdrowia, a także ochrony majątku. Należy przy tym pamiętać, że na przepisie art. 6 ust. 1 lit. d można oprzeć jedynie przetwarzanie danych osobowych, które nie są danymi osobowymi wrażliwymi.

Do przetwarzania danych osobowych wystarczające jest, by odbywało się ono w żywotnym interesie podmiotu danych albo innej osoby fizycznej, albo też zarówno w żywotnym interesie podmiotu danych, jak i innej osoby fizycznej, przy czym dane osobowe podmiotu danych będą mogły być przetwarzane nawet wtedy, gdy jego własne żywotne interesy za tym nie przemawiają, ale uzasadniają to żywotne interesy innej osoby fizycznej (np. podanie do publicznej wiadomości danych osobowych osoby stwarzającej zagrożenie dla życia i zdrowia innych w związku z popełnieniem przez nią przestępstwa i trwającymi poszukiwaniami).

Podmiotem danych jest osoba, której dane dotyczą, natomiast osobą fizyczną każdy człowiek od chwili urodzenia aż do chwili jego śmierci. Jak wynika z powyższego, z zastosowania przepisu wyłączone jest przetwarzanie uzasadnione interesami osoby prawnej czy jednostki organizacyjnej niebędącej osobą prawną, której ustawa przyznaje zdolność prawną.

Dla zastosowania przepisu art. 6 ust. 1 lit. d RODO koniecznymi przesłankami są nie tylko występowanie żywotnego interesu podmiotu danych lub innej osoby, której dane dotyczą, ale także niezbędność przetwarzania dla ochrony tych interesów.

W tym miejscu należy wskazać, iż pojęcie niezbędności należy rozumieć analogicznie jak na gruncie przepisu art. 6 ust. 1 lit. b RODO. Oznacza to zatem, że przetwarzanie danych dla ochrony żywotnych interesów podmiotu danych lub innej osoby fizycznej musi być potrzebne, przy czym podobnie jak na gruncie przepisu art. 6 ust. 1 lit. b RODO również tutaj musi występować bezpośredni związek pomiędzy ochroną żywotnego interesu a potrzebą przetwarzania danych osobowych.

Jak już wskazano, do zaistnienia tak rozumianego związku nie jest konieczne, by podmiot danych nie miał możliwości wyrażenia zgody na przetwarzanie danych osobowych. Prawodawca zaznaczył w motywie 46, że zasadniczo art. 6 ust. 1 lit. d RODO może być zastosowany, gdy nie można oprzeć przetwarzania danych na żadnej innej przesłance legalizującej przetwarzanie.

II. Przesłanki legalizujące przetwarzanie danych wrażliwych

Zgodnie z art. 9 RODO zabrania się przetwarzania tzw. danych osobowych wrażliwych. Katalog ten obejmuje:

1) dane ujawniające pochodzenie rasowe lub etniczne;
2) dane ujawniające poglądy polityczne, przekonania religijne lub światopoglądowe;
3) dane ujawniające przynależność do związków zawodowych;
4) dane genetyczne;
5) dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej;
6) dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Jest to katalog zamknięty, co oznacza, że zabronione jest przetwarzanie tylko tych danych, które ujęte są w przepisie. art. 9 RODO.

Przetwarzanie danych wrażliwych wiąże się ze zwiększonym ryzykiem naruszenia praw i wolności podmiotu danych, dlatego wymagają one zastosowania podwyższonych standardów ochrony.
Jednakże, zakaz ten nie ma charakteru bezwzględnego. Przetwarzanie danych wrażliwych jest dopuszczalne w okolicznościach wymienionych w art. 9 ust 2 RODO i jest to również katalog zamknięty, co oznacza, że wszelkie inne niż wymienione w tym przepisie przesłanki nie będą podstawą do przetwarzania danych wrażliwych.

Do zamkniętego katalogu okoliczności, w których przetwarzanie danych osobowych wrażliwych będzie możliwe należą:

1) zgoda;
2) realizacja praw i obowiązków w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej;
3) ochrona żywotnych interesów osoby fizycznej;
4) wykonywanie działalności o celach politycznych, światopoglądowych, religijnych lub związkowych;
5) upublicznienie danych przez podmiot danych;
6) ustalenie, dochodzenie lub obrona roszczeń oraz sprawowanie wymiaru sprawiedliwości przez sądy;
7) ważny interes publiczny;
8) realizacja celów profilaktyki zdrowotnej lub medycyny pracy, ocena zdolności pracownika do pracy, diagnoza medyczna, zapewnienie opieki zdrowotnej lub zabezpieczenia społecznego, leczenie lub zarządzanie systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego;
9) interes publiczny w dziedzinie zdrowia publicznego oraz
10) erealizacja celów archiwalnych w interesie publicznym, celów badań naukowych lub historycznych lub celów statystycznych.

Przetwarzanie szczególnych kategorii danych osobowych jest dopuszczalne wyłącznie w powyższych okolicznościach.

Każda z wyżej wymienionych okoliczności ma charakter autonomiczny, to znaczy, że wystarczające jest spełnienie jednej z nich, aby administrator mógł wykazać się legalnością przetwarzania danych wrażliwych.

Ad.1 Zgoda.

Osoba, której dane osobowe wrażliwe mają być przetwarzane, powinna wyrazić w sposób wyraźny zgodę na przetwarzanie danych osobowych w jednym lub kilku konkretnych celach. W praktyce może to w szczególności dotyczyć trzech kategorii danych: biometrycznych, genetycznych oraz dotyczących zdrowia.

Ad.2. Realizacja praw i obowiązków w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej.

Przetwarzanie danych wrażliwych musi być dopuszczone, jeśli jest ono niezbędne dla realizacji celów związanych z zatrudnianiem czy zabezpieczeniem społecznym, w wykonywaniu szczególnych praw przez administratora lub osobę, której dane dotyczą. Przetwarzanie danych wrażliwych może być dozwolone przez prawodawcę unijnego lub krajowego, lub może być przewidziane w porozumieniu zbiorowym wydanym na mocy prawa państwa członkowskiego.

Ad.3. Ochrona żywotnych interesów osoby fizycznej.

Ta przesłanka dotyczy sytuacji, gdy przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody.
Żywotny interes oznacza interes mający istotne znaczenie dla życia osoby, której dane dotyczą, lub innej osoby fizycznej. Przesłanka ta dotyczy ochrony życia i zdrowia ludzkiego, ale może również odnosić się do spraw majątkowych. Żywotny interes innej osoby powinien mieć miejsce wyłącznie wówczas, gdy przetwarzania nie da się oprzeć na innej podstawie prawnej, a osoba taka nie jest zdolna do wyrażenia zgody. Będzie to dotyczyć takich sytuacji, w których osoba nie będzie miała zdolności do czynności prawnych lub będzie ograniczona w wyrażeniu zgody w sensie fizycznym, np. osoba, która mogłaby wyrazić zgodę pozostaje np. w stanie śpiączki. Nie ma tutaj kryterium czasowego, np. że przetwarzanie danych wrażliwych na podstawie tej przesłanki możliwe jest tylko do czasu ustanowienia opiekuna prawnego lub kuratora.

Ad. 4. Wykonywanie działalności o celach politycznych, światopoglądowych, religijnych lub związkowych.

Przetwarzanie danych szczególnie chronionych jest dopuszczalne, jeśli odbywa się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem, że dotyczy ono wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami. Organizacje te nie są uprawnione do ujawniania przedmiotowych danych osobom trzecim bez zgody podmiotu danych.

Ad. 5 i Ad. 6. Upublicznienie danych przez podmiot danych oraz ustalenie, dochodzenie lub obrona roszczeń oraz sprawowanie wymiaru sprawiedliwości przez sądy.

Przetwarzanie danych wrażliwych jest dopuszczalne, jeśli dane te zostały w sposób oczywisty upublicznione przez osobę, której dane dotyczą. Upublicznienie informacji przez podmiot danych nie może budzić wątpliwości.
Jeśli chodzi o przetwarzanie danych w celu ustalenia, dochodzenia lub obrony roszczeń oraz sprawowanie wymiaru sprawiedliwości przez sądy dyrektywa ta kierowana jest do sądów i innych organów dokonujących czynności w celu ustalenia, dochodzenia lub ochrony roszczeń. Chodzi tutaj o roszczenia w postępowaniu sądowym, administracyjnym lub innym postępowaniu pozasądowym.

Ad. 7. Ważny interes publiczny.

Pojęcie interesu publicznego nie zostało w rozporządzeniu ogólnym RODO zdefiniowane, co stwarza swobodne pole do interpretacji i przyjmowania odmiennych rozwiązań w różnych państwach członkowskich.
Należy jednak pamiętać, że przetwarzanie danych wrażliwych w interesie publicznym jest dopuszczalne tylko wtedy, gdy względy te są proporcjonalne do wyznaczonego celu i nie naruszają istoty prawa do ochrony danych osobowych oraz przewidziane są odpowiednie i konkretne środki ochrony praw podstawowych i interesów podmiotu danych.

Ad. 8. Realizacja celów profilaktyki zdrowotnej lub medycyny pracy, oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego.

Przetwarzanie danych wrażliwych musi być niezbędne dla realizacji powyższych celów i przewidziane w prawie Unii Europejskiej, prawie krajowym lub umowie zawartej z pracownikiem służby zdrowia. Dane mają być przetwarzane przez pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej (lub na jego odpowiedzialność) lub inną osobę podlegającą obowiązkowi zachowania tajemnicy zawodowej.

Ad. 9. Interes publiczny w dziedzinie zdrowia publicznego.

Interesem publicznym w dziedzinie zdrowia publicznego może być ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych. Bezpośrednia podstawa prawna przetwarzania tych danych musi być przewidziana w prawie unijnym lub krajowym przewidującym odpowiednie, konkretne, środki ochrony praw i wolności osób, których dane dotyczą. Przetwarzanie danych dotyczących zdrowia z uwagi na względy interesu publicznego nie powinno skutkować przetwarzaniem danych do innych celów przez podmioty trzecie, takie jak pracodawcy, banki czy zakłady ubezpieczeń.

Ad. 10. Realizacja celów archiwalnych w interesie publicznym, celów badań naukowych lub historycznych lub celów statystycznych.

Przetwarzanie danych wrażliwych jest dopuszczalne, jeśli jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. Bezpośrednia podstawa przetwarzania musi być przewidziana w prawie unijnym lub krajowym. W tym przypadku także musi być zachowane kryterium proporcjonalności oraz muszą być przewidziane odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą, zaś przetwarzanie ma nie naruszać istoty prawa do ochrony danych osobowych.

Przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, w tym członków lub byłych członków organizacji społecznych, np. stowarzyszeń, może odbywać się bez

zgody tych osób, gdy przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą.

Motyw 71 RODO zwraca uwagę na to, by administrator zabezpieczył dane osobowe w sposób zapobiegający dyskryminacji osób fizycznych z uwagi na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny bądź zdrowotny lub orientację seksualną. Z pewnością więc zakaz przetwarzania danych wrażliwych służy również jako instrument wzmacniający ochronę przed dyskryminacją w różnych dziedzinach życia.

Jednakże prawo do ochrony danych osobowych nie jest prawem bezwzględnym. W świetle motywu 4 RODO prawo to należy wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności. Oznacza to więc, że niekiedy będzie ono musiało ulec ograniczeniu na rzecz ochrony innego prawa. W takim też kontekście należy rozpatrywać przesłanki legalności przetwarzania danych wrażliwych.

W kontekście przetwarzania danych wrażliwych przez organizacje społeczne (fundacje i stowarzyszenia), których celem statutowym jest szeroko pojęta ochrona zdrowia lub/i przetwarzanie danych wrażliwych pacjentów, np. podczas organizowania zbiórki funduszy na świadczenia zdrowotne dla beneficjentów pomocy, zakup leków, sfinansowanie zabiegu lub operacji, udział w niestandardowym procesie leczniczym a także innej pomocy finansowej dla pacjenta można wyróżnić następujące sytuacje:
1. Pierwsza z nich będzie miała miejsce, gdy administratorem danych osobowych beneficjenta (pacjenta) będzie odrębny organizacyjnie od organizacji społecznej podmiot leczniczy (szpital, klinika, przychodnia). W takiej sytuacji organizacja społeczna przekazująca fundusze na leczenie pacjentów kierowanych do organizacji z konkretnego podmiotu leczniczego będzie podmiotem przetwarzającym dane osobowe. Wówczas konieczne będzie zawarcie umowy powierzenia przetwarzania danych osobowych beneficjentów (pacjentów podmiotu leczniczego) pomiędzy organizacją a podmiotem leczniczym. W umowie tej powinny zostać zawarte wszystkie zasady przetwarzania danych osobowych wrażliwych pacjentów oraz prawa i obowiązki stron. Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 4 do niniejszego Kodeksu.
2. Druga z nich będzie miała miejsce, gdy organizacja społeczna (stowarzyszenie, fundacja) będzie samodzielnie zbierała dane osobowe beneficjentów potrzebujących pomocy medycznej. W takiej sytuacji organizacja społeczna będzie samodzielnie przetwarzała dane osobowe beneficjentów. Z reguły jednak przetwarzanie to będzie ograniczało się do danych osobowych zwykłych: imienia i nazwiska, adresu zamieszkania osoby potrzebującej pomocy, numeru rachunku bankowego, na który będą przekazywane darowizny ze zbiórek publicznych bądź od indywidualnych darczyńców. Dane wrażliwe pacjentów dotyczące ich stanu zdrowia nie są niezbędne do realizacji celu, jakim jest zbiórka funduszy na ich leczenie. Jednak w sytuacji, w której do publicznej wiadomości podczas zbiórki funduszy organizacja przekaże informację, iż zbiera środki pieniężne dla określonej z imienia i nazwiska osoby, publikując również jej zdjęcie oraz podając nazwę jednostki chorobowej tej osoby, musi ona uzyskać zgodę na publikację wizerunku i nazwy choroby od beneficjenta lub jego opiekunów prawnych.

Zasady pozyskiwania zgody na upublicznienie wizerunku oraz przetwarzanie danych osobowych zawarte są w Rozdziale IV niniejszego Kodeksu.

3. Trzecia sytuacja będzie miała miejsce, gdy organizacja (przeważnie fundacja, ale także i stowarzyszenie) będzie podmiotem leczniczym. Wówczas podstawowym obowiązkiem takiego podmiotu będzie zapewnienie zastosowania środków technicznych i organizacyjnych, które będą w stanie zapewnić zdecydowanie wyższy poziom bezpieczeństwa przetwarzanych danych, szczególnie danych wrażliwych, jakimi są dane medyczne. Należy tutaj również rozróżnić sytuacje, gdy organizacja jedynie wspomaga podmiot leczniczy od sytuacji, gdy jest założycielem takiego podmiotu – w pierwszej z tych sytuacji podmiotem przetwarzającym dane wrażliwe pacjentów jest zakład leczniczy, zatem to na nim spoczywa odpowiedzialność opisana w RODO. W drugim wypadku organizacja występuje co prawda jako organ założycielski zakładu leczniczego, lecz ponieważ ten zakład jest wpisany do Rejestru Podmiotów Wykonujących Działalność Leczniczą, zatem on również będzie przetwarzał dane wrażliwe pacjentów.

ROZDZIAŁ III.
REALIZACJA PRAW JEDNOSTKI

Podczas przetwarzania danych osobowych organizacja społeczna, dochowując należytej staranności, musi zadbać o prawa osób fizycznych określone w przepisach RODO. Jako administrator organizacja społeczna realizuje te prawa w szczególności w zakresie:

1. prawa do informacji,
2. prawa dostępu do danych,
3. prawa do sprostowania danych,
4. prawa do ograniczenia przetwarzania,
5. prawa do przenoszenia danych,
6. prawa do sprzeciwu wobec przetwarzania danych,
7. prawa do wycofania zgody na przetwarzanie danych
8. prawa do usunięcia danych.

Osoba fizyczna, której dane organizacja przetwarza, może wystąpić z żądaniem realizacji swoich praw. Wówczas korzysta ona z form komunikacji z organizacją ogólnie przyjętych. Forma kontaktu powinna być wyrażona w klauzuli informacyjnej, przy spełnieniu przez administratora obowiązku informacyjnego. Organizacja udziela danej osobie fizycznej informacji w sposób przyjęty u danego administratora opisany w klauzuli informacyjnej.

Odpowiedź na żądanie realizacji praw przez daną osobę fizyczną musi być zrealizowane bez zbędnej zwłoki, nie później niż w terminie 1 miesiąca od daty zgłoszenia żądania przez osobę, której dane są przetwarzane. Jeśli sprawa jest szczególnie skomplikowana możliwe jest wydłużenie terminu realizacji żądania o kolejne 2 miesiące. Administrator zobowiązany jest, przed upływem 30 dni od daty wpływu żądania, powiadomić osobę, której dane są przetwarzane, o przedłużeniu rozpatrzenia żądania do 2 miesięcy. Administrator nie pobiera opłat za czynności związane z odpowiedzią na żądania osób realizujących swoje prawa. Jednak w przypadku wielokrotnych, nieuzasadnionych i nadmiernych żądań administrator może pobrać opłatę w wysokości uwzględniającej koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo odmówić podjęcia działań.

Każde działanie administratora podjęte w celu odpowiedzi na żądania osoby, której dane są przetwarzane, musi zostać w odpowiedni sposób udokumentowane, na przykład poprzez rejestrację zdarzeń w systemach informatycznych, rejestrację listów z żądaniami lub wiadomości wysyłanych drogą elektroniczną, rejestrację rozmów telefonicznych.

Ad. 1. Prawo do informacji.

Prawo to realizowane jest przez organizację poprzez przedstawienie osobom, których dane są przetwarzane, stosowanych, zależnych od poszczególnych podstaw prawnych przetwarzania i czynności przetwarzania, klauzul informacyjnych. Zakres informacji określony jest w art. 13 lub art. 14 RODO, w zależności od tego, czy organizacja zbiera dane osobowe od osoby, której te dane dotyczą, czy też zbiera dane od osoby trzeciej.

W przypadku zbierania danych osobowych bezpośrednio od osoby fizycznej administrator dopełnia obowiązku informacyjnego podczas zbierania danych. Zakres informacji zawiera, co najmniej: (a) nazwę, adres, dane kontaktowe oraz, gdy ma to zastosowanie - tożsamość i dane kontaktowe swojego przedstawiciela; (b) gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych; (c) cele przetwarzania danych; (d) podstawę prawną przetwarzania danych; (e) prawnie uzasadnione interesy realizowane przez Administratora, jeżeli przetwarzanie danych odbywa się na podstawie art. 6 ust. 1 lit. f) RODO; (f) informację o odbiorcach lub kategoriach odbiorców (jeśli istnieją), którym dane zostały lub zostaną ujawnione, jeżeli ma to zastosowanie, informację o zamiarze przekazania danych osobowych do państwa trzeciego na zasadach wskazanych w art. 13 ust. 1 lit. f RODO; (h) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe – kryteriach ustalania tego okresu; (i) informację o prawie osoby do żądania od administratora: dostępu do danych osobowych, sprostowania danych, usunięcia danych, ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania danych a także o prawie do przenoszenia danych; (j) informację o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO; (k) informację o prawie wniesienia skargi do organu nadzorczego; (l) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba fizyczna jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych; (m) gdy ma to zastosowanie – informację o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz przynajmniej w tych przypadkach istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby fizycznej.

W przypadku pozyskiwania danych osobowych nie bezpośrednio od osoby fizycznej, której dane dotyczą, zakres informacji przekazywanych przez administratora obejmuje dodatkowo (a) kategorie odnośnych danych osobowych, (b) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych. Administrator zobowiązany jest dopełnić obowiązku informacyjnego w rozsądnym terminie, nie później jednak niż w terminie miesiąca od pozyskania danych, najpóźniej przy pierwszej komunikacji z osobą fizyczną, której dane przetwarza.

Obowiązek informacyjny nie musi być realizowany, jeżeli: dana osoba dysponuje już tymi informacjami albo udzielenie informacji osobie, której dane zostały zebrane, nie bezpośrednio od niej wymagałoby niewspółmiernego dużego wysiłku technicznego, organizacyjnego lub finansowego po stronie administratora.

Zagadnienie:

Jak wypełnić obowiązek informacyjny wobec osoby, która w rozmowie telefonicznej przekazuje swoje dane osobowe? Czy konieczna jest rejestracja takiej rozmowy telefonicznej w celach dowodowych?

RODO dopuszcza realizację obowiązku informacyjnego w formie warstwowej. W przypadku rozmowy telefonicznej z osobą, która przekazuje organizacji swoje dane osobowe, może ono polegać na wskazaniu takiej osobie jedynie najistotniejszych elementów wynikających z art. 13

RODO, np. kto jest administratorem danych osobowych, w jakim celu dane są przetwarzane, jakie są prawa osoby, której dane dotyczą. Zasadne jest również wskazanie osobie dzwoniącej możliwości zapoznania się z polityką prywatności na stronie internetowej organizacji, o ile organizacja opracowała taki dokument i udostępniła go na swojej stronie internetowej. Należy jednak pamiętać, że polityka prywatności nie może być ogólnikowa, pasująca do wszystkich procesów przetwarzania w organizacji, lecz powinna być sformułowana jasno i przejrzyście, w sposób umożliwiający łatwe dowiedzenie się o prawach osoby, której dane dotyczą oraz podstawach prawnych przetwarzania w konkretnym przypadku. W skonstruowaniu Polityki prywatności pomocne mogą być informacje zawarte w Rozdziale IV w ramach poszczególnych procesów przetwarzania.

W świetle powyższego należy stwierdzić, że klauzula informacyjna nie musi być więc przekazywana w całości w rozmowie telefonicznej z osobą, której dane dotyczą, a rozmowa nagrywana przez organizację w celu wykazania spełnienia obowiązku informacyjnego wobec osoby dzwoniącej do organizacji. Pełna treść klauzuli informacyjnej powinna być wysłana do osoby dzwoniącej za pośrednictwem poczty elektronicznej na podany adres e-mail lub adres do korespondencji.

Przykładowa klauzula informacyjna wysyłana do osoby, której dane zostały zebrane przez organizację podczas rozmowy telefonicznej:

W nawiązaniu do rozmowy telefonicznej w dniu _____ r. uprzejmie potwierdzamy, że Państwa dane są przetwarzane przez Organizację z siedzibą w _____ przy ul.____ (zwaną dalej Organizacją), w ramach utrzymywania stałego kontaktu z Organizacją w związku z jej celami statutowymi, w szczególności poprzez informowanie o organizowanych akcjach społecznych, wydarzeniach publicznych a także o możliwości wspierania działalności Organizacji; przetwarzanie Państwa danych w wyżej wskazanym celu uzasadnione jest prawnie usprawiedliwionymi interesami realizowanymi przez Organizację, zgodnie z art. 6 ust. 1. lit. f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).

Podanie przez Państwa danych jest dobrowolnie, niemniej bez ich wskazania nie będzie możliwe informowanie o realizacji celów statutowych Organizacji.

Informujemy, że przysługuje Państwu prawo dostępu do treści swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu wobec ich przetwarzania a także prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Do Państwa danych osobowych mogą mieć również dostęp podmioty świadczące na rzecz Organizacji usługi, w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze, prawnicze, księgowe, kadrowe.

Państwa dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń.

Podane dane osobowe mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane.
Państwa dane osobowe będą przechowywane nie dłużej niż przez okres przedawnienia roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych w razie otrzymania od Państwa żądania usunięcia danych osobowych.
Ze szczegółowymi informacjami dotyczącymi zasad przetwarzania danych osobowych w Fundacji mogą Państwo zapoznać się w Polityce prywatności Organizacji dostępnej na stronie www.nazwaorganizacji.pl/polityka-prywatnosci>.
W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Państwa danych osobowych prosimy o kontakt z wyznaczonym przez nas Inspektorem Ochrony Danych pisząc na adres siedziby Organizacji, z dopiskiem „Inspektor Ochrony Danych" lub mailowo na adres <iod@nazwaorganizacji.pl>.

Ad. 2. Prawo dostępu do danych.

Administrator powinien udostępnić osobie fizycznej, której dane przetwarza, dostęp do jej danych w następującym zakresie:
- celów przetwarzania, kategorii przetwarzanych danych, odbiorcach lub kategorii odbiorców, okresu przetwarzania danych, a gdy nie jest to możliwe, kryteriów ustalania tego okresu, informacji o prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania, informacji o prawie wniesienia skargi do organu nadzorczego, jeżeli dane osobowe nie zostały zebrane od podmiotu danych – wszelkich dostępnych informacji o ich źródle a gdy ma to zastosowanie - informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotnych informacji o zasadach ich podejmowania a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane są przetwarzane.

Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba fizyczna ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem, w tym w szczególności o fakcie zatwierdzenia przez organ nadzorczy Kodeksu postępowania.

Ad. 3. Prawo do sprostowania danych.

Osoba fizyczna, której dane są przetwarzane ma prawo żądania od administratora sprostowania lub uzupełnienia danych jej dotyczących. Administrator lub w jego imieniu podmiot przetwarzający mogą poinformować o sprostowaniu, uzupełnieniu danych, jeżeli nie będzie to wymagało niewspółmiernego wysiłku ze strony administratora lub podmiotu przetwarzającego.

Ad. 4. Prawo do ograniczenia przetwarzania.

W sytuacjach, w których osoba fizyczna, której dane są przetwarzane, wniesie o sprostowanie, uzupełnienie swoich danych, może żądać ona równocześnie ograniczenia przetwarzania do czasu sprawdzenia przez administratora prawidłowości danych.

Ograniczenie przetwarzania powinno być wprowadzone również wtedy, gdy dane osobowe są konieczne do ustalenia, dochodzenia lub obrony roszczeń lub osoba wniosła sprzeciw wobec przetwarzania jej danych w sytuacji, w której administrator zobowiązany jest stwierdzić, czy jego prawnie uzasadnione interesy są nadrzędne wobec sprzeciwu danej osoby.

Po wprowadzeniu przez administratora ograniczenia przetwarzania powinien on podjąć odpowiednie środki techniczne i organizacyjne w tym zakresie. Np. do wglądu do danych będą mieli dostęp tylko pracownicy wyznaczeni do rozpatrzenia żądania wniesionego przez daną osobę sprzeciwu, w systemie informatycznym dane tej osoby będą w odpowiedni sposób zabezpieczone, np. poprzez oznaczenie ich danych odpowiednim symbolem, który będzie oznaczał dla wszystkich użytkowników systemu informatycznego, że została podjęta decyzja o ograniczeniu ich przetwarzania, jak również mogą być widoczne tylko dla pracowników wyznaczonych do rozpatrywania żądań, dla powołanego inspektora danych osobowych lub informatyka zajmującego się systemem informatycznym, w którym dane są przetwarzane.

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Ad. 5. Prawo do przenoszenia danych.

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:
a) przetwarzanie odbywa się na podstawie zgody lub
b) na podstawie umowy oraz
c) przetwarzanie odbywa się w sposób zautomatyzowany.

Administrator przed realizacją przeniesienia danych musi przedsięwziąć następujące kroki:
a) sprawdzić tożsamość osoby, która zgłosiła żądanie,
b) podjąć wszelkie środki bezpieczeństwa przy przenoszeniu danych, np. w przypadku przenoszenia danych drogą elektroniczną odpowiednio zabezpieczyć plik z danymi poprzez jego zaszyfrowanie hasłem.

Administrator może odmówić żądania przeniesienia danych, jeżeli nie jest możliwe potwierdzenie tożsamości osoby, która wystąpiła z żądaniem, jeśli żądanie będzie nieuzasadnione albo będzie wymagało od administratora niewspółmiernie dużego wysiłku związanego również z nadmiernymi kosztami finansowymi mającymi na celu zakup i wdrożenie systemów technicznych i informatycznych.

Ad. 6. Prawo do sprzeciwu wobec przetwarzania danych osobowych.

Osoba fizyczna, której dane są przetwarzane, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania jej danych.

Sprzeciw powinien zawierać następujące informacje:

1. wobec jakiego celu przetwarzania wnoszony jest sprzeciw,
2. wykazanie swojej szczególnej sytuacji i interesu, który uzasadnia wniesienie sprzeciwu.

Sprzeciw można wnieść w sytuacji, gdy dane przetwarzane są w prawnie uzasadnionym interesie administratora (np. cele statutowe, statystyczne, w ramach marketingu bezpośredniego).

Administrator uwzględniając sprzeciw, zaprzestaje przetwarzania danych osób w celach określonych w sprzeciwie. Jeśli administrator uzna sprzeciw wobec przetwarzania za niezasadny, wówczas zawiadomi o tym osobę, która wniosła sprzeciw, wraz z uzasadnieniem przyczyn, dla których uznał sprzeciw za niezasadny.

Ad. 7. Prawo do wycofania zgody na przetwarzanie danych.

Zgodnie z art. 7 ust. 3 RODO administrator musi zapewnić, by osoba, której dane dotyczą, mogła wycofać zgodę z taką samą łatwością, z jaką jej udzieliła, i w dowolnym momencie, bezpłatnie lub bez obniżenia poziomu usług.

Jeżeli osoba, której dane dotyczą, udzieliła zgody przez interfejs elektroniczny, administrator powinien zapewnić, aby osoba ta mogła wycofać zgodę poprzez ten sam interfejs elektroniczny. Uznaje się, że przełączenie się na inny interfejs wyłącznie w celu wycofania zgody wymagałoby zbędnego wysiłku i nie będzie zgodne z RODO.

Przykład:

Administrator nie może wymagać, aby cofnięcie zgody mogło nastąpić wyłącznie przez połączenie telefoniczne w godzinach pracy, w przypadku gdy zgoda została wyrażona za pośrednictwem formularza na stronie internetowej. Połączenie telefoniczne jest bowiem bardziej uciążliwe niż jedno kliknięcie myszą potrzebne do wyrażenia zgody poprzez wypełnienie formularza na stronie internetowej organizacji.

Co do zasady wycofanie zgody na przetwarzania danych skutkuje usunięciem danych osobowych (realizacją prawa do zapomnienia), chyba że istnieją inne cele uzasadniające dalsze ich przetwarzanie, np. gdy jest ono niezbędne do ustalenia, dochodzenia lub obrony roszczeń. W takim wypadku administrator może przetwarzać dane przez okres przedawnienia danego roszczenia.

Jeżeli przetwarzanie opiera się na więcej niż jednej podstawie prawnej, np. na podstawie umowy i zgody kontrahenta, administrator - pomimo cofnięcia zgody – będzie uprawniony do dalszego przetwarzania danych w celu wykonania umowy i nie ma obowiązku usunięcia danych osobowych.

Jeżeli jednak administrator przetwarza dane osoby, której dane dotyczą, jedynie na podstawie zgody, która następnie została wycofana, a administrator chciałby w dalszym ciągu przetwarzać powyższe dane w innym celu, wówczas powinien poinformować osobę, której dane dotyczą, o następujących kwestiach:

1) zmianie celu przetwarzania danych,
2) okresie przechowywania danych,
3) prawach jednostki,
4) prawie wniesienia skargi do organu nadzorczego;
5) o tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym, lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje braku wskazania danych
6) zautomatyzowanym podejmowaniu decyzji w indywidualnych przypadkach, chyba że osoba ta dysponuje już tymi informacjami.

Ad. 8. Prawo do usunięcia danych.

Osoba, której dane są przetwarzane, może żądać usunięcia jej danych. Jeżeli jednak dane osobowe są niezbędne do ustalenia, dochodzenia lub ochrony roszczeń albo dalsze przetwarzanie jest niezbędne do wywiązania się z obowiązku prawnego, wówczas administrator nie ma obowiązku usunięcia danych osobowych w zakresie, w jakim przetwarzanie tych danych jest niezbędne do osiągnięcia tych celów.

ROZDZIAŁ IV.
TYPOWE CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH W ORGANIZACJACH SPOŁECZNYCH

Typowymi procesami przetwarzania dla tego rodzaju działalności, które zostaną omówione w niniejszym rozdziale to charakterystyczne dla tego sektora, najczęściej występujące w praktyce czynności przetwarzania, jak, np. wpłaty od darczyńców, pomoc potrzebującym, wspieranie akcji społecznych, udział w wydarzeniach publicznych prowadzonych przez organizacje czy wolontariat. Procesy te stanowią łącznik dla wszystkich organizacji w ramach branży organizacji społecznych (NGO).

1. Wpłaty od darczyńców

1. **Opis procesu przetwarzania danych osobowych**

Proces ten obejmuje wspieranie finansowe organizacji społecznych przez darczyńców.

2. **Opis kategorii osób**

Dotyczy osób fizycznych dokonujących darowizn w formie:

- wpłat na konto bankowe organizacji przy użyciu kart płatniczych bądź za pośrednictwem systemu płatności (np. tpay.pl, PayPal),
- wpłat gotówkowych,
- świadczeń niepieniężnych
- przekazania 1% podatku na cele statutowe organizacji i zaznaczenia w formularzu PIT zgody na przekazanie organizacji danych podatnika.

3. **Kategorie danych osobowych**

Typowymi kategoriami danych dla tego procesu będą w zakresie danych zwykłych:

- imię i nazwisko,
- numer rachunku bankowego,
- informacja o banku darczyńcy,
- kwota darowizny,
- adres zamieszkania
- informacje dodatkowe wskazane w tytule przelewu np. adres e-mail, numer telefonu, adres do korespondencji inny niż adres zamieszkania.

Odnośnie danych wrażliwych, zobacz pkt 1 zagadnień szczegółowych poniżej

4. **Cel przetwarzania danych osobowych**	5. **Podstawa prawna przetwarzania danych osobowych**	6. **Okres przetwarzana danych osobowych**
zarządzanie wpłatami od darczyńców, w tym wystawianie	art. 6 ust. 1 lit. b RODO tj. umowa darowizny	okres realizacji darowizny, w tym wystawienia

zaświadczeń do celów podatkowych	przepisy Kodeksy cywilnego, w szczególności dot. darowizn	zaświadczenia pozwalającego na odliczenie kwoty przekazanej darowizny w rozliczeniu PIT
kontaktowanie się z darczyńcami za pomocą poczty tradycyjnej lub elektronicznej w celu odpowiedzi na ich zapytania bądź zgłoszenia a także w celu wysłania podziękowań za wsparcie	art. 6 ust. 1 lit. f RODO tj. uzasadniony interes administratora	okres niezbędny do udzielenia odpowiedzi na zapytania lub zgłoszenie darczyńcy bądź wysłanie mu podziękowań za wsparcie
prowadzenie ksiąg rachunkowych i dokumentacji podatkowej	art. 6 ust. 1 lit. c RODO tj. wypełnienie obowiązku prawnego ciążącego na administratorze w związku z art. 74 ust. 2 ustawy o rachunkowości oraz innymi przepisami szczególnymi	okres przechowywania dokumentacji księgowej i podatkowej wynikający z przepisów prawa
informowanie o realizacji celów statutowych organizacji, w tym informowanie o organizowanych akcjach społecznych oraz możliwości dalszego wsparcia organizacji, o ile darczyńca nie sprzeciwił się takiemu przetwarzaniu	art. 6 ust. 1 lit. f RODO, tj. prawnie uzasadniony interes administratora polegający na utrzymywaniu stałego kontaktu z organizacją społeczną w związku z jej celami statutowymi	okres niezbędny do osiągnięcia celu, jednak nie dłużej niż do złożenia sprzeciwu wobec przetwarzania danych osobowych w tym celu, a po tym czasie dane osobowe darczyńców mogą być przetwarzane przez okres przedawnienia ewentualnych roszczeń (art. 17 ust.3 lit. e RODO)
dochodzenie roszczeń i obrona przed roszczeniami z tytułu zawartej umowy, co stanowi prawnie uzasadniony interes przetwarzania danych przez Administratora	art. 6 ust. 1 lit. f RODO w związku z art. 17 ust. 3 lit. e RODO, tj. uzasadniony interes administratora polegający na ustaleniu, dochodzenia lub obrony roszczeń	okres przedawnienia ewentualnych roszczeń wynikający z przepisów prawa, tj. do końca roku kalendarzowego po upływie 6 letniego okresu przedawnienia (art. 118 Kodeksu cywilnego)

7. **Kategorie odbiorców danych**

Przykładowo: biuro księgowe jako podmiot przetwarzający, które na zlecenie organizacji rozlicza wpłaty od darczyńców.

Z powyższym podmiotem należy zawrzeć umowę powierzenia przetwarzania danych. Wzór takiej umowy stanowi załącznik nr 1 do niniejszego kodeksu.

8. **Współadministratorzy**

Przykładowo: gdy wsparcie udzielane jest na rzecz dwóch organizacji, które wspólnie realizują projekt i zbierają fundusze na realizację wspólnego projektu mieszczącego się w ramach celów statutowych obu organizacji.

Współadministratorzy powinni zawrzeć umowę o współadministrowaniu danymi. Przykładowy wzór ramowej umowy współadministrowania danymi osobowymi został zamieszczony w załączniku nr 2 do niniejszego kodeksu.

9. **Informacje o przekazaniu do państwa trzeciego**

Przykładowo: gdy dane osobowe darczyńców są przechowywane na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

10. **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa**

Zaleca się, aby organizacja określiła techniczne i organizacyjne środki bezpieczeństwa w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

Należy zwrócić uwagę, że formularze wpłat online powinny wykorzystywać szyfrowanie SSL zapewniające ochronę danych wprowadzonych przez darczyńcę do formularza w swojej przeglądarce internetowej.

11. **Obowiązek informacyjny przy zbieraniu danych osobowych darczyńców**

Przykładowa klauzula informacyjna przy zbieraniu danych osobowych darczyńców:

Informujemy, że podane przez Pana/Panią dane osobowe są przetwarzane przez Organizację z siedzibą w Warszawie przy ul. ……. (administrator danych):
(1) w celu zawarcia i realizacji umowy darowizny, w tym identyfikacji darczyńcy oraz ewentualnego wystawienia zaświadczenia dla celów podatkowych w związku z przekazaną darowizną - podstawa prawna przetwarzania: art. 6 ust. 1 lit. B rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO);
(2) w ramach utrzymywania stałego kontaktu z naszą Organizacją w związku z jej celami statutowymi, w szczególności poprzez informowanie o akcjach społecznych organizowanych przez naszą Organizację - podstawa prawna przetwarzania: art. 6 ust. 1 lit. f RODO.
Podanie danych jest dobrowolne, niemniej bez ich wskazania nie będzie możliwe zarejestrowanie wpłaty ani ewentualne wystawienie zaświadczenia niezbędnego do odliczenia podatkowego.
Informujemy, że przysługuje Pana/Pani prawo dostępu do treści swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu wobec ich przetwarzania, a także prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Państwa dane osobowe będą przechowywane przez naszą Organizację nie dłużej niż przez okres przedawnienia roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych w razie otrzymania od Państwa żądania usunięcia danych osobowych.
Do Państwa danych osobowych mogą mieć również dostęp podmioty świadczące na rzecz Organizacji usługi, w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze. prawnicze, księgowe, kadrowe. Państwa dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku nasza Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń. Podane dane osobowe mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem, nie będą zautomatyzowane.
Ze szczegółowymi informacjami dotyczącymi zasad przetwarzania danych osobowych w naszej Organizacji mogą Państwo zapoznać się w Polityce prywatności na stronie internetowej Organizacji dostępnej pod adresem <www.nazwaorganizacji.pl>.
W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pani/Pana danych osobowych, prosimy o kontakt z wyznaczonym przez nas Inspektorem Ochrony Danych pisząc na adres siedziby Organizacji: ul. _____ , _____ , z dopiskiem „Inspektor Ochrony Danych" lub na adres poczty elektronicznej <iod@nazwaorganizacji.pl>.

Zagadnienia szczegółowe

1) **Czy dane darczyńców dokonujących wpłat na rzecz organizacji o sprecyzowanym profilu politycznym, wyznaniowym bądź światopoglądowym stanowią dane wrażliwe ujawniające poglądy polityczne, wyznanie lub przekonania światopoglądowe?**

   Danymi wrażliwymi są dane związane z przynależnością do organizacji o celach politycznych, światopoglądowych, religijnych lub związkowych, która świadczy o identyfikacji osoby z celami statutowymi takiej organizacji. Natomiast sam fakt wspierania takiej organizacji należy uznać za niewystarczający do uznania danych osobowych darczyńcy za dane wrażliwe.

2) **Czy organizacja może wysyłać do darczyńców podziękowania za dokonane przez nich wpłaty na rzecz organizacji?**

   Organizacja posiada prawnie uzasadniony interes, aby wysyłać podziękowania darczyńcom dokonującym wpłat na rzecz organizacji - zarówno pocztą tradycyjną, jak i w formie elektronicznej za pośrednictwem poczty elektronicznej oraz wiadomości tekstowych (SMS) - o ile darczyńca uprzednio przekazał organizacji swój adres e-mail lub numer telefonu. Podstawą prawną przetwarzania danych jest w tym przypadku art. 6 ust. 1 lit. f RODO, tj. prawnie uzasadniony interes administratora. Nie ma zatem konieczności pobierania zgód od darczyńców na wysyłanie podziękowań za dokonaną darowiznę.

   Jeżeli darczyńca nie życzy sobie, aby organizacja przesyłała mu podziękowanie za wsparcie powinien uprzedzić o tym organizację, np. zaznaczając to w opisie przelewu. Informacja o

sprzeciwie darczyńcy powinna być odnotowana przez organizację w jej bazie danych, aby zapobiec wysyłce do niego podziękowań za wsparcie.

3) **Czy organizacja, która przekazuje środki na rzecz konkretnych beneficjentów, może przekazywać im dane osobowe darczyńców, które zostały wskazane przez nich przy wpłacie darowizny?**

Zgodnie ze stanowiskiem Urzędu Ochrony Danych Osobowych nie ma podstaw prawnych, aby organizacja, która przekazuje środki na rzecz konkretnych osób (beneficjentów), mogła udostępnić dane darczyńców beneficjentom, którzy otrzymali wsparcie za pośrednictwem organizacji. W takim wypadku organizacja powinna pozyskać uprzednią zgodę darczyńcy na przekazanie jego danych osobowych beneficjentowi. Organizacja powinna więc zadbać, aby na etapie przyjmowania darowizny pozyskać od darczyńcy zgodę na przekazanie jego danych osobowych beneficjentowi.

4) **Czy organizacja może wysłać podziękowania podatnikowi, który w rozliczeniu rocznym PIT wyraził zgodę na przekazanie organizacji pożytku publicznego swojego imienia, nazwiska i adresu?**

Zgodnie ze stanowiskiem UODO dane podatnika, który w rozliczeniu rocznym PIT wyraził zgodę na przekazanie OPP swojego imienia, nazwiska i adresu, mogą być przetwarzane wyłącznie przez tę organizację. Jeżeli podatnik w rozliczeniu rocznym wyraził zgodę na przekazanie jego danych organizacji, to organizacja może przetwarzać te dane w celu wysłania w imieniu obdarowanego podziękowań do darczyńcy. Podstawą prawną przetwarzania będzie art. 6 ust. 1 lit. f RODO, tj. prawnie uzasadniony interes administratora.

Organizacja pożytku publicznego nie ma jednak żadnych podstaw prawnych do udostępnienia danych darczyńców osobom obdarowanym, chyba że organizacja pozyskałaby na ten cel uprzednią zgodę darczyńcy.

5) **Czy organizacja może informować swoich darczyńców o działalności statutowej, a także o możliwościach dalszego wsparcia organizacji?**

Organizacja może wysyłać informacje o działalności statutowej organizacji oraz o możliwościach dalszego jej wspierania, na adresy pocztowe, adresy e-mail oraz numery telefonów podane w przelewach bankowych bądź udostępnione w serwisie płatniczym w przypadku płatności elektronicznych. W takim przypadku przetwarzanie danych odbywa się na podstawie prawnie uzasadnionego interesu administratora, o których mowa w art. 6 ust. 1 lit. f RODO. Istnieją bowiem rozsądne przesłanki, aby darczyńca mógł się spodziewać, że może nastąpić przetwarzanie danych darczyńcy w powyższych celach, chyba że z testu uzasadnionego interesu wykonanego przed organizację będzie wynikało, że interesy i prawa podstawowe darczyńcy nie są nadrzędne wobec interesu administratora danych.

Więcej informacji o teście uzasadnionego interesu znajdziesz w rozdziale II pkt 1.

Organizacja prowadząca działalność gospodarczą nie może jednak wysyłać informacji handlowych do darczyńcy bez jego uprzedniej zgody, powołując się na prawnie uzasadnione interesy

administratora, ponieważ zgodnie z art. 10 ustawy o świadczeniu usług drogą elektroniczną zakazane jest przesyłanie niezamówionej informacji handlowej za pomocą poczty elektronicznej bądź innych środków komunikacji elektronicznej skierowanej do osoby fizycznej bez jej uprzedniej zgody. Za informację handlową w rozumieniu ustawy o świadczeniu usług drogą elektroniczną należy uznać każdą informację przeznaczoną bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku organizacji pozarządowej prowadzącej działalność gospodarczą, z wyłączeniem informacji umożliwiającej porozumiewanie się za pomocą środków komunikacji elektronicznej z określoną osobą oraz informacji o towarach i usługach nie służącej osiągnięciu efektu handlowego pożądanego przez podmiot, który zleca jej rozpowszechnianie, w szczególności bez wynagrodzenia lub innych korzyści od producentów, sprzedawców i świadczących usługi (art. 2 pkt 2 ustawy o świadczeniu usług drogą elektroniczną).

Nadto, zgodnie z art. 172 Prawa telekomunikacyjnego, zakazane jest używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę.

Organizacja w ramach prowadzonej działalności gospodarczej powinna zatem pozyskać odrębne zgody:

- na otrzymywanie informacji handlowej drogą elektroniczną,
- na używanie telekomunikacyjnych urządzeń końcowych w celu prowadzenia marketingu bezpośredniego,
- na przetwarzanie w celach marketingu własnych produktów lub usług organizacji
- na przetwarzanie w celach marketingu produktów lub usług innych podmiotów.

6) Czy organizacje społeczne, do który ma zastosowanie Dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim wydany przez Konferencję Episkopatu Polski w dniu 13 marca 2018 r., mogą publikować informacje o wpłacie darowizn?

Zgodnie z art. 10 ust. 2 w/w Dekretu „*periodyki informacyjne przeznaczone do użytku wewnętrznego, opisujące najważniejsze wydarzenia z życia i działalności redagujących je podmiotów kościelnych, mogą zawierać dane dotyczące osób, które złożyły darowiznę, o ile w poszczególnych przypadkach zainteresowani nie wnosili o ich nieujawnianie*." Zgodnie z art. 10 ust. 3 Dekretu powyższe zasady stosuje się odpowiednio do publikacji cyfrowych i stron internetowych. Organizacje społeczne, do których ma zastosowanie Dekret, powinny zapewnić darczyńcy możliwość wyrażenia sprzeciwu na ujawnienie jego danych osobowych w wyżej wymienionych periodykach informacyjnych, w publikacjach cyfrowych lub na stronach internetowych organizacji. Dobrą praktyką jest, aby w periodyku informacyjnym zawierającym dane darczyńców umieścić notkę informację, że jest on przeznaczony do użytku wewnętrznego organizacji.

2. Zbieranie funduszy na działalność organizacji

1. **Opis procesu przetwarzania danych osobowych**

Proces polega na zbieraniu i analizie informacji o osobach fizycznych w celu oceny zdolności potencjalnego darczyńcy do wsparcia finansowego organizacji i dostosowania działań fundrisingowych, aby były one jak najbardziej komfortowe dla potencjalnego darczyńcy i jednocześnie efektywne z perspektywy organizacji.

Zbieranie informacji o zainteresowaniach lub zamożności potencjalnych darczyńców w celach fundrisingowych może polegać w szczególności na tworzeniu profilu potencjalnego darczyńcy na podstawie:

1) informacji z publicznie dostępnych źródeł takich jak:
   a) rejestry publiczne w celu ustalenia, czy osoba taka wchodzi w skład organów wykonawczych bądź nadzorczych osób prawnych,
   a) informacje prasowe zawierające informacje o poziomie zamożności lub zainteresowaniach potencjalnego darczyńcy,
2) informacji o darczyńcy, który aktualnie wspiera organizację, poprzez zestawienie danych zawierających dane o jego zamożności z innymi danymi dostępnymi w organizacji w celu identyfikacji potencjalnie największych darczyńców wśród ogółu osób, które wspierają organizację.

2. **Opis kategorii osób**

Proces ten obejmuje dwie kategorie osób fizycznych:

1) potencjalnych darczyńców, którzy nie wspierali jeszcze organizacji
2) dotychczasowych darczyńców, którzy mogą potencjalnie wesprzeć organizację w większym zakresie.

3. **Kategorie danych osobowych**

Typowymi kategoriami danych dla tego procesu będą w zakresie danych zwykłych:

- imię i nazwisko,
- dane adresowe, np. adres zamieszkania,
- dane kontaktowe, adres e-mail, numer telefonu,
- data urodzin,
- stan cywilny,
- przynależność do organizacji społecznej lub gospodarczej, np. spółki, organizacji społecznej, spółdzielni,
- stanowisko zajmowane w organizacji, w tym udział w składzie organów wykonawczych lub nadzorczych organizacji,
- informacja o majątku
- wysokość udzielonego wsparcia w przeszłości w przypadku dotychczasowych darczyńców.

Odnośnie danych wrażliwych zobacz pkt 1 zagadnień szczegółowych w rozdziale IV pkt 1 poświęconemu wpłatom od darczyńców.

4. Cel przetwarzania danych osobowych	5. Podstawa prawna przetwarzania danych osobowych	6. Okres przetwarzana danych osobowych
ocena zdolności potencjalnego darczyńcy do wsparcia finansowego organizacji a także efektywne zarządzania zbiórką funduszy na rzecz organizacji	art. 6 ust. 1 lit. f RODO , tj. prawnie uzasadniony interes administratora, chyba że test uzasadnionego interesu wykaże konieczność pozyskania zgody potencjalnego darczyńcy – wówczas podstawą prawną jest zgoda potencjalnego darczyńcy (art. 6 ust. 1 lit. a RODO) Odnośnie wyboru właściwej podstawy prawnej zobacz pkt 1 zagadnień szczegółowych poniżej	okres niezbędny do osiągnięcia celu, jednak nie dłużej niż do złożenia sprzeciwu wobec przetwarzania danych osobowych lub cofnięcia zgody na przetwarzanie danych osobowych
informowanie o realizacji celów statutowych organizacji oraz możliwości dalszego wsparcia organizacji, o ile potencjalny darczyńca nie sprzeciwił się takiemu przetwarzaniu	art. 6 ust. 1 lit. f RODO, co stanowi prawnie uzasadniony interes administratora, którym jest utrzymywanie stałego kontaktu z organizacją w związku z jego celami statutowymi	okres niezbędny do osiągnięcia celu, jednak nie dłużej niż do złożenia sprzeciwu wobec przetwarzania danych osobowych w tym celu
dochodzenie roszczeń i obrona przed roszczeniami ze strony potencjalnego darczyńcy, co stanowi prawnie uzasadniony interes przetwarzania danych przez organizację	art. 6 ust. 1 lit. f RODO art. 17 ust. 3 lit. e RODO	okres przedawnienia ewentualnych roszczeń wynikający z przepisów prawa

7. Kategorie odbiorców danych

Przykładowo:

- drukarnia wykonująca na zlecenie organizacji materiały promocyjne adresowane do potencjalnych darczyńców
- profesjonalne organizacja fundrisingowa realizująca usługi na rzecz organizacji społecznej

Z powyższymi podmiotami należy zawrzeć umowę powierzenia przetwarzania danych. Wzór takiej umowy stanowi załącznik nr 1 do niniejszego kodeksu.

8. Współadministratorzy

Przykładowo: gdy zbieranie funduszy odbywa się przez dwie organizacje w celu realizacji wspólnego projektu, w ramach którego zebrane fundusze zostaną wydatkowane na rzecz beneficjentów wskazanych przez obie organizacje.

Współadministratorzy powinni zawrzeć umowę o współadministrowaniu danymi. Przykładowy wzór ramowej umowy współadministrowania danymi osobowymi został zamieszczony w załączniku nr 2 do niniejszego kodeksu.

9. Informacje o przekazaniu do państwa trzeciego

Przykładowo: gdy dane osobowe potencjalnych darczyńców są przechowywane na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG)

10. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa:

Zaleca się, aby organizacja określiła techniczne i organizacyjne środki bezpieczeństwa w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

11. Obowiązek informacyjny przy zbieraniu danych osobowych w procesie zbieraniu funduszy na rzecz organizacji

Zgodnie z motywem 39 RODO wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne. Dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. Nadto zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem.

Należy założyć, że zbieranie informacji o zamożności lub zainteresowaniach potencjalnych darczyńców może nie mieścić się w granicach rozsądnych oczekiwań, stąd istotne jest zrozumiałe i jasne komunikowanie w stosunku do potencjalnych darczyńców o możliwości dokonywania operacji na zebranych danych osobowych potencjalnych darczyńców w celach fundrisingowych.

Uzyskane przez potencjalnych darczyńców informacje powinny pozwolić im zrozumieć, w jaki sposób organizacja przetwarza ich dane osobowe w aspekcie oceny ich zamożności lub zainteresowań a tym samym umożliwić im podjęcie świadomej decyzji, czy chcą sprzeciwić się takiemu przetwarzaniu.

Zgodnie z art. 14 ust. 3 RODO organizacja powinna spełnić obowiązek informacyjny wobec osoby, o której zbiera dane:

a) w rozsądnym terminie, najpóźniej w ciągu miesiąca po pozyskaniu danych osobowych lub
b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą lub

c) jeżeli organizacja planuje ujawnienie dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.

Klauzula informacyjna powinna uwzględniać w szczególności następujące informacje:

- wyjaśnienie, że dane osobowe potencjalnego darczyńcy zostaną wykorzystane do utworzenia profilu w celu zbieraniu funduszy przez organizację (cel fundrisingowy),
- wyjaśnienie, że dane osobowe, których osoba fizyczna nie podała, zostały uzyskane z innych źródeł,
- zapewnienie o zachowaniu przejrzystości, w szczególności w zakresie informacji o stanie zamożności i celu pozyskania takiej informacji
- podkreślenie, że w procesie przetwarzania danych potencjalnego darczyńcy mogą być zaangażowane podmioty zewnętrzne.

Przykładowe postanowienia w klauzuli informacyjnej:

Uprzejmie informujemy, że Organizacja z siedzibą w _____ przy ul. ……. (administrator danych) w celu efektywnego zarządzania zbiórką funduszy korzysta Twoich danych osobowych:
a) dostarczanych przez Ciebie takich jak imię, nazwisko, adres poczty elektronicznej, informacje o dotychczasowym wsparciu na rzecz naszej Organizacji,
b) pozyskanych z publicznie dostępnych źródeł takich jak Krajowy Rejestr Sądowy (KRS), Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEiDG), media, takich jak przynależność do organizacji społecznej lub gospodarczej, a także zajmowane w niej stanowisko.
Przetwarzanie powyższych danych daje nam lepsze zrozumienie naszych darczyńców, ich zainteresowań, pozwala dostosować naszą komunikację w taki sposób, aby kierowane przez nas prośby o pomoc finansową do potencjalnych darczyńców pozwalały na bardziej efektywną realizację celów fundrisingowych, jakim jest zbiórka funduszy na realizację celów statutowych naszej Organizacji.
Publicznie dostępne informacje są wykorzystywane przez naszą organizację w celu znalezienia potencjalnych darczyńców i zachęcenia ich do zaangażowania się we wspieranie naszej Organizacji w formie komunikacji dopasowanej do ich potrzeb i zainteresowań.
Dopuszczalność przetwarzania danych w wyżej wskazanym celu uzasadniona jest prawnie usprawiedliwionymi interesami realizowanymi przez administratora danych osobowych zgodnie z art. 6 ust. 1 lit. f rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).
Informujemy, że przysługuje Tobie prawo dostępu do treści swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do przenoszenia danych, a także prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
Twoje dane osobowe będą przechowywane przez naszą Organizację nie dłużej niż przez okres przedawnienia roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych w razie otrzymania od Ciebie żądania usunięcia danych osobowych.
Do Twoich danych osobowych mogą mieć również dostęp podmioty świadczące na rzecz Organizacji usługi, w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze. prawnicze, księgowe, kadrowe. Twoje dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom

ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń. Podane dane osobowe mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem, nie będą zautomatyzowane.
Ze szczegółowymi informacjami dotyczącymi zasad przetwarzania danych osobowych w naszej Organizacji możesz zapoznać się w Polityce prywatności na stronie internetowej dostępnej pod adresem <www.nazwaorganizacji.pl>.
Jeśli nie życzysz sobie, abyśmy wykorzystywali Twoje dane w powyższy sposób, poinformuj nas o tym pisząc na e-mail <iod@nazwaorganizacji.pl> bądź używając link: <wypisuję się>.

Jeżeli organizacja posługuje się polityką prywatności, wskazane jest opisanie w niej procesu zbierania danych o potencjalnych darczyńcach. Przykładowe postanowienia w Polityce prywatności:

Nasza Organizacja może zbierać informacje o Tobie z publicznie dostępnych źródeł - na przykład z Krajowego Rejestru Sądowego (KRS), Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEiDG) oraz mediów - aby pomóc nam lepiej zrozumieć zdolność do wspierania działalności naszej Organizacji, w tym udzielania wsparcia finansowego.
Na podstawie danych z powyższych źródeł możemy przeprowadzić analizę Twoich zainteresowań oraz ocenę zamożności w celach fundrisingowych. W każdym czasie będziesz miał prawo do złożenia sprzeciwu wobec przetwarzania danych osobowych w powyższym celu.
W przypadku gdy nasza Organizacja przetwarza Twoje dane osobowe wskazane przez Ciebie, możemy wykorzystać informacje pozyskane ze źródeł publicznych dostępnych, a następnie zestawić je z informacjami, które nam uprzednio podałeś w celu przeprowadzenia analizy w celu zrozumienia Twoich preferencji i oczekiwań w zakresie kierowanej do Ciebie komunikacji, organizowanych przez nas wydarzeń a także innych działań podejmowanych przez naszą Organizację w ramach realizacji celów statutowych. W ten sposób możemy dostosować naszą komunikację dotyczącą pozyskiwania funduszy na realizację celów statutowych naszej Organizacji do Twoich potrzeb i możliwości w taki sposób, aby była ona dla Ciebie jak najbardziej efektywna i odpowiednia jako potencjalnego darczyńcy.
W celach fundrisingowych nasza organizacja może przeszukiwać dane kontaktowe naszych dotychczasowych darczyńców, aby pozostać w kontakcie z jak największą liczbą naszych darczyńców.

Zagadnienia szczegółowe

1) **Jaką podstawę prawną powinna wskazać organizacja, przetwarzając dane w ramach procesu zbierania funduszy na realizację działań statutowych organizacji? Czy bardziej odpowiednia będzie zgoda potencjalnego darczyńcy, czy też prawnie uzasadniony interes administratora?**

   Przed przystąpieniem do zbiórki funduszy, w ramach której będą wykorzystywane dane o potencjalnych darczyńcach, organizacja powinna wykonać test uzasadnionego interesu a następnie należycie go udokumentować.

   Test uzasadnionego interesu ma na celu weryfikację, czy planowane zbieranie informacji o potencjalnych darczyńcach nie będzie miało istotnego negatywnego wpływu na osoby, których

dane będą przetwarzane. Test powinien prowadzić do konkluzji, czy zbieranie danych o potencjalnych darczyńcach w celach fundrisingowych jest dla nich zbyt uciążliwe i w konsekwencji wymaga uzyskiwania od nich odrębnej zgody, czy też wystarczające będzie oparcie się na prawnie uzasadnionym interesie administratora jako przesłance legalizującej przetwarzanie danych osobowych potencjalnych darczyńców.

Wykonując test uzasadnionego interesu, organizacja powinna wziąć pod uwagę czy zbieranie danych w celach fundrisingowych można uznać za zbyt inwazyjną dla potencjalnego darczyńcy a także, czy dana osoba może oczekiwać, że organizacja będzie przetwarzać jej dane w taki sposób. Przy ocenie inwazyjności dobrym podejściem może być postawienie się w sytuacji odbiorców i rozważenie, jakie byłyby ich odczucia w związku z podejmowanymi działaniami przez organizację. Należy przy tym uwzględnić takie czynniki jak:

1) dostępność informacji o potencjalnym darczyńcy;

   Przykładowo: poszukiwanie informacji na temat sytuacji finansowej jest mniej uciążliwe, jeżeli obejmuje, np. listę najbogatszych Polaków lub wpisy w publicznie dostępnych rejestrach o zajmowanych stanowiskach w organach zarządczych lub nadzorczych spółek, niż przeglądanie publicznych postów zamieszczonych w mediach społecznościowych.

2) rodzaj powiązania między osobą, której dane dotyczą, a organizacją, w szczególności fakt, że osoba wspierała organizację w przeszłości bądź była beneficjentem organizacji;

   Przykładowo: prawnie uzasadniony interes administratora może stanowić podstawę prawną dla działań związanych z segregowaniem bazy danych potencjalnych darczyńców według miejsca zamieszkania po kodach pocztowych, czy też według innych informacji o darczyńcach, które są w posiadaniu organizacji, i dlatego nie wymagają zgody potencjalnego darczyńcy.

3) ilość i wagę zbieranych informacji o potencjalnym darczyńcy;

   Wykonując test uzasadnionego interesu, należy zwrócić uwagę na kwestię profilowania potencjalnych darczyńców, w szczególności, czy ocena ich zamożności lub zainteresowań wiąże się ze zbieraniem większej ilości informacji, których osoba nie przekazała uprzednio organizacji. W takich przypadkach jest mało prawdopodobne, aby zastosowanie miały postanowienia dotyczące uzasadnionego interesu administratora. W związku z tym przed przystąpieniem do takiego przetwarzania należy zasięgnąć zgody osób fizycznych.

Więcej informacji na temat testu uzasadnionego interesu administratora znajdziesz w rozdziale II pkt 1 powyżej.

2) Czy można korzystać z danych osobowych darczyńców, które nie zostały zebrane zgodnie z przepisami o ochronie danych osobowych?

Jeżeli organizacja posiada historyczne dane osobowe, które zostały zebrane niezgodnie z przepisami o ochronie danych osobowych , np. bez ich zgody bądź bez spełnienia obowiązku informacyjnego, co do zasady nie może korzystać z tych danych do komunikacji fundrisingowej.

3) Jakie zasady obowiązują w komunikacji fundrisingowej w zależności od kanału komunikacji kierowanej do potencjalnego darczyńcy?

Jeżeli komunikacja fundrisingowa jest kierowana za pośrednictwem:

1) poczty tradycyjnej - zgoda potencjalnego darczyńcy nie jest wymagana, jeżeli z testu uzasadnionego interesu wynika, że organizacja może przy przetwarzaniu danych darczyńców oprzeć się na prawnie uzasadnionym interesie administratora, a nie na zgodzie potencjalnego darczyńcy jako przesłance legalizującej przetwarzanie ich dane osobowe. Potencjalny darczyńca powinien mieć możliwości wyrażenia sprzeciwu wobec przetwarzania jego danych osobowych, zatem powinien być o takiej możliwości uprzednio poinformowany w odpowiedniej klauzuli informacyjnej.

2) telefonu lub wiadomości tekstowych (SMS) – komunikacja jest dopuszczalna bez zgody osoby, której dane dotyczą, o ile organizacja nie prowadzi działalności gospodarczej a komunikacja z potencjalnym darczyńcą nie stanowi oferty handlowej w rozumieniu ustawy o świadczeniu usług drogą elektroniczną.

Przykład:

Pan Tomasz z organizacji społecznej wykonuje telefon do osoby, która przekazała numer swojego telefonu podczas wydarzenia organizowanego przez organizację kilka miesięcy temu, z prośbą o wsparcie organizacji.
Pan Tomasz może wykonać taki telefon, ponieważ osoba, która brała udział w wydarzeniu, (i) została poinformowana w klauzuli informacyjnej pod formularzem zapisu w wydarzeniu o celu przetwarzania jej danych osobowych polegającego na informowaniu przez organizację o możliwości udzielenia wsparcia jej działalności,
(ii) osoba ta nie wyraziła sprzeciwu wobec przetwarzania jej danych osobowych w powyższym celu.

3) poczty elektronicznej – jest dopuszczalne bez zgody osoby, której dane dotyczą, o ile organizacja nie prowadzi działalności gospodarczej a komunikacja z potencjalnym darczyńcą nie stanowi oferty handlowej w rozumieniu ustawy o świadczeniu usług drogą elektroniczną.

   Wiadomość e-mail nadawana przez organizację powinna zawierać instrukcję o możliwości rezygnacji z otrzymywania kolejnych e-maili tego rodzaju od organizacji, np. w formie linku <wypisz> w stopce wiadomości pocztowej. Organizacja powinna rejestrować takie sprzeciwy w swojej bazie danych, aby zapobiec w przyszłości wysyłaniu podobnych wiadomości do osoby, która nie życzy sobie otrzymywania tego rodzaju wiadomości.

Jeżeli komunikacja fundrisingowa kierowana przez organizację do potencjalnego darczyńcy ma związek z prowadzoną działalnością gospodarczą, organizacja powinna pozyskać uprzednią zgodę potencjalnego darczyńcy.

4) mediów społecznościowych – jest dopuszczalna bez zgody osoby, której dane dotyczą, jeżeli nie ma związku z działalnością gospodarczą prowadzoną przez organizację.

Przyjmuje się, że osoba zakładając konto w portalu społecznościowym, który umożliwia swobodną komunikację pomiędzy użytkownikami takiego portalu, może spodziewać się kontaktu ze strony innych użytkowników w bliżej nieokreślonych celach.

Różnice pomiędzy komunikacją związaną z działalnością gospodarczą organizacji, a komunikacją niezwiązaną z taką działalnością przedstawia poniższa tabela:

Kanał komunikacji z potencjalnym darczyńcą	**Czy wymagana jest zgoda potencjalnego darczyńcy na komunikację**	
	w ramach działalności statutowej niezwiązanej z działalnością gospodarczą prowadzoną przez organizację?	**w ramach działalności gospodarczej prowadzonej przez organizację?**
poczta tradycyjna	Nie, o ile potencjalny darczyńca ma możliwość zgłoszenia sprzeciwu lub nie zgłosił takiego sprzeciwu wcześniej*	Nie, o ile dotyczy to dotychczasowych darczyńców, klientów i innych osób utrzymujących stały kontakt z organizacją a osoby te mają możliwość zgłoszenia sprzeciwu wobec marketingu bezpośredniego lub nie zgłosił takiego sprzeciwu wcześniej
e-mail	Nie*	Tak
telefon	Nie*	Tak
wiadomości tekstowe (SMS)	Nie*	Tak
media społecznościowe	Nie*	Tak

***** od organizacji społecznych, które komunikują się z potencjalnym darczyńcą w związku z realizacją swoich statutowych, a nie w ramach prowadzonej działalności gospodarczej, nie wymaga się pozyskania zgody potencjalnego darczyńcy:
a) na otrzymywanie informacji handlowych określonych w art. 10 ustawy o świadczeniu usług drogą elektroniczną (Dz.U.2019.123 t.j. z późn. zm.),
b) na używanie telekomunikacyjnych urządzeń końcowych oraz automatycznych systemów wysyłających dla celów marketingu bezpośredniego, o jakich mowa w art. 172 Prawa telekomunikacyjnego.

Więcej informacji na temat komunikacji znajdziesz w rozdziale IV pkt 3 poświęconej liście mailingowej.

3. Lista mailingowa

1. **Opis procesu przetwarzania danych osobowych**

Proces ten obejmuje zbieranie danych osób, które zapisały się do listy mailingowej (newslettera), wysyłkę mailingu do subskrybentów newslettera a także obsługę uprawnień podmiotów danych, w szczególności żądania usunięcia danych osobowych.

Za pośrednictwem listy mailingowej organizacja informuje odbiorców o realizacji działań statutowych organizacji, w szczególności o prowadzonych programach, organizowanych wydarzeniach, akcjach społecznych, kampaniach, debatach, seminariach, konferencjach naukowych i prasowych a także możliwościach wspierania działalności organizacji.

W przypadku organizacji prowadzących działalność gospodarczą lista mailingowej może służyć promocji oferowanych przez nią usług lub towarów.

2. **Opis kategorii osób**

Osoby fizyczne, które zapisały się do listy mailingowej, zarówno w formie formularza elektronicznego , np. na stronie internetowej organizacji, jak i formularzy papierowych, na których organizacja zbiera zapisy do listy mailingowej, np. na organizowanych przez siebie wydarzeniach publicznych.

3. **Kategorie danych osobowych**

Typowymi kategoriami danych, które organizacja przetwarza w ramach prowadzenia listy mailingowej, będą w zakresie danych zwykłych: imię i nazwisko, adres poczty elektronicznej, rzadziej numer telefonu czy też adres do korespondencji subskrybenta newslettera.

Odnośnie danych wrażliwych zobacz pkt 3 zagadnień szczegółowych poniżej

4. **Cel przetwarzania danych osobowych**	5. **Podstawa prawna przetwarzania danych osobowych**	6. **Okres przetwarzania danych osobowych**
informowanie o realizacji celów statutowych organizacji oraz o możliwości wspierania działalności organizacji	art. 6 ust. 1 lit. f RODO realizacja prawnie uzasadnionego interesu administratora, którym jest utrzymywanie stałego kontaktu z organizacją w związku z jej celami	okres niezbędny do osiągnięcia celu przetwarzania danych, tj. informowania o realizacji celów statutowych w ramach prowadzonej listy mailingowej, jednak nie dłużej niż do uwzględnienia sprzeciwu wobec przetwarzania danych

	statutowymi wyjaśnienia wyboru odpowiednich podstaw prawnych przetwarzania danych odbiorców newslettera znajdziesz w pkt 1 i 3 zagadnień szczegółowych poniżej	osobowych złożonego przez subskrybenta newslettera
promocja usług lub towarów oferowanych przez organizację prowadzącą działalność gospodarczą	art. 6 ust. 1 lit. a RODO w zw. z art. 10 ustawy o świadczeniu usług drogą elektroniczną w przypadku mailingu promującego usługi lub towary oferowane przez organizację prowadzącą działalność gospodarczą więcej o podstawach prawnych przetwarzania danych odbiorców newslettera w powyższym celu znajdziesz w pkt 2 zagadnień szczegółowych poniżej	okres niezbędny do osiągnięcia celu przetwarzania danych, tj. promocji usług i towarów za pośrednictwem listy mailingowej, jednak nie dłużej niż do uwzględnienia cofnięcia przez subskrybenta newslettera zgody na przetwarzania jego danych osobowych w celu otrzymywania informacji handlowych
ustalenie, dochodzenie roszczeń i obrona przed roszczeniami, w tym udokumentowanie zgłoszonych przez subskrybentów newslettera sprzeciwów wobec przetwarzania ich danych osobowych	art. 6 ust. 1 lit. f RODO art. 17 ust. 3 lit. e RODO prawnie uzasadniony interes administratora danych	okres przedawnienia ewentualnych roszczeń wynikający z przepisów prawa

7. **Kategorie odbiorców danych**

Przykładowo:

- agencje marketingowe zajmujące się profesjonalnie wysyłką mailingów,
- hostingodawca udostępniający zasoby serwerowni na rzecz organizacji, która gromadzi tam dane subskrybentów newslettera

Z powyższymi podmiotami należy zawrzeć umowę powierzenia przetwarzania danych. Wzór takiej umowy stanowi załącznik nr 1 do niniejszego kodeksu.

8. **Współadministratorzy**

Przykładowo: gdy dwie organizację prowadzą wspólny projekt, w ramach którego zbierają dane osób, które prenumerują listę mailingową, aby być na bieżąco z postępami prowadzonego projektu.

Współadministratorzy powinni zawrzeć umowę o współadministrowaniu danymi. Przykładowy wzór ramowej umowy współadministrowania danymi osobowymi został zamieszczony w załączniku nr 2 do niniejszego kodeksu.

9. **Informacje o przekazaniu do państwa trzeciego**

Przykładowo: gdy dane osobowe subskrybentów newslettera są przechowywane na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG)

10. **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa:**

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w Rozdziale VI poświęconym analizie ryzyka i środkom bezpieczeństwa.

Należy zwrócić uwagę, że elektroniczny formularz zapisu do newslettera na stronie internetowej organizacji powinien wykorzystywać szyfrowanie SSL, które zapewnia ochronę danych wprowadzonych w przeglądarce internetowej przez subskrybenta.

11. **Obowiązek informacyjny przy zbieraniu danych osobowych osób, które zaprenumerowały newsletter**

Przy zapisywaniu się na listę mailingową na stronie internetowej organizacji pozarządowej subskrybent powinien mieć możliwość zapoznania się z klauzulą informacyjną dotyczącą przetwarzania danych osobowych w organizacji będącej wydawcą newslettera.

Przykładowa klauzula informacyjna pod formularzem subskrypcji newslettera na stronie internetowej organizacji:

*Informujemy, że Pani/Pana dane osobowe są przetwarzane przez Organizację z siedzibą w _____ przy ul. _____ (**administrator danych** lub **Organizacja**) **w ramach utrzymywania stałego kontaktu** z naszą Organizacją w związku z jej celami statutowymi, w szczególności poprzez informowanie o organizowanych akcjach społecznych.*
***Podstawę prawną** przetwarzania danych osobowych stanowi art. 6 ust. 1 lit. f rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).*
*Podanie danych jest **dobrowolne**, niemniej bez ich wskazania nie będzie możliwa wysyłka zamówionego newslettera.*

*Informujemy, że przysługuje Pani/Panu **prawo** dostępu do treści swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu wobec ich przetwarzania, a także prawo do wniesienia **skargi do organu nadzorczego**.*
*Korzystanie z newslettera jest **bezterminowe**. W każdej chwili przysługuje Pani/Panu prawo do wniesienia **sprzeciwu** wobec przetwarzania danych osobowych. W takim przypadku dane wprowadzone przez Pana/Panią w procesie rejestracji zostaną usunięte niezwłocznie po upływie okresu przedawnienia ewentualnych roszczeń i uprawnień przewidzianego w Kodeksie cywilnym.*
*Do Pani/Pana danych osobowych mogą mieć również **dostęp** podmioty świadczące na naszą rzecz usługi w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze, prawnicze, księgowe, kadrowe.*
*Państwa dane osobowe mogą być przekazywane do **państwa trzeciego**, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń.*
*Podane dane osobowe mogą być przetwarzane w sposób **zautomatyzowany**, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem, nie będą zautomatyzowane.*
Ze szczegółowymi informacjami dotyczącymi zasad przetwarzania danych osobowych w Organizacji mogą Państwo zapoznać się w Polityce prywatności dostępnej na stronie internetowej <www.nazwaorganizacji.pl>.
*W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pani/Pana danych osobowych prosimy o kontakt z wyznaczonym przez nas **Inspektorem Ochrony Danych** pisząc na adres siedziby naszej Organizacji: _____, z dopiskiem „Inspektor Ochrony Danych" lub na adres poczty elektronicznej <iod@nazwaorganziacji.pl> .*

Zagadnienia szczegółowe

1) **Jaka jest podstawa prawna przetwarzania danych osobowych subskrybentów newslettera realizowanego przez organizację, która nie prowadzi działalności gospodarczej?**

   Mailing realizowany przez organizację, który nie jest związany z działalnością gospodarczą organizacji, nie stanowi informacji handlowych w rozumieniu ustawy o świadczeniu usług drogą elektroniczną. W konsekwencji nie jest wymagana zgoda subskrybentów newslettera na otrzymywanie informacji handlowych przekazywanej za pośrednictwem poczty elektronicznej na podstawie art. 10 powyższej ustawy. W takim przypadku właściwą podstawę prawną stanowi prawnie uzasadniony interes administratora przewidziany w art. 6 ust. 1 lit. f RODO polegający na utrzymywaniu stałego kontaktu pomiędzy subskrybentem newslettera a organizacją w związku z jej celami statutowymi.

2) **Jaka jest podstawa prawna przetwarzania danych osobowych subskrybentów newslettera realizowanego w celu promocji towarów i usług oferowanych przez organizację w związku z prowadzoną działalnością gospodarczą?**

Jeżeli organizacja społeczna prowadzi działalność gospodarczą, wówczas mailing dotyczący oferowanych przez nią usług lub towarów należy kwalifikować jako informację handlową w rozumieniu ustawy o świadczeniu usług drogą elektroniczną i zgodnie z art. 10 ust. 2 powyższej ustawy. Przy czym sam fakt udostępnienia adresu elektronicznego przez odbiorcę newslettera w celu otrzymania informacji handlowej stanowi wyraźne działanie potwierdzające, które zgodnie z art. 4 pkt 11 RODO (obok oświadczenia osoby, której dane dotyczą) jest z jedną form wyrażenia zgody. Co do zasady nie ma zatem konieczności stosowania pola wyboru pod formularzem zapisu w celu pozyskania zgody subskrybenta. Jeżeli jednak organizacja przewiduje inne cele przetwarzania danych , np. używanie telekomunikacyjnych urządzeń końcowych, w tym telefonu, w celu prowadzenia marketingu bezpośredniego, wówczas na każdy z celów organizacja powinna pozyskać osobne zgody. W tym celu niezbędne będzie wyodrębnienie pod formularzem zapisu dwóch pól wyboru (checkbox'ów), aby zgoda na otrzymywania informacji handlowych była wyodrębniona od zgody na marketing bezpośredni kierowany przez organizację na telekomunikacyjne urządzenia końcowe. Organizacja powinna bowiem zapewnić zapisującemu się swobodę w dysponowaniu swoimi danymi osobowymi na wskazane powyżej cele.

Więcej na temat zgody osoby, której dane dotyczą, znajdziesz w Rozdziale II pkt 3 wyżej.

3) **Czy dane odbiorców newslettera zebrane przez organizację o celach politycznych, światopoglądowych, religijnych lub związkowych stanowią dane wrażliwe?**

Nie, sam fakt zapisania się do listy mailingowej prowadzonej przez organizację o celach politycznych, światopoglądowych, religijnych lub związkowych nie uzasadnia twierdzenia, że subskrybent ujawnia w ten sposób swoje poglądy polityczne, przekonania religijne lub światopoglądowe, czy też przynależność do związków zawodowych. Dane wskazane przez subskrybenta, np. imię, nazwisko, adres poczty elektronicznej, stanowią dane zwykłe.

4) **Jakie obowiązki ciążą na organizacji przy pozyskiwaniu danych za pośrednictwem formularza zapisu do newslettera?**

Organizacja projektując formularz zapisu do newslettera, powinna wziąć pod uwagę zasadę minimalizacji, która zakazuje pobierania danych zbędnych dla celu przetwarzania (w tym przypadku informowania o działalności statutowej organizacji w formie newslettera). Tytułem przykładu należy wskazać, że danymi nadmiarowymi byłyby adres zamieszkania bądź numer telefonu subskrybenta newslettera, w sytuacji w której organizacja planuje jedynie komunikację elektroniczną z odbiorcą newslettera.

Organizacja powinna wywiązać się z obowiązku informacyjnego wobec osoby zapisującej się do newslettera. Formularz zapisu do newslettera na stronie internetowej powinien być wyposażony w klauzulę informacyjną. Wzór takiej klauzuli został zamieszczony w punkcie 11 powyżej.

5) **Na co organizacja powinna zwrócić szczególną uwagę przy wysyłce mailingu, aby nie naruszyć ochrony przetwarzanych danych osobowych?**

Newsletter polega na wysłania wiadomości o tej samej treści do wielu adresatów (odbiorców newslettera). Organizacja powinna zwrócić szczególną uwagę, aby zachować prywatność pozyskanych danych osobowych i nie ujawnić w wiadomości pocztowej w polu adresata danych adresowych innych odbiorców newslettera, do których kierowana jest korespondencja. Odbiorcy ci bowiem nie są upoważnieni do przetwarzania nawzajem swoich danych kontaktowych.

Aby uniknąć sytuacji, w której poszczególne osoby uzyskają adresy innych odbiorców, należy w wiadomości pocztowej wpisywać adresy odbiorców w polu 'ukryta kopia', 'UDW', 'BCC', zamiast w polu 'do', 'do wiadomości', 'kopia', 'CC' bądź innym równoważnym w zależności od programu pocztowego.

6) Co organizacja powinna uwzględnić, gdy odbiorca chciałby zrezygnować z otrzymywania newslettera?

Osoby, które zapisały się na listy mailingowe, powinny mieć łatwą możliwość rezygnacji z subskrypcji, np. poprzez kliknięcie w link 'wypisz się' w stopce wiadomości e-mail. Rezygnacja taka jest równoznaczna ze sprzeciwem wobec przetwarzania danych osobowych i powinna skutkować usunięciem danych z baz danych organizacji po upływie okresu niezbędnego do ustalenia, dochodzenia lub obrony ewentualnych roszczeń w związku z realizacją newslettera. Okres ten może ulec przedłużeniu, jeżeli istnieje inna podstawa przetwarzania danych przez organizację, np. odbiorca newslettera jest jednocześnie beneficjentem, który otrzymuje wsparcie od organizacji.

Jeżeli organizacja planuje kontynuowanie wysyłki mailingów w przyszłości, w szczególności do osób, których dane ma zamiar pozyskać z publicznie dostępnych źródeł, wówczas może stworzyć listę osób, które sprzeciwiły się przetwarzaniu ich danych osobowych i sprzeciw ten został uwzględniony przez organizację (wewnętrzna lista Robinsonów). Dane osób wpisanych na taką wewnętrzną listę mogą być nadal przetwarzane przez organizację, pomimo uwzględnienia sprzeciwu subskrybenta, ponieważ ma prawnie uzasadniony interes w tym, aby takie osoby nie otrzymały mailingu kierowanego przez organizację.

Więcej informacji o przetwarzania danych osobowych z publicznie dostępnych źródeł można znaleźć w rozdziale IV pkt 4 niniejszego kodeksu.

4. Komunikacja z osobami, których dane zostały pozyskane ze źródeł publicznie dostępnych

1. **Opis procesu przetwarzania danych osobowych**

Proces ten obejmuje zbieranie i korzystanie z danych osób fizycznych, które są publicznie dostępne, w celu:

1. informowania o realizacji działań statutowych organizacji, w szczególności o prowadzonych programach, organizowanych wydarzeniach, debatach, seminariach, konferencjach naukowych i prasowych, akcjach społecznych, apelach, kampaniach etc.;

2. informowania o możliwości wsparcia organizacji (zobacz Rozdział IV pkt 2 poświęcony zbieraniu funduszy na działalność organizacji)
3. promocji usług lub towarów oferowanych przez organizację prowadzącą działalność gospodarczą.

W powyższych celach organizacja może korzystać z następujących kanałów komunikacji:

- pisemnego na adres korespondencyjny
- elektronicznego za pośrednictwem e-maila, SMSa, komunikatora itp.
- telefonicznego
- bezpośredniego

2. **Opis kategorii osób**

Osoby fizyczne, których dane zostały pozyskane przez organizację, z publicznie dostępnych źródeł obejmujące w szczególności:

- dane osób fizycznych zamieszczone w jawnych rejestrach publicznych takich jak Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEiDG), baza REGON Głównego Urzędu Statystycznego, Monitor Sądowy i Gospodarczy, w którym publikowane są ogłoszenia o wpisach w Krajowym Rejestrze Sądowym;
- dane osobowe z ogólnodostępnych baz osób wykonujących wolne zawody, np.lekarzy, dentystów, dziennikarzy, adwokatów, radców prawnych, rzeczników patentowych, komorników sądowych, doradców podatkowych etc.;
- dane osobowe opublikowane na prywatnych i służbowych stronach internetowych, np. na stronach internetowych kancelarii prawnych;
- dane osobowe opublikowane w prasie oraz w innych mediach
- dane osób fizycznych zamieszczone w mediach społecznościowych.

3. **Kategorie danych osobowych**

Typowymi kategoriami danych, które organizacja pozyskuje z publicznie dostępnych źródeł, będą w zakresie danych zwykłych:

- imiona i nazwiska,
- adresy poczty elektronicznej,
- numery telefonów,
- adres do korespondencji,
- wykonywany zawód
- udział w organach osób prawnych.

Odnośnie danych wrażliwych zobacz pkt 6 zagadnień szczegółowych poniżej.

4. **Cel przetwarzania danych osobowych**	5. **Podstawa prawna przetwarzania danych osobowych**	6. **Okres przetwarzania danych osobowych**

informowanie o realizacji celów statutowych oraz o możliwościach wspierania działalności organizacji	art. 6 ust. 1 lit. f RODO realizacja prawnie uzasadnionego interesu administratora, którym jest utrzymywanie stałego kontaktu z organizacją w związku z jej celami statutowymi wyjaśnienia wyboru odpowiednich podstaw prawnych przetwarzania danych odbiorców mailingu znajdziesz w pkt 2 zagadnień szczegółowych poniżej	okres niezbędny do osiągnięcia celu przetwarzania danych, tj. informowania o realizacji celów statutowych w ramach prowadzonego mailingu, jednak nie dłużej niż do uwzględnienia sprzeciwu wobec przetwarzania danych osobowych złożonego przez osobę, której dane zostały pozyskane z publicznie dostępnych źródeł
promocja usług lub towarów oferowanych przez organizację prowadzącą działalność gospodarczą	art. 6 ust. 1 lit. a RODO w zw. z w art. 10 ustawy o świadczeniu usług drogą elektroniczną, tj. zgoda na otrzymywanie informacji handlowych za pośrednictwem poczty elektronicznej lub telefonu w przypadku komunikacji promującej usługi lub towary oferowane przez organizację prowadzącą działalność gospodarczą więcej o podstawach prawnych przetwarzania danych odbiorców mailingu znajdziesz w pkt 2 zagadnień szczegółowych poniżej	okres niezbędny do osiągnięcia celu przetwarzania danych, tj. promocji usług i towarów w ramach e-mail marketingu, jednak nie dłużej niż do uwzględnienia cofnięcia przez odbiorcę mailingu zgody na przetwarzania jego danych osobowych w celu otrzymywania informacji handlowych
	art. 6 ust. 1 lit. a RODO w zw. z art. 172 Prawa a telekomunikacyjnego, tj. zgoda na używanie telekomunikacyjnych urządzeń końcowych oraz automatycznych systemów wysyłających dla celów marketingu bezpośredniego w przypadku mailingu i callingu promującego usługi lub towary oferowane przez	okres niezbędny do osiągnięcia celu przetwarzania danych, tj. promocji usług i towarów w ramach marketingu bezpośredniego przy użyciu telekomunikacyjnych urządzeń końcowych oraz automatycznych systemów wysyłających, jednak nie dłużej niż do uwzględnienia cofnięcia przez odbiorcę

	organizację prowadzącą działalność gospodarczą więcej o podstawach prawnych przetwarzania danych znajdziesz w pkt 2 zagadnień szczegółowych poniżej	mailingu zgody na przetwarzania jego danych osobowych w powyższym celu
ustalenie, dochodzenie roszczeń i obrona przed roszczeniami, w tym udokumentowanie zgłoszonych przez odbiorców komunikacji sprzeciwów bądź oświadczeń o cofnięciu zgody na przetwarzanie ich danych osobowych	art. 6 ust. 1 lit. f RODO art. 17 ust. 3 lit. e RODO prawnie uzasadniony interes administratora danych	okres przedawnienia ewentualnych roszczeń wynikający z przepisów prawa

7. **Kategorie odbiorców danych**

Przykładowo:

- agencje marketingowe zajmujące się profesjonalnie wysyłką mailingów,
- hostingodawca udostępniający zasoby serwerowni na rzecz organizacji, która gromadzi tam dane osobowe pozyskane z publicznie dostępnych źródeł

Z powyższymi podmiotami należy zawrzeć umowę powierzenia przetwarzania danych. Wzór takiej umowy stanowi załącznik nr 1 do niniejszego kodeksu.

8. **Współadministratorzy**

Do współadministrowania danymi osobowymi może dojść, gdy dwie organizacje prowadzą wspólny projekt, w ramach którego wysyłają mailing do osób, których dane zostały pozyskane z publicznie dostępnych źródeł.

Współadministratorzy powinni zawrzeć umowę o współadministrowaniu danymi. Przykładowy wzór ramowej umowy współadministrowania danymi osobowymi został zamieszczony w załączniku nr 2 do niniejszego kodeksu.

9. **Informacje o przekazaniu do państwa trzeciego**

Przykładowo: gdy dane osób pozyskane z publicznie dostępnych źródeł są przechowywane na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

10. **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa**

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

11. **Obowiązek informacyjny wobec osób fizycznych, których dane zostały pozyskane z publicznie dostępnych źródeł**

W przypadku gdy organizacja uzyskała dane ze publicznie dostępnych źródeł, powinna dopełnić obowiązku podania informacji wskazanych w art. 14 ust. 1 i 2 RODO, w szczególności powinna ona poinformować osobę, której dane dotyczą, o kategorii pozyskanych danych oraz źródle ich pochodzenia.

Zgodnie motywem 61 preambuły RODO *„jeżeli osobie, której dane dotyczą, nie można podać pochodzenia danych osobowych, ponieważ korzystano z różnych źródeł, informacje należy przedstawić w sposób ogólny".*

W świetle art. 14 ust. 3 RODO obowiązek informacyjny powinien być spełniony:

- w rozsądnym terminie, najpóźniej w ciągu miesiąca po pozyskaniu danych osobowych lub
- jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą lub
- jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.

Organizacja powinna zapewnić możliwość złożenia sprzeciwu, np. w formie kliknięcia linku rezygnacji w treści e-maila bądź w formie przesłania e-maila do administratora, która co do zasady powinna skutkować usunięciem danych takiej osoby z bazy kontaktów organizacji. O możliwości dłuższego gromadzenia danych osób, które sprzeciwiły się przetwarzaniu danych, szerzej w pkt. 4 zagadnień szczegółowych poniżej.

Przykładowy wzór klauzuli informacyjnej wysyłanej na adresy poczty elektronicznej, które zostały pozyskane z publicznie dostępnych źródeł w celu informowania o realizacji działań statutowych organizacji:

Uprzejmie informujemy, że Pana/Pani dane osobowe w zakresie imienia, nazwiska, zawodu oraz adresu poczty elektronicznej zostały pozyskane przez Organizację … z siedzibą w …, przy ul. …, (administrator danych), ze źródeł publicznie dostępnych w celu informowania o realizacji działań statutowych naszej Organizacji, w tym do informowania o organizowanych przez nas akcjach społecznych. Dopuszczalność przetwarzania danych w wyżej wskazanym celu uzasadniona jest prawnie usprawiedliwionymi interesami realizowanymi przez administratora danych osobowych zgodnie z art. 6 ust. 1 lit. f RODO.
Informujemy, że przysługuje Pana/Pani prawo dostępu do treści swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu wobec ich przetwarzania a także prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Do Państwa danych osobowych mogą mieć również dostęp podmioty świadczące na rzecz Organizacji usługi, w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze. prawnicze, księgowe, kadrowe. Państwa dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń. Podane dane osobowe mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem, nie będą zautomatyzowane.
Ze szczegółowymi informacjami dotyczącymi zasad przetwarzania danych osobowych w Organizacji mogą Państwo zapoznać się w Polityce prywatności dostępnej na stronie internetowej Organizacji. W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pana/Pani danych osobowych prosimy o kontakt z wyznaczonym przez nas Inspektorem Ochrony Danych Osobowych pisząc na adres siedziby Organizacji: ul. _____, z dopiskiem „Inspektor Ochrony Danych" lub na adres poczty elektronicznej <iod@nazwaorganizacji.pl>.
Pana/Pani dane osobowe będą przechowywane przez naszą Organizacji nie dłużej niż przez okres przedawnienia roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych w razie otrzymania od Pana/Pani sprzeciwu wobec przetwarzania danych, który można złożyć klikając na przycisk: <wypisz się>.

Zagadnienia szczegółowe

1) Pod jakimi warunkami organizacje mogą tworzyć bazy danych osób fizycznych na podstawie informacji dostępnych publicznie?

Każda organizacja może korzystać z danych dostępnych w Internecie, w ogólnodostępnych rejestrach takich jak KRS, CEIDG, REGON, informacji opublikowanych w prasie, w książce telefonicznej bądź na liście najbogatszych Polaków, i na tej podstawie tworzyć bazy danych osób fizycznych, o ile wywiązuje się z obowiązków nałożonych na administratora przez RODO. Dotyczy to w szczególności:
1) wskazania celu oraz podstawy prawnej przetwarzania danych zebranych z publicznie dostępnych źródeł,
2) spełnienia obowiązku informacyjnego wobec osób, których dane zostały zgromadzone w bazie
3) zaewidencjonowania procesu przetwarzania w rejestrze czynności przetwarzania prowadzonym przez organizację.

Możliwe cele przetwarzania oraz odpowiadające im podstawy prawne zostały ujęte w tabeli powyżej w pkt 4 i 5.

Wobec osób fizycznych, których dane zostały pozyskane z publicznie dostępnych źródeł, organizacja powinna spełnić obowiązek informacyjny określony w art. 14 RODO poprzez bezpośrednie przekazanie informacji osobie, której dane dotyczą, m.in. informacji o swoich

danych identyfikacyjnych organizacji jako administratora danych, skąd organizacja posiada dane tych osób, w jakim celu i jak długo zamierza je przetwarzać a także informacji o przysługujących osobom prawach na gruncie RODO. Przykładowa klauzula informacyjna przeznaczona dla odbiorców informacji o działalności statutowej organizacji została zamieszczona w pkt 11 powyżej.

Klauzula informacyjna powinna być wysłana za pośrednictwem dostępnego kanału komunikacji, np. pocztą elektroniczną lub pocztą tradycyjną. Wysoki koszt wysyłki takiej klauzuli informacyjnej pocztą tradycyjną nie stanowi podstawy do zwolnienia z obowiązku informacyjnego. Nie ma obowiązku informacyjnego wobec danych archiwalnych ujętych w ogólnodostępnych rejestrach publicznych z uwagi na fakt, że wskazane tam dane kontaktowe mogą być nieaktualne.

Jeśli osoba fizyczna, której dane zostały pozyskane przez organizację z publicznie dostępnych źródeł, nie życzy sobie, aby jej dane były wykorzystywane przez organizację, może zażądać usunięcia jej danych osobowych, zgłaszając sprzeciw wobec ich przetwarzania przez organizację.

2) Na jakiej podstawie prawnej organizacje prowadzące działalność gospodarczą mogą kierować komunikację marketingową w formie wiadomości e-mail, SMS bądź połączenia telefonicznego z osobami fizycznymi, których dane zostały pozyskane z publicznie dostępnych źródeł?

W przypadku gdy organizacja w ramach prowadzonej działalności gospodarczej chciałaby za pośrednictwem wskazanych wyżej kanałów komunikacji promować swoje towary lub usługi wobec osoby, których dane pozyskała z publicznie dostępnych źródeł, powinna w tym celu wykonać wobec niej obowiązek informacyjny oraz pozyskać uprzednią zgodę takiej osoby:

a. na otrzymywanie informacji handlowych – zgodnie z art. 10 ustawy o świadczeniu usług drogą elektroniczną (Dz.U.2019.123 t.j. z późn. zm.),
b. na używanie telekomunikacyjnych urządzeń końcowych oraz automatycznych systemów wysyłających dla celów marketingu bezpośredniego – zgodnie z art. 172 Prawa telekomunikacyjnego.

Organizacja może skontaktować z taką osobą za pośrednictwem e-maila, SMS-a, komunikatora bądź nawiązując połączenie telefoniczne w celu ustalenia, czy wyraża ona zgodę na dalszy kontakt w celach marketingowych. Jeżeli osoba nie wyrazi zgody na taką komunikację, dalszy kontakt w tym zakresie jest zakazany. Jeżeli natomiast osoba wyrazi zgodę, organizacja może podejmować komunikację marketingową wobec takiej osoby przy użyciu narzędzi elektronicznych.

Wymóg pozyskania zgody osoby, której dane zostały zebrane z publicznie dostępnych źródeł, w zależności rodzaju i kanału komunikacji przedstawia poniższa tabela:

Kanał komunikacji z osobą, której dane zostały pozyskane z publicznie dostępnych źródeł	**Czy wymagana jest zgoda osoby na przesyłanie informacji**	
	o działaniach statutowych, tj. niezwiązanych z działalnością gospodarczą	**promujących towary i usługi oferowane przez organizację w**

	prowadzoną przez organizację?	ramach prowadzonej przez nią działalności gospodarczej?
poczta tradycyjna	Nie, o ile osoba, które dane zostały zebrane z publicznie dostępnych źródeł, ma możliwość zgłoszenia sprzeciwu wobec przetwarzania jego danych i nie zgłaszała takiego sprzeciwu w przeszłości*	Nie, o ile z testu uzasadnionego interesu przeprowadzonego przez organizację wynika, że może ona oprzeć się na przesłance prawnie uzasadnionego interesu administratora, a nie na przesłance zgody osoby, której dane dotyczą (, np. w zakresie danych wrażliwych) **
e-mail	Nie*	Tak
telefon	Nie*	Tak
wiadomości tekstowe (SMS)	Nie*	Tak
media społecznościowe	Nie*	Tak

***** od organizacji społecznych, która komunikuje się z osobą, której dane pozyskała z publicznie dostępnych źródeł w związku z realizacją swoich statutowych, a nie w ramach prowadzonej działalności gospodarczej, nie jest wymagana zgoda takiej osoby:

a. na otrzymywanie informacji handlowych określonych w art. 10 ustawy o świadczeniu usług drogą elektroniczną,
b. na używanie telekomunikacyjnych urządzeń końcowych oraz automatycznych systemów wysyłających dla celów marketingu bezpośredniego, o jakich mowa w art. 172 Prawa telekomunikacyjnego.

****** więcej informacji na temat testu uzasadnionego interesu znajdziesz w rozdziale II pkt 1 poświęconemu prawnie uzasadnionemu interesowi administratora.

3) Czy organizacja może wysyłać mailing do osób, których dane zostały pozyskane z publicznie dostępnych źródeł na służbowe adresy poczty elektronicznej składające się z imienia i nazwiska?

RODO nie ma zastosowania do przetwarzania danych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, np. spółek kapitałowych zarejestrowanych w Krajowym Rejestrze Sądowym. Dotyczy to w szczególności firmy, formy prawnej osoby a także danych kontaktowych osoby prawnej. Organizacja może zatem wysyłać informacje handlowe na dane kontaktowe osób prawnych bez konieczności pozyskiwania zgody na przetwarzanie danych ani wykonywać wobec niej obowiązku informacyjnego.

Należy jednak pamiętać, że służbowe adresy poczty elektronicznej zawierające imię, nazwisko oraz nazwę organizacji, np. <imie.nazwisko@nazwaorganizacji.pl> stanowią dane osobowe w rozumieniu RODO. Stąd organizacja powinna wywiązać się wobec takich osób z obowiązku

informacyjnego stosownie do art. 14 RODO. Przykładowa klauzula informacyjna przeznaczona dla odbiorców informacji o działalności statutowej organizacji została zamieszczona w pkt 11 powyżej.

Organizacja nie ma obowiązku informacyjnego w stosunku do adresów anonimowych, takich jak, np. <biuro@nazwaorganizacji.pl>, <kontakt@nazwaorganizacji.pl>.

4) Czy na potrzeby przyszłych mailingów organizacja może tworzyć tzw. listę wyjątków zawierającą dane osób, które zgłosiły sprzeciw wobec przetwarzania ich danych osobowych?

Jeżeli organizacja planuje w przyszłości mailing do osób, których dane pozyskała ze źródeł publicznie dostępnych, powinna utworzyć listę wyjątków zawierającą dane osób, które zgłosiły sprzeciw na wysyłanie do nich mailingu. Ma to na celu uniknięcie sytuacji, w której osoba taka otrzymuje od organizacji niezamówioną korespondencję, pomimo zgłoszonego sprzeciwu wobec przetwarzania jej danych osobowych. Podstawą prawną przetwarzania danych w powyższym celu jest prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO).

Lista wyjątków powinna zawierać jedynie te dane, które są niezbędne do identyfikacji osób, które należy pominąć w przyszłych mailingach. Nadto dane tych osób powinny być odpowiednio zabezpieczone przed dostępem osób nieupoważnionych, zarówno spoza organizacji, jak i osób zatrudnionych w organizacji, np. przez ograniczenie dostępu do członków zarządu organizacji i jej informatyka.

5) Czy organizacja może dokonywać oceny osób publicznych ma podstawie danych pozyskanych z publicznie dostępnych źródeł?

Organizacja społeczna może wykorzystać publicznie dostępne dane polityków, np. obietnice złożone w czasie wyborów oraz faktyczną historię głosowań, w celu ich oceny ich pracy, mimo że wpływ na zainteresowanych polityków może być znaczący. Okoliczność, że przetwarzanie jest oparte na informacji publicznej oraz związane z ich obowiązkami publicznymi powoduje, organizacja może oprzeć przetwarzania danych osobowych na podstawie prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f RODO).

6) Czy dane odbiorców mailingu, których dane zostały zebrane z publicznie dostępnych źródeł, a przetwarzane przez organizację o celach politycznych, światopoglądowych, religijnych lub związkowych stanowią dane wrażliwe?

Nie, sam fakt pozyskania danych z publicznie dostępnych źródeł przez organizację o celach politycznych, światopoglądowych, religijnych lub związkowych nie uzasadnia twierdzenia, że dane osób, które zostały zebrane z publicznie dostępnych źródeł ujawniają poglądy polityczne, przekonania religijne lub światopoglądowe czy też przynależność do związków zawodowych takich osób. Dane pozyskane w powyższy sposób takie jak, np. imię, nazwisko, adres poczty elektronicznej, stanowią dane zwykłe.

5. Media społecznościowe

1. Opis procesu przetwarzania danych osobowych

Proces ten obejmuje korzystanie przez organizację z danych osób będących użytkownikami mediów społecznościowych, którzy pozostają w kontakcie z organizacją, np. w formie polubienia, obserwowania profilu organizacji, udostępnienia, komentarzy czy wiadomości prywatnej wysłanej za pośrednictwem komunikatora dostępnego w portalu społecznościowym.

2. Opis kategorii osób

Użytkownicy będący osobami fizycznymi, którzy zarejestrowali swoje konta w portalach społecznościowych, takich jak F*acebook, Twitter, Youtube, Pinterest, n*a których organizacja prowadzi swoje kanały, konta, fanpage, grupy etc., a następnie weszły na portalu społecznościowym w interakcję z organizacją w sposób ujawniający organizacji dane osobowe użytkownika.

3. Kategorie danych osobowych

Typowymi kategoriami danych, które organizacja pozyskuje, korzystając z mediów społecznościowych w zakresie danych zwykłych są:

- imiona i nazwiska,
- adresy poczty elektronicznej,
- numery telefonów,
- wizerunek.

Odnośnie danych wrażliwych zobacz pkt 3 zagadnień szczegółowych poniżej.

4. Cel przetwarzania danych osobowych	5. Podstawa prawna przetwarzania danych osobowych	6. Okres przetwarzania danych osobowych (planowane terminy usunięcia danych)
utrzymywanie stałego kontaktu, w tym informowanie o realizacji celów statutowych oraz o możliwościach wspierania działalności organizacji	art. 6 ust. 1 lit. f RODO realizacja prawnie uzasadnionego interesu administratora, którym jest utrzymywanie stałego kontaktu użytkownika portalu społecznościowego z organizacją w związku z jej celami statutowymi	okres niezbędny do osiągnięcia celu przetwarzania danych, tj. informowania o realizacji celów statutowych na portalu społecznościowym, jednak nie dłużej niż do złożenia przez użytkownika sprzeciwu wobec przetwarzania jego danych osobowych
ustalenie, dochodzenie roszczeń i obrona przed roszczeniami, w tym udokumentowanie sprzeciwów wobec	art. 6 ust. 1 lit. f RODO art. 17 ust. 3 lit. e RODO prawnie uzasadniony interes administratora danych	okres przedawnienia ewentualnych roszczeń wynikający z przepisów prawa

przetwarzanie ich danych osobowych		

7. Kategorie odbiorców danych

Przykładowo: agencja wykonująca na zlecenie organizacji przenoszenie danych kontaktowych z listy mailingowej do narzędzi portalu społecznościowego w celu pozyskania na nim kontaktów i poszerzenia zasięgu oddziaływania organizacji.

Organizacja powinna zawrzeć z agencją umowę powierzenia przetwarzania danych. Wzór takiej umowy stanowi załącznik nr 1 do niniejszego kodeksu.

8. Współadministratorzy

Wspólne administrowanie danymi użytkowników portali społecznościowego zachodzi pomiędzy operatorem takiego portalu a organizacją, która prowadzi na nim swój fanpage.

Administratorem danych osobowych użytkowników danego portalu społecznościowego jest operator takiego portalu, który przetwarza dane osobowe na podstawie własnego regulaminów. Jeżeli jednak użytkownik wchodzi w interakcję z organizacją poprzez polubienie fanpaga, obserwowanie strony, reakcje na posty, udostępnienia/retweety, komentarze, wiadomości prywatne na portalu społecznościowym, administratorem danych osobowych staje się także organizacja pozarządowa, ponieważ przyczynia się ona (wraz z operatorem portalu społecznościowego) do określenia celów i sposobów przetwarzania danych osobowych osób odwiedzających stronę organizacji na takim portalu.

W konsekwencji oba podmioty powinny zawrzeć umowę o współadministrowaniu danych użytkowników portali społecznościowego, przy czy elektroniczna akceptacja regulaminu portalu przez organizację spełnia ten wymóg.

9. Informacje o przekazaniu do państwa trzeciego

Przykładowo: gdy dane użytkowników portalu społecznościowego przechowywane są przez jego operatora na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

W takim przypadku organizacja powinna sprawdzić w szczególności, czy operator uzyskał certyfikat potwierdzający spełnianie unijnych wymagań dotyczących ochrony prywatności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony, standardowych klauzul ochrony danych lub standardowych klauzul umownych przyjętych przez właściwy organ nadzorczy i zatwierdzonych przez Komisję Europejską.

10. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych.

Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

11. Obowiązek informacyjny wobec osób fizycznych będących użytkownikami portali społecznościowych

Zasadnicza treść uzgodnień pomiędzy współadministratorami, w szczególności w odniesieniu do wykonywania praw przysługujących podmiotom danych, powinna być im udostępniana w klauzuli informacyjnej. Jeżeli operator portalu społecznościowego nie zapewnia możliwości zamieszczenia przez organizację klauzuli informacyjnej na portalu, wystarczające będzie uzupełnienie klauzuli informacji na stronie internetowej organizacji.

Odnośnie wspólnego administrowania danymi użytkowników portalu społecznościowego zobacz pkt 8 powyżej

Poniżej przedstawiamy wzór klauzuli informacyjnej dotyczącej przetwarzania danych osobowych w celu informowania o realizacji działań statutowych organizacji na portalu społecznościowym.

*Informujemy, że Organizacja używa mediów społecznościowych **w ramach utrzymywania stałego kontaktu** z naszą Organizacją w związku z jej celami statutowymi, w szczególności poprzez informowanie o organizowanych akcjach społecznych. Są to w szczególności fanpage na Facebooku, kanał YouTube oraz konto Twitter. Strona internetowa naszej Organizacji oferuje również możliwość udostępniania informacji poprzez Facebook, Twitter, LinkedIn, Pinterest lub Reddit. Dostęp do wskazanych mediów jest możliwy poprzez ikonki znajdujące się na stronie internetowej Organizacji. Owe media społecznościowe prowadzą **własną politykę w zakresie ochrony prywatności**. Wchodząc na te strony, opuszcza Pan/Pani stronę Organizacji i Pana/Pani dane są przetwarzane przez te media społecznościowe. Zachęcamy do zapoznania się z ich polityką w dziedzinie poszanowania prywatności.*
***Podstawę prawną** przetwarzania danych osobowych stanowi art. 6 ust. 1 lit. f rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).*
*Podanie danych jest **dobrowolne**, niemniej bez ich wskazania nie będzie możliwe informowanie o realizacji celów statutowych naszej Organizacji za pośrednictwem mediów społecznościowych .*
*Informujemy, że przysługuje Pani/Panu **prawo** dostępu do treści swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu wobec ich przetwarzania a także prawo do wniesienia **skargi do organu nadzorczego**.*
*Korzystanie ze strony prowadzonej przez naszą Organizację na portalu społecznościowym jest **bezterminowe**. W każdej chwili możesz przysługuje Pani/Panu prawo do wniesienia **sprzeciwu** wobec przetwarzania danych osobowych. W takim przypadku dane wprowadzone przez Pana/Panią w procesie rejestracji zostaną usunięte niezwłocznie po upływie okresu przedawnienia ewentualnych roszczeń i uprawnień przewidzianego w Kodeksie cywilnym.*
*Do Pani/Pana danych osobowych mogą mieć również **dostęp** podmioty świadczące na naszą rzecz usługi w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze, prawnicze, księgowe, kadrowe.*

*Podane dane osobowe mogą być przetwarzane w sposób **zautomatyzowany**, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane.*
*W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pani/Pana danych osobowych prosimy o kontakt z wyznaczonym przez nas **Inspektorem Ochrony Danych** pisząc na adres siedziby naszej Organizacji: _____, z dopiskiem „Inspektor Ochrony Danych" lub na adres poczty elektronicznej <iod@nazwaorganizacji,pl>*

Zagadnienia szczegółowe

1) **Jak powinna postępować organizacja, jeżeli w portalu społecznościowym nie ma technicznej możliwości spełnienia obowiązku informacyjnego wobec użytkownika portalu?**

   Jeżeli operator portalu społecznościowego nie zapewnia możliwości zamieszczenia przez organizację klauzuli informacyjnej na portalu, wystarczające będzie uzupełnienie klauzuli informacyjnej lub polityki prywatności opublikowane na stronie internetowej organizacji.

2) **Czy organizacja może bez uprzedzenia kontaktować się użytkownikami mediów społecznościowych w sprawach dotyczących realizacji celów statutowych?**

   Tak, organizacja może bez uprzedzenia podejmować kontakt z użytkownikami portalu w celach informowania o realizacji celów statutowych oraz o możliwościach wsparcia organizacji. Jest dopuszczalne nawet jeżeli użytkownik nie wszedł uprzednio w interakcję z organizacją na portalu. Przyjmuje się bowiem, że osoba, która zakłada konto w portalu społecznościowym umożliwiającym swobodną komunikację, może spodziewać się kontaktu ze strony innych użytkowników w bliżej nieokreślonych celach.

3) **Czy dane użytkowników, którzy na portalu społecznościowym polubili fanpage organizacji o celach politycznych, światopoglądowych, religijnych lub związkowych, stanowią dane wrażliwe?**

   Nie, sam fakt wejścia w interakcję z organizacją o celach politycznych, światopoglądowych, religijnych lub związkowych poprzez polubienie jej fanpage'a bądź obserwowanie strony prowadzonej na portalu społecznościowym nie uzasadnia twierdzenia, że użytkownik ujawnia w ten sposób swoje poglądy polityczne, przekonania religijne lub światopoglądowe czy też przynależność do związków zawodowych. Dane użytkowników portalu społecznościowego należy traktować jako dane zwykłe.

6. Bezpłatne publikacje

1. Opis procesu przetwarzania danych osobowych

Proces ten obejmuje udostępnianie przez organizację - zarówno w formie papierowej, jak i elektronicznej - bezpłatnych publikacji, w tym książek, broszur, raportów, informatorów, biuletynów, analiz, ekspertyz, stanowisk, ulotek, plakatów, kalendarzy, kartek okolicznościowych etc.

2. **Opis kategorii osób**

Osoby fizyczne, które wskazały swoje dane osobowe, zamawiając bezpłatną publikację w organizacji.

3. **Kategorie danych osobowych**

Typowymi kategoriami danych, które organizacja przetwarza przy realizacji zamówienia bezpłatnej publikacji, będą w zakresie danych zwykłych:

- imię i nazwisko,
- adres poczty elektronicznej,
- numer telefonu
- adres do korespondencji.

Odnośnie danych wrażliwych, zobacz pkt 1 zagadnień szczegółowych poniżej.

4. Cel przetwarzania danych osobowych	5. Podstawa prawna przetwarzania danych osobowych	6. Okres przetwarzana danych osobowych
realizacja zamówienia bezpłatnej publikacji, w tym dostarczenie jej zamawiającemu	art. 6 ust. 1 lit. b RODO tj. wykonanie zamówienia na bezpłatną publikację	okres niezbędny do osiągnięcia celu przetwarzania danych osobowych
Informowanie zamawiających bezpłatne publikacje o realizacji celów statutowych organizacji oraz o możliwościach wspierania działalności organizacji	art. 6 ust. 1 lit. f RODO prawnie uzasadniony interes administratora, którym jest utrzymywanie stałego kontaktu z organizacją w związku z jej celami statutowymi	okres niezbędny do osiągnięcia celu, jednak nie dłużej niż do złożenia sprzeciwu wobec przetwarzania danych osobowych
dochodzenie roszczeń i obrona przed ewentualnymi roszczeniami, w tym kontakt w związku z rozpatrywaniem ewentualnych reklamacji	art. 6 ust. 1 lit. f RODO art. 17 ust. 3 lit. e RODO prawnie uzasadniony interes administratora danych	okres przedawnienia ewentualnych roszczeń wynikający z przepisów prawa

7. **Kategorie odbiorców danych**

Przykładowo: kurier, który na zlecenie organizacji, doręcza bezpłatną publikację zamawiającemu.

Z powyższym podmiotem należy zawrzeć umowę powierzenia przetwarzania danych. Wzór takiej umowy stanowi załącznik nr 1 do niniejszego kodeksu.

8. **Współadministratorzy**

Do współadministrowania danymi osobowymi może dojść, gdy dwie organizacje prowadzą wspólny projekt, w ramach którego wysyłają bezpłatne publikacje do zamawiających.

Współadministratorzy powinni zawrzeć umowę o współadministrowaniu danymi. Przykładowy wzór ramowej umowy współadministrowania danymi osobowymi został zamieszczony w załączniku nr 2 do niniejszego kodeksu.

9. **Informacje o przekazaniu do państwa trzeciego**

Przykładowo: gdy dane osobowe zamawiających bezpłatne publikacje są przechowywane na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

10. **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa:**

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

Należy zwrócić uwagę, że elektroniczny formularz zamówienia bezpłatnej publikacji na stronie internetowej organizacji powinien wykorzystywać szyfrowanie SSL, które zapewnia ochronę danych wprowadzonych przez zamawiającego w przeglądarce internetowej.

11. **Obowiązek informacyjny przy zbieraniu danych osób, które zamówiły bezpłatną publikację**

Przy składaniu zamówienia na bezpłatną publikację zamawiający powinien mieć możliwość zapoznania się z klauzulą informacyjną dotyczącą przetwarzania danych osobowych w organizacji wysyłającej bezpłatną publikację

Przykładowa klauzula informacyjna pod formularzem zamówienia na bezpłatną publikację na stronie internetowej organizacji:

Informujemy, że Państwa dane są przetwarzane przez Organizację w następujących celach:
(a) w celu wykonania zamówienia; przetwarzanie Państwa danych w wyżej wskazanym celu służy podjęciu działań przed zawarciem umowy zgodnie z art. 6 ust. 1 lit. b rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO),
(b) w ramach utrzymywania stałego kontaktu z naszą Organizacją w związku z jej celami statutowymi, w szczególności poprzez informowanie o organizowanych akcjach społecznych i możliwościach wspierania działalności Organizacji; przetwarzanie Państwa danych w wyżej wskazanym celu uzasadnione jest prawnie usprawiedliwionymi interesami realizowanymi przez naszą Organizację, zgodnie z art. 6 ust.1 lit. f RODO.

Podanie przez Państwa danych jest dobrowolnie, niemniej bez ich wskazania nie będzie możliwe wykonanie zamówienia ani informowanie o realizacji celów statutowych Organizacji.
Informujemy, że przysługuje Pana/Pani prawo dostępu do treści swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu wobec ich przetwarzania, a także prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
Do Państwa danych osobowych mogą mieć również dostęp podmioty świadczące na rzecz Organizacji usługi, w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze, prawnicze, księgowe, kadrowe.
Państwa dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń.
Podane dane osobowe mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane.
Państwa dane osobowe będą przechowywane przez naszą Organizację bezterminowo. W każdej chwili przysługuje Panu/Pani prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych. W takim przypadku dane podane przez Pana/Panią w niniejszym formularzu zostaną usunięte niezwłocznie po upływie okresu przedawnienia ewentualnych roszczeń przewidzianego w przepisach prawa.
W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pana/Pani danych osobowych prosimy o kontakt z wyznaczonym przez nas Inspektorem Ochrony Danych pisząc na adres siedziby Organizacji przy ul. _____, z dopiskiem „Inspektor Ochrony Danych" lub mailowo na adres <iod@nazwaorganziacji.pl>

Zagadnienia szczegółowe

1) **Czy dane osób zamawiających bezpłatne publikacje pozyskane w procesie zamówienia przez organizację o celach politycznych, światopoglądowych, religijnych lub związkowych stanowią dane wrażliwe?**

   Nie, sam fakt złożenia zamówienia bezpłatnej publikacji w organizacji o celach politycznych, światopoglądowych, religijnych lub związkowych nie uzasadnia twierdzenia, że zamawiający ujawnia w ten sposób swoje poglądy polityczne, przekonania religijne lub światopoglądowe czy też przynależność do związków zawodowych. Dane wskazane przez zamawiającego bezpłatną publikację, np. imię, nazwisko, adres poczty elektronicznej czy adres do korespondencji, stanowią dane zwykłe.

7. Wydarzenia publiczne

1. **Opis procesu przetwarzania danych osobowych**

Działalność organizacji w tym procesie polega na organizowaniu, podejmowaniu działań i aktywności o różnorakim charakterze i zasięgu w zależności od podmiotu je organizującego, w szczególności prowadzeniu różnego rodzaju wydarzeń, akcji i kampanii, spotkań, debat, seminariów, konferencji naukowych i prasowych. Wszystkie podmioty organizując akcje i kampanie, osobno czy to wspólnie, czynią to w oparciu o swoje statuty, przyjęte założenia i obowiązujące prawo.

2. **Opis kategorii osób**

Dotyczy osób fizycznych, które wyraziły chęć udziału w danym wydarzeniu publicznym (spotkaniu, debacie, seminarium, konferencji naukowej i prasowej) jako ich uczestnik bądź słuchacz przez wypełnienie formularza na stronie internetowej informującej o danym wydarzeniu publicznym lub wypełnienie formularza papierowego, np. w recepcji bezpośrednio przed wydarzeniem.

Będzie dotyczyć również osób, które uczestniczą w danym wydarzeniu publicznym w roli prelegenta lub wykładowcy.

3. **Typowe kategorie danych osobowych**

Typowymi kategoriami danych dla tego procesu będą w zakresie danych zwykłych:

- imię i nazwisko,
- stopień naukowy / tytuł zawodowy,
- przynależność do organizacja,
- adres do korespondencji w celu wysłania certyfikatu uczestnictwa,
- adres e-mail,
- numer telefonu komórkowego lub numer telefonu biurowego,
- rodzaj zakwaterowania podczas konferencji,
- informacje o posiłku podczas konferencji,
- informacja o metodzie dokonania płatności za uczestnictwo w wydarzeniu
- numer rachunku bankowego oraz nazwa banku, w którym jest prowadzony rachunek bankowy w celu zapłaty wynagrodzenia za zrealizowanie czynności w roli prelegenta, wykładowcy podczas wydarzenia publicznego.

4. **Cel przetwarzania danych osobowych**	5. **Podstawa prawna przetwarzania danych osobowych**	6. **Okres przetwarzana danych osobowych**
przygotowanie i realizacja wydarzeń publicznych takich jak: spotkania, konkursy, debaty, seminaria, konferencje naukowe i prasowe	art. 6 ust. 1 lit. f RODO tj. realizacja prawnie uzasadnionych interesów administratora w postaci komunikacji z osobami, które wyraziły chęć uczestnictwa w danym wydarzeniu publicznym	okres niezbędny do organizacji wydarzenia publicznego , jednak nie dłużej niż do uwzględnienia sprzeciwu wobec przetwarzania danych osobowych złożonego przez osobę, której dane dotyczą

informowanie o realizacji celów statutowych organizacji oraz o możliwościach wspierania działalności ADO	art. 6 ust. 1 lit. f RODO prawnie uzasadniony interes administratora, którym jest utrzymywanie stałego kontaktu z organizacją w związku z jej celami statutowymi	okres niezbędny do osiągnięcia celu, jednak nie dłużej niż do uwzględnienia sprzeciwu wobec przetwarzania danych osobowych złożonego przez osobę, które dane dotyczą, a po tym czasie mogą być przetwarzane przez okres przedawnienia ewentualnych roszczeń (art. 17 ust.3 lit. e RODO)
ustalenie, dochodzenie roszczeń i obrona przed roszczeniami, w tym udokumentowanie zgłoszonych sprzeciwów wobec przetwarzania danych osobowych	art. 6 ust. 1 lit. f RODO art. 17 ust. 3 lit. e RODO prawnie uzasadniony interes przetwarzania danych przez administratora	okres przedawnienia ewentualnych roszczeń wynikający z przepisów prawa

4. Kategorie odbiorców danych

Przykładowo: firma hostingowa jako podmiot przetwarzający, która na zlecenie organizacji zajmuje się hostingiem strony internetowej, na której rejestrują się uczestnicy zamierzający wziąć udział w konferencji naukowej organizowanej przez organizację.

Z powyższym podmiotem należy zawrzeć umowę powierzenia przetwarzania danych. Wzór takiej umowy stanowi załącznik nr 1 do niniejszego kodeksu.

5. Współadministratorzy

Przykładowo: gdy dwie organizacje wspólnie organizują debatę mieszczącą się w ramach celów statutowych każdej organizacji.

Współadministratorzy powinni zawrzeć umowę o współadministrowaniu danymi. Przykładowy wzór ramowej umowy współadministrowania danymi osobowymi został zamieszczony w załączniku nr 2 do niniejszego kodeksu.

6. Informacje o przekazaniu do państwa trzeciego

Przykładowo: gdy dane osobowe uczestników wydarzeń publicznych są przechowywane na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

7. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych.

Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

Należy zwrócić uwagę, że formularze zapisu na wydarzenia publiczne umieszczane na stronach internetowych powinny wykorzystywać szyfrowanie SSL zapewniające ochronę danych w prowadzonych przez uczestników wydarzeń publicznych do formularza w swojej przeglądarce internetowej.

11. **Obowiązek informacyjny przy zbieraniu danych osób, które biorą udział w wydarzeniu publicznym**

Osoby rejestrujące się jako uczestnicy wydarzenia publicznego, powinny mieć możliwość zapoznania się z klauzulą informacyjną dotyczącą przetwarzania danych osobowych , np. poprzez umieszczenie jej pod formularzem zapisu na wydarzenie na stronie internetowej organizacji.

Przykładowa klauzula informacyjna pod formularzem uczestnictwa w konferencji naukowej:

Informujemy, że podane przez Pana/Panią dane osobowe są przetwarzane przez Organizację z siedzibą w ….. przy ul. ……. (administrator danych lub Organizacja) w celu informowania o organizowanej konferencji naukowej oraz w ramach utrzymywania stałego kontaktu z naszą Organizacją w związku z jej celami statutowymi, w szczególności poprzez informowanie o organizowanych akcjach społecznych i możliwościach wspierania działalności naszej Organizacji; przetwarzanie Pana/Pani danych w wyżej wskazanych celach uzasadnione jest prawnie usprawiedliwionymi interesami realizowanymi przez administratora zgodnie z art. 6 ust.1 lit. f RODO.
Podanie przez Pana/Panią danych jest dobrowolne, niemniej bez ich wskazania nie będzie możliwe informowanie o organizowanej przez nas konferencji naukowej, a także informowanie o realizacji celów statutowych Organizacji.
Informujemy, że przysługuje Pana/Pani prawo dostępu do treści swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu wobec ich przetwarzania, a także prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
Do Państwa danych osobowych mogą mieć również dostęp podmioty świadczące na rzecz Organizacji usługi, w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze. prawnicze, księgowe, kadrowe. Państwa dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń. Podane dane osobowe mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane.
Państwa dane osobowe będą przechowywane przez nas bezterminowo. W każdej chwili przysługuje Panu/Pani prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych. W takim przypadku dane podane przez Pana/Panią w niniejszym formularzu zostaną usunięte niezwłocznie po upływie okresu przedawnienia ewentualnych roszczeń przewidzianego w przepisach prawa.

W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pani/Pana danych osobowych prosimy o kontakt z wyznaczonym przez nas Inspektorem Ochrony Danych pisząc na adres siedziby Organizacji: ul. ……. , ……., z dopiskiem „Inspektor Ochrony Danych" lub na adres poczty elektronicznej <iod@nazwaorganziacji.pl>

Zagadnienia szczegółowe:

1) **Czy organizacja może informować uczestnika wydarzenia publicznego (np. otwartego wydarzenia w formie wykładu) po zakończonym wydarzeniu o organizacji kolejnego, wysyłając uczestnikowi zaproszenie? Czy organizacja może także informować uczestnika o swojej działalności statutowej?**

   Organizacja może wysyłać informacje o swojej działalności statutowej poprzez poinformowanie o możliwości wzięcia udziału w kolejnym wydarzeniu publicznym na dane podane przez uczestnika wydarzenia publicznego (np. adres e-mail). W takim przypadku przetwarzanie danych odbywa się na podstawie prawnie uzasadnionego interesu administratora, o którym mowa w art. 6 ust. 1 lit. f RODO.

2) **Czy z wydarzeń publicznych, np. konferencji, szkoleń, sympozjów, w czasie których jest nagrywany dźwięk i obraz wydarzenia, organizacja może opublikować w Internecie film, na którym znajdują się wizerunki uczestników lub ich imiona i nazwiska, jeśli przedstawią się podczas zadawania pytania? Czy należy posiadać zgodę takich osób lub z góry określić w regulaminie wydarzenia informacje o możliwości opublikowania filmu w Internecie?**

   Podczas organizacji wydarzeń publicznych, organizacja ma do czynienia z dwoma kategoriami podmiotów w nim uczestniczących. Z jednej strony są to osoby, które działając na podstawie zawartej umowy z organizację biorą udział w wydarzeniu, pełniąc role prelegenta/wykładowcy. Z drugiej strony mamy osoby, które zapisując się na organizowane wydarzenie, deklarując swój udział bądź uczestnicząc w wydarzeniu (, np. w sympozjum, konferencji, wykładzie), bez wymaganego przez organizację uprzedniego zapisu, stają się jego uczestnikami (2).

   (1) Odnosząc się do pierwszego typu uczestnika wydarzeń, a mianowicie prelegenta, preferowane będzie pozyskanie przez organizację uprzedniej zgody (przed zorganizowaniem wydarzenia) na nieograniczone czasowo i terytorialnie używanie i rozpowszechnianie w ramach działalności organizacji, wizerunku, głosu, wypowiedzi prelegenta zarejestrowanej w trakcie danego wydarzenia. Wyrażenie zgody, o czym organizacja powinna pisemnie uprzedzić prelegenta, oznaczać może dodatkowo, jeśli ma to zastosowanie w danym przypadku, że fotografie, filmy lub nagrania wykonane podczas tego wydarzenia mogą zostać wykorzystane , np. w publikacjach wydawanych przez organizację, umieszczonych na stronach internetowych organizacji jako organizatora wydarzenia lub w innych materiałach rozpowszechnianych za pomocą wizji bądź fonii. Należy mieć dodatkowo na uwadze art. 81 Prawa autorskiego, z którego wynika wymóg pozyskania zgody na rozpowszechnianie wizerunku. Choć przepisy prawa nie przewidują żadnych wymogów co do szczególnej formy takiej zgody, preferowana jest forma oświadczenia zawierająca zgodę

prelegenta i jego podpis. Wówczas nie ma wątpliwości, że zgoda została wyrażona przez prelegenta. Nie ma również prawnych przeszkód, aby uznać za dopuszczalną, odpowiedź prelegenta w formie elektronicznej, że wyraża on zgodę na przesłane mu e-mailem oświadczenie o wyrażeniu zgody na rozpowszechnianie wizerunku z jednoczesnym przekazaniem mu klauzuli informacyjnej dotyczącej przetwarzania danych.

(2) Biorąc pod uwagę drugą kategorię uczestników wydarzeń, a mianowicie osoby będące słuchaczami, publicznością, np. konferencji, wykładu, organizacja, podobnie jak o tym była mowa w pkt (1) wyżej, powinna mieć na względzie uzyskanie zgody od osoby na opublikowanie jej wizerunku. Jak przyjmuje się w orzecznictwie *zgoda osoby na publikowanie jej wizerunku winna być wyrażona wprost, aczkolwiek w dowolnej formie, jednak zgody tej nie można domniemywać* (wyrok Sądu Apelacyjnego z dnia 10.02.2005r., I ACa 509/04), jak również *zezwolenie na rozpowszechnianie wizerunku może być udzielone w dowolnej formie, ale zgoda musi być zawsze niewątpliwa* (wyrok Sądu Apelacyjnego z dnia 18.06.2009r., I ACa 459/09). Organizacja mogłaby uzyskiwać zatem pisemne oświadczenia zawierające zgodę na używanie i rozpowszechnianie wizerunku, głosu lub wypowiedzi uczestników, zarejestrowanych w trakcie konkretnego wydarzenia publicznego według określonej daty. Wyrażenie przez uczestnika zgody oznacza w szczególności, że fotografie, filmy lub nagrania wykonane podczas wydarzenia mogą zostać wykorzystane w publikacjach wydawanych przez organizację jako organizatora, umieszczone na stronach internetowych organizacji lub innych przez nich zarządzanych, a także w innych materiałach rozpowszechnianych za pomocą wizji bądź fonii. Zgoda na rozpowszechnianie wizerunku powinna być uzupełniona o klauzulę informacyjną dotyczącą przetwarzania danych osobowych.

Przykładowa zgoda na rozpowszechnianie wizerunku

Zgadzam się na bezpłatne oraz nieograniczone czasowo i terytorialnie utrwalanie, zwielokrotnianie i rozpowszechnianie w ramach działalności statutowej Organizacji z siedzibą w Warszawie przy ul. ……. (administrator danych) mojego wizerunku, głosu, wypowiedzi zarejestrowanych w trakcie wydarzenia …….. organizowanego w dniu …….. w ……. przy ul. …… przez …….. (zwanego dalej łącznie: Organizatorem). Wyrażenie zgody oznacza w szczególności, że fotografie, filmy lub nagrania wykonane podczas powyższego wydarzenia mogą zostać wykorzystane w publikacjach wydawanych przez Organizatora, umieszczone na stronach internetowych Organizatora lub innych przez nich zarządzanych a także w innych materiałach rozpowszechnianych za pomocą wizji bądź fonii.
W związku z powyższym, zrzekam się wszelkich roszczeń majątkowych z tytułu utrwalenia, zwielokrotnienia i rozpowszechniania mojego wizerunku, głosu, wypowiedzi na potrzeby określone w niniejszym oświadczeniu.

_____
imię i nazwisko, data, podpis

3) Na jakich zasadach organizacje społeczne, które zobowiązane są do stosowania zarówno RODO, jak i Dekretu ogólnego w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych

osobowych w Kościele katolickim, wydanego 13 marca 2018 r. przez Konferencję Episkopatu Polski, (w skrócie Dekret) mogą wykorzystywać fotografie w swojej działalności wewnętrznej?

W przypadku wykorzystania fotografii w działalności wewnętrznej Kościoła i kościelnych publicznych osób prawnych ma zastosowanie art. 10 ust. 2 Dekretu, który stanowi, że periodyki informacyjne przeznaczone do użytku wewnętrznego (np. gazetki organizacji społecznej, gablotka z ogłoszeniami) opisujące najważniejsze wydarzenia z życia i działalności redagujących je podmiotów kościelnych mogą zawierać dane dotyczące osób uczestniczących w uroczystościach i wydarzeniach, w tym również ich wizerunki utrwalone na fotografiach, o ile w poszczególnych przypadkach zainteresowani nie wnosili o ich nieujawnianie. Oznacza to, że publikacja zdjęcia osoby w czasopiśmie organizacji dystrybuowanym wyłącznie w ramach tej organizacji i dla jej członków bez wcześniejszego uzyskania zgody osoby widocznej na zdjęciu jest dopuszczalna na mocy prawa. Wyjątkiem od powyższej zasady będą następujące sytuacje:
a) upublicznienia wizerunku utrwalonego na fotografii poza organizację, np. poprzez umieszczenie w Internecie lub wydanie publikacji (np. książki) przeznaczonej do szerszego grona odbiorców niż członkowie organizacji - wówczas znajdą zastosowanie, poza Dekretem, także przepisy RODO i innych ustaw obowiązujących w polskim porządku prawnym, w szczególności Prawa autorskiego, które wymagają zgody osoby na rozpowszechnianie jej wizerunku,
b) wyraźnie zastrzeżenie osoby zamieszczonej na zdjęciu lub - w przypadku osoby małoletniej - jej rodzica lub opiekuna prawnego, aby nie ujawniać jej wizerunku (lub wizerunku małoletniego) w periodyku informacyjnym przeznaczonym do użytku wewnętrznego organizacji.
Dobrą praktyką jest, aby periodyk przeznaczony do użytku wewnętrznego organizacji został opatrzony na pierwszej stronie odpowiednią klauzulą np. “Do użytku wewnętrznego”.

4) **Czy organizacja ma obowiązek uzyskania zgody od uczestnika wydarzenia publicznego na rozpowszechnianie jego wizerunku w sytuacji, gdy wizerunek osoby utrwalony jest w dużej grupie lub w tłumie innych osób stanowiąc wyłącznie szczegół całości?**

Jeśli organizacja utrwala wizerunek osób podczas wydarzenia publicznego i ze względu na ilość uczestniczących w nim osób, jako organizator, nie może nawiązać bezpośredniego kontaktu z uczestnikami tego wydarzenia, przyjmuje się, że, z uwagi na powszechność utrwalania wydarzeń publicznych na zdjęciach i innych nośnikach, uczestnicy tego wydarzenia przez swoje wyraźnie działanie potwierdzające przyzwolili w sposób dorozumiany na przetwarzanie i upublicznianie, rozpowszechnianie swego wizerunku. Jeżeli jednak jakakolwiek osoba wniesie sprzeciw wobec jej fotografowania lub w inny sposób utrwalania jej wizerunku, należy zaniechać czynności i usunąć wizerunek tej osoby. Ze względu na dużą liczbę fotografowanych osób spełnienie obowiązku informacyjnego z powodów organizacyjnych i finansowych wymagałoby od organizatora zbyt dużego wysiłku, dlatego należy przyjąć, że organizacja nie musi spełnić tego obowiązku.
Może zdarzyć się również tak, że organizacja będzie wykonywała zdjęcia osób uczestniczących w wydarzeniu publicznym, konferencji, prelekcji, wykładzie a liczba osób będzie niewielka i organizacja będzie mogła nawiązać ze wszystkimi uczestnikami kontakt. Wówczas również można uznać, że uczestnicy takiego wydarzenia wyrażają na przetwarzanie swojego wizerunku zgodę dorozumianą i przyjąć, że osoba zgodziła się z tym, że będą wykonywane jej zdjęcia. Jednakże dla odmiotów, które przystąpiły do Kodeksu zaleca się uzyskanie od tych osób zgody na rozpowszechnianie wizerunku na podstawie przepisów prawa autorskiego. Zasady uzyskania zgody

zostały opisane w pkt. 2) powyżej, dotyczącym upubliczniania wizerunków osób uczestniczących w wydarzeniach publicznych w Internecie. Organizacja powinna również spełnić w takim przypadku obowiązek informacyjny w stosunku do osób fotografowanych.

5) Czy od osoby publicznej należy uzyskać zgodę na rozpowszechnianie jej wizerunku?

Wizerunek osoby utrwalony poprzez fotografię, rysunek czy obraz stanowi jej dane osobowe. Zgodnie bowiem z art. 4 pkt 1 RODO dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Ochronę wizerunku przewiduje również art. 81 prawa autorskiego. Stanowi on, że rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej, chyba, że otrzymała ona zapłatę za pozowanie. Natomiast takiego zezwolenia nie wymaga rozpowszechnianie wizerunku:
1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych,
2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.
Organizacja może rozpowszechniać wizerunek osoby powszechnie znanej pod warunkiem, że wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności zawodowych, społecznych czy też politycznych. Nie ma definicji osoby powszechnie znanej. Podmiot, który przy okazji organizowania wydarzeń publicznych zamierza utrwalić i rozpowszechnić wizerunek osoby publicznej, powinien więc wziąć pod uwagę, czy dana osoba z racji pełnionych funkcji jest znana osobom z konkretnego środowiska, np. prelegent jest wykładowcą uczelni wyższej, znanym pisarzem albo dyrektorem instytucji znanej na lokalnym rynku, np. Domu Kultury w danej miejscowości, starostą, burmistrzem. Jeśli prelegent w wyniku takiej oceny będzie osobą publicznie znaną i jego wystąpienie będzie związane z pełnioną przez niego funkcją, nie jest wymagana zgoda na publikację i rozpowszechnianie jego wizerunku.

6) Czy wizerunek danej osoby można uznać za dane biometryczne?

W niektórych przypadkach wizerunek danej osoby w postaci fotografii jej twarzy może być uznany za dane biometryczne (zgodnie z art. 4 pkt 14 RODO, jeśli fotografia będzie odzwierciedlała cechy fizyczne, fizjologiczne lub behawioralne osoby fizycznej oraz będzie umożliwiała lub potwierdzała jednoznaczną identyfikację danej osoby i jeśli przetwarzanie tego wizerunku będzie odbywało się przy użyciu technik biometrycznych). W przypadku uznania wizerunku twarzy danej osoby za dane biometryczne, przetwarzanie tego wizerunku możliwe jest w przypadku spełnienia jednej z przesłanek określonych w art. 9 ust. 2 RODO, stanowiących podstawę prawną przetwarzania szczególnych kategorii danych osobowych (danych wrażliwych).
W związku z powyższym, mając na uwadze przepisy prawa obowiązującego w Polsce, w szczególności przepis art. 81 prawa autorskiego, który zawiera nakaz ochrony wizerunku idący dalej niżby to wynikało z uznania go za daną osobową zwykłą, zaleca się, aby organizacje społeczne przystępujące do niniejszego Kodeksu pozyskiwały zgody od osób, których wizerunek zamierzają rozpowszechniać czy też przetwarzać dane osobowe, mając na uwadze wyjątki od zasady uzyskania zgody, tj. jeśli chodzi o rozpowszechnianie (przetwarzanie) wizerunku:
1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;

2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza
3) osoby, która uzyskała wynagrodzenie za pozowanie.

7) Czy organizacja musi uzyskiwać zgodę osoby w przypadku, gdy na zdjęciu stanowi ona jedynie część, szczegół wydarzenia?

Organizacja nie musi uzyskiwać zgody w przypadku wykorzystywania wizerunku osób, które są uczestnikami wydarzeń publicznych (imprez publicznych, zgromadzeń) organizowanych przez siebie, gdy stanowi on jedynie szczegół całości, tzn. służy zaprezentowaniu wydarzenia i uczestników tego wydarzenia. Przesłanka krajobrazu oznacza, że rozpowszechnianie (wykorzystywanie) wizerunku nie wymaga zezwolenia, jeśli wizerunek osoby stanowi jedynie pewien element przedstawionej całości, tzn. w razie usunięcia wizerunku nie zmieniłby się przedmiot i charakter przedstawienia (wyrok Sądu Apelacyjnego w Krakowie z dnia 19 grudnia 2001 r., I ACa 957/01). Należy jednak pamiętać o tym, że jeżeli dana osoba jest dominującym elementem kadru rozpowszechnianie wizerunku wymaga zgody osoby przedstawionej w kadrze. W przypadku fotografii przedstawiających jedną osobę, nawet jeśli jest to fotografia wykonana w trakcie wydarzenia publicznego, w celu wykorzystania tej fotografii (wykorzystania wizerunku osoby) administrator powinien uzyskać zgodę tej osoby.

8) Czy organizacje mogą rozpowszechniać wizerunki dzieci?

Organizacje społeczne w związku z wykonywaniem swoich celów statutowych mogą również rozpowszechniać wizerunki dzieci. W takiej sytuacji dany podmiot, jako organizator jakiegokolwiek przedsięwzięcia związanego z uczestnictwem małoletnich, podczas którego będzie utrwalany i rozpowszechniany wizerunek dzieci (organizowanie warsztatów, kolonii, półkolonii i in. dla dzieci) będzie miała obowiązek uzyskania zgody na jego rozpowszechnianie i przetwarzanie.
Małoletni, który nie ukończył lat 13, nie ma możliwości samodzielnego wyrażenia zgody na rozpowszechnianie swojego wizerunku. Zgoda może zostać udzielona w imieniu dziecka, które nie ukończyło 13 lat, przez jego rodziców, o ile pozostaje ono pod ich władzą rodzicielską lub opiekunów prawnych. Jeśli dziecko pozostaje pod władzą rodzicielską obojga rodziców, każdy z nich może działać w tym zakresie samodzielnie. Podejmując taką decyzję, rodzice dysponują cudzym dobrem osobistym, co nakłada na nich szczególny obowiązek dbałości o ochronę praw małoletniego, w tym zwłaszcza jego godności. Zgoda rodziców lub opiekunów prawnych na rozpowszechnienie wizerunku dziecka sprzeczna z zasadami współżycia społecznego będzie nieważna, ponieważ rodzicie/opiekunowie są zobowiązani do dbania o ochronę praw małoletniego, w tym jego godności osobistej.
Po ukończeniu 13 roku życia małoletni może samodzielnie decydować o rozpowszechnianiu swojego wizerunku.
Natomiast towarzyszenie przez dziecko osobie powszechnie znanej w trakcie pełnienia przez nią funkcji publicznych nie stanowi, w świetle art. 81 ust. 2 pkt 1 prawa autorskiego okoliczności dające podstawę do publikacji wizerunku małoletniego.

9) Jakie obowiązki ciążą na organizacji w związku ze zbieraniem danych osobowych w wersji papierowej w ramach organizowanych wydarzeń publicznych?

Podczas organizowania akcji społecznych i wydarzeń publicznych, ale również podczas organizowania konferencji, spotkań, również w przypadku uczestnictwa w klubach dyskusyjnych i wszelkich innych formach działalności organizacji społecznej może zaistnieć konieczność zbierania i przetwarzania danych osobowych w formie papierowej, np. wówczas, gdy dana osoba nie wypełniła formularza uczestnictwa na stronie internetowej organizacji, a chce uczestniczyć w wydarzeniu publicznym, akcji społecznej, konferencji i innego rodzaju spotkaniu albo organizacja nie wprowadza zapisów na tego typu wydarzenia poprzez rejestrację w Internecie lub osoba fizyczna chce skorzystać z papierowej formy zapisu. W takiej sytuacji, gdy dane osobowe zbierane są w kontakcie bezpośrednim, organizacja powinna zadbać o udostępnienie i wypełnianie przez daną osobę fizyczną formularza rejestracji w formie papierowej.

Aby zapewnić zgodność przetwarzania z prawem, formularze w wersji papierowej muszą być wypełnione własnoręcznie przez osobę uczestniczącą w wydarzeniu. Jeśli organizacja zbiera dane osobowe na podstawie zgody, wówczas dla każdej ze zgód wyrażanych w formularzu powinien być przewidziany odrębny checkbox. Jeśli dane osobowe będą przetwarzane na podstawie innych przesłanek, np. prawnie usprawiedliwionego celu, wówczas na formularzu zapisu powinna znaleźć się odpowiednia klauzula informacyjna z podaniem podstawy prawnej przetwarzania danych osobowych. Formularz zapisu na wydarzenie powinien zawierać również miejsce na własnoręczny podpis osoby w nim uczestniczącej. Wszystkie formularze w formie powinny być zabezpieczone przed dostępem osób niepowołanych lub nieupoważnionych. Niedopuszczalne jest pozostawienie formularzy bez opieki upoważnionej osoby (pracownika organizacji, osoby odpowiedzialnej za organizację danego wydarzenia). Organizacja może spełnić obowiązek informacyjny wynikający z RODO w ten sposób, że w formularzu zapisu na wydarzenie umieści klauzulę informacyjną, zgodną z art. 13 RODO.

Przykładowa lista uczestników wydarzenia i klauzula informacyjna może mieć następujące brzmienie:

Lista uczestników spotkania …….. w dniu …….. wraz zapisami do dalszego kontaktu z Organizacją.

l.p.	*Wydarzenie*	*Imię i nazwisko*	*Adres korespondencyjny, adres e-mail, numer telefonu*	*Podpis*

Informujemy, że Państwa dane są przetwarzane przez Organizację z siedzibą w …… przy ul……. (Administrator danych osobowych lub Organizacja), w następujących celach:

a) w ramach utrzymywania stałego kontaktu z Organizacją w związku z jego celami statutowymi, w szczególności poprzez informowanie o organizowanych spotkaniach, kampaniach i akcjach społecznych oraz możliwościach wspierania działalności Organizacji. Przetwarzanie Państwa danych w wyżej wskazanym celu uzasadnione jest prawnie usprawiedliwionymi interesami realizowanymi przez Organizację, zgodnie z art. 6 ust. 1. lit. f RODO.

Podanie przez Państwa danych jest dobrowolne, niemniej bez ich wskazania nie będzie możliwe wykonanie przez Organizację powyżej wskazanych celów statutowych.

Mają Państwo prawo dostępu do swoich danych, ich sprostowania, usunięcia lub ograniczenia ich przetwarzania, jak również prawo wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych. Wszystkie te żądania będziecie mogli Państwo zgłaszać na adres siedziby Organizacji przy ul. …… lub na adres e-mail: <iod@nazwaorganizacji.pl>.
Mają również Państwo prawo do wniesienia skargi do organu nadzorczego. Do Państwa danych osobowych mogą mieć również dostęp podmioty świadczące na rzecz Organizacji usługi, w szczególności hostingowe, informatyczne, wysyłkowe.
Podane dane osobowe mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane.
Państwa dane osobowe będą przechowywane przez nas bezterminowo, jednak nie dłużej niż przez okres przedawnienia roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych w razie otrzymania od Państwa sprzeciwu wobec przetwarzania danych.

9. Akcje społeczne

1. Opis procesu przetwarzania danych osobowych

Działalność organizacji w tym procesie polega na podejmowaniu i prowadzeniu akcji społecznych (kampanii, akcji, protestów, petycji) i informowaniu o ich dalszym przebiegu. Wszystkie podmioty organizując akcje i kampanie, osobno, czy to wspólnie, czynią to w oparciu o swoje statuty, przyjęte założenia i obowiązujące prawo.

2. Opis kategorii osób

Osoby, które udzieliły wsparcia dla danej akcji społecznej (proteście, petycji). W tym zakresie osoby wypełniły formularze papierowe i nadesłały je na adres organizacji bądź wypełniły formularze na stronach internetowych prowadzonych przez organizacje w celu poparcia prowadzonych akcji społecznych, protestów.

3. Typowe kategorie danych osobowych

Typowymi kategoriami danych dla tego procesu będą w zakresie danych zwykłych:

- imię, nazwisko,
- adres e-mail,
- numer telefonu,
- adres zamieszkania lub adres do korespondencji,
- obywatelstwo,
- PESEL.

4. Cel przetwarzania danych osobowych	5. Podstawa prawna przetwarzania danych osobowych	6. Okres przetwarzana danych osobowych

informowanie osób, które udzieliły wsparcia dla danej akcji społecznej, o jej dalszym przebiegu	art. 6 ust. 1 lit. f RODO realizacja prawnie uzasadnionych interesów administratora w postaci komunikacji z osobami udzielającymi wsparcia dla danej akcji społecznej	okres niezbędny do informowania o organizowanym wydarzeniu, jednak nie dłużej niż do złożenia przez osobę, której dane dotyczą sprzeciwu wobec przetwarzania danych osobowych
informowanie o realizacji celów statutowych organizacji, w tym informowanie o organizowanych akcjach społecznych (kampaniach, akcjach, protestach, wydarzeniach, spotkaniach, konkursach, debatach, seminariach, konferencjach naukowych i prasowych), a także możliwościach wspierania działalności ADO	art. 6 ust. 1 lit. f RODO realizacja prawnie uzasadnionego interesu administratora, którym jest utrzymywanie stałego kontaktu z naszym organizacją w związku z jego celami statutowymi	okres niezbędny do osiągnięcia celu, jednak nie dłużej niż do złożenia sprzeciwu wobec przetwarzania danych osobowych
ustalenie, dochodzenie roszczeń i obrona przed roszczeniami, w tym udokumentowanie zgłoszonych sprzeciwów wobec przetwarzania danych osobowych	art. 6 ust. 1 lit. f RODO art. 17 ust. 3 lit. e RODO prawnie uzasadniony interes przetwarzania danych przez Administratora	okres przedawnienia ewentualnych roszczeń wynikający z przepisów prawa

4. Kategorie odbiorców danych

Przykładowo: firma hostingowa jako podmiot przetwarzający, która na zlecenie organizacji zajmuje się hostingiem strony internetowej, na której rejestrują się uczestnicy zamierzający wziąć udział w konferencji naukowej organizowanej przez organizację.

Z powyższym podmiotem należy zawrzeć umowę powierzenia przetwarzania danych. Wzór takiej umowy stanowi załącznik nr 1 do niniejszego kodeksu.

5. Współadministratorzy

Przykładowo: w przypadku gdy dwie organizacje wspólnie organizują protest mieszczący się w ramach celów statutowych każdej organizacji.

Współadministratorzy powinni zawrzeć umowę o współadministrowaniu danymi. Przykładowy wzór ramowej umowy współadministrowania danymi osobowymi został zamieszczony w załączniku nr 2 do niniejszego kodeksu.

6. **Informacje o przekazaniu do państwa trzeciego**

Przykładowo: gdy dane osobowe uczestników wydarzeń publicznych są przechowywane na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

7. **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa**

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

Należy zwrócić uwagę, że formularze poparcia określonych akcji społecznych, protestów umieszczane na stronach internetowych powinny wykorzystywać szyfrowanie SSL zapewniające ochronę danych w prowadzonych przez uczestników wydarzeń publicznych do formularza w swojej przeglądarce internetowej.

11. **Obowiązek informacyjny wobec osób, które udzieliły wsparcia dla danej akcji społecznej**

Osoby popierające akcję społeczną, powinny mieć możliwość zapoznania się z klauzulą informacyjną dotyczącą przetwarzania danych osobowych, np. poprzez umieszczenie jej pod formularzem na stronie internetowej organizacji.

Przykładowa klauzula informacyjna przy zbieraniu danych osobowych w przypadku wspólnego apelu:

Informujemy, że Państwa dane są przetwarzane przez Fundację z siedzibą w _____, dalej jako Fundacja, oraz Stowarzyszenie z siedzibą we _____, dalej jako Stowarzyszenie (łącznie: współadministratorzy danych osobowych), w następujących celach:
(1) w celu złożenia wspólnego apelu do Rzecznika Praw Dziecka, a także informowania o przebiegu kampanii – na podstawie prawnie usprawiedliwionego interesu realizowanego przez Fundację i Stowarzyszenie zgodnie z art. 6 ust.1. lit. f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).
(2) w celu utrzymywania stałego kontaktu z Fundacją lub Stowarzyszeniem w związku z ich celami statutowymi, w szczególności poprzez informowanie o organizowanych akcjach społecznych i możliwościach wspierania działalności Fundacji i Stowarzyszenia – przetwarzanie Państwa danych w wyżej wskazanym celu uzasadnione jest prawnie usprawiedliwionymi interesami realizowanymi przez Fundację i Stowarzyszenie, zgodnie z art. 6 ust. 1. lit. f RODO.
Podanie przez Państwa danych jest dobrowolne, niemniej bez ich wskazania nie będzie możliwe złożenie petycji do Rzecznika Praw Dziecka, informowanie o przebiegu kampanii, ani informowanie o realizacji celów statutowych Fundacji lub Stowarzyszenia.

Mają Państwo prawo dostępu do swoich danych, ich sprostowania, usunięcia lub ograniczenia ich przetwarzania, jak również prawo wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych.
Każdy ze Współadministratorów będzie realizował obowiązki informacyjne wobec Państwa oraz wobec organu nadzoru wynikające z przepisów o ochronie danych osobowych. Fundacja zapewnia odpowiednie udokumentowanie dla potrzeb wykazania zgodności przetwarzania danych osobowych z przepisami prawa. Każdy ze Współadministratorów we własnym zakresie wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z przepisami prawa, a w razie konieczności dokonuje oceny skutków dla ochrony danych. Fundacja będzie odpowiedzialna wobec Państwa za umożliwienie wykonywania Państwa praw. Niezależnie od tego ustalenia, mogą Państwo wykonywać swoje prawa również wobec Stowarzyszenia. W takim przypadku Fundacja przekaże Państwa żądanie Stowarzyszeniu, które zrealizuje Państwa żądanie. Wszystkie te żądania będą mogli Państwo zgłaszać na adres siedziby Fundacji, przy ul. _____, z dopiskiem „Inspektor Ochrony Danych" bądź na adres poczty elektronicznej <l>.
Mają również Państwo prawo do wniesienia skargi do organu nadzorczego.
Do Państwa danych osobowych mogą mieć również dostęp podmioty świadczące na rzecz Fundacji i Stowarzyszenia usługi, w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze, prawnicze, księgowe, kadrowe.
Każdy ze Współadministratorów we własnym zakresie odpowiada za zastosowanie odpowiednich mechanizmów ochrony w przypadku ewentualnych transferów danych poza Europejski Obszar Gospodarczy (EOG). W takim wypadku każdy ze współadministratorów zapewni możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń.
Podane dane osobowe mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane.
Państwa dane osobowe będą przechowywane przez każdego współadministratorów nie dłużej niż przez okres przedawnienia roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych w razie otrzymania od Państwa żądania usunięcia danych osobowych.
*Ze szczegółowymi informacjami dotyczącymi zasad przetwarzania danych osobowych u Współadministratorów mogą Państwo zapoznać się w Polityce prywatności Fundacji dostępnej na stronie https://www.*nazwafundacji.pl*/polityka-prywatnosci/ oraz w Polityce prywatności Stowarzyszenia dostępnej na stronie https://*nazwastowarzyszenia.pl */polityka-prywatnosci/.*

Zagadnienia szczegółowe

1) Czy organizacja ma obowiązki informacyjne wobec osób, których dane wykorzystała w materiałach o charakterze informacyjnym na konferencji prasowej?

Nie, zgodnie z art. 2 ustawy o ochronie danych osobowych w związku z art. 85 RODO, nie jest konieczne informowanie o przetwarzaniu danych osoby, której dane zostały wykorzystane w materiale informacyjnym na potrzeby zorganizowanej konferencji prasowej.
Zgodnie z motywem 153 RODO mając na względzie wolność wypowiedzi dla społeczeństwa, pojęcia dotyczące tej wolności, takie jak dziennikarstwo, należy interpretować szeroko.

2) **Czy komitet inicjatywy uchwałodawczej zbierający podpisy poparcia dla projektu uchwały w ramach obywatelskiej inicjatywy uchwałodawczej może informować o przebiegu i dalszych losach inicjatywy?**

Tak, komitet inicjatywy uchwałodawczej posiada prawnie uzasadniony interes, aby informować osoby, które poparły projekt uchwały, o przebiegu zbierania podpisów, o dalszych losach inicjatywy uchwałodawczej, w szczególności o zakończeniu postępowania uchwałodawczego, tj. o podjęciu bądź niepodjęciu uchwały przez odpowiedni organ uchwałodawczy jednostki samorządu terytorialnego. Podstawą prawną przetwarzania danych osobowych w powyższym celu jest prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO).
Komitet inicjatywy uchwałodawczej może zbierać dane kontaktowe osób popierających projekt uchwały np. adres e-mail, adres do korespondencji, numer telefonu, w celu późniejszego informowania o przebiegu obywatelskiej inicjatywy uchwałodawczej. Powinien jednak spełnić obowiązek informacyjny wobec osób, od których zbiera dane kontaktowe w powyższym celu (art. 13 RODO).
Analogiczne zasady obowiązują wobec przetwarzania danych przez komitety inicjatywy ustawodawczej a także w przypadku innych inicjatyw, apeli, petycji, kampanii, w ramach których organizacja zbiera podpisy poparcia.

9. Wolontariusze

1. Opis procesu przetwarzania danych osobowych

Proces ten polega na świadczeniu nieodpłatnej pomocy wolontariuszy w realizacji celów statutowych organizacji.

2. Opis kategorii osób

Osoby, które, stosownie do definicji zawartej w art. 2 pkt 3) ustawy o działalności pożytku publicznego i o wolontariacie, ochotniczo i bez wynagrodzenia wykonują świadczenia na zasadach określonych w przedmiotowej ustawie (wolontariusze). Są to również osoby, z którymi organizacja zawarła umowy w charakterze wolontariatu (umowa o wolontariacie).

3. Typowe kategorie danych osobowych

Typowymi kategoriami danych dla tego procesu będą w zakresie danych zwykłych:

- imię,
- nazwisko,
- PESEL,
- adres zamieszkania lub zameldowania
- numer dowodu osobistego,
- adres e-mail,
- numer telefonu.

4. Cel przetwarzania danych osobowych	5. Podstawa prawna przetwarzania danych osobowych	6. Okres przetwarzana danych osobowych
realizacja praw i obowiązków w związku z nieodpłatną pomocą wolontariuszy w realizacji celów statutowych organizacji	art. 6 ust. 1 lit. b RODO niezbędność do wykonania umowy o wolontariat	okres obowiązywania umowy o wolontariacie
ubezpieczenia wolontariusza w przypadkach przewidzianych przepisami, w szczególności art. 46 ustawy o działalności pożytku publicznego i o wolontariacie	art. 6 ust. 1 lit c. RODO przepisy prawa art. 46 ustawy o działalności pożytku publicznego i o wolontariacie	okres obowiązywania umowy o wolontariacie, a po jego rozwiązaniu lub wygaśnięciu okres przedawnienia ewentualnych roszczeń związanych z umową o wolontariacie, tj. nie dłużej niż 6 lat
dochodzenie roszczeń i obrona przed roszczeniami z tytułu zawartej umowy o wolontariacie	art. 6 ust. 1 lit. f RODO prawnie uzasadniony interes administratora	okres przedawnienia ewentualnych roszczeń związanych z umową o wolontariacie

7. Kategorie odbiorców danych

Przykładowo: towarzystwa ubezpieczeniowe, brokerzy ubezpieczeniowi w przypadku ubezpieczania wolontariusza za pośrednictwem organizacji w zakresie ubezpieczenia NNW (następstw nieszczęśliwych wypadków) lub objęcia ubezpieczeniem zdrowotnym.

8. Współadministratorzy

Nie dotyczy.

9. Informacje o przekazaniu do państwa trzeciego

Przykładowo: gdy dane osobowe wolontariuszy są przechowywane przez organizację na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG)

10. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

11. Obowiązek informacyjny wobec wolontariusza

Przed rozpoczęciem wolontariatu na rzecz organizacji, wolontariusz powinien być upoważniony przez organizację do przetwarzania administrowanych przez nią danych osobowych. Organizacja powinna spełnić obowiązek informacyjny wobec wolontariusza.

Przykładowe upoważnienie i klauzula informacyjna:

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH
NR ../../2020

Działając w imieniu Organizacji z siedzibą w Warszawie (zwanej dalej Administratorem) na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej RODO – nadaję Pani/Panu:

<imię i nazwisko wolontariusza>

upoważnienie do przetwarzania danych osobowych w ramach wykonywania powierzonych zadań, zleceń lub obowiązków na podstawie umowy o wolontariat zawartej z Administratorem.

Upoważnienie obowiązuje do dnia zakończenia realizacji wolontariatu u Administratora bądź do dnia odwołania niniejszego upoważnienia.

Upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych na nośnikach papierowych oraz systemach informatycznych w ramach następujących procesów przetwarzania:
1) Kampanie społeczne
2) Korespondencja przychodząca i wychodząca
3) Wydarzenia publiczne
4) Media społecznościowe
5) Kontrahenci
bez ograniczeń – obejmujących podgląd danych, wprowadzanie danych, opracowywanie danych, zmienianie danych, usuwanie danych.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem, przepisami RODO, ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, Kodeksem pracy a także z Polityką ochrony danych osobowych oraz Instrukcją zarządzania systemem Informatycznym obowiązującą u Administratora.

_____ _____

podpis wolontariusza *podpisy osób uprawnionych do nadania upoważnienia*

Klauzula informacyjna dot. przetwarzania danych wolontariusza

Zgodnie z art. 13 ust. 1 i 2 Ogólnego Rozporządzenia o Ochronie Danych Osobowych (RODO) informuję, że:

1. *administratorem Pani/Pana danych osobowych jest Organizacja z siedzibą w _____ (zwanej dalej Organizacją),*
2. *Pani/Pana dane osobowe przetwarzane będą w celu związanym z nawiązaniem i przebiegiem współpracy na podstawie umowy o wolontariat, na podstawie art. 6 ust. 1 lit. a i b RODO w związku z art. 46 ustawy o działalności pożytku publicznego i o wolontariacie,*
3. *podanie przez Pana/Panią danych osobowych jest dobrowolne, ale niezbędne do nawiązania współpracy na podstawie umowy o wolontariat,*
4. *do Pani/Pana danych osobowych mogą mieć również dostęp podmioty świadczące na rzecz Organizacji usługi, w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze, prawnicze, księgowe, kadrowe,*
5. *Pani/Pana dane osobowe będą przechowywane przez okres wynikający z przepisów dotyczących przedawnienia roszczeń z tytułu umowy o wolontariat lub okresów przechowywania dokumentacji księgowej wynikających z przepisów o rachunkowości,*
6. *posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu albo cofnięcia zgody na ich przetwarzanie w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody wyrażonej przed jej cofnięciem,*
7. *Pani/Pana dane mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane.*
8. *Pan/Pani dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń.*
9. *ma Pani/Pana prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy o ochronie danych osobowych*
10. *W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pani/Pana danych osobowych prosimy o kontakt z wyznaczonym przez nas Inspektorem Ochrony Danych pisząc na adres siedziby Organizacji przy ul. _____ z dopiskiem „Inspektor Ochrony Danych" lub mailowo na adres <iod@nazwaorganizacji.pl>.*

W przypadku, gdy wolontariusz współpracuje z organizacją nie korzystając z jej zasobów technicznych i organizacyjnych, organizacja powinna podpisać z wolontariuszem umowę powierzenia przetwarzania danych.

Przykładowy przedmiot umowy powierzenia przetwarzania danych osobowych z wolontariuszem zajmującym się na stałe obsługą profilu organizacji w serwisie społecznościowym Facebook:

Zważywszy, że:
(1) Strony zawarły umowę o współpracy w charakterze wolontariatu z dnia _____ roku („Umowa Podstawowa"), której przedmiotem jest obsługa profilu Organizacji w serwisie społecznościowym Facebook, w związku, z wykonywaniem której Administrator powierzy Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym niniejszą Umową;

(2) intencją Stron jest takie uregulowanie zasad przetwarzania danych osobowych określonych w niniejszej Umowie, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej „Rozporządzeniem".
Strony postanowiły zawrzeć Umowę o następującej treści:

§1.
Przedmiot Umowy

1. Administrator powierza Przetwarzającemu przetwarzanie danych osobowych wyłącznie na warunkach i w celu określonym w niniejszej Umowie oraz Umowie Podstawowej.
2. Zakres danych osobowych powierzonych Przetwarzającemu ze wskazaniem opisu kategorii danych osobowych w ramach poszczególnych czynności przetwarzania określa Załącznik nr 1 do niniejszej Umowy.
3. Dane osobowe będą przetwarzane przez Przetwarzającego wyłącznie w celu realizacji Umowy podstawowej, tj. obsługa profilu Organizacji w serwisie społecznościowym Facebook.
4. Poprzez przetwarzanie danych osobowych rozumie się: zbieranie, zapisywanie, modyfikację, utrwalanie, przechowywanie, opracowywanie, udostępnianie oraz usuwanie danych osobowych.

Wzór umowy powierzenia przetwarzania danych stanowi załącznik nr 1 do niniejszego kodeksu.

Zagadnienia szczegółowe:

1) Jaki jest status prawny wolontariusza?

Wolontariuszem w rozumieniu ustawy o działalności pożytku publicznego i o wolontariacie jest osoba fizyczna, która ochotniczo i bez wynagrodzenia wykonuje świadczenia na zasadach określonych w ww. ustawie. Należy mieć na uwadze, że organizacja powinna zadbać o zawarcie z wolontariuszem umowy o wolontariacie, która to, stosownie do ustawy, określa ją jako porozumienie pomiędzy wolontariuszem a korzystającym (na poczet niniejszego kodeksu należy przyjąć, że korzystającym będzie właściwa organizacja społeczna). Zakres świadczeń wolontariusza, jak również sposób i czas ich wykonywania powinno określać porozumienie. Należy w nim również uwzględnić możliwość jego rozwiązania. Stosunek prawny łączący korzystającego z wolontariuszem jest stosunkiem cywilnoprawnym. Zgodnie z poglądami nauki, „wykonywane przez wolontariusza świadczenie na rzecz korzystającego jest świadczeniem odpowiadającym świadczeniu pracy, a nie świadczeniem pracy lub usług."(J. Blicharz, *Komentarz do ustawy o działalności pożytku publicznego i wolontariacie*, w: *Ustawa o działalności pożytku publicznego i wolontariacie. Ustawa o spółdzielniach socjalnych. Komentarz*, Warszawa 2012).

Jeśli wykonywanie świadczeń przez wolontariusza nie ma charakteru incydentalnego, jednorazowego, organizacja powinna rozważyć zawarcie porozumienia, o którym mowa wyżej, w formie pisemnej. Porozumienie powinno być również sporządzone na piśmie, jeżeli świadczenie

wolontariusza wykonywane jest przez okres dłuższy niż 30 dni (art. 44 ust. 4 ustawy o działalności pożytku publicznego i o wolontariacie).

W działalności organizacji, podobnie jak osoby w nich zatrudnione, wolontariusze niejednokrotnie mogą mieć status „osób utrzymujących z nimi stałe kontakty w związku z ich działalnością", o której mowa w art. 9 ust. 2 lit. d RODO. W literaturze zaprezentowany jest pogląd, że takie sformułowanie wskazuje, że osobami takimi mogą być wszelkie osoby utrzymujące stałe kontakty z członkami organizacji.

2) Czy organizacja powinna wręczyć wolontariuszowi upoważnienie do przetwarzania danych osobowych?

Biorąc pod uwagę, że podstawą współpracy między wolontariuszem a organizacją pozarządową jest porozumienie mające charakter cywilnoprawny, organizacja powinna upoważnić wolontariusza z nią współpracującego do określonych czynności na zasadach ogólnych. Wzór upoważnienia wraz z klauzulą informacyjną został zamieszczony w pkt 11 powyżej.

3) Jak długo organizacja przechowuje dane wolontariuszy?

Organizacja powinna przetwarzać dane osobowe wolontariusza przez okres obowiązywania porozumienia (umowy) o wolontariacie, a po jego rozwiązaniu lub wygaśnięciu przez okres przedawnienia ewentualnych roszczeń związanych z porozumieniem o wolontariacie, tj. nie dłużej niż 6 lat.

10. Beneficjenci, potrzebujący i podopieczni

1. Opis procesu przetwarzania danych osobowych

Działalność organizacji w tym procesie polega na udzielaniu pomocy na rzecz osób i organizacji w ramach realizacji celów statutowych organizacji. Pomoc ta najczęściej polega na pomocy finansowej, materialnej czy prawnej osobom, które jej potrzebują.

2. Opis kategorii osób

Osoby, które są beneficjentami rozmaitych programów wsparcia prowadzonych przez organizacje.

3. Typowe kategorie danych osobowych

Typowymi kategoriami danych dla tego procesu będą w zakresie danych zwykłych:

- imiona,
- nazwiska,
- NIP,
- REGON,

- adresy e-mail,
- adres zamieszkania lub prowadzenia działalności gospodarczej
- numer telefonu.

Szczególnymi kategoriami danych mogą być:

- dane o stanie zdrowia,
- dane o światopoglądzie
- dane o przynależności religijnej.

4. Cel przetwarzania danych osobowych	5. Podstawa prawna przetwarzania danych osobowych	6. Okres przetwarzana danych osobowych
realizacja praw i obowiązków w związku z nieodpłatną pomocą beneficjentom, podopiecznym	art. 6 ust. 1 lit. b RODO niezbędność do wykonania umowy, której stroną jest osoba, której dane dotyczą	dane usuwane do końca roku kalendarzowego po upływie 3 lat od dnia rozwiązania lub wygaśnięcia porozumienia o świadczenie nieodpłatnej pomocy prawej zawartej z beneficjentem
informowanie osób, które organizacja wspiera o realizowanej dla nich pomocy	art. 6 ust. 1 lit. f RODO niezbędność do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora	okres przedawnienia roszczeń w konkretnej sprawie beneficjenta, podopiecznego, potrzebującego (np. 10 lat w zakresie roszczeń stwierdzonych prawomocnym wyrokiem sądu)
wypełnienia obowiązku prawnego w związku z wymogami określonymi w przepisach proceduralnych przed sądami i urzędami	art. 6 ust. 1 lit. c RODO wypełnienie obowiązku prawnego ciążącego na administratorze	okres przedawnienia ewentualnych roszczeń wynikający z przepisów prawa (np. okresu przechowywania wynikający z art. 74 ust. 1 i 2 Ustawy o rachunkowości)

7. Kategorie odbiorców danych

Przykładowo: pełnomocnicy reprezentujący beneficjentów w postępowaniu sądowym na podstawie udzielonego pełnomocnictwa

8. Współadministratorzy

Przykładowo: gdy dwie organizacje świadczą pomoc na rzecz beneficjenta.

Współadministratorzy powinni zawrzeć umowę o współadministrowaniu danymi. Przykładowy wzór ramowej umowy współadministrowania danymi osobowymi został zamieszczony w załączniku nr 2 do niniejszego kodeksu.

9. Informacje o przekazaniu do państwa trzeciego

Przykładowo: gdy dane osobowe beneficjentów są przechowywane na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

10. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

11. Obowiązek informacyjny wobec beneficjenta wolontariusza

Przed rozpoczęciem świadczenia pomocy na rzecz beneficjenta, które wiąże się z przetwarzaniem jego danych osobowych, organizacja powinna spełnić obowiązek informacyjny wobec wolontariusza.

Przykładowa klauzula informacyjna wobec studentów, którego dane organizacja pozyskała od szkoły wyższej w ramach programu pomocowego realizowanego na rzecz studentów na podstawie umowy zawartej pomiędzy organizacją a szkołą wyższą:

Działając na podstawie art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO) informujemy, że Państwa dane są przetwarzane przez Organizację z siedzibą przy ____(zwana dalej Organizacją), w następujących celach: (a) w celu wykonania porozumienia dot. przystąpienia do programu „____" zawartej pomiędzy naszą Organizacją a Państwa Szkołą Wyższą, w szczególności świadczenia pomocy na Pana/Pani rzecz w ramach powyższego programu - podstawę prawną przetwarzania danych stanowi realizacja prawnie uzasadnionych interesów Organizacji w postaci komunikacji w ramach sprawnego wykonywania wyżej wymienionego Porozumienia: art. 6 ust. 1 lit. f RODO; (b) w ramach utrzymywania stałego kontaktu z naszą Organizacją w związku z jej celami statutowymi, w szczególności poprzez informowanie o akcjach społecznych organizowanych przez naszą Organizację - podstawa prawna przetwarzania: art. 6 ust. 1 lit. f RODO.
Kategorie przetwarzanych danych osobowych obejmują: imię i nazwisko, numer telefonu oraz adres e-mail i zostały wskazane przez Szkołę w formularzu zgłoszeniowym lub formularzu aktualizacyjnym programu „_____".
Mają Państwo prawo dostępu do swoich danych, ich sprostowania, usunięcia lub ograniczenia ich przetwarzania, jak również prawo wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych. Wszystkie te żądania będziecie mogli Państwo zgłaszać na adres siedziby Organizacji, przy ul. _____, z dopiskiem „Inspektor Ochrony Danych" lub mailowo: <iod@nazwaorganizacji.pl>
Mają również Państwo prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Do Państwa danych osobowych mogą mieć również dostęp podmioty świadczące na naszą rzecz usługi w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze, prawnicze, księgowe, kadrowe.
Podane dane osobowe mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane. Państwa dane osobowe nie będą przekazywane do państwa trzeciego. Jednak w przyszłości może się okazać, że Fundacja zadecyduje o przekazaniu danych do państwa trzeciego lub organizacji międzynarodowej, wyłącznie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Administrator zapewni możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń.
W każdej chwili przysługuje Państwu prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych. W takim przypadku Państwa dane osobowe zostaną usunięte niezwłocznie po upływie okresu przedawnienia ewentualnych roszczeń przewidzianym w Kodeksie cywilnym.

Zagadnienia szczegółowe

1) Czy w ramach prowadzonych przez organizację programów na rzecz beneficjentów, potrzebujących, podopiecznych organizacja może przetwarzać dane osobowe szczególnej kategorii?

W ramach prowadzonych przez organizację programów dotyczących pomocy beneficjentom, podopiecznym, którzy zgłaszają się do danej organizacji w ramach jej celów statutowych z prośbą np. o wsparcie finansowe, organizacja przetwarza dane takich osób (beneficjentów, podopiecznych, potrzebujących) w celu niezbędnym do podjęcia przez organizację działań, na żądanie osoby zgłaszającej się, zmierzającym do zawarcia umowy o udzielenie pomocy społecznej (art. 6 ust. 1 lit. b) RODO). Z kolei w odniesieniu do danych dotyczących, np. zdrowia beneficjenta, jego sytuacji materialnej, życiowej, organizacja może przetwarzać dane osobowe na podstawie wyraźnej zgody (art. 9 ust. 2 lit. a) RODO). Natomiast w odniesieniu do wizerunku beneficjenta na podstawie udzielonej zgody na określone fotografie, na których utrwalono wizerunek potrzebującego (art. 6 ust. 1 lit. a) RODO). W zakresie, w jakim organizacja przetwarza dane w celu ustalenia, dochodzenia lub obrony roszczeń - art. 6 ust. 1 lit. f) RODO (prawnie uzasadniony interes) oraz art. 9 ust. 2 lit. f) RODO (przetwarzanie danych o stanie zdrowia jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń).

11. Organizacja konkursów

1. **Opis procesu przetwarzania danych osobowych**

Proces ten obejmuje przygotowywanie i przeprowadzanie konkursów, gier, warsztatów itp.

2. **Opis kategorii osób**

Osoby fizyczne, które biorą udział w konkursach, grach, warsztatach itp. przeprowadzanych przez organizację.

3. **Kategorie danych osobowych**

Typowymi kategoriami danych osobowych przetwarzanych w ramach organizacji konkursów będą w zakresie danych zwykłych:

- imię i nazwisko, adres poczty elektronicznej, numer telefonu – w stosunku do uczestników konkursu a nadto
- adres do korespondencji, PESEL lub NIP, data urodzenia, nazwa i adres właściwego urzędu skarbowego, numer rachunku bankowego, wizerunek – w stosunku do laureatów konkursu.

4. **Cel przetwarzania danych osobowych**	5. **Podstawa prawna przetwarzania danych osobowych**	6. **Okres przetwarzana danych osobowych**
przygotowanie i realizacja konkursu, identyfikacja jego uczestników, wyłonienie laureatów, przyznanie i wydanie nagród, archiwizacja dokumentów	art. 6 ust. 1 lit. f RODO tj. prawnie uzasadniony interes administratora	okres niezbędny do osiągnięcia celu przetwarzania danych osobowych
publikacja informacji o wynikach konkursu, w tym imienia, nazwiska i wizerunku laureatów konkursu, a przez to promocja laureatów i osiągnięć, a także promocja organizacji i jej działalności	art. 6 ust. 1 lit. a RODO tj. zgoda laureata konkursu na upublicznienie jego danych osobowych, art. 81 Prawa autorskiego – zgoda na rozpowszechnianie wizerunku	okres niezbędny do osiągnięcia celu przetwarzania danych osobowych
rozliczenie nagród, w tym pobranie i wpłacenie zaliczek na podatek dochodowy od osób fizycznych od nagród przyznanych laureatom konkursu	art. 6 ust. 1 lit. c RODO tj. wypełnienia obowiązku prawnego ciążącego na administratorze w związku z art. 30 i art. 41 ust. 7 ustawy o podatku dochodowym od osób fizycznych	okres przechowywania dokumentacji księgowej i podatkowej wynikający z przepisów prawa
informowanie uczestników konkursu o realizacji celów statutowych organizacji oraz o możliwościach wspierania działalności organizacji	art. 6 ust. 1 lit. f RODO prawnie uzasadniony interes administratora, którym jest utrzymywanie stałego kontaktu z organizacją w związku z jej celami statutowymi	okres niezbędny do osiągnięcia celu, jednak nie dłużej niż do złożenia sprzeciwu wobec przetwarzania danych osobowych
dochodzenie roszczeń i obrona przed ewentualnymi roszczeniami, w tym rozpatrywanie reklamacji	art. 6 ust. 1 lit. f RODO art. 17 ust. 3 lit. e RODO tj. prawnie uzasadniony interes administratora danych	okres przedawnienia ewentualnych roszczeń wynikający z przepisów prawa

4. **Kategorie odbiorców danych**

Przykładowo: agencje marketingowe, które na zlecenie organizacji wykonują działania na potrzeby marketingu bezpośredniego.

Z powyższym podmiotem należy zawrzeć umowę powierzenia przetwarzania danych. Wzór takiej umowy stanowi załącznik nr 1 do niniejszego kodeksu.

5. **Współadministratorzy**

Do współadministrowania danymi osobowymi może dojść, gdy dwie organizacje zaangażowane są w prowadzenie wspólnego konkursu.

Współadministratorzy powinni zawrzeć umowę o współadministrowaniu danymi. Przykładowy wzór ramowej umowy współadministrowania danymi osobowymi został zamieszczony w załączniku nr 2 do niniejszego kodeksu.

6. **Informacje o przekazaniu do państwa trzeciego**

Przykładowo: gdy dane osobowe uczestników konkursu są przechowywane na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

7. **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa:**

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego Kodeksu.

Należy zwrócić uwagę, że elektroniczny formularz zapisu uczestników konkursu na stronie internetowej organizacji powinien wykorzystywać szyfrowanie SSL, które zapewnia ochronę danych wprowadzonych przez zamawiającego w przeglądarce internetowej.

8. **Obowiązek informacyjny przy zbieraniu danych osobowych uczestników konkursu**

Osoby rejestrujące się jako uczestnicy konkursu powinny mieć możliwość zapoznania się z klauzulą informacyjną dotyczącą przetwarzania danych osobowych, np. poprzez umieszczenie jej pod formularzem udziału na stronie internetowej organizacji.

Przykładowa klauzula informacyjna:

Informujemy, że Pani/Pana dane osobowe przetwarzane będą przez Organizację z siedzibą w __....._ (zwaną dalej Organizacją lub administratorem danych) w następujących celach:

(a) przeprowadzenia konkursu, w tym identyfikacji jego uczestników, wyłonienia laureatów, przyznania i wydania nagród, archiwizacji dokumentów - podstawą do przetwarzania danych osobowych jest prawnie uzasadniony interes administratora danych (art. 6 ust. 1 lit. f RODO);
(b) w ramach utrzymywania stałego kontaktu z naszą Organizacją w związku z jej celami statutowymi, w szczególności poprzez informowanie o organizowanych akcjach społecznych - podstawę prawną przetwarzania w powyższym celu stanowi realizacja prawnie uzasadnionych interesów administratora danych (art. 6 ust. 1 lit. f RODO).
Podanie danych jest dobrowolne, jednak konieczne do realizacji celów, do jakich zostały zebrane.
Informujemy, że przysługuje Pani prawo dostępu do treści swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu wobec ich przetwarzania, a także prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
Pani dane osobowe będą przechowywane przez naszą Organizację nie dłużej niż przez okres przedawnienia roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych w razie otrzymania od Państwa żądania usunięcia danych osobowych.
Do Pani danych osobowych mogą mieć również dostęp podmioty świadczące na rzecz Organizacji usługi, w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze. prawnicze, księgowe, kadrowe.
Pani dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie, na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń. Podane dane osobowe mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane.
Ze szczegółowymi informacjami dotyczącymi zasad przetwarzania danych osobowych w naszej Organizacji może Pani zapoznać się w Polityce prywatności dostępnej na naszej stronie internetowej pod adresem: ___.
W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pani/Pana danych osobowych prosimy o kontakt z wyznaczonym przez nas Inspektorem Ochrony Danych pisząc na adres siedziby Organizacji: ul.____, z dopiskiem „Inspektor Ochrony Danych" lub na adres poczty elektronicznej <iod@nazwaorganizacji.pl>.

W przypadku gdy organizacja planuje upublicznienie danych osobowych laureatów konkursu powinna uprzednio pozyskać od nich odpowiednie zgody.

Przykładowy wzór klauzuli zgody i klauzuli informacyjnej:

Wyrażam nieodpłatnie zgodę na:

a) na utrwalenie, zwielokrotnianie i rozpowszechnianie dowolną techniką bez ograniczeń terytorialnych i czasowych swojego wizerunku i głosu utrwalonego w związku z moim udziałem w konkursie pt. _____ za pośrednictwem dowolnego medium w celu dokumentacyjnym, reklamowym, promocyjnym, informacyjnym lub informowania o wyłonionych zwycięzcach konkursu. Powyższa zgoda obejmuje wszelkie formy publikacji mojego wizerunku i głosu, w szczególności rozpowszechnianie za pośrednictwem wizji i fonii a także w Internecie między

innymi na takich portalach jak Facebook, Twitter, YouTube oraz zamieszczanie w materiałach drukowanych lub wyświetlanych publicznie;

b) *podawanie do publicznej wiadomości mojego imienia i nazwiska w związku z moim udziałem w konkursie pt. _____ we wszelkich ogłoszeniach, zapowiedziach i informacjach o nim i jego wynikach.*

Jednocześnie oświadczam, że zapoznałem się z klauzulą informacyjną zamieszczoną poniżej.

_____

<miejscowość, data, czytelny podpis uczestnika konkursu>

Klauzula informacyjna:

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej: RODO) (Dz. Urz. UE L119/1) wskazujemy, że:

1. *Administratorem Pani/Pana danych osobowych jest Organizacja z siedzibą w _____, przy ul. _____.*
2. *Pana/Pani dane osobowe podane w powyższym oświadczeniu, w tym imię, nazwisko, wizerunek i głos będą przetwarzane przez Administratora w celach określonych w powyższym oświadczeniu na podstawie zgody w oparciu o art. 6 ust. 1 lit. a) RODO.*
3. *Podanie danych osobowych, o których mowa w pkt 2 powyżej, jest dobrowolne, ale jest niezbędne do zrealizowania celów określonych w powyższym oświadczeniu.*
4. *Przysługuje Panu/Pani prawo żądania dostępu do swoich danych osobowych, ich sprostowania, usunięcia, ograniczenia przetwarzania oraz przenoszenia danych, a także prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.*
5. *W każdym czasie przysługuje Panu/Pani prawo do cofnięcia zgody bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.*
6. *Pana/Pani dane osobowe będą usunięte niezwłocznie po upływie okresu przedawnienia ewentualnych roszczeń i uprawnień przewidzianym w Kodeksie cywilnym.*
7. *Do Pana/Pani danych osobowych mogą mieć również dostęp podmioty świadczące na naszą rzecz usługi, w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze. prawnicze, księgowe, kadrowe, a także związane z organizacją konkursu.*
8. *Pana/Pani dane osobowe nie będą przekazywane do państwa trzeciego. Jednak w przyszłości może się okazać, że Administrator zadecyduje o przekazaniu danych do państwa trzeciego lub organizacji międzynarodowej, wyłącznie w zakresie, na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Administrator zapewni możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń.*
9. *Podane przez Pana/Pani dane osobowe mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane.*
10. *Wszystkie powyższe żądania będzie mógł Pan/Pani zgłaszać na adres: ___, z dopiskiem „Inspektor Ochrony Danych" lub na adres poczty elektronicznej <iod@nazwaorganizacji.pl>.*

Zagadnienia szczegółowe

1) **Czy zamieszczenie w regulaminie konkursu postanowień dotyczących ochrony danych osobowych zwalnia z obowiązku zbierania zgód na przetwarzanie wizerunku od uczestników konkursu?**

Nie, akceptacja regulaminu konkursu nie będzie równoznaczna z wyrażaniem zgody na rozpowszechnianie wizerunku, o której mowa w art. 81 Prawa autorskiego. Organizacja powinna pozyskać od uczestników konkursu odrębne oświadczenia zawierające klauzule zgody na rozpowszechnianie wizerunku oraz klauzule informacyjne dotyczące przetwarzania danych osobowych.
W przypadku zamieszczenia postanowień dotyczących rozpowszechniania wizerunku w regulaminie konkursu, osoba, której dane dotyczą, nie ma rzeczywistego ani wolnego wyboru oraz nie może odmówić wyrażenia zgody, która według intencji organizatorów miałaby wynikać jedynie z treści regulaminu konkursu. W takim wypadku wyrażenia zgody nie należy uznawać za dobrowolne, co stanowi podstawowy warunek legalności przetwarzania danych osobowych. Nadto organizator konkursu nie jest w stanie na tej podstawie wykazać, że uczestnik konkursu wyraził zgodę na rozpowszechnianie wizerunku. Powyższe dotyczy również upublicznienia danych osobowych uczestników konkursu bez ich zgody.
Więcej informacji na temat zgody jako przesłanki przetwarzania danych znajdziesz w rozdziale II pkt 3 powyżej.

12. Kontakty służbowe

1. **Opis procesu przetwarzania danych osobowych**

Proces ten obejmuje wszelkie kontakty służbowe, o ile nie mieszczą się w innych procesach przetwarzania danych w organizacji. Mogą one przybrać następujące formy:

- formularza kontaktowego na stronie internetowej,
- komunikacji tekstowej (np. SMS),
- komunikacji telefonicznej,
- kontaktów bezpośrednich.

2. **Opis kategorii osób**

Osoby fizyczne, z którymi organizacja pozostaje w kontakcie służbowym, w tym mediami, dziennikarzami, politykami, urzędnikami, a także z osobami, które kontaktują się z organizacją za pośrednictwem formularza na stronie internetowej.

3. **Kategorie danych osobowych**

Typowymi kategoriami danych osobowych przetwarzanych w ramach kontaktów służbowych będą w zakresie danych zwykłych:

- imię i nazwisko,
- stanowisko służbowe,
- zawód,

- adres poczty elektronicznej,
- numer telefonu,
- adres do korespondencji.

Odnośnie danych wrażliwych zobacz pkt 1 zagadnień szczegółowych.

3. Cel przetwarzania danych osobowych	7. **Podstawa prawna przetwarzania danych osobowych**	8. **Okres przetwarzana danych osobowych**
kontakt mediami, dziennikarzami, politykami, urzędnikami w związku z prowadzoną działalnością statutową lub gospodarczą kontakt w związku z pytaniem lub zgłoszeniem złożonym za pośrednictwem formularza kontaktowego na stronie internetowej	art. 6 ust. 1 lit. f RODO tj. prawnie uzasadniony interes administratora polegający na zarządzaniu relacjami	okres niezbędny do osiągnięcia celu przetwarzania danych osobowych, najpóźniej do złożenia sprzeciwu wobec przetwarzania danych
informowanie o realizacji celów statutowych organizacji, a także możliwościach wspierania działalności organizacji	art. 6 ust. 1 lit. f RODO prawnie uzasadniony interes administratora, którym jest utrzymywanie stałego kontaktu z organizacją w związku z jej celami statutowymi	okres niezbędny do osiągnięcia celu, jednak nie dłużej niż do złożenia sprzeciwu wobec przetwarzania danych osobowych w tym celu
dochodzenie roszczeń i obrona przed ewentualnymi roszczeniami	art. 6 ust. 1 lit. f RODO art. 17 ust. 3 lit. e RODO tj. prawnie uzasadniony interes administratora danych	okres przedawnienia ewentualnych roszczeń wynikający z przepisów prawa

9. **Kategorie odbiorców danych**

Przykładowo: dostawca usługi poczty elektronicznej, z której korzysta organizacja.

Z powyższym podmiotem należy zawrzeć umowę powierzenia przetwarzania danych. Wzór takiej umowy stanowi załącznik nr 1 do niniejszego kodeksu.

10. **Współadministratorzy**

Do współadministrowania danymi osobowymi może dojść, gdy prowadzi korespondencję z osobą fizyczną, która dotyczy sprawy objętej uzgodnieniami z inną organizacją w ramach prowadzonego wspólnego projektu.

Współadministratorzy powinni zawrzeć umowę o współadministrowaniu danymi. Przykładowy wzór ramowej umowy współadministrowania danymi osobowymi został zamieszczony w załączniku nr 2 do niniejszego kodeksu.

11. **Informacje o przekazaniu do państwa trzeciego**

Przykładowo: gdy korespondencja e-mail zawierająca dane osobowe jest przechowywana przez dostawcę usług poczty elektronicznej na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

12. **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa:**

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

Należy zwrócić uwagę, że elektroniczny formularz kontaktowy na stronie internetowej organizacji powinien wykorzystywać szyfrowanie SSL, które zapewnia ochronę danych wprowadzonych przez zamawiającego w przeglądarce internetowej.

13. **Obowiązek informacyjny wobec osób kontaktujących się z organizacją**

Osoby kontaktujące się po raz pierwszy z organizacją, powinny mieć możliwość zapoznania się z informacją dotyczącą przetwarzania danych osobowych. Organizacja w zależności od kontekstu może zrealizować obowiązek informacyjny w następujący sposób:

- poprzez umieszczenie jej pod formularzem kontaktowym na stronie internetowej organizacji,
- w rozmowie telefonicznej z pracownikiem organizacji,
- w formie nagrania odtwarzanego automatycznie przed rozpoczęciem rozmowy telefonicznej,
- w formie linku w stopce e-maila, który odsyła do strony internetowej organizacji z pełną treścią klauzuli informacyjnej,
- w formie autorespondera w poczcie elektronicznej,
- w formie postanowienia w polityce prywatności bądź klauzuli informacyjnej umieszczonej na stronie internetowej organizacji,
- w formie papierowej ulotki dostępnej w organizacji, np. wywieszonej na tablicy ogłoszeń lub udostępnianej w recepcji.

Przykładowa klauzula informacyjna pod formularzem kontaktowym:

Informujemy, że Pana/Pani dane osobowe będą przetwarzane przez Organizację z siedzibą w ____ (zwaną dalej Administratorem) w celu udzielenia odpowiedzi na pytanie zawarte w formularzu kontaktowym oraz w ramach utrzymywania stałego kontaktu z Administratorem w związku z jego celami statutowym, w tym informowania o możliwości wspierania działalności naszej organizacji. Podstawę prawną przetwarzania danych stanowi realizacja prawnie uzasadnionych interesów

Administratora w postaci komunikacji z użytkownikami strony (art. 6 ust. 1 lit. f rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).
Podanie danych jest dobrowolne, ale konieczne do tego, żeby odpowiedzieć na Pana/Pani pytanie. Pana/Pani dane będą przetwarzane nie dłużej, niż jest to konieczne do udzielenia Panu/Pani odpowiedzi, a po tym czasie mogą być przetwarzane przez okres przedawnienia ewentualnych roszczeń.
Informujemy, że przysługuje Panu/Pani prawo dostępu do treści swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu wobec ich przetwarzania, a także prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
Pana/Pani dane osobowe będą przechowywane przez naszą Organizację nie dłużej niż przez okres przedawnienia roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych w razie otrzymania od Pana/Pani żądania usunięcia danych osobowych.
Do Pani danych osobowych mogą mieć również dostęp podmioty świadczące na rzecz Organizacji usługi, w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze, prawnicze, księgowe, kadrowe.
Pana/Pani dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń. Podane dane osobowe mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane.
Ze szczegółowymi informacjami dotyczącymi zasad przetwarzania danych osobowych w naszej Organizacji może Pan/Pani zapoznać się w Polityce prywatności dostępnej na naszej stronie internetowej pod adresem: ___.
W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pana/Pani danych osobowych prosimy o kontakt z wyznaczonym przez nas Inspektorem Ochrony Danych pisząc na adres siedziby Organizacji: ul.____, z dopiskiem „Inspektor Ochrony Danych" lub na adres poczty elektronicznej <iod@nazwaorganizacji.pl>.

13. Członkowie i byli członkowie organizacji

1. Opis procesu przetwarzania danych osobowych

Proces ten obejmuje wykonywanie uprawnień i obowiązków wobec członków oraz byłych członków organizacji, np. w związku z zawiadamianiem o obradach organów stowarzyszeń bądź fundacji, bądź w związku z procesem rejestracji organizacji, w tym piastunów jej organów, o ile są członkami organizacji.

2. Opis kategorii osób

Osoby fizyczne posiadające status członka bądź byłych członków organizacji, np. członka stowarzyszeń, członka organów fundacji bądź stowarzyszenia.

3. **Kategorie danych osobowych**

Typowymi kategoriami danych osobowych przetwarzanych w ramach tego procesu będą:

- imiona,
- nazwiska,
- PESEL,
- seria i numer dowodu osobistego,
- dane kontaktowe jak adres zamieszkania lub korespondencji, adres poczty elektronicznej, numer telefonu,
- funkcja pełniona w organizacji.

W odniesieniu do danych wrażliwych członków i byłych członków organizacji o celach politycznych, światopoglądowych, religijnych lub związkowych RODO przewiduje odrębną podstawę prawną. Zgodnie bowiem z art. 9 ust. ust. 2 lit. d RODO dane wrażliwe można również przetwarzać w ramach uprawnionej działalności fundacji, stowarzyszeń oraz innych niezarobkowych podmiotów o celach politycznych, światopoglądowych, religijnych lub związkowych - pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą.

Dane wrażliwe obejmują dane dotyczące:

- pochodzenia rasowego lub etnicznego,
- zdrowia,
- seksualności,
- poglądów politycznych,
- religii,
- światopoglądu,
- przynależności do związków zawodowych a nadto
- dane genetyczne,
- dane biometryczne służących do jednoznacznego zidentyfikowania osoby fizycznej.

4. Cel przetwarzania danych osobowych	**5. Podstawa prawna przetwarzania danych osobowych**	**6. Okres przetwarzana danych osobowych**
kontakt z członkami lub z byłymi członkami organizacji w związku z ich członkostwem bądź byłym członkostwem w organizacji	art. 6 ust. 1 lit. f RODO tj. prawnie uzasadniony interes administratora polegającego na zarządzaniu relacjami art. 9 ust. 2 lit. d RODO odnośnie do danych wrażliwych	okres niezbędny do osiągnięcia celu przetwarzania danych osobowych, najpóźniej do złożenia sprzeciwu wobec przetwarzania danych

informowanie o realizacji celów statutowych organizacji, a także możliwościach wspierania działalności organizacji	art. 6 ust. 1 lit. f RODO prawnie uzasadniony interes administratora, którym jest utrzymywanie stałego kontaktu z organizacją w związku z jej celami statutowymi	okres niezbędny do osiągnięcia celu, jednak nie dłużej niż do złożenia sprzeciwu wobec przetwarzania danych osobowych w tym celu
dochodzenie roszczeń i obrona przed ewentualnymi roszczeniami	art. 6 ust. 1 lit. f RODO art. 17 ust. 3 lit. e RODO tj. prawnie uzasadniony interes administratora danych	okres przedawnienia ewentualnych roszczeń wynikający z przepisów prawa

7. Kategorie odbiorców danych

Przykładowo: dostawca usługi poczty elektronicznej, z której korzystają członkowie organizacji.

Z powyższym podmiotem należy zawrzeć umowę powierzenia przetwarzania danych. Wzór takiej umowy stanowi załącznik nr 1 do niniejszego kodeksu.

8. Współadministratorzy

Nie dotyczy.

9. Informacje o przekazaniu do państwa trzeciego

Przykładowo: gdy korespondencja e-mail prowadzona między członkami organizacji jest przechowywana przed dostawcę usług poczty elektronicznej na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

10. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

11. Obowiązek informacyjny wobec członków organizacji

Osoby fizyczne nabywające członkostwo w organizacji bądź w jej organach powinny mieć możliwość zapoznania się z informacją dotyczącą przetwarzania danych osobowych.

Przykładowa klauzula informacyjna dla nowego członka organizacji:

Informujemy, że Pana/Pani dane osobowe będą przetwarzane przez Organizację z siedzibą w ____ (zwaną dalej Administratorem lub Organizacją) w celu kontaktu w związku z członkostwem w naszej Organizacji oraz informowania o realizacji jej celów statutowych, a także możliwości wspierania jej

działalności. Podstawę prawną przetwarzania danych stanowi realizacja prawnie uzasadnionych interesów Administratora w postaci komunikacji z użytkownikami strony (art. 6 ust. 1 lit. f rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).
Podanie danych jest dobrowolne, ale niezbędne do tego, aby na bieżąco informować Pana/Panią o planowanych obradach organów naszej Organizacji, o realizacji jej celów statutowych, a także możliwości wspierania jej działalności. Pana/Pani dane będą przetwarzane nie dłużej, niż jest to konieczne dla powyższych celów, a po tym czasie mogą być przetwarzane przez okres przedawnienia ewentualnych roszczeń.
Informujemy, że przysługuje Pani prawo dostępu do treści swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu wobec ich przetwarzania, a także prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
Pana/Pani dane osobowe będą przechowywane przez naszą Organizację nie dłużej niż przez okres przedawnienia roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych w razie otrzymania od Pana/Pani żądania usunięcia danych osobowych.
Do Pani danych osobowych mogą mieć również dostęp podmioty świadczące na rzecz Organizacji usługi, w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze. prawnicze, księgowe, kadrowe.
Pana/Pani dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie, na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń. Podane dane osobowe mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane.
Ze szczegółowymi informacjami dotyczącymi zasad przetwarzania danych osobowych w naszej Organizacji może Pan/Pani zapoznać się w Polityce prywatności dostępnej na naszej stronie internetowej pod adresem: <www.nazwaorganizacji.pl>.
W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pana/Pani danych osobowych prosimy o kontakt z wyznaczonym przez nas Inspektorem Ochrony Danych pisząc na adres siedziby Organizacji: ul.____, z dopiskiem „Inspektor Ochrony Danych" lub na adres poczty elektronicznej <iod@nazwaorganizacji.pl>.

Zagadnienia szczegółowe

1) **Czy organizacja może wysyłać życzenia świąteczne np. w formie kartek świątecznych do swoich darczyńców, beneficjentów, kontrahentów, klientów lub na inne administrowane przez organizację kontakty służbowe?**

   Tak, organizacja ma prawnie uzasadniony interes w wysyłaniu życzeń świątecznych w postaci utrzymywania dobrych relacji z darczyńcami, beneficjentami, kontrahentami, klientami oraz innymi osobami, których dane pozyskała w ramach kontaktów służbowych (art. 6 ust. 1 lit. f RODO).

Organizacja powinna jednak uprzednio poinformować powyższe osoby o tym, że ich dane będą przetwarzane w celu wysyłania życzeń świątecznych (art. 13 RODO).

14. Korespondencja przychodząca i wychodząca

1. Opis procesu przetwarzania danych osobowych

Proces ten polega na realizacji uprawnień i obowiązków wynikających z przepływem korespondencji przychodzącej i wychodzącej do i z organizacji.

2. Opis kategorii osób

Osoby, z którymi prowadzona jest korespondencja (zarówno papierowa, jak i elektroniczna), nadawcy i odbiorcy korespondencji.

3. Typowe kategorie danych osobowych

Typowymi kategoriami danych dla tego procesu będą w zakresie danych zwykłych:

- imię (imiona),
- nazwisko,
- adres e-mail,
- adres zamieszkania
- adres do korespondencji.

4. Cel przetwarzania danych osobowych	5. Podstawa prawna przetwarzania danych osobowych	6. Okres przetwarzana danych osobowych
(1) Kontakt z klientami, kontrahentami, pracownikami, współpracownikami (2) prowadzenie korespondencji papierowej (3) prowadzenie korespondencji elektronicznej (4) nadzór nad obiegiem dokumentacji (5) informowanie o realizacji działań statutowych, w tym informowanie o organizowanych akcjach społecznych, wydarzeniach publicznych etc. (6) obieg dokumentacji w wykonaniu umów	Zgoda (art. 6 ust. 1 lit a RODO), wykonanie umowy (art. 6 ust. 1 lit. b RODO), niezbędność do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora (art. 6 ust. 1 lit. f RODO)	dane są przechowywane a następnie usuwane zgodnie ze szczególnymi aktami prawnymi dotyczącymi przechowania dokumentacji, np. księgowej, dotyczącej umów etc., na żądanie osoby, która wyraziła zgodę na przetwarzanie
dochodzenie roszczeń lub obrona przed ewentualnymi roszczeniami	art. 6 ust. 1 lit. f RODO art. 17 ust. 3 lit. e RODO	okres przedawnienia roszczeń z tytułu umowy zawartej z danym

	uzasadniony interes realizowany przez administratora	kontrahentem, brak przesłanki niezbędności celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora

3. Kategorie odbiorców danych

Przykładowo: biuro księgowe, hostingodawca, firma zajmująca się niszczeniem dokumentacji.

4. Współadministratorzy

Przykładowo: gdy organizacja prowadzi akcję społeczną wspólnie z innym administratorem w ramach wspólnego projektu.

5. Informacje o przekazaniu do państwa trzeciego

Przykładowo: gdy dane osobowe kontrahentów przechowywane są przez organizację na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

6. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

7. Obowiązek informacyjny

Prowadząc korespondencję organizacja powinna spełnić obowiązek informacyjny wobec osoby, z którą organizacja koresponduje. Przykładowa klauzula informacyjna:

Klauzula informacyjna dot. przetwarzania danych w korespondencji

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – dalej jako RODO), informuję, że:

1. *administratorem Pani/Pana danych osobowych jest Organizacja z siedzibą w _____ (zwana dalej Organizacją),*
2. *celem przetwarzania Pana/Pani danych osobowych są* uzasadnione interesy realizowane przez administratora*, związane z realizacją jego celów statutowych, w szczególności informowanie w ramach utrzymywania stałego kontaktu z Organizacją o organizowanych spotkaniach,*

kampaniach, akcjach społecznych i wydarzeniach publicznych oraz możliwościach wspierania działalności Organizacji, na podstawie art. 6 ust. 1 lit. f RODO,

3. *ma Pan/Pani prawo dostępu do swoich danych, ich sprostowania, żądania ich usunięcia, prawo ograniczenia przetwarzania i prawo przenoszenia danych a także wniesienia sprzeciwu wobec przetwarzania danych osobowych.*
4. *przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, jeżeli w Pana/Pani ocenie dane są przetwarzane niezgodnie z wymogami prawnymi,*
5. *odbiorcami Pana/Pani danych osobowych mogą być podmioty świadczące na rzecz Organizacji usługi w szczególności hostingowe, księgowe, informatyczne, doradcze, płatnicze, prawne, kadrowe, wysyłkowe,*
6. *Pani/Pana dane osobowe będą przechowywane do upływu okresu przedawnienia roszczeń bądź wygaśnięcia obowiązków przechowywania danych wynikających z przepisów podatkowych i przepisów o rachunkowości,*
7. *Pana/Pani dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń,*
8. *przekazanie nam Państwa danych osobowych odbywa się w sposób całkowicie dobrowolny, jednakże odmowa przekazania tych danych może uniemożliwić Organizacji zawarcie oraz realizację praw lub obowiązków wynikających z umowy,*
9. *Pani/Pana dane mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem, nie będą zautomatyzowane,*
10. *W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pani/Pana danych osobowych prosimy o kontakt z wyznaczonym przez nas Inspektorem Ochrony Danych pisząc na adres siedziby Organizacji przy ul. _____ z dopiskiem „Inspektor Ochrony Danych" lub mailowo na adres <iod@nazwaorganizacji.pl>.*

15. Kontrahenci

1. Opis procesu przetwarzania danych osobowych

Proces ten polega na realizacji uprawnień i obowiązków wynikających z umów zawieranych przez organizację społeczną z osobami fizycznymi prowadzącymi działalność gospodarczą. Proces obejmuje również podejmowanie działań na żądanie powyższych osób przed zawarciem umowy.

2. Opis kategorii osób

Osoby fizyczne prowadzące działalność gospodarczą, z którymi organizacja zawarła umowy na dostawę towarów lub wykonanie usług bądź podejmuje działania w celu zawarcia takiej umowy.

3. Typowe kategorie danych osobowych

Typowymi kategoriami danych dla tego procesu będą w zakresie danych zwykłych:

- imię (imiona),
- nazwisko,
- stanowisko,
- adresy e-mail,
- numer telefonu,
- adres zamieszkania lub korespondencji,
  (ulica, numer, kod pocztowy, miejscowość, państwo),
- nazwa (firma) przedsiębiorcy
- NIP firmy/PESEL osoby fizycznej.

4. Cel przetwarzania danych osobowych	5. Podstawa prawna przetwarzania danych osobowych	6. Okres przetwarzana danych osobowych
podejmowanie działań przed zawarciem umowy z potencjalnym kontrahentem, na jego żądanie, w tym weryfikacja kontrahenta pod kątem spełniania przez niego określonych wymogów	art. 6 ust. 1 lit. b RODO	do momentu zawarcia umowy z kontrahentem, a w przypadku podjęcia decyzji o niezawieraniu umowy – najpóźniej przez 6 miesięcy od zebrania danych osobowych kontrahenta
wykonanie umowy zawartej pomiędzy organizacją a kontrahentem	art. 6 ust. 1 lit. b RODO	okres wykonywania umowy zawartej z kontrahentem
prowadzenie ksiąg rachunkowych i dokumentacji podatkowej	art. 6 ust. 1 lit c. RODO w związku z art. 74 ust. 1 i 2 ustawy o rachunkowości oraz innymi przepisami szczególnymi	do momentu wygaśnięcia obowiązków przechowywania danych wynikających z przepisów podatkowych i przepisów o rachunkowości
dochodzenie i obrona roszczeń wynikających z umów z kontrahentami	art. 6 ust. 1 lit. f RODO art. 17 ust. 3 lit. e RODO uzasadniony interes realizowany przez administratora	okres przedawnienia roszczeń z tytułu umowy zawartej z danym kontrahentem

3. Kategorie odbiorców danych

Przykładowo: biuro księgowe, hostingodawca.

4. Współadministratorzy

Przykładowo: gdy organizacja zawiera umowę z kontrahentem wspólnie z innym administratorem w ramach wspólnego projektu.

5. **Informacje o przekazaniu do państwa trzeciego**

Przykładowo: gdy dane osobowe kontrahentów przechowywane są przez organizację na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

6. **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa**

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

7. **Obowiązek informacyjny wobec kontrahenta**

Wraz z zawarciem umowy, organizacja powinna spełnić obowiązek informacyjny wobec kontrahenta. Przykładowa klauzula informacyjna:

Klauzula informacyjna dot. przetwarzania danych kontrahenta

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – dalej jako RODO), informuję, że:

1. *administratorem Pani/Pana danych osobowych jest Organizacja z siedzibą w _____ (zwana dalej Organizacją),*
2. *celem przetwarzania Pana/Pani danych osobowych jest podejmowanie działań przed zawarciem umowy, w tym weryfikacja kontrahenta pod kątem spełniania przez niego określonych wymogów, a w razie zawarcia umowy - realizacja praw i obowiązków wynikających z zawartej umowy, na podstawie art. 6 ust. 1 lit. b RODO, prowadzenia prowadzenie ksiąg rachunkowych i dokumentacji podatkowej w związku z wykonaniem umowy na podstawie art. 6 ust. 1 lit. b i c RODO, ustalenie, obrona lub dochodzenie ewentualnych roszczeń, na podstawie art. 6 ust. 1 lit. f RODO,*
3. *ma Pan/Pani prawo dostępu do swoich danych, ich sprostowania, żądania ich usunięcia, prawo ograniczenia przetwarzania i prawo przenoszenia danych a także wniesienia sprzeciwu wobec przetwarzania danych osobowych.*
4. *przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, jeżeli w Pana/Pani ocenie dane są przetwarzane niezgodnie z wymogami prawnymi,*
5. *odbiorcami Pana/Pani danych osobowych mogą być podmioty świadczące na rzecz Organizacji usługi w szczególności hostingowe, księgowe, informatyczne, doradcze, płatnicze, prawne, kadrowe, wysyłkowe,*
6. *Pani/Pana dane osobowe będą przechowywane do upływu okresu przedawnienia roszczeń bądź wygaśnięcia obowiązków przechowywania danych wynikających z przepisów podatkowych i przepisów o rachunkowości,*
7. *Pana/Pani dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w*

szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń,

8. *przekazanie nam Państwa danych osobowych odbywa się w sposób całkowicie dobrowolny, jednakże odmowa przekazania tych danych może uniemożliwić Organizacji zawarcie oraz realizację praw lub obowiązków wynikających z umowy,*
9. *Pani/Pana dane mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane,*
10. *W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pani/Pana danych osobowych prosimy o kontakt z wyznaczonym przez nas Inspektorem Ochrony Danych pisząc na adres siedziby Organizacji przy ul. _____ z dopiskiem „Inspektor Ochrony Danych" lub mailowo na adres <iod@nazwaorganizacji.pl>.*

16. Pracownicy i współpracownicy

1. Opis procesu przetwarzania danych osobowych

Działalność organizacji w tym procesie polega na zawieraniu i wykonywaniu umów o pracę oraz umów cywilnoprawnych.

2. Opis kategorii osób

Osoby fizyczne, która zgodnie z przepisami polskiego prawa:

- pozostają z organizacją społeczną w stosunku pracy,
- współpracującą z organizacją społeczną, niezależnie od formy prawnej tej współpracy, w szczególności na podstawie umów cywilnoprawnych, takich jak umowa zlecenia lub umowa o dzieło
- odbywają w organizacji społecznej praktyki lub staż.

3. Typowe kategorie danych osobowych

Typowymi kategoriami danych dla tego procesu mogą być:

- dane identyfikacyjne (imiona, nazwiska, data urodzenia, numer PESEL, a w przypadku jego braku rodzaj i numer dokumentu potwierdzającego tożsamość),
- dane kontaktowe wskazane przez pracownika (np. numer telefonu, adresy e-mail, adres zamieszkania bądź do korespondencji),
- wykształcenie, kwalifikacje zawodowe, przebieg dotychczasowego zatrudnienia,
- numer rachunku bankowego (o ile pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych),
- dane kadrowe przetwarzane na podstawie przepisów prawa pracy oraz innych przepisów prawa (wysługa lat pracy, stawka wynagrodzeń, przebieg pracy, dane o czasie pracy, absencje, tj. urlopy, zwolnienia lekarskie, rehabilitacyjne, szkoleniowe, dane o zakresie obowiązków,

dane o potrąceniach (składki związkowe, zajęcia komornicze itp.), dane o karach i przyznanych nagrodach oraz inne dane wymagane zgodnie z Kodeksem pracy).

4. Cel przetwarzania danych osobowych	5. Podstawa prawna przetwarzania danych osobowych	6. Okres przetwarzana danych osobowych
realizacja praw i obowiązków wynikających z zawieranych umów o pracę oraz umów cywilnoprawnych	art. 6 ust. 1 lit. b RODO niezbędność do wykonania umowy o pracę	okres obowiązywania umowy o pracę bądź umowy cywilnoprawnej
wypełnienie obowiązku prawnego ciążącego na organizacji w związku z nawiązaniem stosunku pracy bądź nawiązaniu współpracy na podstawie umów cywilnoprawnych	art. 6 ust. 1 lit c. RODO art. 9 ust. 2 lit. b RODO przepisy prawa ubezpieczeń społecznych, przepisy podatkowe	• w przypadku pracowników, zleceniobiorców - dane usuwane do końca roku kalendarzowego po upływie 50 lat od zakończenia zatrudnienia; a w przypadku złożenia raportu informacyjnego do ZUS - 10 lat od zakończenia zatrudnienia (od 1.1.2019) • w przypadku umów o dzieło - dane usuwane do końca roku kalendarzowego po upływie okresu przedawnienia roszczeń z tytułu umów o dzieło, • w przypadku praktykantów i stażystów - dane usuwane do końca roku kalendarzowego po upływie roku od zakończenia praktyki lub stażu
w przypadku pracowników, którzy na zasadzie dobrowolności wskazali pracodawcy dane zwykłe wykraczające poza zakres danych określonych w Kodeksie pracy	art. 6 ust. 1 lit. a RODO	dane usuwane po cofnięciu zgody na przetwarzanie danych osobowych przez pracownika
dochodzenie roszczeń i obrona przed roszczeniami z tytułu zawartej umowy o pracę	art. 6 ust. 1 lit. f RODO prawnie uzasadniony interes administratora	okres przedawnienia ewentualnych roszczeń związanych z umową o pracę bądź umowy cywilnoprawnej

3. Kategorie odbiorców danych

Przykładowo: biura księgowe, towarzystwa ubezpieczeniowe, brokerzy ubezpieczeniowi w przypadku

ubezpieczania pracownika za pośrednictwem organizacji w zakresie ubezpieczenia NNW (następstw nieszczęśliwych wypadków) lub objęcia ubezpieczeniem zdrowotnym.

4. Współadministratorzy

Nie dotyczy.

5. Informacje o przekazaniu do państwa trzeciego

Przykładowo: gdy dane osobowe pracowników są przechowywane przez organizację na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

6. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

11. Obowiązek informacyjny wobec pracownika

Przed rozpoczęciem świadczenia pracy na rzecz organizacji, pracownik powinien być upoważniony przez organizację do przetwarzania administrowanych przez nią danych osobowych. Organizacja powinna spełnić obowiązek informacyjny wobec pracownika.

Przykładowe upoważnienie i klauzula informacyjna:

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH
NR ../../2020

Działając w imieniu Organizacji z siedzibą w Warszawie (zwanej dalej Administratorem) na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej RODO – nadaję Pani/Panu:

<imię i nazwisko pracownika>

upoważnienie do przetwarzania danych osobowych w ramach wykonywania powierzonych zadań lub obowiązków na podstawie umowy o pracę zawartej z Administratorem.

Upoważnienie obowiązuje do dnia zakończenia świadczenia pracy u Administratora bądź do dnia odwołania niniejszego upoważnienia.

Upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych na nośnikach papierowych oraz systemach informatycznych w ramach następujących procesów przetwarzania:
1) Kampanie społeczne
2) Korespondencja przychodząca i wychodząca
3) Wydarzenia publiczne
4) Media społecznościowe
5) Kontrahenci
bez ograniczeń – obejmujących podgląd danych, wprowadzanie danych, opracowywanie danych, zmienianie danych, usuwanie danych.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem, przepisami RODO, ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, Kodeksem pracy, a także z Polityką ochrony danych osobowych oraz Instrukcją zarządzania systemem Informatycznym obowiązującą u Administratora.

_____ _____

podpis pracownika *podpisy osób uprawnionych do nadania upoważnienia*

Klauzula informacyjna dot. przetwarzania danych pracownika

Zgodnie z art. 13 ust. 1 i 2 Ogólnego Rozporządzenia o Ochronie Danych Osobowych (RODO) informuję, że:

(1) *administratorem Pani/Pana danych osobowych jest Organizacja z siedzibą w _____ (zwana dalej Organizacją),*
(2) *Pani/Pana dane osobowe przetwarzane będą w celu związanym z nawiązaniem i przebiegiem procesu zatrudnienia, na podstawie art. 6 ust. 1 lit. a i c oraz art. 9 ust. 2 lit. b RODO,*
(3) *podanie przez Pana/Panią danych osobowych jest obowiązkowe w zakresie określonym w art. 221 § 1, 2 i 4 kodeksu pracy, art. 68 ust. 3 ustawy z dnia 27 sierpnia 2004 o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych a także innych powszechnie obowiązujących przepisów praca, a w pozostałym zakresie jest zaś dobrowolne, ale konieczne dla celów związanych z nawiązaniem i przebiegiem Pani/Pana zatrudnienia.*
(4) *Pani/Pana dane osobowe będą przechowywane przez okres wynikający z przepisów dotyczących przechowywania akt pracowniczych,*
(5) *posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu albo cofnięcia zgody na ich przetwarzanie w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody wyrażonej przed jej cofnięciem,*
(6) *ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy o ochronie danych osobowych,*
(7) *do Pani/Pana danych osobowych mogą mieć również dostęp podmioty świadczące na rzecz Organizacji usługi, w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze, prawnicze, księgowe, kadrowe,*
(8) *Pani/Pana dane mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem nie będą zautomatyzowane.*

(9) *Pan/Pani dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń.*

(10) *W razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pani/Pana danych osobowych prosimy o kontakt z wyznaczonym przez nas Inspektorem Ochrony Danych pisząc na adres siedziby Organizacji przy ul. _____ z dopiskiem „Inspektor Ochrony Danych" lub mailowo na adres <iod@nazwaorganizacji.pl>.*

17. Rekrutacje pracowników i współpracowników

1. Opis procesu przetwarzania danych osobowych

Działalność organizacji w tym procesie polega na wyłanianiu pracowników, współpracowników, stażystów, praktykantów spośród kandydatów do pracy, współpracy, na staż bądź praktyki.

2. Opis kategorii osób

Osoby fizyczne, która kandydują do pracy, współpracy, na staż bądź praktyki.

3. Typowe kategorie danych osobowych

Typowymi kategoriami danych dla tego procesu mogą być:

- dane identyfikacyjne (imiona, nazwiska, data urodzenia, numer PESEL, a w przypadku jego braku - rodzaj i numer dokumentu potwierdzającego tożsamość),
- dane kontaktowe wskazane przez pracownika (np. numer telefonu, adresy e-mail, adres zamieszkania bądź do korespondencji),
- wykształcenie, kwalifikacje zawodowe, przebieg dotychczasowego zatrudnienia, informacje o odbytych kursach oraz otrzymanych certyfikatach.

4. Cel przetwarzania danych osobowych	5. Podstawa prawna przetwarzania danych osobowych	6. Okres przetwarzana danych osobowych
wyłonienie kandydatów do pracy, na staż lub praktyki na potrzeby konkretnego procesu rekrutacyjnego, ewentualnie na poczet przyszłych rekrutacji	art. 6 ust. 1 lit. b RODO w związku z art. 22^1 § 1 pkt. 4–6 Kodeksu pracy niezbędność do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy	• dane kandydatów niezatrudnionych, którzy nie wyrazili zgody na przetwarzanie ich danych w przyszłych celach rekrutacyjnych - do końca roku kalendarzowego po upływie okresu przedawnienia ewentualnych roszczeń wynikających z przepisów prawa

	art. 6 ust. 1 lit. c RODO w związku z art. 22^1 § 1 pkt. 1–3 Kodeksu pracy niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze	dotyczących dyskryminacji w zatrudnieniu; • dane kandydatów niezatrudnionych, którzy wyrazili zgodę na przetwarzanie ich danych w przyszłych rekrutacjach - na okres wskazany w oświadczeniu o w wyrażeniu zgody na korzystanie z danych w przyszłych rekrutacjach liczony od podania danych osobowych przez kandydata; jednak nie później niż do dnia otrzymania oświadczenia o wycofaniu zgody na przetwarzanie danych osobowych na poczet przyszłych rekrutacji
w przypadku kandydatów do pracy, którzy na zasadzie dobrowolności wskazali pracodawcy dane zwykłe lub wrażliwe wykraczające poza zakres danych określonych w Kodeksie pracy	art. 6 ust.1 lit. a RODO zgoda osoby na przetwarzanie danych zwykłych art. 9 ust. 2 lit. a RODO wyraźna zgoda osoby na przetwarzanie danych wrażliwych	dane usuwane po cofnięciu zgody na przetwarzanie danych osobowych przez pracownika
dochodzenie roszczeń i obrona przed roszczeniami	art. 6 ust. 1 lit. f RODO prawnie uzasadniony interes administratora	okres przedawnienia ewentualnych roszczeń związanych z umową o pracę bądź umowy cywilnoprawnej

4. Kategorie odbiorców danych

Przykładowo: podmioty, z którymi organizacja zawarła umowę na świadczenie usług serwisowych dla systemów informatycznych wykorzystywanych przy ich przetwarzaniu.

5. Współadministratorzy

Nie dotyczy.

6. Informacje o przekazaniu do państwa trzeciego

Przykładowo: gdy dane osobowe kandydatów są przechowywane przez organizację na serwerach zlokalizowanych poza Europejskim Obszarem Gospodarczym (EOG).

7. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Zaleca się, aby opis technicznych środków bezpieczeństwa wdrożonych przez organizację został określony w Instrukcji zarządzania systemami informatycznymi i Polityce ochrony danych osobowych. Przykładowy i zalecany dla organizacji wykaz technicznych i organizacyjnych środków bezpieczeństwa opisany został w rozdziale VI niniejszego kodeksu.

8. Obowiązek informacyjny wobec pracownika

Na etapie rekrutacji organizacja powinna spełnić obowiązek informacyjny wobec kandydatów do pracy, współpracy, na staż bądź praktyki. Przykładowa klauzula informacyjna:

Szanowny Kandydacie!

Wysyłając swoje zgłoszenie rekrutacyjne na stanowisko wskazane w ogłoszeniu rekrutacyjnym, zgadza się Pan/Pani na przetwarzanie przez naszą Organizację dodatkowych danych osobowych, które nie zostały wskazane w Kodeksie pracy lub w innych przepisach prawa (np. Pana/Pani zdjęcie, zainteresowania). Dane osobowe wskazane w Kodeksie pracy lub w innych przepisach prawa (m.in. Pana/Pani imię, nazwisko, dane kontaktowe, wykształcenie, kwalifikacje zawodowe, przebieg dotychczasowego zatrudnienia) przetwarzamy na podstawie przepisów prawa. Jeżeli nie chce Pan/Pani, abyśmy przetwarzali dodatkowe dane o Panu/Pani, uprzejmie prosimy o niezamieszczanie ich w swoich dokumentach. Pana/Pani zgoda jest dobrowolna i nie ma wpływu na możliwość udziału w rekrutacji. Może Pan/Pani ją cofnąć w każdym momencie, jednak nie będzie to miało wpływu na zgodność z prawem przetwarzania przed cofnięciem zgody.
Jeżeli w dokumentach zawarte są dane wrażliwe, o których mowa w art. 9 ust. 1 RODO konieczna będzie Pana/Pani zgoda na ich przetwarzanie.

Jeżeli chciałby Pan/Pani w wziąć udział w przyszłych rekrutacjach prowadzonych przez naszą Organizację, prosimy o załączenie do swoich dokumentów aplikacyjnych następującego oświadczenia: "Wyrażam zgodę na przetwarzanie przez ……. z siedzibą w …….. przy ul. ……. moich danych osobowych zawartych w CV lub innych dokumentach aplikacyjnych na potrzeby przyszłych rekrutacji prowadzonych przez …….. z siedzibą w ……. w okresie kolejnych 5 lat."

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119) – dalej RODO informujemy, że:
1) administratorem Pani/Pana danych osobowych jest Organizacja …… z siedzibą w …….. przy ul. ……..; dane Inspektora Ochrony Danych: <iod@nazwaorganizacji.pl>,
2) nasza Organizacja zbiera i przetwarza dane osobowe przekazane nam w CV, liście motywacyjnym, a także w innych formularzach niezbędnych w ramach procesu rekrutacji, w zakresie i na podstawie

właściwych przepisów, tj. Kodeksu pracy (w przypadku ubiegania się o zatrudnienia o umowę o pracę) i Kodeksu cywilnego (w przypadku ubiegania się o współpracę na podstawie umowy cywilnoprawnej),
3) podanie przez Pana/Panią danych osobowych w zakresie wynikającym z art. 22(1) Kodeksu pracy jest niezbędne, aby uczestniczyć w postępowaniu rekrutacyjnym. Podanie przez Państwa innych danych jest dobrowolne,
4) w przypadku udanej rekrutacji, Pana/Pani dane osobowe będą przechowywane w celu przygotowania umowy o pracę lub umowy cywilnoprawnej, zgodnie z przepisami ustawowymi. Dokumenty odrzuconych kandydatów będą usuwane najpóźniej po upływie okresu przedawnienia roszczeń z tytułu dyskryminacji w zatrudnieniu,
5) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody na ich przetwarzanie w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody wyrażonej przed jej cofnięciem,
6) ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO,
7) odbiorcą Pana/Pani danych osobowych mogą być podmioty świadczące na naszą rzecz usługi w szczególności hostingowe, informatyczne, drukarskie, wysyłkowe, płatnicze. prawnicze, księgowe, kadrowe,
8) Pana/Pani dane osobowe mogą być przekazywane do państwa trzeciego, tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Organizacja zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń,.
9) Pani/Pana dane mogą być przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Jednak decyzje dotyczące indywidualnej osoby, związane z tym przetwarzaniem, nie będą zautomatyzowane,.
10) ze szczegółowymi informacjami dotyczącymi zasad przetwarzania danych osobowych w Instytucie może Pan/Pani zapoznać się w naszej Polityce prywatności,.
*11) w razie jakichkolwiek żądań, pytań lub wątpliwości co do przetwarzania Pani/Pana danych osobowych prosimy o kontakt z wyznaczonym przez nas Inspektorem Ochrony Danych pisząc na adres siedziby Organizacji: ul. _____ , z dopiskiem „Inspektor Ochrony Danych" lub na adres poczty elektronicznej <*iod@nazwaorganizacji.pl*>*

ROZDZIAŁ V.
UJAWNIANIE DANYCH OSOBOWYCH PRZEZ ORGANIZACJĘ ORAZ PRZETWARZANIE DANYCH ADMINISTROWANYCH PRZEZ INNE PODMIOTY

Organizacje mogą przetwarzać również dane osobowe innych podmiotów, tj. same nie będąc administratorem, mogą przetwarzać dane osobowe innego administratora lub też mogą przekazywać, udostępniać dane osobowe innemu podmiotowi, który wówczas będzie podmiotem przetwarzającym.

Do takich sytuacji może dojść na przykład, gdy organizacje w ramach współpracy przekazują sobie dane osobowe w celu prowadzenia akcji i kampanii społecznych. Organizacja może również przetwarzać dane osobowe innej organizacji, innego podmiotu podczas organizacji szkoleń dla innego podmiotu albo na przykład pomagając innej organizacji w wysyłce materiałów, broszur, zaproszeń na wydarzenia publiczne. W takiej sytuacji organizacja sama staje się przetwarzającym dane osobowe innego podmiotu.

Do sytuacji, w których inny podmiot jest przetwarzającym, może dojść, gdy organizacja podpisuje umowę z firmą kurierską, administratorem serwera, firmami świadczącymi na rzecz organizacji różne usługi, np. księgowe, prawne, podatkowe.

Może wystąpić również sytuacja, gdy organizacja, chcąc dotrzeć ze swoją kampanią społeczną do określonego grona odbiorców, będzie chciała zakupić bazę danych innego podmiotu. Może również podjąć wspólną z innymi organizacjami społecznymi akcję społeczną lub zorganizować wydarzenie publiczne.

Wszystkie te sytuacje wiążą się z określonymi obowiązkami organizacji społecznych i ich partnerów, w zależności od tego, czy organizacje są podmiotami tylko przetwarzającymi dane, powierzającymi do przetwarzania, współadministratorami, czy też kupującymi bazę danych od podmiotu trzeciego.

Nadto w niniejszym rozdziale zostanie omówiona problematyka ujawniania danych przez organizacje społeczne dysponującymi środkami publicznymi w formie dotacji, grantów lub w innych formach lub gdy wykonują zadania publiczne, w ramach udostępniania informacji publicznej.

1. Przetwarzanie danych osobowych innego podmiotu.

Warunki konieczne, aby organizacja, jako podmiot przetwarzający dane innego administratora, postępowała zgodnie z prawem:

Konieczne jest podpisanie z podmiotem, dla którego organizacja wykonuje usługi i korzysta z danych, umowy powierzenia przetwarzania danych osobowych. Umowa taka powinna być dla celów dowodowych zawarta na piśmie. Umowa powierzenia przetwarzania danych może zostać zawarta odrębnie od innej umowy, tzw. umowy głównej pomiędzy administratorem danych oraz organizacją będącą podmiotem przetwarzającym, z której wykonaniem wiąże się przetwarzanie danych lub zostać ujęta jako element samej umowy o powierzenie przetwarzania danych jako jeden z paragrafów takiej umowy.

Przekazywanie danych osobowych pomiędzy administratorem a organizacją jako podmiotem przetwarzającym powinno odbywać się w sposób bezpieczny pod względem organizacyjnym oraz technicznym. Ważne jest, aby umowa powierzenia pomiędzy stronami określała, kto jest upoważniony do przekazania lub odbioru danych oraz jakimi środkami dane osobowe będą przekazywane. W przypadku przekazywania danych osobowych w formie papierowej, dokumentacja powinna zostać przekazana bezpośrednio pomiędzy osobami upoważnionymi do tych czynności. W przypadku przekazywania danych w formie elektronicznej, korespondencja między upoważnionymi osobami powinna być odpowiednio szyfrowana. Można również użyć hasła do otworzenia pliku z danymi. Hasło to musi zostać wysłane drugiej stronie innym środkiem komunikowania, np. poprzez wiadomość SMS). Jeżeli przetwarzanie danych osobowych przez organizację jako podmiot przetwarzający jest dokonywane w imieniu administratora, organizacja zobowiązana jest do zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi wynikające z przepisów prawa i chroniło prawa osób, których dane dotyczą. Wystarczające gwarancje organizacja może wykazać między innymi poprzez uzyskanie statusu podmiotu przestrzegającego Kodeksu. Zawierając umowy powierzenia przetwarzania danych osobowych, organizacje przestrzegające Kodeksu mogą stosować postanowienia zawarte we wzorze umowy powierzenia przetwarzania danych osobowych, stanowiącym Załącznik nr 1 do Kodeksu. Wzór umowy powierzenia przetwarzania każdorazowo powinien zostać poddany analizie i dostosowany do zakresu, rodzaju i kontekstu powierzenia przetwarzania danych osobowych. Organizacja może korzystać z własnych wzorów umów powierzenia przetwarzania danych osobowych

2. Udostępnienie, przekazanie do używania danych osobowych przez jednego administratora drugiemu administratorowi. Zakup bazy danych.

Jeśli organizacja podejmie decyzję, aby przekazać, zbyć, czasowo „wydzierżawić", tj. przekazać do użytkowania dane swoich darczyńców, sympatyków innemu administratorowi, powinna przestrzegać następujących zasad (zasady te dotyczą również sytuacji, w której organizacja społeczna chce zakupić, „wydzierżawić", tj. przeznaczyć do wykorzystania na jakiś czas dane osobowe innego podmiotu).

Zasady przy zakupie/sprzedaży, udostępnieniu, czasowym wykorzystaniu baz danych:

1. Podmioty powinny między sobą podpisać umowę o przekazanie danych osobowych (zakup/czasowa „dzierżawa", tj. czasowe wykorzystanie),
2. Administrator przekazujący dane musi wykazać się podstawą prawną dla takiego działania. Może to być zgoda osoby, której dane są przetwarzane, prawnie uzasadniony interes,
3. Administrator może przekazać dane innemu podmiotowi po uprzednim poinformowaniu osoby, której dane dotyczą, przy okazji zbierania danych o znanych mu na dany dzień odbiorcach lub kategoriach (np. określona branża) odbiorców danych osobowych; poinformowanie to musi nastąpić nie później niż przed pierwszym przekazaniem danych. Kategorie odbiorców danych mogą zostać wykazane w klauzuli informacyjnej przekazanej osobie, której dane są przetwarzane,
4. Umowa pomiędzy podmiotami powinna określać co najmniej:
a) ilość przekazanych danych,
b) zasady przekazania, udostępnienia danych oraz okres na jaki dane zostaną udostępnione,
c) cel udostępnienia/przekazania danych,

d) udostępnienie/przekazanie danych może być poprzedzone opisanym w umowie procesem deduplikacji, polegającym na tym, że administrator i podmiot, któremu mają być przekazane/udostępnione dane porównują swoje dane w celu określenia, czy przekazanie/wymiana danych jest uzasadniona. Sprawdzenie to może odbywać się według różnych modeli: np. wiek osób, terytorium z którego pochodzą dane. Proces ten powinien odbyć się na wyselekcjonowanej grupie rekordów (danych) z wykorzystaniem metody pseudonimizacji a po jego zakończeniu dane niezbędne do przeprowadzenia tego procesu powinny przez obie strony zostać usunięte. Jest to proces weryfikacyjny i nie jest on jest uznawany za proces udostępnienia danych.

Gdy organizacja zakupiła bazę i zrobiła z jej wykorzystaniem np. kampanię społeczną, wysyłając list, e-mail do osoby z zakupionej przez nią bazy, ma obowiązek, przy pierwszej wysyłce, poinformować osobę do której kierowana jest kampania społeczna, o swojej nazwie, adresie do korespondencji, poinformować z jakiego źródła posiada dane osoby i jakie prawa przysługują osobie, do której wysłała apel, kampanię społeczną, zgodnie z art. 14 RODO.
Co do zasady przekazywanie/udostępnianie danych do wykorzystania innemu podmiotowi, który nie będzie przetwarzał danych w państwie trzecim nie wymaga innych warunków. Jeśli jednak dane będą przetwarzane w państwie trzecim, np. na serwerze państwa, które nie jest objęte rozwiązaniami RODO, wówczas wymagane jest spełnienie wszystkich wymogów obowiązujących w RODO.

3. Ujawnianie danych osobowych organom publicznym w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej.

Udostępnianie danych może wynikać również nie z samej umowy między dwoma podmiotami, ale zachodzić na mocy przepisów prawa. Np. gdy uprawniony podmiot zwróci się do organizacji o przekazanie danych osobowych. Podmiotami najczęściej występującymi o udostępnienie danych osobowych są: policja, prokuratura, sądy, komornik, ZUS, KRUS oraz bank. Udostępnianie danych osobowych należy do czynności przetwarzania danych osobowych. Zgodnie bowiem z art. 4 pkt 2 RODO przetwarzanie oznacza „operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak m.in. ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie". Zgodnie z powyższym udostępnianie danych osobowych należy do czynności ujawniania danych osobowych. Należy podkreślić, że w RODO nie znalazły się odrębne regulacje odnoszące się do udostępniania danych osobowych. Organizacja udostępnia dane osobowe wtedy, gdy istnieje podstawa prawna, która z jednej strony uprawnia podmiot występujący o udostępnienie danych do uzyskania danych, a z drugiej strony zobowiązuje organizację jako administratora do przekazania danych. Podstawa prawna musi istnieć w postaci konkretnego przepisu prawa krajowego stanowiącego podstawę prawną takiego działania, np. ustawa o policji, prokuraturze, komornikach sądowych, kodeks postępowania cywilnego, kodeks postępowania karnego, ustawa o systemie ubezpieczeń społecznych.

Udostępnienie danych osobowych może nastąpić także między innymi w przypadku, gdy osoba, której dane dotyczą, wyrazi zgodę na udostępnienie jej danych. Tak jak w przypadku przekazywania danych innemu podmiotowi w wykonaniu umowy przekazania danych, zbycia danych, współadministrowania organizacja musi zabezpieczyć dane osobowe przed dostępem osób nieuprawnionych (np. poprzez zastosowanie szyfrowania). Każda organizacja dokonuje samodzielnie oceny zasadności wniosku o udostępnienie danych osobowych. W tym celu musi ustalić istnienie podstawy prawnej udostępnienia

danych osobowych. W przypadku braku podstawy prawnej udostępnienia danych osobowych, może odmówić ich udostępnienia.

4. Współadministrowanie.

Może dojść do sytuacji, gdy dwie lub więcej organizacji społecznych w celu realizacji wspólnych dla nich celów statutowych będą organizowały wspólnie np. kampanie społeczne, wydarzenia publiczne. Wówczas organizacje te będą wspólnie decydowały i ustalały cele i sposoby przetwarzania. Będą one współadministratorami. Wówczas organizacje, jako współadministratorzy, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO w zakresie określonym w art. 26 RODO.

Uzgodnienia współadministratotrów powinny określać m.in.:

a) zasady spełnienia obowiązku informacyjnego wobec osób, których dane są przetwarzane,
b) zasady i sposoby wzajemnej komunikacji pomiędzy współadministratorami.

Wszystkie uzgodnienia między administratorami powinny być podane do wiadomości osób, których dane są przetwarzane. Może to nastąpić w klauzuli informacyjnej wysyłanej/udostępnianej osobom, których dane są przetwarzane. W informacji takiej powinny się znaleźć wszystkie informacje wymagane przez art. 13 lub 14 RODO, a osoba, której dane dotyczą, może wykorzystywać przysługujące jej prawa wynikające z RODO wobec każdego z administratorów.

Obie organizacje, będące współadministratorami, zobowiązane są do zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi wynikające z przepisów prawa i chroniło prawa osób, których dane dotyczą. Wystarczające gwarancje organizacje mogą wykazać między innymi poprzez uzyskanie statusu podmiotu przestrzegającego Kodeksu. Zawierając umowy o współadministrowanie danymi, organizacje przestrzegające Kodeksu mogą stosować postanowienia zawarte we wzorze umowy o współadministrowanie danymi osobowymi, stanowiącym Załącznik nr 2 do Kodeksu. Wzór umowy o współadiministrowanie danymi osobowymi każdorazowo powinien zostać poddany analizie i dostosowany do zakresu, rodzaju i kontekstu przetwarzania danych osobowych. Organizacja może korzystać z własnych wzorów.

5. Informacja publiczna.

Organizacje społeczne mogą być podmiotami zobowiązanymi do udostępnienia informacji publicznej, pod warunkiem, że dysponują one środkami publicznymi w formie dotacji, grantów lub w innych formach lub gdy wykonują zadania publiczne.

Obowiązek udostępniania informacji publicznej przez organizacje pozarządowe wynika z art. 4a–art. 4c ustawy z dnia 24 kwietnia 2003 roku o działalności pożytku publicznego i wolontariacie (Dz.U. z 2020 r. poz. 1057 t.j.). Również w orzecznictwie sądów administracyjnych przyjął się pogląd, zgodnie z którym, jeżeli dany podmiot wykonuje zadania publiczne, jest to wystarczające by uznać, że zobowiązany jest do udostępnienia informacji publicznych. (np. Wyrok WSA w Warszawie z dnia 9 maja 2019 r., sygn. VIII SAB/Wa 10/19).

Kto może żądać informacji publicznej?

Każdy obywatel ma prawo do uzyskiwania informacji: (1) o działalności organów władzy publicznej oraz (2) osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. Uprawnienie to wynika wprost z art. 61 Konstytucji Rzeczpospolitej Polskiej. Konkretyzuje go ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2019.1429 z pózn.zm.). Prawo dostępu do informacji publicznej przysługuje według ustawy każdemu, tak więc zarówno osobie fizycznej, jak i podmiotowi prawa prywatnego.

Na jakich zasadach organizacja udziela informacji publicznej?

Udostępnianie informacji publicznej następuje:
1. poprzez ogłaszanie informacji publicznej w Biuletynie Informacji Publicznej na zasadach, o których mowa w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2019 r. poz. 1429 z pózn.zm.) albo
2. poprzez ogłaszanie informacji publicznej na stronie internetowej organizacji pozarządowych oraz podmiotów, o których mowa w art. 4a działalności pożytku publicznego i wolontariacie, albo
3. na wniosek na zasadach, o których mowa w ustawie z dnia 6 września 2001 roku o dostępie do informacji publicznej.

Jakie informacje są informacjami publicznymi, a których nie zalicza się do katalogu informacji publicznych?

Katalog informacji publicznej określa art. 6 ustawy o dostępie do informacji publicznej. Będą to informacje o organach i osobach sprawujących w nich funkcje, zarobkach osób pełniących funkcje publiczne, kompetencjach tych osób, strukturze własnościowej podmiotów, majątku, treść aktów administracyjnych i innych rozstrzygnięć, dokumentacja przebiegu i efektów kontroli oraz wystąpienia, stanowiska, wnioski i opinie podmiotów ją przeprowadzających, a także stanowiska w sprawach publicznych zajęte przez organy władzy publicznej i przez funkcjonariuszy publicznych.

<u>Przykłady informacji uznanych za informację publiczną.</u>

Informacją publiczną będą:
- treść umów cywilnoprawnych, dotyczących majątku publicznego (wyroki WSA w Poznaniu z 24 marca 2006 r.,IV SA/Po 224/06 oraz WSA w Warszawie z 16 listopada 2004 r.,II SAB/Wa 238/04, wyrok NSA z 11 grudnia 2014 r.,I OSK 213/14, LEX nr 1622184),
- mapy stanowiące załączniki graficzne do studium uwarunkowań i kierunków zagospodarowania przestrzennego i będące jego integralną częścią są informacją publiczną. wyrok NSA z 30 sierpnia 2011 r.,I OSK 1048/11),
- informacja o charakterze archiwalnym, niezależnie od daty jej wytworzenia

- informacja o kosztach ponoszonych przez daną jednostkę w związku z używaniem przez pracowników służbowych telefonów komórkowych jest informacją publiczną, dotyczy bowiem majątku publicznego (wyrok WSA we Wrocławiu z 13 czerwca 2013 r.,IV SAB/Wr 51/13).

Przykłady informacji nieuznanych za informację publiczną.

Informacją publiczną nie będą:
- wnioski w sprawie indywidualnej oraz polemiki z dokonanymi ustaleniami (wyrok NSA z 12 lipca 2011 r., I OSK 610/11),
- interpretacje znanego stronie dokumentu,
- projekt uchwały organów danej jednostki (wyrok WSA z 16 grudnia 2004 r.,IV SA/Wr 241/04, Sąd w orzeczeniu tym wyjaśnił, że informacja tylko wtedy ma charakter informacji publicznej, jeżeli jest to informacja istniejąca i będąca w posiadaniu organu, od którego wnioskodawca żąda jej udostępnienia,
- konkretne indywidualne sprawy danej osoby o charakterze prywatnym lub podmiotu niebędącego władzą publiczną lub innym podmiotem wykonującym zadania publiczne, (wyrok NSA OZ w Katowicach z 25 czerwca 2002 r., II SA/Ka 655/02),
- numer telefonu komórkowego pracownika. Nie można uznać zestawu liczb, jakim jest numer służbowego telefonu komórkowego, za informację publiczną (zob. wyrok NSA z 28 sierpnia 2015 r.I OSK 1700/14i z 14 października 2015 r.,I OSK 2056/14),
- dokumenty wewnętrzne, na przykład korespondencja mailowa osoby wykonującej zadania publiczne ze współpracownikami, nawet jeżeli w jakiejś części dotyczy wykonywanych przez tę osobę zadań publicznych (wyroki NSA z 21 czerwca 2012 r.,I OSK 666/12, z 14 września 2012 r.,I OSK 1203/12 i z 25 marca 2014 r.,I OSK 2320/13, LEX nr 1487793);
– pisemne wyjaśnienia złożone przez pracowników organu, które mają charakter porządkowy i dotyczą sposobu wykonywania obowiązków służbowych (wyrok NSA z 17 października 2013 r.,I OSK 1105/13),
– opinie prawne i ekspertyzy będące podstawą podjęcia decyzji. Dokumenty takie są dokumentami wewnętrznymi, służącymi gromadzeniu informacji, które w przyszłości mogą zostać wykorzystane w procesie decyzyjnym. Mają charakter poznawczy i nie odnoszą się wprost do przyszłych działań i zamierzeń podmiotu zobowiązanego, mają jedynie poszerzyć zakres wiedzy i informacji posiadanych przez ten podmiot (wyroki NSA z 29 lutego 2012 r.,I OSK 2196/11 i z 11 marca 2014 r.,I OSK 118/14),
– materiały szkoleniowe i informacyjne (wyrok NSA z 4 lutego 2015 r.,I OSK 502/14),
– dokumenty o charakterze wewnętrznym, np. karty drogowe. Dotyczą wyłącznie kwestii organizacji pracy w zakresie rozliczania czasu pracy pracowników uprawnionych do używania pojazdów służbowych przy wykonywaniu obowiązków pracowniczych (wyrok NSA z 21 sierpnia 2013 r.,I OSK 681/13),
- dokumenty prywatne, nawet jeśli znajdują się w posiadaniu podmiotu zobowiązanego do udzielania informacji publicznej i w jakimś stopniu dotyczą „sprawy publicznej" w rozumieniu art. 1 ust. 1, bo w związku z nią zostały zgromadzone (wyrok NSA z 11 maja 2006 r.,II OSK 812/05, wyrok NSA z 11 maja 2011 r.,I OSK 189/11).
Orzecznictwo sądów administracyjnych dotyczące dokumentu wewnętrznego zaakceptował Trybunał Konstytucyjny, który w wyroku z 13 listopada 2013 r.,P 25/12(Dz.U. poz. 1435, OTK-A 2013, nr 8, poz. 122) stwierdził, że: „z szerokiego zakresu przedmiotowego informacji publicznej wyłączeniu podlegają jednak treści zawarte w dokumentach wewnętrznych, rozumiane jako informacje o charakterze roboczym (zapiski, notatki), które zostały utrwalone w formie tradycyjnej lub elektronicznej i stanowią pewien proces myślowy, proces rozważań, etap wypracowywania finalnej koncepcji".

Informacja publiczna a prawo do prywatności i przepisy RODO.

Niejednokrotnie informacje publiczne pokrywają się z prawem do ochrony danych osobowych oraz prawem do prywatności. Wówczas należy zastosować art. 86 RODO, który stanowi, że dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy Rozporządzenia RODO.

Takim przepisem krajowym jest art. 1 ust. 2 ustawy o dostępie do informacji publicznej, który stanowi, że przepisy tej ustawy nie naruszają przepisów innych ustaw określających odmienne zasady i tryb dostępu do informacji będących informacjami publicznymi. Oznacza to, że przepisy dotyczące ochrony danych osobowych mają tu pierwszeństwo.

RODO nie ogranicza stosowania polskich przepisów o dostępie do informacji publicznej. Ponadto RODO nie może być podstawą do odmowy jej udostępniania. W najnowszym orzecznictwie stoi się na stanowisku, że: „w razie kolizji między zasadą jawności informacji publicznych a ochroną prywatności i danych osobowych osób fizycznych, dopuszczalny będzie jedynie taki sposób udostępniania informacji publicznej, który nie naruszy dóbr chronionych (np. anonimizacja danych wrażliwych). W przypadku, gdy pomimo dokonania takiego zabiegu, możliwa będzie identyfikacja osoby, której dane dotyczą, należy odmówić udostępnienia informacji publicznej" (Wyrok Wojewódzkiego Sądu Administracyjnego w Krakowie z dnia 9 kwietnia 2019, II SA/Kr 133/19).

Organizacja jako podmiot żądający dostępu do informacji publicznej.

Prawo dostępu do informacji publicznej przysługuje według ustawy każdemu, tak więc zarówno osobie fizycznej, jak i podmiotowi prawa prywatnego. W związku z powyższym organizacja społeczna może również wystąpić z wnioskiem o informację publiczną.

Dane o obywatelach, na mocy art. 51 ust. 2 Konstytucji, mogą być udostępniane osobom trzecim jedynie w zakresie niezbędnym w demokratycznym państwie prawnym, przy czym każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych.

W związku z powyższym dostęp do umów jest możliwy, jednak powinno to być czynione w formie zanonimizowanej przez wyłączenie z ich treści określonych danych osobowych w postaci brzmienia imion i nazwisk wykonawców określonych umów zlecenia lub umów o dzieło, daty ich urodzenia, miejsca zamieszkania, stanu zdrowia, stanu cywilnego i innych informacji, które są chronione przepisami prawa o ochronie danych osobowych zawartych w RODO a także przez art. 51 Konstytucji.

Organ administracji publicznej nie powinien ujawniać również daty urodzenia osoby, która jest stroną umowy, miejsca zamieszkania strony umowy, ponieważ nie są to informacje, których zakres jest niezbędny do uzyskania przez osobę trzecią w demokratycznym państwie prawnym i nie wpływają na istotę udostępnianej informacji publicznej.

Organ administracji publicznej nie może odmówić organizacji społecznej dostępu do danych ujawniających wynagrodzenie osoby pełniącej funkcję publiczną. Jednak przy ujawnieniu tego typu informacji podmiot władzy publicznej powinien brać pod uwagę następujące zasady:

1. za każdym razem podmiot zobowiązany musi ustalić, czy mamy do czynienia z osobą/osobami pełniącymi funkcję publiczną w rozumieniu art. 5 ust. 2 ustawy o dostępie do informacji publicznej, korzystając z interpretacji wyroku Trybunału Konstytucyjnego o sygn. akt. K 17/05,
2. Jeśli zapytanie dotyczy osoby pełniącej funkcję publiczną, należy podać dokładne jej wynagrodzenie, jakie otrzymuje ze środków publicznych
3. Jeśli jednak w składniku wynagrodzenia znajdują się inne składniki lub potrącenia, które są objęte prywatnością w zakresie wykraczającym poza związek z pełnioną funkcją publiczną, wtedy ten element nie podlega ujawnieniu.

Powyższe zasady oparte są na uzasadnieniu wyroku Naczelnego Sądu Administracyjnego z dnia 18 lutego 2017 r. o sygn. akt I OSK 796/14, dotyczącego kontroli procesu realizacji prawa do informacji publicznej. NSA w uzasadnieniu wyroku stwierdził, że: „udzielenie informacji publicznej w postaci danych o wysokości wynagrodzenia osób zatrudnionych w jednostkach finansowanych ze środków publicznych (zarówno pełniących funkcje publiczne, jak też personelu pomocniczego) zazwyczaj nie musi wiązać się z koniecznością ingerencji w ich prawnie chronioną sferę prywatności. Dzieje się tak przede wszystkim wówczas, gdy w danym podmiocie na określonym stanowisku zatrudnionych jest kilka osób. Udostępnienie informacji publicznej polega, bowiem na ujawnieniu wysokości wynagrodzenia wypłacanego na określonym stanowisku, bez wskazywania danych osobowych konkretnej osoby".

NSA nie uwzględnił jednak sytuacji, gdy na danym rodzaju stanowiska może zasiadać tylko jedna osoba. W takiej sytuacji również należy udzielić informacji o wynagrodzeniu, ale bez podania imienia i nazwiska osoby oraz z wyłączeniem ujawniania takich składników wynagrodzenia, które wykraczają poza związek z pełnioną funkcją publiczną.

Organ administracji publicznej może odmówić wydania oryginału lub kserokopii umowy o pracę osoby pełniącej funkcję publiczną. Umowa taka może zawierać bowiem tajemnice chronione prawem, chociaż nie oznacza to, że nie może być uznana za informację publiczną. Jednak prawo do jej uzyskania może być stosownie ograniczone poprzez zastosowanie art. 5 ustawy o dostępie do informacji publicznej, np. ze względu na prywatność osoby fizycznej, ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych.

Na takim stanowisku stoi również orzecznictwo sądów administracyjnych. Prawo do informacji obejmuje prawo dostępu do informacji publicznej, nie zaś prawo domagania się doręczenia samego egzemplarza dokumentu. Fakt, że część informacji będzie stanowiła informację publiczną a część informacje prawem chronione nie może przesądzić o konieczności doręczenia wnoszącemu o udzielenie informacji publicznej tychże dokumentów lub ich kserokopii i to w całości (np. Wyrok NSA z dnia 19 sierpnia 2008 roku, sygn. akt I ISK 683/09).

ROZDZIAŁ VI.
OCENA RYZYKA i ŚRODKI BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

1. Ogólna ocena ryzyka i dobór metod adekwatnych do przetwarzania danych.

Organizacja przed rozpoczęciem przetwarzania danych osobowych powinna przeprowadzić ocenę ryzyka jakie przetwarzanie może spowodować zarówno dla praw i wolności osób, których te dane dotyczą, jak i dla organizacji, biorąc pod uwagę potencjalne negatywne skutki. W tym celu organizacja powinna podjąć działania w celu identyfikacji ryzyka związanego z przetwarzaniem, jego oceny pod kątem źródła, charakteru, prawdopodobieństwa i wagi oraz doboru środków pozwalające zminimalizować to ryzyko.

Organizacja powinna przeprowadzić ocenę ryzyka w szczególności w następujących sytuacjach:

a) przed wprowadzeniem nowej grupy odbiorców (osób, których dane zamierza przetwarzać),
b) przed wprowadzeniem realizacji nowego celu statutowego (nowej inicjatywy: prowadzenie konferencji, akcji społecznych, wydarzeń publicznych, kierowanie do odbiorców nowych produktów, np. publikacji, broszur, książek itp.),
c) przed zakupem bazy danych od innych podmiotów,
d) przed wprowadzeniem nowych systemów informatycznych, w których będą przetwarzane dane,
e) przed przekazywaniem danych do państwa trzeciego (poza Europejski Obszar Gospodarczy),
f) gdy zachodzi zautomatyzowane przetwarzanie, w tym profilowanie, i jest to podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną,
g) gdy zachodzi przetwarzanie na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10 RODO lub
h) gdy zachodzi systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie,
i) gdy doszło do naruszenia ochrony danych osobowych, np. poprzez przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,
j) w sytuacji, gdy stwierdzi, że przetwarzanie ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Przy ogólnej ocenie ryzyka każda organizacja powinna:

1. określić zagrożenia, które mogą pojawić się w związku z przetwarzaniem danych osobowych, mając na względzie sytuacje opisane powyżej.

Konieczna jest ocena, jakie jest prawdopodobieństwo wystąpienia zagrożeń lub jakie mogą one pociągnąć za sobą skutki. Znając ryzyko, administrator danych może podjąć działania zmierzające ku ich obniżeniu.

Przy tej ocenie należy kierować się Wytycznymi Grupy Roboczej Art. 29, dotyczącymi oceny skutków dla ochrony danych oraz pomagającymi ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679. Pomocny jest również dwuczęściowy poradnik przygotowany przez Prezesa Urzędu Ochrony Danych Osobowych (dawniej GIODO), pt. *Jak rozumieć podejście oparte na ryzyku według RODO? (cz. 1) oraz Jak stosować podejście oparte na ryzyku? (cz. 2)* – dostępny na stronie internetowej Urzędu.

Grupa Robocza Art. 29 (obecnie Europejska Rada Ochrony Danych) podaje przykład niedopuszczalnego wysokiego ryzyka. Obejmuje ono przypadki, w których osoby, których dane dotyczą, mogą ponieść znaczne lub nawet nieodwracalne konsekwencje, z którymi nie będą mogły sobie poradzić (np.: bezprawne uzyskanie dostępu do danych prowadzące do zagrożenia życia osób, których dane dotyczą, zwolnienie, zagrożenie o charakterze finansowym) lub w których wydaje się oczywiste, że wystąpi ryzyko (np.: ograniczenie liczby osób mających dostęp do danych nie jest możliwy ze względu na sposób ich udostępniania, wykorzystywania lub rozprowadzania lub gdy luka w zabezpieczeniach, o której istnieniu wiadomo, nie zostanie usunięta).

2. dokonać identyfikacji swoich zasobów tj. określić wszystko to, co ma wartość dla organizacji i ma lub może mieć związek z bezpieczeństwem danych osobowych.

   W tym przypadku należy zidentyfikować zasoby tj. dokonać spisu budynków, w których przetwarzane są dane osobowe, systemów informatycznych, w których przetwarzane są dane osobowe, sprzętu elektronicznego służącego do przetwarzania informacji, stron internetowych, oprogramowania, zbiorów danych osobowych prowadzonych zarówno w formie papierowej, jak i elektronicznej. Zalecane jest dokonanie jak najbardziej szczegółowej identyfikacji zasobów, tak aby w dalszej kolejności możliwe było jak najbardziej precyzyjne określenie ryzyka wystąpienia zagrożeń do ochrony danych.

   Każda organizacja przy określeniu swoich zasobów ocenia ewentualną jego podatność na ryzyko naruszenia danych osobowych, opisując przy danym zasobie źródło zagrożeń. Może to być brak wystarczających zabezpieczeń wejścia do budynku poprzez kodowanie wejścia, niedokładnie opracowany proces zarządzania systemami informatycznymi, brak zabezpieczeń przy wykorzystywaniu wspólnych dla pracowników dysków sieciowych, na których przechowywane są dane – tzw. zagrożenia wewnętrzne. Może to być również włamanie do budynku, lokalu organizacji, kradzież, powódź, pożar, przerwa w dostawie energii elektrycznej – zagrożenia zewnętrzne.

3. wprowadzić kryteria minimalizowania ryzyka i zapewnienie bezpieczeństwa przetwarzania danych

   Podczas wprowadzania tych kryteriów należy przede wszystkim:
   - określić, w jakim stopniu naruszenie danego zasobu w organizacji będzie miało wpływ na prawa i wolności osób, których dane dotyczą,

- określić, w jakim stopniu brak dostępu do zasobu, w założonym okresie, może spowodować zagrożenie praw i wolności osób, których dane dotyczą.

Dla każdego zagrożenia można określić odpowiednie działania. Przykładowymi działaniami mogą być:
- wprowadzenie zasady wykonywania codziennie kopii bezpieczeństwa,
- wprowadzanie szyfrowanych wiadomości
- zaszyfrowanie pliku z dokumentacją znajdującą się na wspólnym dysku sieciowym i upoważnienie do dostępu do pliku tylko kilku osób z niego korzystających
- określenie metody i częstotliwości sprawdzania obecności wirusów oraz metody ich usuwania,
- oznaczenie dwóch niezależnych od siebie miejsc przechowywania nośników informatycznych, w tym również wydruków,
- określenie codziennego dokonywania przeglądów i konserwacji systemów
- określenie cotygodniowego wykonywania kontroli spójności danych osobowych w systemach lub częściej, jeżeli wymaga tego zaobserwowany sposób pracy systemu.

2. Ocena skutków dla ochrony danych

.

Ocena skutków dla ochrony danych jest obowiązkowa w każdy wypadku, gdy istnieje wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą. W organizacjach społecznych podczas większości czynności przetwarzania administrator nie będzie miał obowiązku przeprowadzania procesu oceny skutków dla ochrony danych. Czynności przetwarzania danych osobowych w granicach niezbędnych do zbierania funduszy na działalność organizacji, wpłat od darczyńców, zaproszeń na wydarzenia publiczne, akcje społeczne, konkursy, prelekcje i wykłady, kontakty z członkami i byłymi członkami organizacji, jak również wysyłka materiałów promujących działalność organizacji społecznej co do zasady nie wiążą się z dużym prawdopodobieństwem wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

Jednak istnieją przypadki, gdy procesy przetwarzania danych mogą wiązać się z wysokim prawdopodobieństwem ryzyka naruszenia praw i wolności osób, których dane dotyczą. Będzie to dotyczyło m.in. takich sytuacji, gdy:

a) organizacja społeczna będzie zbierała w sposób systematyczny na masową skalę dane osobowe wrażliwe lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, niezależnie od źródła ich pochodzenia, czyli zarówno gdy dane zbierane są bezpośrednio od osoby oraz wówczas, gdy są pozyskiwane z innych źródeł np. z baz dostępnych publicznie albo zakupionych od podmiotu trzeciego,
b) organizacja będzie dokonywała w sposób kompleksowy i systematyczny zautomatyzowanego przetwarzania, w tym profilowania, np. oceny preferencji osobistych danej osoby, sytuacji ekonomicznej, zdrowia, zainteresowań itp., i będzie to podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną.

W przypadku gdy organizacja planuje przetwarzanie mogące powodować wysokie ryzyko dla praw i wolności osób, których dane dotyczą, w szczególności jeśli organizacja stwierdzi możliwość wystąpienia

wyżej opisanych sytuacji, powinna dokonać szczególnej oceny ryzyka, jakie wiąże się tymi czynnościami, tj. oceny skutków dla ochrony danych. Ocena taka będzie w każdej organizacji inna, w zależności od zakresu jej działalności i wystąpienia możliwych sytuacji stwarzających wysokie zagrożenie dla praw osób, których dane dotyczą.

W ramach oceny skutków dla ochrony danych organizacja powinna podjąć następujące czynności:

1. wybrać metodykę dokonywania oceny skutków dla ochrony danych, która spełnia kryteria określone w załączniku 2 Wytycznych Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych oraz pomagających ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, lub określić i wdrożyć systematyczny proces dokonywania oceny skutków dla ochrony danych, który jest zgodny z kryteriami zawartymi w załączniku 2 Wytycznych Grupy Roboczej Art. 29, dotyczących oceny skutków dla ochrony danych oraz pomagających ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679,

   Dokonanie opisu wszystkich możliwych czynników wpływających na prawdopodobieństwo wystąpienia lub na wielkość skutków naruszenia praw i metod adekwatnych do przetwarzania danych jest niewykonalne. W związku z powyższym decyzję o odpowiedniej metodyce ochrony danych i oceny skutków każda organizacja podejmuje samodzielnie, kierując się przy tym Wytycznymi Grupy Roboczej Art. 29, dotyczącymi oceny skutków dla ochrony danych oraz pomagającymi ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679.
2. konsultować się przy ocenie skutków dla ochrony danych z inspektorem ochrony danych, jeżeli został on wyznaczony przez organizację,
3. przedłożyć właściwym organom nadzorczym sprawozdanie z oceny skutków dla ochrony danych, gdy jest to wymagane,
4. konsultować się z organem nadzorczym, jeżeli określenie środków wystarczających do zminimalizowania wysokiego ryzyka zakończyło się niepowodzeniem, tj. jeżeli w toku oceny skutków dla ochrony danych ujawniono istnienie wysokiego ryzyka albo gdy organizacja nie może znaleźć środków wystarczających do zmniejszenia ryzyka do dopuszczalnego poziomu organizacja zobowiązana jest zwrócić się do organu nadzorczego o uprzednie konsultacje dotyczące przetwarzania.
5. okresowo dokonywać przeglądu oceny skutków dla ochrony danych i przetwarzania, którego oceny dokonano w jej ramach, przynajmniej gdy doszło do zmiany ryzyka wynikającego z przetwarzania operacji
6. dokumentować podjęte decyzje.

3. Środki techniczne i organizacyjne

Środki techniczne i organizacyjne są niezbędne każdej organizacji do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Na podstawie dokonanej oceny ryzyka każda organizacja ustala możliwe do zastosowania środki bezpieczeństwa i ocenia koszt ich wdrażania.

Do elementów zabezpieczenia danych osobowych w organizacjach zalicza się:

a) stosowane metody ochrony pomieszczeń, w których przetwarzane są dane osobowe (zabezpieczenia fizyczne),
b) opracowanie i aktualizacja polityki ochrony danych osobowych oraz instrukcji zarządzania systemami informatycznym służącymi do przetwarzania danych osobowych, powołanie i nadzór inspektora ochrony danych osobowych (zabezpieczenie organizacyjne i prawne),
c) odpowiednie środki zabezpieczenia danych w systemach informatycznych (zabezpieczenia techniczne).

Zabezpieczenia fizyczne

Przykładowe zabezpieczenia fizyczne w organizacji obejmują:

a. wydzielenie obszaru przetwarzania danych,
b. nadzorowanie dostępu do pomieszczeń przez portiera, ochronę budynku lub monitorowany przez kamery system zainstalowany w budynku, w którym znajduje się siedziba organizacji,
c. dostęp do pomieszczeń organizacji wyłącznie dla osób upoważnionych, wstęp osób postronnych jest możliwy jedynie podczas obecności pracowników organizacji,
d. dodatkowe zabezpieczenie części biurowej zaplecza technicznego poprzez wydzielenie pomieszczenia serwerowni, z dostępem tylko dla osób upoważnionych,
e. przechowywanie akt w wersji papierowej w specjalnie do tego celu przeznaczonych pomieszczeniach, w zamykanych na klucz szafach,
f. kopie zapasowe zbioru danych osobowych przechowywane są w sejfie lub w szafie pancernej w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco,
g. w pomieszczeniu, w którym znajduje się serwerownia, uruchomiony jest ciągły system kontroli warunków klimatycznych (temperatura, wilgotność, zasilanie, dym) z powiadomieniem SMS w przypadku przekroczenia wartości granicznych,
h. budynki, w których odbywa się przetwarzanie danych osobowych, dodatkowo są zabezpieczone przez system alarmowy.

Zabezpieczenia techniczne

Przykładowe zabezpieczenia techniczne w organizacji obejmują:

a. mechanizmy kontroli dostępu do systemów informatycznych i ich zasobów; nadawanie różnych uprawnień dla różnych grup użytkowników;
b. zastosowanie odpowiednich i regularnych aktualizacji narzędzi ochronnych (firewall, system antywirusowy);
c. system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem;
d. dane wykorzystywane do uwierzytelnienia są przesyłane w sieci publicznej przy wykorzystaniu VPN (CheckPoint),
e. tworzenie regularnych kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych oraz kopii programów służących do przetwarzania danych osobowych;

f. zastosowanie zabezpieczeń systemu przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (UPS-y w szafach teleinformatycznych oraz UPS-y przy stanowiskach, gdzie są przetwarzane dane osobowe),
g. wdrożenie ochrony sprzętu komputerowego (serwery, komputery osobiste, w tym laptopy i inne urządzenia zewnętrzne), oprogramowania, danych osobowych zapisanych na informatycznych nośnikach danych oraz danych przetwarzanych w systemach informatycznych, haseł użytkowników, baz danych i kopii zapasowych, wydruków, dokumentacji papierowej zawierającej dane osobowe;
h. przechowywanie nośników danych w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczających je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych);
i. zamykanie dokumentów na klucz, np. w szafach, biurkach, sejfach podczas nieobecności w pomieszczeniach lub po zakończeniu pracy (tzw. polityka czystego biurka);
j. niszczenie dokumentów i tymczasowych wydruków w niszczarce, niezwłocznie po ustaniu celu ich przetwarzania;
k. nie pozostawianie wydruków i ksero na urządzeniach lub w ich okolicy bez nadzoru;
l. analizowanie w miarę potrzeb zagrożenia i ryzyka w celu weryfikacji środków zabezpieczających. W szczególności taka analiza będzie dokonywana w każdym przypadku istotnych zmian działania lub struktury organizacji. Oprócz tego będzie w miarę potrzeb dokonywać inwentaryzacji systemów informatycznych i czynności przetwarzania danych osobowych.

Szczególną uwagę należy zwrócić na korzystanie przez organizację z usług w chmurze obliczeniowej.

Chmura obliczeniowa (również przetwarzanie w chmurze lub *cloud computing*) to model przetwarzania oparty na użytkowaniu usług dostarczonych przez usługodawcę (podmiot zewnętrzny ale również dział np. informatyczny danej organizacji), bez konieczności zakupu licencji, instalowania i administrowania oprogramowaniem. Podmiot, który podejmuje decyzję o skorzystaniu z usług w chmurze, np. organizacja pozarządowa (usługobiorca) opłaca jedynie użytkowanie, dostęp do określonej usługi.

Korzystanie z tzw. chmury polega na elektronicznym przetwarzaniu danych za pomocą usług dostępnych zdalnie przez sieć komputerową lub Internet.

Usługa chmurowa polega na przeniesieniu ciężaru świadczenia usług informatycznych (danych, oprogramowania lub mocy obliczeniowej) na serwer i umożliwienie stałego dostępu do niego. Po zalogowaniu się z jakiegokolwiek urządzenia z dostępem do Internetu, można rozpocząć korzystanie z usług w chmurze.

Chmury dostępne na rynku można podzielić na trzy rodzaje:

a. publiczne, będące zewnętrznym, ogólnie dostępnym dostawcą, są własnością firm zewnętrznych i są dostępne dla każdego, kto chce z nich korzystać,

b. prywatne tworzone w obrębie własnej sieci komputerowej organizacji i tylko w niej udostępniane,

c. mieszane, będące połączeniem chmury prywatnej i publicznej. Część aplikacji i infrastruktury pracuje w chmurze prywatnej, a część w przestrzeni publicznej.

Usługa Chmury a przepisy RODO.

Organizacjom przystępującym do Kodeksu zaleca się ostrożne korzystanie z usług chmurowych, w szczególności w przypadku przetwarzania danych, które organizacja zamierza przetwarzać w tzw. chmurach publicznie dostępnych. Korzystanie bowiem z usług chmurowych wiąże się z potencjalnym ryzykiem, że do danych może mieć dostęp osoba niepowołana. Organizacja jako administrator może nie mieć pełnej wiedzy w zakresie miejsc przechowywania danych i tego, kto po stronie usługodawcy uzyskuje do nich wgląd.

Przy wyborze dostawcy usług chmurowych zaleca się:
1. kierować się gwarancjami bezpieczeństwa i zgodności z przepisami, które usługodawca jest w stanie zapewnić. Odpowiednie gwarancje powinny być częścią umowy z usługodawcą, powinny być wyrażone w formie oświadczenia, o ile to możliwe popartych dowodami, np. uzyskanymi certyfikatami.
2. analizę postanowień umownych oraz regulaminu usług. Powinien przeprowadzić ją informatyk i inspektor ochrony danych osobowych, jeśli został powołany oraz prawnik,
3. podpisać umowę powierzenia danych osobowych, zgodnie z wymaganiami art. 28 RODO, jeśli dostawca nie chce podpisać umowy nie należy wybierać jego usług,
4. wybierać dostawców, którzy gwarantują, że przetwarzanie odbywa się w krajach EOG,
5. wybierać dostawców spoza obszaru EOG na podstawie pozytywnej decyzji Komisji Europejskiej. Oznacza to, że należy wybierać dostawców z krajów, które zostały uznane przez Komisję Europejską za dające wystarczające gwarancje bezpieczeństwa. Wówczas takie przetwarzanie nie wymaga specjalnego zezwolenia. Komisja publikuje w *Dzienniku Urzędowym Unii Europejskiej* i na swojej stronie internetowej wykaz państw trzecich, co do których przyjęła decyzję stwierdzającą odpowiedni stopień ochrony lub jego brak.
6. wybierać dostawców - w razie braku powyższej decyzji Komisji Europejskiej wyłącznie, gdy dostawcy spoza obszaru EOG zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia, o których mowa można zapewnić za pomocą:
a. standardowych klauzul ochrony danych przyjętych przez Komisję Europejską,
b. tzw. standardowych klauzul umownych (SCC, *standard contractual clauses).* W tym celu należy zawrzeć z dostawcą spoza EOG odpowiednią umowę zawierającą konkretne wzorce postanowień umownych. Dodatkowym warunkiem jest przyjęcie klauzul przez właściwy organ nadzorczy i zatwierdzonych przez Komisję,
c. klauzul umownych między administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej, pod warunkiem uzyskania zezwolenia właściwego organu nadzorczego,
7. przed wyborem właściwego dostawcy chmury kierować się zasadami określonymi w art. 45 i 46 RODO,
8. przed wyborem dostawcy chmury należy sprawdzić na stronie internetowej Komisji Europejskiej lub w *Dzienniku Urzędowym Unii Europejskiej* wykaz państw trzecich, terytoriów i określonych sektorów w państwie trzecim oraz organizacji międzynarodowych, co do których Komisja przyjęła decyzję stwierdzającą odpowiedni stopień ochrony lub jego brak.
Zaleca się podstawowe wymogi bezpieczeństwa chmury:

1. Tworzenie lokalnych kopii zapasowych,

2. Zmienianie regularnie hasła / haseł dostępu do chmury, korzystanie z menadżera haseł,
3. Unikanie – w miarę możliwości – przechowywania danych wrażliwych,
4. Szyfrowanie danych w chmurze (najlepiej przed umieszczeniem w chmurze)
5. Dwuskładnikowe uwierzytelnianie (potwierdzenie tożsamości użytkowników chmury), a więc nie tylko przez login i hasło, ale również przy użyciu innego składnika np. PIN. kodu wysłanego przez usługodawcę za pomocą wiadomości SMS.

Zabezpieczenia organizacyjne i prawne

Przykładowe zabezpieczenia organizacyjne i prawne w organizacji obejmują:

a. powołanie Inspektora Ochrony Danych (IOD) oraz Administratora Systemów Informatycznych (ASI),
b. odpowiednie upoważnienie pracowników organizacji na bieżąco kontrolujących pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą, o zaobserwowanych nieprawidłowościach informują IOD oraz ASI;
c. pouczanie i instruowanie osób, które dopuściły się uchybień, a także wydawanie im poleceń mających na celu przywrócenie stanu prawidłowego, przez Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych lub inne osoby upoważnione przez Administratora Danych, przy czym ASI posiada to uprawnienie wyłącznie odnośnie korzystania z systemu informatycznego;
d. informowanie Inspektora Ochrony Danych lub Administratora Danych przez Administratora Systemów Informatycznych o przypadkach naruszeń ochrony danych osobowych w organizacji;
e. utrzymywanie w tajemnicy danych osobowych i sposobów ich zabezpieczenia przez pracowników mających dostęp do danych osobowych, które są w dyspozycji organizacji (w tym celu pracownicy mający dostęp do danych osobowych podpisują oświadczenie o utrzymywaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia);
f. przetwarzanie danych osobowych jest wykonywane wyłącznie przez osoby, które zostały upoważnione do przetwarzania danych osobowych
g. upoważnienie do przetwarzania danych osobowych osób przetwarzających dane osobowe poprzez wpisanie określonych kompetencji do zakresu obowiązków na danym stanowisku oraz prowadzenie i aktualizowanie ewidencji osób upoważnionych do przetwarzania danych osobowych,
h. wprowadzenie Polityki Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym; przykładowe wzory wymienionych wyżej dokumentów stanowią odpowiednio Załącznik nr 3 i 4 do niniejszego kodeksu.

Ad. a) powołanie Inspektora Ochrony Danych Osobowych.

Zgodnie z art. 37 ust. 1 RODO wyznaczenie inspektora ochrony danych jest obowiązkowe zawsze gdy:

1. przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości (art. 37 ust. 1 a RODO)

2. główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę (art. 37 ust. 1 b RODO)
lub
3. główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 (art. 37 ust. 1 c RODO)

Mając powyższe na uwadze, przed podjęciem decyzji o wyznaczeniu inspektora danych osobowych konieczne jest ustalenie, czy działalność organizacji odpowiada którejś z przesłanek wymienionych w art. 37 RODO – przy czym należy zwrócić uwagę, iż treść art. 37 ust. 1 a RODO odnosi się tylko do organów publicznych.

Jeżeli więc zgodnie ze statutem lub też z zasadniczym profilem działalności organizacja przetwarza dane w taki sposób, iż systematycznie lub regularnie monitoruje osoby, których dane przetwarza, a skala tego przetwarzania jest duża (RODO nie definiuje tego pojęcia, wskazując jedynie w motywie 91 ewentualną interpretację dużej skali jako operacji, które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko, na przykład (ze względu na swój szczególny charakter) gdy zgodnie ze stanem wiedzy technicznej stosowana jest na dużą skalę nowa technologia) lub też jeżeli organizacja przetwarza na dużą skalę szczególne kategorie danych wymienionych w art. 9 (są to dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby) lub przetwarza dane osobowe dotyczące wyroków skazujących i naruszeń prawa – przy czym w tym wypadku wolno przetwarzania dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującym odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych - warto zauważyć, iż w tym ostatnim wypadku nie jest wymagane działanie na dużą skalę

Po dokonaniu powyższej analizy organizacja, w razie wystąpienia przesłanki określonej w art. 37 ust. 1 RODO, wyznacza inspektora ochrony danych osobowych. Ponieważ wyznaczanie inspektora danych osobowych jest dobrowolne, zatem zgodnie z art. 37 ust. 4 RODO w przypadkach innych niż te, o których mowa w art. 37 ust. 1 RODO , administrator, podmiot przetwarzający, zrzeszenia lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających mogą wyznaczyć lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznaczają inspektora ochrony danych, przy czym inspektor ochrony danych może działać w imieniu takich zrzeszeń i innych podmiotów reprezentujących administratorów lub podmioty przetwarzające.

Należy też wskazać, iż grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.
Odnośnie kwalifikacji osoby wyznaczonej, należy podnieść, iż zgodnie z art. 37 ust. 5 RODO Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO, przy czym zgodnie z art. 37 ust. 6 inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.

W tym miejscu należy zaznaczyć, iż zgodnie z art. 39 RODO do zadań Inspektora ochrony danych osobowych należy:
a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
d) współpraca z organem nadzorczym;
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Konieczne jest zwrócenie uwagi, iż przy wykonywaniu powyższych zadań, zgodnie z treścią art. 39 ust. 2 RODO, inspektor ochrony danych jest zobowiązany do działania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Po wyznaczeniu inspektora, ostatnim zadaniem administratora lub podmiotu przetwarzającego jest publikacja danych kontaktowych inspektora ochrony danych i zawiadomienie o nich organu nadzorczego, zgodnie z art. 37 ust. 7 RODO.

ROZDZIAŁ VII.
PRZYJĘCIE I ZMIANY KODEKSU

1. Zagadnienia ogólne.

Opracowanie, wykładnia, bieżący nadzór nad przestrzeganiem oraz zmiany Kodeksu należą do wyłącznej kompetencji Związku Stowarzyszeń „Konfederacji Inicjatyw Pozarządowych Rzeczypospolitej Polskiej" z siedzibą w Warszawie, przy ul. S. Jaracza 10/1, 00-378 Warszawa, Nr KRS: 0000668126, w skrócie KIPR.
Zarząd KIPR jest uprawniony do złożenia wnioski o zatwierdzenie, zmianę, rozszerzenie Kodeksu i jest stroną postępowania w tym zakresie, jako wnioskodawca.
KIPR może wnioskować do Prezesa Urzędu Ochrony Danych Osobowych o przedstawienie wyjaśnień dotyczących przepisów o ochronie danych osobowych i stosowania ich w Kodeksie.
Do wyłącznych kompetencji Zarządu KIPR należy współpraca z podmiotem monitorującym i organem nadzorczym.

2. Przystąpienie do Kodeksu.

Przystąpienie do Kodeksu jest dobrowolne. Każda działająca na terytorium Rzeczpospolitej Polskiej organizacja społeczna może przystąpić do Kodeksu, zobowiązując się w ten sposób do jego przestrzegania.
Aby przystąpić do Kodeksu, należy złożyć do Zarządu KIPR oświadczenie o przystąpieniu do Kodeksu stanowiące załącznik nr 5 do niniejszego Kodeksu. Oświadczenie powinno być podpisane zgodnie z zasadami reprezentacji podmiotu przystępującego.
Przystąpienie następuje z momentem doręczenia KIPR podpisanego oświadczenia o przystąpieniu.
Od momentu przystąpienia do Kodeksu, podmiot przystępujący zobowiązany jest do jego przestrzegania.
Organizacja społeczna może złożyć oświadczenie o wystąpieniu ze stosowania Kodeksu. Oświadczenie o wystąpieniu powinno być złożone w takiej samej formie i trybie jak przy przystąpieniu do Kodeksu.

3. Zmiana Kodeksu

Zmiana Kodeksu następuje w drodze uchwały Zarządu KIPR. Zmiana poprzedzona będzie konsultacjami, z odpowiednimi stronami, których sprawa dotyczy, w tym jeżeli jest to wykonalne, z osobami, których dane dotyczą.
Informacja o zmianie Kodeksu zostanie podana do wiadomości na stronie internetowej KIPR. Dodatkowo, KIPR powiadomi wszystkie podmioty, które przystąpiły do Kodeksu, o jego zmianie.
Zmiana wchodzi w życie nie wcześniej niż po upływie 14 dni od dnia podjęcia uchwały o zmianie, pod warunkiem jej zatwierdzenia przez Prezesa Urzędu Ochrony Danych Osobowych.
Nie stanowią zmiany Kodeksu poprawki oczywistych błędów pisarskich w tekście Kodeksu.

ROZDZIAŁ VIII.
PODMIOT MONITORUJĄCY

Podmiotem monitorującym przestrzeganie Kodeksu jest podmiot powołany przez KIPR, który uzyskał wcześniej akredytację organu nadzorczego, po wykazaniu spełnienia przesłanek określonych w art. 41 ust. 1 i 2 RODO.

1. Zadania podmiotu monitorującego:

Zgodnie z art. 41 ust. 1 i 2 RODO Podmiot monitorujący jest uprawniony do:

a) dokonywania przeglądu stosowania Kodeksu, w tym zdolności organizacji do stosowania Kodeksu, przy czym pierwszy przegląd ma miejsce po upływie roku od przystąpienia organizacji do Kodeksu, a każdy następny przegląd odbywa się raz na dwa lata,

b) wykonywania czynności sprawdzających w związku z powzięciem uprawdopodobnionej informacji o naruszeniu postanowień Kodeksu przez organizację stosującą Kodeks,

c) rozpatrywania skarg na naruszenie Kodeksu,

d) stosowania środków zaradczych w przypadku stwierdzenia braku zdolności organizacji do stosowania Kodeksu lub w przypadku stwierdzenia naruszenia przez organizację Kodeksu,

e) zawieszenia organizacji spośród organizacji stosujących Kodeks w przypadkach, gdy organizacja ta naruszyła nieumyślnie przepisy Kodeksu w sposób skutkujący nałożeniem na nią kary administracyjnej przez organ nadzorczy przewidzianej w RODO oraz poinformowania o tym działaniu i powodach jego podjęcia organu nadzorczego,

f) wykluczenia organizacji spośród organizacji stosujących Kodeks w przypadkach, gdy organizacja ta naruszyła umyślnie przepisy Kodeksu w sposób skutkujący nałożeniem na nią kary administracyjnej przez organ nadzorczy przewidzianej w RODO oraz poinformowania o tym działaniu i powodach jego podjęcia organu nadzorczego.

Środki zaradcze.

W przypadku stwierdzenia nieprzestrzegania przepisów Kodeksu przez organizację, podmiot monitorujący stosuje następujące środki zaradcze:

a) Wzywa organizację na piśmie, aby w terminie 30 dni od dnia jej zawiadomienia o wynikach przeprowadzonej kontroli wdrożyła działania zmierzające do zaprzestania naruszania przepisów Kodeksu. Działania te i wytyczne podmiot monitorujący opisuje w wezwaniu,
b) Przeprowadza szkolenie dla organizacji z przestrzegania postanowień Kodeksu w zakresie objętym przez organizację naruszeniem,
c) Wydaje wobec organizacji ostrzeżenie, w którym wskazuje, że po upływie określonego w nim terminu, w ciągu którego organizacja nie dostosuje się do wytycznych, zostanie zawieszona lub wykluczona spośród podmiotów stosujących Kodeks.

Zawieszenie podmiotu stosującego Kodeks.

Sankcja zawieszenia organizacji w stosowaniu Kodeksu stosowana jest przez podmiot monitorujący tylko w przypadku, gdy środki zaradcze zastosowane w stosunku do organizacji nie odniosły skutku i tylko w sytuacji nałożenia przez organ nadzorczy kary administracyjnej przewidzianej przepisami RODO.
Podmiot monitorujący zawiesza organizację spośród stosujących Kodeks, jeżeli w toku kontroli stwierdzono, iż naruszyła ona nieumyślnie przepisy Kodeksu w sposób uzasadniający nałożenie na nią przez organ nadzorczy kary administracyjnej przewidzianej w RODO.
Przed zawieszeniem podmiot monitorujący powiadamia organ nadzorczy o nieumyślnym naruszeniu przez organizację przepisów Kodeksu i zgłasza naruszenie organowi nadzorczemu.
Po przeprowadzeniu postępowania przed organem nadzorczym i wydaniu przez organ prawomocnej decyzji o naruszeniu przepisów RODO skutkującej nałożeniem kary administracyjnej, podmiot monitorujący zawiesza organizację w stosowaniu Kodeksu.
Podmiot monitorujący zawieszając organizację spośród stosujących Kodeks wyznacza jej 30 - dniowy termin na usunięcie naruszenia będącego przyczyną zawieszenia.
Organizacja niezwłocznie po usunięciu naruszenia będącego przyczyną zawieszenia w terminie określonym powyżej informuje o tym podmiot monitorujący.
Po otrzymaniu informacji o usunięciu naruszenia podmiot monitorujący przeprowadza kontrolę, przy czym kontrola ta jest powtórzona jedynie w zakresie stwierdzonego naruszenia, które było przyczyną zawieszenia organizacji w stosowaniu Kodeksu.
Po przeprowadzeniu kontroli podmiot monitorujący wydaje pisemną ocenę zgodności z Kodeksem przetwarzania danych osobowych przez kontrolowaną organizację, jeżeli wcześniej stwierdzone naruszenie zostało usunięte.
Podmiot monitorujący informuje KIPR o zawieszeniu organizacji spośród stosujących Kodeks. W przypadku poważnych naruszeń Kodeksu KIPR może podać do publicznej wiadomości informację o zawieszeniu statusu organizacji stosującej Kodeks, zamieszczając ją na stronie internetowej KIPR.
Podmiot monitorujący informuje KIPR o uchyleniu zawieszenia organizacji spośród stosujących Kodeks. Jeżeli informację o zawieszeniu statusu organizacji stosującej Kodeks była zamieszona na stronie internetowej KIPR, KIPR w ten sam sposób podaje do publicznej wiadomości informację o uchyleniu zawieszenia oraz przywróceniu organizacji statusu stosującej Kodeks.

Wykluczenie podmiotu stosującego Kodeks.

Podmiot monitorujący wyklucza organizację spośród stosujących Kodeks jeżeli:
a) organizacja nie usunęła naruszeń, będących podstawą zawieszenia jej w stosowaniu Kodeksu, w terminie 30 dni od dnia doręczenia jej wezwania podmiotu monitorującego do usunięcia naruszeń,
b) gdy organizacja naruszyła umyślnie przepisy Kodeksu w sposób uzasadniający nałożenie na nią przez organ nadzorczy kary administracyjnej przewidzianej w RODO.

Podmiot monitorujący informuje KIPR o wykluczeniu organizacji spośród stosujących Kodeks. Wówczas KIPR skreśla organizację z listy podmiotów stosujących Kodeks i może podać do publicznej wiadomości informację o jej wykluczeniu, zamieszczając tą informację na stronie internetowej KIPR.

2. Szczegółowy zakres zadań i obowiązków podmiotu monitorującego.

Szczegółowy zakres zadań i obowiązków podmiotu monitorującego określa umowa zawarta pomiędzy KIPR a podmiotem monitorującym oraz procedury przyjęte przez podmiot monitorujący, o których mowa w art. 41 ust. 2 pkt b i c RODO.

3. Uprawnienia kontrolne podmiotu monitorującego.

Podmiot monitorujący przeprowadza kontrolę w organizacji wpisanej na listę podmiotów stosujących Kodeks:
- raz na 2 lata, przy czym kontrola może być kompleksowa lub fragmentaryczna (np. dotycząca tylko jednego bądź kilku procesów przetwarzania danych osobowych w organizacji, w zależności od potrzeb,
- w sytuacji, gdy podmiot monitorujący poweźmie uzasadnione wątpliwości co do naruszenia Kodeksu przez stosującą go organizację.

Podmiot monitorujący przeprowadza kontrolę w sposób szczegółowo opisany w procedurach, o których mowa w art. 41 ust. 2 pkt b i c RODO, jednakże z zachowaniem co najmniej poniższych wymogów:
- podmiot monitorujący przedstawia certyfikat akredytacyjny wydany przez organ nadzorczy,
- podmiot monitorujący przedstawia upoważnienie dla swoich przedstawicieli do przeprowadzenia kontroli,
- podmiot monitorujący powiadamia organizację o podjęciu czynności kontrolnych przynajmniej na 10 dni przed planowaną kontrolą,
- kontrola może być przeprowadzana tylko w dni robocze, od poniedziałku do piątku w godzinach od 9.00 do 15.00,
- kontrola może trwać maksymalnie 10 dni roboczych,
- podmiot monitorujący z przeprowadzonej kontroli sporządza protokół,
- organizacja ma prawo wnieść w terminie 7 dni od dnia przedstawienia jej przez podmiot monitorujący protokołu swoje zastrzeżenia,
- w razie zgłoszenia zastrzeżeń, o których mowa powyżej, podmiot monitorujący zobowiązany jest je zbadać, a w przypadku stwierdzenia zasadności zastrzeżeń - zmienić lub uzupełnić odpowiednią część protokołu,
- podmiot monitorujący zawiadamiania organizację oraz KIPR o wynikach kontroli, w szczególności o potwierdzeniu stosowania Kodeksu, a w wypadkach wskazanych powyżej podmiot monitorujący zawiadamia organ nadzorczy o zawieszeniu lub wykluczeniu organizacji spośród podmiotów stosujących Kodeks,
-podmiot monitorujący wydaje pisemną ocenę zgodności przetwarzania danych osobowych z Kodeksem przez kontrolowaną organizację jeżeli:
- w toku kontroli nie stwierdzono naruszeń stosowania Kodeksu lub
- w toku kontroli stwierdzono naruszenia mniejszej wagi w stosowaniu Kodeksu, a jest mało prawdopodobne, by te uchybienia skutkowały ryzykiem naruszenia przepisów RODO.

4. Współpraca z podmiotem monitorującym.

KIPR i podmiot monitorujący na wspólnych spotkaniach analizują stosowanie Kodeksu w praktyce przez organizacje oraz ewentualną konieczność zmiany Kodeksu.
Spotkania odbywają się raz na kwartał/sześć miesięcy w siedzibie KIPR.
Spotkania odbywają się przy udziale organizacji lub ich przedstawicieli/delegatów stosujących Kodeks.
Zaproszenie dotyczące planowanego spotkania powinno być wysłane pocztą tradycyjną lub na udostępnione w tym celu przez organizacje stosujące Kodeks adresy e-mail, co najmniej 14 dni przed spotkaniem w celu umożliwienia uczestnictwa w spotkaniu.
Na spotkaniu podmiot monitorujący przekazuje KIPR informacje o stosowaniu Kodeksu.
Ze spotkania KIPR sporządza podsumowanie, którego obligatoryjną częścią jest ocena zasadności ewentualnej zmiany Kodeksu.

5. Zawiadamianie o problemach z ochroną danych osobowych.

Każdy podmiot, który przystąpił do Kodeksu, może zawiadomić KIPR o:
a) problemach w interpretacji postanowień Kodeksu,
b) kluczowych kwestiach związanych z ochroną danych osobowych, które powinny zostać uregulowane w Kodeksie.

ZAŁĄCZNIKI do KODEKSU

1. *Wzór umowy powierzenia przetwarzania danych osobowych*
2. *Wzór umowy współadministrowania danymi osobowymi*
3. *Wzór Polityki ochrony danych osobowych*
4. *Wzór Instrukcji zarządzania systemami informatycznymi*
5. *Wzór oświadczenia o przystąpieniu do Kodeksu postępowania*

Załącznik nr 1 - Wzór umowy powierzenia przetwarzania danych osobowych

Umowa powierzenia przetwarzania danych osobowych

zawarta w Warszawie w dniu 25 maja 2018 roku pomiędzy:

Organizacja z siedzibą w … , przy ul … , … , zarejestrowaną … nr KRS … , NIP: … , REGON: … , reprezentowaną przez … – Prezesa Zarządu i … – Wiceprezesa Zarządu, zwaną dalej „**Administratorem**"

a

…... (*imię i nazwisko*) prowadzącą działalność gospodarczą pod firmą … Drukarnia pod adresem: … , … , zarejestrowaną w … , posiadającą nr NIP …, zwaną dalej „**Przetwarzającym**"

zwanymi dalej łącznie „**Stronami**"

Zważywszy, że:

i. Organizacja zleca Przetwarzającemu usługę drukowania i wysyłki wydrukowanych materiałów do osób wskazanych przez Organizację („**Zlecenia**"),
ii. w związku z wykonywaniem Zleceń Administrator powierza Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym niniejszą Umową,
iii. intencją Stron jest takie uregulowanie zasad przetwarzania danych osobowych określonych w niniejszej Umowie, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej zwanego „**Rozporządzeniem"**.

Strony postanowiły zawrzeć Umowę o następującej treści:

§1.
Przedmiot Umowy

1. Administrator powierza Przetwarzającemu przetwarzanie danych osobowych wyłącznie na warunkach i w celu określonym w niniejszej Umowie oraz Zleceniach.
2. Zakres danych osobowych powierzonych Przetwarzającemu ze wskazaniem opisu kategorii danych osobowych w ramach poszczególnych czynności przetwarzania określa Załącznik nr 1 do niniejszej Umowy.
3. Dane osobowe będą przetwarzane przez Przetwarzającego wyłącznie w celu realizacji Zleceń.
4. Poprzez przetwarzanie danych osobowych rozumie się w szczególności zbieranie, zapisywanie, modyfikację, utrwalanie, przechowywanie, opracowywanie, udostępnianie oraz usuwanie danych osobowych.

§2.

Oświadczenia Stron

1. Organizacja oświadcza, że jest administratorem danych osobowych, o których mowa w § 1 ust. 2 powyżej.
2. Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem danych osobowych objętych niniejszą Umową i Zleceniami, posiada w tym zakresie niezbędną wiedzę i doświadczanie, daje rękojmię należytego wykonania niniejszej Umowy a także dysponuje odpowiednimi środkami bezpieczeństwa zarówno technicznymi, jak i organizacyjnymi, w szczególności należytymi zabezpieczeniami umożliwiającymi przetwarzanie danych osobowych a także że przygotował stosowną dokumentację wymaganą od podmiotu, któremu powierzono przetwarzanie danych osobowych zgodnie z Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Przetwarzający oświadcza, że w odniesieniu do danych osobowych powierzonych na podstawie niniejszej Umowy zapewnia obsługę praw jednostki, o których mowa w rozdziale III Rozporządzenia.

§3.

Obowiązki Stron

1. Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu niniejszej Umowy, w szczególności udzielać Przetwarzającemu wyjaśnień w razie zgłaszanych przez niego wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków określonych niniejszą Umową.
2. Przetwarzający może przetwarzać dane osobowe przekazane przez Administratora wyłącznie w zakresie i w celu określonych w niniejszej Umowie a także zgodnie z poleceniami lub instrukcjami Administratora. Jeżeli Przetwarzający poweźmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast poinformuje Administratora o stwierdzonej wątpliwości (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.
3. Przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych, a w szczególności zobowiązuje się do:
   a) wdrożenia przed przystąpieniem do przetwarzania powierzonych danych i utrzymania przez okres obowiązywania niniejszej Umowy wszelkich środków technicznych i organizacyjnych zapewniających poziom zabezpieczenia odpowiadający ryzyku związanemu z przetwarzaniem danych, zgodnie z wymaganiami Rozporządzenia oraz innych przepisów krajowych dotyczących ochrony danych osobowych,
   b) posiadania stosownej dokumentacji wymaganej od Przetwarzającego zgodnie z Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą,
   c) nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej Umowy,
   d) zapewnienia osobom upoważnionym do przetwarzania danych odpowiedniego szkolenia z zakresu ochrony danych osobowych,

a) zapewnienia zachowania w tajemnicy przetwarzanych danych przez osoby, które Przetwarzający upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zarówno w trakcie zatrudnienia ich u Przetwarzającego, jak i po jego ustaniu,
b) usunięcia danych w terminie 14 dni od zakończeniu niniejszej Umowy bądź - według wyboru Administratora - zwrotu mu wszelkich danych osobowych oraz usunięcia wszelkich istniejących kopii takich danych, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych,
c) odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III Rozporządzenia dot. praw osoby, której dane dotyczą,
d) przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego (Podprzetwarzającego),
e) udzielania pomocy Administratorowi w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia, dotyczących w szczególności ochrony danych osobowych, zgłaszania naruszeń organowi nadzorczemu, zawiadamiania osób dotkniętych naruszeniem ochrony danych, oceny skutków dla ochrony danych i uprzednich konsultacji z organem nadzorczym,
f) udostępnienia Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w niniejszym paragrafie,
g) umożliwienia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów i inspekcji a także efektywnego przyczyniania się do nich,
h) prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych, w tym rejestr wszystkich kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu Administratora - o ile Przetwarzający ma taki obowiązek na podstawie art. 30 ust. 2 Rozporządzenia; w takim przypadku Przetwarzający zobowiązuje się do udostępniania na żądanie Administratora prowadzonego rejestru wszystkich kategorii czynności przetwarzania, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego
i) informowania Administratora o stosowaniu zautomatyzowanego przetwarzania w celu realizacji niniejszej Umowy, w tym profilowania - w celu i w zakresie niezbędnym do wykonania przez Administratora obowiązku informacyjnego.

§4.

Podpowierzenie danych osobowych

1. Przetwarzający może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania podwykonawcom (Podprzetwarzającym) jedynie w celu wykonania niniejszej Umowy po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Dokonując podpowierzenia, Przetwarzający ma obowiązek zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy,
3. Przetwarzający ma obowiązek zapewnić, aby Podprzetwarzający złożył Administratorowi zobowiązanie do wykonania obowiązków, o których mowa w poprzednim ustępie. Może to zostać wykonane przez podpisanie stosownego oświadczenia adresowanego do Administratora wraz z podpisaniem Umowy Podpowierzenia zawierającego listę obowiązków Podprzetwarzającego.

§5.

Przekazywanie danych do państwa trzeciego

Przekazanie powierzonych danych do państwa trzeciego lub organizacji międzynarodowej, tj. poza Europejski Obszar Gospodarczy, może nastąpić jedynie na pisemne polecenie Administratora, chyba, że obowiązek taki nakłada na Przetwarzającego prawo Unii lub prawo państwa członkowskiego, któremu podlega Przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

§6.

Prawo kontroli

1. Administrator na podstawie art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Przetwarzającego przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia niniejszej Umowy.
2. Administrator będzie wykonywał prawo kontroli w godzinach pracy Przetwarzającego i z minimum dwudniowym wyprzedzeniem.
3. Administrator lub wyznaczone przez niego osoby są uprawnione do wstępu do pomieszczeń, w których przetwarzane są dane osobowe powierzone na podstawie niniejszej Umowy a także do wglądu do dokumentacji związanej z przetwarzaniem powyższych danych.
4. Przetwarzający zobowiązuje się udostępniać Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami Rozporządzenia oraz innych przepisów dotyczących ochrony danych osobowych, w szczególności do udzielania informacji dotyczących przebiegu przetwarzania powierzonych danych osobowych oraz udostępnienia rejestr wszystkich kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu Administratora.
5. Przetwarzający zobowiązuje się umożliwić Administratorowi lub upoważnionemu przez niego audytorowi przeprowadzanie audytów lub inspekcji a także ściśle współpracować przy ich realizacji.
6. Przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora.
7. Przetwarzający jest zobowiązany, na pisemne wezwanie otrzymane od Administratora, informować Administratora o środkach podejmowanych w celu zapewnienia zgodności z Rozporządzeniem oraz z innymi przepisami prawa z zakresu ochrony danych osobowych a także o wszelkich innych krokach, jakie są niezbędne dla zapewnienia bezpieczeństwa powierzonych danych osobowych.

§7.

Zasady zachowania poufności

1. Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy, w formie ustnej, pisemnej lub elektronicznej.
2. Przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych, o których mowa w ustępie powyżej, nie będą one wykorzystywane, ujawniane ani udostępniane bez uprzedniej pisemnej zgody Administratora w innym celu niż wykonanie niniejszej Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub niniejszej Umowy.

3. W wypadku, gdy Przetwarzający zostanie zobowiązana nakazem sądu bądź organu administracji państwowej do ujawnienia danych poufnych, o których mowa w ust. 1 niniejszego paragrafu, albo konieczność ich ujawnienia będzie wynikała z przepisów prawa, zobowiązuje się niezwłocznie pisemnie powiadomić o tym fakcie Administratora oraz poinformować odbiorcę informacji lub materiałów o ich poufnym charakterze.

§8.

Powiadomienie o naruszeniach danych osobowych

Przetwarzający niezwłocznie powiadamia Administratora o każdym podejrzeniu naruszenia ochrony danych osobowych jednak nie później niż w 24 godziny od stwierdzenia podejrzenia naruszenia, umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia. Powiadomienie o stwierdzeniu naruszenia powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organu nadzoru oraz osób, których dane dotyczą.

§9.

Odpowiedzialność Przetwarzającego

1. Przetwarzający odpowiada za szkody, jakie powstaną u Administratora lub osób trzecich w wyniku udostępnienia powierzonych do przetwarzania danych osobowych osobom nieupoważnionym lub wykorzystania danych osobowych niezgodnie z niniejszą Umową, w szczególności odpowiada za niedopełnienie obowiązków, które Rozporządzenie bądź inne przepisy prawa dotyczące ochrony danych osobowych nakłada bezpośrednio na Przetwarzającego, w tym w związku z brakiem zastosowania bądź zastosowaniem niewystarczających środków bezpieczeństwa. W takim przypadku Administrator jest uprawniony do dochodzenia od Powierzającego kary umownej w wysokości 5.000,00 zł (pięć tysięcy złotych) za każdy przypadek naruszenia. Powyższe nie ogranicza prawa Administratora do dochodzenia od Przetwarzającego odszkodowania uzupełniającego na zasadach ogólnych w przypadku, gdy wielkość szkody przekracza wysokość zastrzeżonej kary umownej.
2. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Przetwarzającego danych osobowych powierzonych na podstawie niniejszej Umowy, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania przez Przetwarzającego tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez organ nadzorczy.
3. W przypadku, gdy osoba trzecia wystąpi w stosunku do Administratora z roszczeniami wynikającymi z naruszenia przez Przetwarzającego obowiązujących przepisów w zakresie ochrony danych osobowych, Przetwarzający zobowiązuje się przystąpić do postępowania sądowego lub administracyjnego na wezwanie Administratora, w stosunku do którego wszczęto postępowanie. W takim przypadku, pod warunkiem stwierdzenia przez sąd lub organ administracji zasadności roszczenia osoby trzeciej w całości lub w części prawomocnym orzeczeniem lub ostateczną decyzją administracyjną, Przetwarzający zobowiązany będzie pokryć poniesione przez Administratora, w stosunku do którego wszczęto postępowanie, koszty postępowania sądowego lub

administracyjnego, w tym koszty zastępstwa procesowego oraz zapłacić zasądzone odszkodowanie, koszty polubownego rozstrzygnięcia sporu oraz wszelkie inne koszty wynikające z takich roszczeń. Postanowienia niniejszej Umowy nie ograniczają prawa Administratora, w stosunku do którego wszczęto postępowanie, do dochodzenia od Przetwarzającego odszkodowania na zasadach ogólnych.

4. Na podstawie art. 28 ust. 4 Rozporządzenia Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na Podprzetwarzającego obowiązków ochrony danych jak za swoje własne działania.

§10.

Obowiązywanie i rozwiązanie Umowy

1. Niniejsza Umowa wchodzi w życie z dniem jej podpisania i zostaje zawarta na czas nieokreślony.
2. Przetwarzający może przetwarzać dane przekazane przez Administratora wyłącznie w okresie jej obowiązywania, z zastrzeżeniem, iż po zakończeniu jej realizacji przetwarzanie danych osobowych przez Przetwarzającego dopuszczalne jest jedynie w zakresie przechowywania danych ich usuwania bądź zwrotu Administratorowi.
3. Obowiązki i zasady określone niniejszą umową, w szczególności obowiązek zachowania poufności, o którym mowa w § 7 niniejszej Umowy, obowiązuje przez czas obowiązywania Umowy oraz przez okres 5 lat po wygaśnięciu pozostałych zobowiązań wynikających z Umowy, po jej rozwiązaniu lub odstąpieniu od Umowy przez którąkolwiek ze Stron.
4. Umowa może być rozwiązana przez każdą ze stron z zachowaniem jednomiesięcznego okresu wypowiedzenia lub w drodze obopólnego porozumienia stron.
5. Administrator może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym w przypadku, gdy Przetwarzający:
   a) nie zaprzestał niewłaściwego przetwarzania danych osobowych, pomimo upomnienia go przez Administratora,
   b) nie usunie uchybień stwierdzonych podczas kontroli lub inspekcji w terminie wyznaczonym przez Administratora,
   c) przetwarza dane osobowe w sposób niezgodny z niniejszą Umową bądź rażąco narusza zasady przetwarzania danych osobowych
   d) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.

§11.

Koordynatorzy Umowy

1. Dla bieżących kontaktów i nadzoru nad realizacją Umowy Strony ustanawiają następujących Koordynatorów Umowy:
   - ze strony Administratora: …… , tel. …….. , ……@.....
   - ze strony Przetwarzającego: …… , tel. …….. , ……@.....
2. Koordynatorzy Umowy będą uprawnieni do prowadzenia bieżącej komunikacji, omawiania i rozwiązywania problemów pojawiających się w trakcie realizacji Umowy a także zmiany Załączników do niniejszej Umowy ze skutkami prawnymi dla każdej ze Stron.
3. Każda ze Stron może dokonać zmiany swojego Koordynatora Umowy, zawiadamiając o tym drugą Stronę na piśmie.
4. Dla uniknięcia wątpliwości zmiana Załączników do niniejszej Umowy oraz zmiany Koordynatorów Umowy przez Strony nie stanowią zmiany Umowy.

§12.

Postanowienia końcowe

1. W razie sprzeczności pomiędzy postanowieniami niniejszej Umowy, a warunkami poszczególnych Zleceń, pierwszeństwo mają postanowienia niniejszej Umowy.
2. Z zastrzeżeniem §11 ust. 4 Umowy wszelkie uzupełnienia lub zmiany niniejszej Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
3. Żadna ze Stron nie może przenieść praw lub obowiązków wynikających z niniejszej Umowy bez pisemnej zgody drugiej Strony.
4. W sprawach nieuregulowanych niniejszą Umową zastosowanie znajdują przepisy Kodeksu cywilnego, Rozporządzenia oraz innych przepisów dotyczących ochrony danych osobowych.
5. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy dla siedziby Administratora.
6. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Administrator Przetwarzający

Załączniki:

1. Zakres danych osobowych powierzonych Przetwarzającemu przez Organizację

Załącznik nr 1
do umowy powierzenia przetwarzania danych osobowych pomiędzy Organizacją a Drukarnią

Zakres danych osobowych powierzonych Przetwarzającemu obejmuje - w odniesieniu do osób fizycznych, które wyraziły chęć udziału w wydarzeniu publicznym organizowanym przez Organizację - następujące rodzaje danych:

a) imiona
b) nazwiska
c) płeć
d) tytuł / stopień naukowy / tytuł zawodowy
e) organizacja/instytucja
f) adres e-mail
g) adres do korespondencji
h) numer telefonu komórkowego
i) numer telefonu biurowego

Załącznik nr 2 - Wzór umowy współadministrowania danymi osobowymi

Ramowa umowa o współadministrowanie danymi osobowymi

zawarta w Warszawie w dniu _____ 2019 roku pomiędzy:

Organizacja I z siedzibą w Warszawie, przy ul. …, zarejestrowaną w Sądzie Rejonowym dla m.st. Warszawy w Warszawie, … Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS … , NIP: …. , REGON: … , reprezentowaną przez:
-… – Prezesa Zarządu,
- … – Członka Zarządu,
zwaną dalej „**Administratorem 1**"

a

Organizacja II z siedzibą w Warszawie, przy ul. …, zarejestrowaną w Sądzie Rejonowym dla m.st. Warszawy w Warszawie, … Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS … , NIP: …. , REGON: … , reprezentowaną przez:
-… – Prezesa Zarządu,
- … – Członka Zarządu,
zwaną dalej „**Administratorem 2**"

zwanymi dalej łącznie „**Stronami**" lub **„Współadministratorami"**

Zważywszy, że intencją Stron jest takie uregulowanie zasad przetwarzania danych osobowych określonych w niniejszej Umowie, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej zwane **Rozporządzeniem** lub **RODO** i w przejrzysty sposób ustalały zakresy odpowiedzialności Współadministratorów dotyczące wypełniania obowiązków wynikających z przepisów „Rozporządzenia" i innych przepisów prawa powszechnie obowiązującego, jak również relacji pomiędzy Współadministratorami a podmiotami, których dane osobowe dotyczą, Strony postanowiły zawrzeć Umowę o następującej treści:

§1.
Przedmiot Umowy

1. Niniejsza Umowa stanowi regulację pomiędzy Współadministratorami, o której mowa w art. 26 ust. 1 RODO i normuje wzajemne stosunki pomiędzy Stronami w zakresie współadministrowania danymi osobowymi a w szczególności ustala w przejrzysty sposób zakresy odpowiedzialności Współadministratorów dotyczące wypełniania obowiązków wynikających z przepisów RODO i innych przepisów prawa powszechnie obowiązującego, jak również określa reprezentację Współadministratorów w stosunku do podmiotów, których dane osobowe dotyczą oraz ich relacje z tymi podmiotami.

2. Kategorie i zakres danych osobowych przetwarzanych przez Współadministratorów przy wspólnych projektach zawarte są w Załączniku nr 1 do niniejszej Umowy.
3. Dla potrzeb prawidłowej realizacji niniejszej Umowy Współadministratorzy zobowiązują się:
   a) współpracować przy realizacji obowiązków ciążących na Współadministratorach danych osobowych;
   b) przetwarzać udostępnione im dane osobowe zgodnie z niniejszą Umową, przepisami RODO oraz innymi przepisami prawa powszechnie obowiązującego;
   c) powstrzymywać się od działań faktycznych i prawnych, które mogłyby w jakikolwiek sposób naruszyć bezpieczeństwo danych osobowych albo narazić drugiego Współadministratora na odpowiedzialność cywilną, administracyjną lub karną.
4. Każdy Współadministrator pokrywa własne koszty i wydatki związane z prawidłowym wykonaniem niniejszej Umowy.

§2.

Oświadczenia Stron

4. Każda Strona oświadcza i zapewnia, że została prawidłowo ustanowiona i istnieje zgodnie z obowiązującymi przepisami prawa i posiada wszelkie wymagane uprawnienia prawne oraz prawo do zawarcia Umowy i wykonywania swoich zobowiązań z niej wynikających, a niniejsza Umowa stanowi ważne i wiążące zobowiązanie podlegające wykonaniu przez Strony.
5. Współadministratorzy oświadczają, iż wszelkie definicje użyte w Rozporządzeniu mają zastosowanie bezpośrednio w niniejszej Umowie.
6. Współadministratorzy oświadczają i zapewniają, iż są uprawnieni do ustalania łącznie z drugim Współadministratorem celów i sposobów przetwarzania danych osobowych.
7. Współadministratorzy oświadczają, że w ramach prowadzonej działalności profesjonalnie zajmują się przetwarzaniem danych osobowych objętych Umową, posiadają w tym zakresie niezbędną wiedzę i doświadczanie, dają rękojmię należytego wykonania niniejszej Umowy a także dysponują odpowiednimi środkami bezpieczeństwa zarówno technicznymi, jak i organizacyjnymi, w szczególności należytymi zabezpieczeniami umożliwiającymi przetwarzanie danych osobowych a także, że przygotowali stosowną dokumentację wymaganą zgodnie z Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą, ze szczególnym uwzględnieniem obowiązków administratora danych osobowych.
8. Współadministratorzy oświadczają, że w odniesieniu do danych osobowych zapewniają obsługę praw jednostki, o których mowa w rozdziale III Rozporządzenia.

§3.

Obowiązki Stron

4. Współadministratorzy zobowiązani są zapewnić bezpieczeństwo przetwarzania danych osobowych poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych, adekwatnych do rodzaju danych osobowych oraz ryzyka naruszenia praw osób, których te dane dotyczą.
5. Każdy ze Współadministratorów zobowiązuje się dołożyć należytej staranności przy przetwarzaniu danych osobowych a w szczególności zobowiązuje się do:
   e) wdrożenia przed przystąpieniem do przetwarzania danych i utrzymania przez okres obowiązywania niniejszej Umowy wszelkich środków technicznych i organizacyjnych zapewniających poziom zabezpieczenia odpowiadający ryzyku związanemu z przetwarzaniem

danych, zgodnie z wymaganiami Rozporządzenia oraz innych przepisów krajowych dotyczących ochrony danych osobowych,

f) posiadania stosownej dokumentacji wymaganej od administratora zgodnie z Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą,

g) nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały współadministrowane dane osobowe w celu realizacji niniejszej Umowy,

h) zapewnienia osobom upoważnionym do przetwarzania danych odpowiedniego szkolenia z zakresu ochrony danych osobowych,

i) zapewnienia zachowania w tajemnicy, przetwarzanych danych przez osoby, które każdy z Administratorów upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zarówno w trakcie zatrudnienia ich u każdego z Administratorów, jak i po jego ustaniu,

j) udostępnienia Współadministratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w niniejszym paragrafie

k) wdrożenia procedury zapewniania osobom, których dane osobowe dotyczą, prawa dostępu do danych oraz związaną z tym procedurę wymiany informacji z drugim Współadministratorem.

6. Współadministratorzy ustalają, że w zakresie udzielania odpowiedzi na żądania osoby, której dane dotyczą, (w szczególności dotyczy to żądań i oświadczeń w zakresie prawa do informowania i przejrzystej komunikacji, dostępu do danych osobowych, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych osobowych, sprzeciwu wobec przetwarzania danych osobowych) właściwy będzie Współadministrator, który otrzymał dane żądanie lub oświadczenie. W przypadku, gdy żądanie zostanie skierowane do obydwu Współadministratorów, to obydwaj Współadministratorzy zobowiązani będą, każdy z osobna, do udzielenia ww. odpowiedzi, po wcześniejszym uzgodnieniu wspólnego stanowiska. Niezależnie od powyższego, Współadministratorzy są zobowiązani współpracować między sobą w zakresie udzielania odpowiedzi na żądania osoby, której dane dotyczą. W tym celu Współadministrator zobowiązany jest niezwłocznie poinformować drugiego Współadministratora o każdym żądaniu osoby uprawnionej w ramach wykonywania przez tę osobę praw wynikających z RODO oraz udzielać drugiemu Współadministratorowi wszelkich niezbędnych informacji w tym zakresie.

7. Współadministratorzy ustalają, że w zakresie wywiązywania się przez Współadministratorów z obowiązków w zakresie zarządzania naruszeniami ochrony danych osobowych oraz ich zgłaszania do organu nadzoru oraz osoby, której dane dotyczą, właściwy będzie Współadministrator, który stwierdził naruszenie. W przypadku, gdy naruszenie zostanie stwierdzone przez obydwu Współadministratorów (np. gdy zostało zgłoszone obydwu Współadministratorom), to właściwy do wykonania obowiązków określonych w art. 33 - 34 RODO będzie ten Współadministrator, z którego działania bądź zaniechania naruszenie wynikło. Niezależnie od powyższego, Współadministratorzy są zobowiązani współpracować między sobą w zakresie spełniania obowiązków określonych w art. 33 - 34 RODO. W tym celu Współadministrator zobowiązany jest niezwłocznie, jednak nie później niż w terminie 24 godzin od stwierdzenia podejrzenia naruszenia, poinformować drugiego Współadministratora o każdym stwierdzonym naruszeniu ochrony danych osobowych, podjętych w związku z naruszeniem krokach, umożliwić drugiemu Współadministratorowi uczestnictwo w czynnościach wyjaśniających, poinformować o treści zgłoszenia przekazanego organowi nadzorczemu

w związku z naruszeniem oraz udzielić drugiemu Współadministratorowi wszelkich niezbędnych informacji w tym zakresie.

§4.

Powierzanie przetwarzania danych osobowych

1. Współadministratorzy mogą zlecać podmiotom przetwarzającym realizację określonych czynności w zakresie przetwarzania danych osobowych bez konieczności uzyskania zgody drugiego Współadministratora. Podmioty Przetwarzające mogą przetwarzać dane osobowe wyłącznie w celu realizacji czynności, w odniesieniu, do których dane osobowe zostały przekazane Współadministratorom, i nie mogą przetwarzać danych osobowych w żadnych innych celach. W przypadku zlecenia czynności podmiotowi przetwarzającemu przez Współadministratora, podmiot przetwarzający będzie podlegać pisemnym zobowiązaniom w zakresie ochrony danych osobowych określonym w art. 28 RODO, zapewniając co najmniej taki sam poziom ochrony, jak określono w niniejszej Umowie.
2. W przypadku niewykonania przez podmiot przetwarzający ciążących na nim obowiązków w zakresie ochrony danych osobowych, Współadministrator, który powierzył podmiotowi przetwarzającemu przetwarzanie danych osobowych - zgodnie z postanowieniami dotyczącymi odpowiedzialności w Umowie - ponosi pełną odpowiedzialność wobec drugiego Współadministratora za wykonanie zobowiązań ciążących na podmiocie przetwarzającym.

§5.

Przekazywanie danych do państwa trzeciego

1. Przekazanie współadministrowanych danych do państwa trzeciego lub organizacji międzynarodowej, tj. poza Europejski Obszar Gospodarczy, może nastąpić bez zgody drugiego Współadministratora. Przekazanie takie nastąpi wyłącznie jedynie w zakresie, na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku każdy ze Współadministratorów zapewni możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń.
2. W przypadku gdy prawo Unii lub prawo polskie nakłada obowiązek przekazania współadministrowanych danych do państwa trzeciego lub organizacji międzynarodowej, przed rozpoczęciem przetwarzania Współadministratorzy informują się wzajemnie o tym obowiązku prawnym. Każdy ze Współadministratorów we własnym zakresie odpowiada za zastosowanie odpowiednich mechanizmów ochrony w przypadku ewentualnych transferów danych poza Europejski Obszar Gospodarczy (EOG).

§6.

Prawo kontroli

1. Współadministratorzy zobowiązani są udzielać sobie nawzajem wszelkich informacji niezbędnych dla wykazania wywiązywania się ze wszystkich obowiązków określonych w RODO.
2. Każdy Współadministrator zobowiązany jest, bez zbędnej zwłoki, powiadomić drugiego Współadministratora o wszelkich skargach, pismach, kontrolach organu nadzoru, postępowaniach sądowych i administracyjnych pozostających w związku z przetwarzanymi danymi osobowymi oraz udostępniać Współadministratorowi wszelką dokumentację z tym związaną.

§7.

Zasady zachowania poufności

1. Współadministratorzy zobowiązują się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od siebie wzajemnie i od współpracujących z nimi osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy, w formie ustnej, pisemnej lub elektronicznej.
2. Współadministratorzy oświadczają, że w związku ze zobowiązaniem się do zachowania w tajemnicy danych poufnych, o których mowa w ustępie powyżej, nie będą one wykorzystywane, ujawniane ani udostępniane bez uprzedniej pisemnej zgody drugiego Administratora w innym celu niż wykonanie niniejszej Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub niniejszej Umowy.
3. W wypadku, gdy jeden z Administratorów zostanie zobowiązany nakazem sądu bądź organu administracji państwowej do ujawnienia danych poufnych, o których mowa w ust. 1 niniejszego paragrafu, albo konieczność ich ujawnienia będzie wynikała z przepisów prawa, zobowiązuje się niezwłocznie pisemnie powiadomić o tym fakcie drugiego Administratora oraz poinformować odbiorcę informacji lub materiałów o ich poufnym charakterze.

§8.

Dokumentowanie przetwarzania danych osobowych

Współadministratorzy, każdy w swoim zakresie zapewnią odpowiednie udokumentowanie procesów przetwarzania danych osobowych dla potrzeb wykazania ich zgodności z przepisami prawa, w tym dla potrzeb spełnienia wymogu rozliczalności.

§9.

Odpowiedzialność

1. Każdy Współadministrator odpowiada za działania i zaniechania osób, przy pomocy których będzie przetwarzał dane osobowe (w tym podmiotów przetwarzających), jak za działania lub zaniechania własne.
2. Każdy Współadministrator odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Administratora.
3. Każdy Współadministrator odpowiada za szkody spowodowane niezastosowaniem właściwych środków bezpieczeństwa.
4. Współadministrator dopuszczający się naruszenia przepisów RODO lub innych przepisów prawa powszechnie obowiązującego, jest zobowiązany, w ramach swojej odpowiedzialności za przetwarzanie danych osobowych, do współpracy z drugim Współadministratorem w razie postępowania przed organem nadzorczym lub sporu sądowego z podmiotem danych osobowych.
5. W przypadku, gdy podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych osobowych, pełna odpowiedzialność za wypełnienie obowiązków przez podmiot przetwarzający spoczywa na Współadministratorze, który powierzył mu przetwarzanie.

§10.

Obowiązywanie i rozwiązanie Umowy

1. Niniejsza Umowa wchodzi w życie z dniem jej podpisania i zostaje zawarta na czas nieokreślony.
2. Obowiązki i zasady określone niniejszą umową, w szczególności obowiązek zachowania poufności, o którym mowa w § 7 niniejszej Umowy, obowiązuje przez czas obowiązywania

Umowy oraz przez okres 5 lat po wygaśnięciu pozostałych zobowiązań wynikających z Umowy, po jej rozwiązaniu lub odstąpieniu od Umowy przez którąkolwiek ze Stron.

3. Umowa może być rozwiązana przez każdą ze Stron z zachowaniem jednomiesięcznego okresu wypowiedzenia lub w drodze obopólnego porozumienia stron.
4. Każdy ze Współadministratorów może rozwiązać niniejszą umowę ze skutkiem natychmiastowym w przypadku, gdy drugi Administrator:
   e) nie zaprzestał niewłaściwego przetwarzania danych osobowych, pomimo upomnienia go przez Współadministratora
   f) przetwarza dane osobowe w sposób niezgodny z niniejszą Umową bądź rażąco narusza zasady przetwarzania danych osobowych.

§11.

Koordynatorzy Umowy

1. Dla bieżących kontaktów i nadzoru nad realizacją Umowy Strony ustanawiają następujących Koordynatorów Umowy:
   a) ze strony Administratora 1: … , tel. … , e-mail: …,
   b) ze strony Administratora 2: … , tel. … , e-mail: …,
2. Koordynatorzy Umowy będą uprawnieni do prowadzenia bieżącej komunikacji, omawiania i rozwiązywania problemów pojawiających się w trakcie realizacji Umowy, zmiany Załączników do niniejszej Umowy ze skutkami prawnymi dla każdej ze Stron a także przeprowadzania kontroli w zakresie ochrony danych osobowych, w trakcie każdego wspólnego projektu.
3. Każda ze Stron może dokonać zmiany swojego Koordynatora Umowy, zawiadamiając o tym drugą Stronę na piśmie.
4. Dla uniknięcia wątpliwości zmiana Załączników do niniejszej Umowy oraz zmiany Koordynatorów Umowy przez Strony nie stanowią zmiany Umowy.

§12.

Postanowienia końcowe

1. Z zastrzeżeniem §11 ust. 4 Umowy wszelkie uzupełnienia lub zmiany niniejszej Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
2. Żadna ze Stron nie może przenieść praw lub obowiązków wynikających z niniejszej Umowy bez pisemnej zgody drugiej Strony.
3. W sprawach nieuregulowanych niniejszą Umową zastosowanie znajdują przepisy Kodeksu cywilnego, Rozporządzenia oraz innych przepisów dotyczących ochrony danych osobowych.
4. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy dla siedziby Administratora 1.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Administrator 1 Administrator 2

Załączniki:

1. Kategorie i zakres danych osobowych przetwarzanych przez Współadministratorów

Załącznik nr 1
do umowy o współadministrowanie danymi osobowymi

Zakres danych osobowych współadministrowanych przez Administratorów obejmuje w odniesieniu osób popierających kampanie społeczne, w tym składających protesty i petycje na portalach prowadzonych przez Współadministratorów - następujące rodzaje danych:

a) imiona
b) nazwiska
c) płeć
d) adresy e-mail
e) numer telefonu
f) adres zamieszkania lub korespondencji (ulica, numer, kod pocztowy, miejscowość, państwo)
g) obywatelstwo
h) PESEL

Załącznik nr 3 - Wzór Polityki ochrony danych osobowych

POLITYKA OCHRONY DANYCH OSOBOWYCH

I. Podstawa prawna

Niniejsza „*Polityka ochrony danych osobowych*", zwana dalej „*Polityką*" stanowi wykonanie obowiązku, o którym mowa w ROZPORZĄDZENIU PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Dz.U.UE.L.2016.119.1 z dnia 2016.05.04.

II. Definicje

1) **Administrator danych** Organizacja …. z siedzibą w … (zwana również jako **ADO**),
2) **Inspektor Ochrony Danych Osobowych** lub **IOD** – osoba wyznaczona przez Administratora danych na podstawie art. 37 RODO, realizująca zadania przewidziane w Rozporządzeniu oraz inne obowiązki powierzone przez administratora danych,
3) **Administrator Systemów Informatycznych** lub **ASI** – osoba wyznaczona przez Administratora danych, realizująca obowiązki powierzone przez Administratora danych w zakresie dotyczącym systemów informatycznych,
4) **dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
5) **informatyczne nośniki danych** – materiały lub urządzenia służące do zapisywania, przechowywania i odczytywania danych osobowych w postaci cyfrowej lub analogowej,
6) **integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
7) **minimalizacja danych** – właściwość zapewniająca, że dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,
8) **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
9) **przejrzystość** – właściwość zapewniająca, że dane są przetwarzane zgodnie z prawem, rzetelnie a osoba, której dane są przetwarzane jest informowana w sposób jasny i zrozumiały o swoich prawach i obowiązkach,
10) **przetwarzanie** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie,

rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

11) **podmiot przetwarzający -** oznacza organizację lub osobę, której … powierzyła przetwarzanie danych osobowych,
12) **rozliczalność danych** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi i podmiot ten wykazuje przestrzeganie zasad ochrony danych osobowych, zgodnie z Rozporządzeniem
13) **RODO** lub **Rozporządzenie** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Dz.U.UE.L.2016.119.1 z dnia 2016.05.04,
14) **Rejestr** lub **RCPD** – oznacza Rejestr Czynności Przetwarzania Danych Osobowych,
15) **ustawa** ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000, z późn. zm.),
16) **usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą (”anonimizacja”),
17) **użytkownik** – osoba upoważniona przez Administratora danych do przetwarzania danych osobowych,
18) **państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego
19) **zasady przetwarzania danych osobowych** – zbiór wytycznych realizowanych przez Administratora danych w wykonaniu obowiązków na podstawie Rozporządzenia.

III. Cel Polityki ochrony danych osobowych

Celem niniejszej Polityki jest ochrona danych osobowych przetwarzanych w … przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.

IV. Zasady przetwarzania danych osobowych

W … przestrzegane są następujące zasady przetwarzania danych osobowych:

1) *zasada zgodności z prawem, rzetelności i przejrzystości*
2) *zasada ograniczenia celu przetwarzania danych*
3) *zasada minimalizacji danych*
4) *zasada prawidłowości danych*
5) *zasada ograniczenia przechowania danych*
6) *zasada integralności i poufności danych*
7) *zasada rozliczalności*
8) *prawo do przenoszenia danych*
9) *zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach.*

Ad.1) Zasada zgodności z prawem, rzetelności i przejrzystości.

Komunikaty związane z przetwarzaniem danych osobowych są łatwo dostępne i zrozumiałe ***oraz*** sformułowane jasnym i prostym językiem. Informacje te są przekazywane w formie elektronicznej za pomocą stron internetowych. Ponadto administrator w sposób bezpośredni powiadamia osoby, których dane dotyczą, wysyłając do nich bezpośrednio w formie tradycyjnej papierowej lub w formie elektronicznej klauzule informacyjne, w których podaje informacje przewidziane w Rozporządzeniu. Administrator podaje te informacje zarówno w przypadku zbierania danych od osoby, której dane dotyczą, jak i w przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą.

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawnił dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Ad. 2) Zasada ograniczenia celu przetwarzania danych

Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach, wynikających z działań statutowych administratora i nieprzetwarzane dalej niezgodnie z tymi celami. Osoby, których dane dotyczą, są informowane o celach przetwarzania, zgodnie z zasadami i w sposób określony w pkt. 1) powyżej.

Administrator, w sytuacji gdy planuje przetwarzać dane w innym celu niż zostały zebrane, wysyła przed dalszym przetwarzaniem stosowną informację do osoby, której danej dotyczą i dostarcza jej wszystkich niezbędnych informacji w tym zakresie. Administrator może podjąć decyzję, że dane osobowe będą przetwarzane do celów archiwalnych i statystycznych.

Ad.3) Zasada minimalizacji danych

Zbierane dane nie mogą być gromadzone nadmiernie ilościowo. Muszą one być odpowiednie i stosowne do osiągnięcia celu ich zebrania. Dane mogą być więc przetwarzane tylko w takim zakresie, który jest niezbędny dla osiągnięcia celu ich zebrania. Zbieranie danych, które potencjalnie w przyszłości mogą być użyteczne, ale organizacja nie określiła celu ich wykorzystania, nie jest dopuszczalne. Administrator jest zobowiązany wdrożyć odpowiednie środki techniczne i organizacyjne, aby przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Organizacja stosując zasadę minimalizacji danych, powinna:

- ograniczyć zbieranie danych jedynie do tych, które są niezbędne do osiągnięcia celu oraz
- usunąć dane, gdy staną się one zbędne do osiągnięcia celu przetwarzania.

Administrator powinien wdrożyć odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Środki te powinny umożliwić zapewnienie, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Dane osobowe przetwarzane są w sposób i w czasie niezbędnym do celów, w których są przetwarzane. Celami Administratora są jego prawnie uzasadnione cele wyrażające się w jego działalności statutowej.

Administrator dokonuje okresowo selekcji danych i wybiera tylko taką ilość danych, jaka jest dla niego niezbędna do realizacji celów statutowych.

Ad.4) Zasada prawidłowości danych

Administrator zapewnia prawidłowość i aktualność danych. Każda osoba, której dane dotyczą, może zgłosić administratorowi prośbę o poprawienie, uaktualnienie, sprostowanie danych a także usunięcie danych, które są nieprawidłowe. Po zgłoszeniu pracownicy administratora do tego upoważnieni dokonują poprawienia, aktualizacji, sprostowania lub usunięcia nieprawidłowych danych w zbiorze danych.

Ad.5). Zasada ograniczenia przechowania danych

Dane osobowe są adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Celem administratora jest realizacja prawnie uzasadnionego celu, tj. jego celów statutowych. Działalność administratora jest nieograniczona w czasie. Dlatego też administrator nie określa czasu przechowania danych. Wdraża natomiast procedurę okresowego przeglądu danych i wybiera tylko taką ilość danych, jaka jest dla niego niezbędna do realizacji celów statutowych.

Ad.6). Zasada integralności i poufności danych

Dane osobowe są przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu. Służą temu rozwiązania organizacyjne i techniczne stosowane przez administratora a opisane w pkt. V niniejszej Polityki.

Ad.7). Zasada rozliczalności

Administrator wykazuje przestrzeganie zasad przetwarzania danych osobowych poprzez:

a) informacje dla osób, których dane są przetwarzane na stronach internetowych,
b) informacje dla osób, których dane są przetwarzane przekazywane w sposób bezpośredni w formie elektronicznej lub papierowej w formie klauzul informacyjnych,
c) możliwość uzyskania przez każdą osobę w powszechnie używanym formacie jej danych osobowych,
d) możliwość uzyskania informacji dotyczących danych osobowych na specjalnie przeznaczonych do tego skrzynkach pocztowych, np. <iod@nazwaorganizacji.pl>,
e) dokumentowanie obsługi obowiązków informacyjnych, zawiadomień i żądań osób, których dane dotyczą,
f) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych),
g) rejestr czynności przetwarzania danych dokumentujący podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania,
h) upoważnienia do przetwarzania danych osobowych,

i) umowy z podmiotami, którym powierzono przetwarzanie danych,
j) ewidencja osób upoważnionych do przetwarzania danych osobowych
k) inne rozwiązania organizacyjne i techniczne.

Ad. 8). Prawo do przenoszenia danych

Administrator zapewnia osobie, której dane dotyczą, otrzymanie w powszechnie używanym formacie danych osobowych jej dotyczących. Osoba, której dane dotyczą, ma prawo przesłać te dane osobowe innemu administratorowi. Żądanie przesłania danych osobowych może być zgłoszone drogą elektroniczną na skrzynkę podawczą administratora podaną do powszechnej wiadomości na stronie internetowej lub drogą poczty tradycyjnej. Przesłanie danych odbywa się drogą elektroniczną na podany przez osobę, której dane dotyczą, adres e-mail lub drogą poczty tradycyjnej.

Ad. 9). Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach

Administrator nie podejmuje decyzji w indywidualnych przypadkach, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu.

V. Zakres stosowania Polityki

Niniejsza Polityka dotyczy przetwarzania wszystkich danych osobowych administrowanych przez ADO: w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych a także w systemach informatycznych będących w dyspozycji ADO i zawiera następujące informacje:

A. wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych),
B. rejestr czynności przetwarzania danych osobowych,
C. analiza ryzyka i ocena skutków dla ochrony danych,
D. środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,
E. powierzenie przetwarzania danych osobowych,
F. zasady przekazywania danych osobowych do państwa trzeciego,
G. projektowanie prywatności
H. naruszenia zasad ochrony danych osobowych.

Niniejsza Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych ADO.

A. Obszar przetwarzania danych osobowych

1. Przetwarzanie danych osobowych w ADO odbywa się zarówno przy wykorzystaniu systemów informatycznych, jak i poza nimi, tj. w wersji tradycyjnej, „papierowej". Obszar przetwarzania danych osobowych w ADO został określony w Załączniku nr 1 do niniejszej Polityki pt.: „Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe".

2. Za obszar przetwarzania danych należy rozumieć obszar, w którym wykonywana jest choćby jedna z czynności przetwarzania danych osobowych, w szczególności stanowią go wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarami wskazanym w Załączniku nr 1 do niniejszej Polityki.

B. Rejestr Czynności Przetwarzania Danych

1. ADO opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Rejestr jest jednym z podstawowych narzędzi rozliczania zgodności z ochroną danych u ADO.
2. Dla każdej czynności przetwarzania danych, którą ADO uznał za odrębną dla potrzeb Rejestru, ADO odnotowuje co najmniej:
   a) nazwę czynności,
   b) cel przetwarzania,
   c) opis kategorii osób,
   d) opis kategorii danych,
   e) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu administratora, jeśli podstawą jest prawnie uzasadniony interes,
   f) sposób zbierania danych,
   g) opis kategorii odbiorców danych (w tym przetwarzających),
   h) informację o przekazaniu poza EOG
   i) ogólny opis technicznych i organizacyjnych środków ochrony danych.
3. Wzór Rejestru stanowi Załącznik nr 2 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych". Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych … rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

C. Analiza ryzyka i ocena skutków dla ochrony danych

1. ADO zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez ADO.
2. ADO przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu ADO:
   a) zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych,
   b) kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają,
   c) przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. ADO analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia
3. ADO dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

D. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. ADO ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. Do elementów zabezpieczenia danych osobowych u ADO zalicza się:
   d) stosowane metody ochrony pomieszczeń, w których przetwarzane są dane osobowe (zabezpieczenia fizyczne),
   e) nadzór inspektora ochrony danych nad wprowadzonymi zasadami i procedurami zabezpieczenia danych (zabezpieczenie organizacyjne),
   f) odpowiednie środki zabezpieczenia danych w systemach informatycznych w … (zabezpieczenia techniczne).

   a) zabezpieczenia fizyczne obejmują:
      a. wydzielenie obszaru przetwarzania danych u ADO,
      b. dostęp do pomieszczeń ADO jest pilnowany przez portiera oraz monitorowany przez kamery systemu telewizji dozorowej z rejestracją,
      c. samodzielny dostęp do pomieszczeń ADO jest możliwy wyłącznie dla osób upoważnionych, wstęp osób postronnych jest możliwy jedynie podczas obecności pracowników ADO,
      d. dodatkowe zabezpieczenie części biurowej zaplecza technicznego poprzez wydzielenie pomieszczenia serwerowni, z dostępem tylko dla osób upoważnionych,
      e. przechowywanie akt w wersji papierowej w specjalnie do tego celu przeznaczonych pomieszczeniach, w zamykanych na klucz szafach,
      f. kopie zapasowe zbioru danych osobowych przechowywane są w sejfie w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco,
      g. w pomieszczeniu, w którym znajduje się serwerownia uruchomiony jest ciągły system kontroli warunków klimatycznych (temperatura, wilgotność, zasilanie, dym) z powiadomieniem SMS w przypadku przekroczenia wartości granicznych
      h. budynki, w których odbywa się przetwarzanie danych osobowych dodatkowo są zabezpieczone przez system alarmowy.

   b) zabezpieczenia organizacyjne obejmują:
      a. osobą odpowiedzialną za bezpieczeństwo danych osobowych u ADO jest Inspektor Ochrony Danych (IOD) oraz Administrator Systemów Informatycznych (ASI), którzy opracowują i aktualizują niniejszą Politykę wraz z załącznikami do niej oraz Instrukcję zarządzania systemami informatycznym służącymi do przetwarzania danych osobowych,
      b. pracownicy ADO, którzy na bieżąco kontrolują pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą, o zaobserwowanych nieprawidłowościach informują IOD oraz ASI;
      c. Inspektorowi Ochrony Danych oraz Administratorowi Systemów Informatycznych przysługują następujące kompetencje dla wykonywania funkcji nadzoru:
         i. aktualizacja wymaganej prawem dokumentacji, w skład której wchodzą m.in. następujące dokumenty wewnętrzne: „Polityka Ochrony Danych Osobowych" oraz „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania

danych osobowych" a także nadzorowanie opracowywania wymaganej prawem dokumentacji,

ii. nadawanie upoważnień do przetwarzania danych osobowych u ADO wypadkach przewidzianych w niniejszej Polityce; wzór upoważnienia stanowi Załącznik nr 3 do niniejszej Polityki,

iii. udział w czynnościach kontrolnych dokonywanych u ADO przez organy państwowe uprawnione w zakresie ochrony danych osobowych,

iv. weryfikowanie sprzętu i oprogramowania eksploatowanego przez ADO pod względem zgodności z przepisami o ochronie danych osobowych,

v. podejmowanie działań w przypadku naruszeń ochrony danych osobowych u ADOADO, w tym przywrócenie stanu prawidłowego, zidentyfikowanie przyczyn naruszenia
i osób odpowiedzialnych, przedstawienie wniosków członkom Zarządu ADO,

vi. informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów,

vii. monitorowanie przestrzegania Rozporządzenia oraz procedur i polityk Administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, podejmowanie działań zwiększających świadomość, organizowanie szkoleń personelu uczestniczącego w operacjach przetwarzania oraz przeprowadzanie audytów zgodności przetwarzania danych z obowiązującym prawem,

viii. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania, zgodnie z art. 35 RODO,

ix. współpraca z organem nadzorczym,

x. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z konsultacjami o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,

xi. wykonywanie innych zadań określonych w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

d. Inspektorowi Ochrony Danych przysługują następujące kompetencje do wykonywania funkcji nadzoru:

i. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz przeprowadzanie audytów w tym zakresie i opracowanie sprawozdania dla administratora danych,

ii. zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,

iii. kontrolowanie prawidłowego wykonania wdrożonych do stosowania u ADO dokumentów wewnętrznych,

iv. kontrolowanie w miarę możliwości zabezpieczeń technicznych i organizacyjnych podmiotów trzecich, którym ADO powierzył do przetwarzania dane osobowe,

v. żądanie od pracowników stosownych informacji i dokumentów związanych z przetwarzaniem danych osobowych u ADO,

vi. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia bezpieczeństwa ochrony danych osobowych w ADO.

e. W przypadku stwierdzenia nieprawidłowości w zakresie przetwarzania, w szczególności zabezpieczenia danych osobowych, Inspektor Ochrony Danych oraz Administrator Systemów Informatycznych ma prawo pouczać i instruować osoby, które dopuściły się uchybień a także wydawać im polecenia mające na celu przywrócenie stanu prawidłowego, z tym, że ASI posiada to uprawnienie wyłącznie odnośnie korzystania z systemu informatycznego.

f. W przypadku stwierdzenia nieprawidłowości w zakresie przetwarzania, w szczególności zabezpieczenia danych osobowych, Inspektor Ochrony Danych ma prawo:
   i. zwracać się do członków Zarządu ADO o dokonanie zmian w zakresie stosowanych zabezpieczeń organizacyjnych i technicznych,
   ii. zwracać się do upoważnionych w tym zakresie osób u ADO o zmianę zasad powierzenia danych osobowych podmiotom trzecim,
   iii. przedstawiać członkom Zarządu ADO raporty dotyczące stanu zabezpieczenia danych osobowych w ADO, w tym propozycje poprawiające bezpieczeństwo danych oraz wnioski dotyczące odpowiedzialności osób winnych uchybień,
   iv. Inspektor Ochrony Danych kontroluje zasady przestrzegania ochrony danych osobowych. W przypadkach wykrycia rażących zaniedbań w tym zakresie, IOD sporządza ich opis i niezwłocznie przedkłada Zarządowi ADO.

g. Administrator Systemów Informatycznych ma obowiązek informowania IOD o przypadkach naruszeń ochrony danych osobowych w ADO.

h. Pracownicy mający dostęp do danych osobowych, które są w dyspozycji ADO zobowiązani są do utrzymywania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu z określonego stanowiska a także po ustaniu zatrudnienia; w tym celu pracownicy mający dostęp do danych osobowych podpisują oświadczenie o utrzymywaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia,

i. Przetwarzanie danych osobowych może być wykonywane wyłącznie przez osoby, które zostały upoważnione do przetwarzania danych osobowych,

j. Osoby przetwarzające dane osobowe zostały upoważnione do przetwarzania danych osobowych poprzez wpisanie określonych kompetencji do zakresu obowiązków na danym stanowisku. Określone stanowiska wraz z przypisanym zakresem upoważnienia znajdują się w ewidencji osób upoważnionych do przetwarzania danych osobowych, stanowiącej załącznik 4 do niniejszej Polityki.

c) zabezpieczenia techniczne obejmują:

a. mechanizmy kontroli dostępu do systemów informatycznych i ich zasobów; uprawnienia są różne dla różnych grup użytkowników,

b. zastosowanie odpowiednich i regularnych aktualizacji narzędzi ochronnych (firewall, system antywirusowy),

c. system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,

d. dane wykorzystywane do uwierzytelnienia są przesyłane w sieci publicznej przy wykorzystaniu VPN (CheckPoint),

e. tworzone są regularnie kopie zapasowe zbiorów danych przetwarzanych w systemach informatycznych oraz kopie programów służących do przetwarzania danych osobowych,
f. zastosowano zabezpieczenia systemu przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (UPS-y w szafach teleinformatycznych oraz UPS-y przy stanowiskach gdzie są przetwarzane dane osobowe),

2. W ramach zabezpieczenia danych osobowych ochronie podlegają:
   a) sprzęt komputerowy – serwer, komputery osobiste (w tym laptopy) i inne urządzenia zewnętrzne,
   b) oprogramowanie,
   c) dane osobowe zapisane na informatycznych nośnikach danych oraz dane przetwarzane w systemach informatycznych,
   d) hasła użytkowników,
   e) bazy danych i kopie zapasowe,
   f) wydruki
   g) związana z przetwarzaniem danych dokumentacja papierowa.

3. Inspektor Ochrony Danych oraz Administrator Systemów Informatycznych będą w miarę potrzeb analizowali zagrożenia i ryzyko w celu weryfikacji środków zabezpieczających. W szczególności taka analiza będzie dokonywana w każdym przypadku istotnych zmian działania lub struktury ADO. Oprócz tego będą w miarę potrzeb dokonywać inwentaryzacji systemów informatycznych i czynności przetwarzania danych osobowych w celu zapewnienia aktualności opisu zawartego w punkcie V niniejszej Polityki oraz Załączniku nr 1 do niniejszej Polityki pt. „Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe u ADO" i Załączniku nr 2 do niniejszej Polityki pt. „Rejestr Czynności Przetwarzania Danych".

E. Powierzenie przetwarzania danych osobowych

1. ADO może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO. ADO przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące Załącznik nr 5 do niniejszej Polityki – „Wzór umowy powierzenia przetwarzania danych".
2. W celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na ADO, przed powierzeniem przetwarzania danych osobowych ADO w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.
3. ADO rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z powyższych zasad powierzenia danych osobowych.

F. Zasady przekazywania danych osobowych do państwa trzeciego

1. ADO rejestruje w Rejestrze przypadki przekazywania danych poza Europejski Obszar Gospodarczy.

2. W przypadku korzystania z rozwiązań informatycznych opartych na usługach świadczonych w chmurze obliczeniowej lub serwisowanych poza Europejskim Obszarem Gospodarczym ADO zapewnia mechanizm, który zgodnie z prawem Unii Europejskiej legalizuje transfer danych osobowych i zapewnia odpowiednie gwarancje ich ochrony.

G. Projektowanie prywatności

ADO zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania. W tym celu zasady prowadzenia projektów i inwestycji przez ADO odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

H. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, należy niezwłocznie powiadomić Inspektora Ochrony Danych Osobowych.
2. Typowe sytuacje, gdy użytkownik powinien powiadomić Inspektora Ochrony Danych Osobowych:
   a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
   b) dokumentacja jest niszczona bez użycia niszczarki;
   c) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
   d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;
   e) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
   f) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz firmy bez upoważnienia IOD;
   g) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej;
   h) telefoniczne próby wyłudzenia danych osobowych;
   i) kradzież komputerów lub CD, twardych dysków, pendrive z danymi osobowymi;
   j) maile zachęcające do ujawnienia identyfikatora lub hasła;
   k) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów
   l) hasła do systemów przechowywane są w pobliżu komputera.
3. W razie niemożliwości zawiadomienia Inspektora Ochrony Danych Osobowych lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.
4. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Inspektora Ochrony Danych Osobowych lub upoważnionej przez niego osoby, należy:
   a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   c) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,

d) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
e) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
f) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
g) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD lub osoby upoważnionej.

5. Po przybyciu na miejsce naruszenia ochrony informacji, Inspektor Ochrony Danych Osobowych lub osoba go zastępująca:
   a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy,
   b) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   c) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych,
   d) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, z zewnętrznymi specjalistami.
6. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Inspektor Ochrony Danych Osobowych zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
7. Inspektor Ochrony Danych Osobowych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:
   a) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   b) określenie czasu i miejsca naruszenia i powiadomienia,
   c) określenie okoliczności towarzyszących i rodzaju naruszenia,
   d) kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
   e) wyszczególnienie wziętych pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   f) wstępną ocenę przyczyn wystąpienia naruszenia,
   g) opis możliwe konsekwencje naruszenia ochrony danych osobowych,
   h) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego, w szczególności opis zastosowanych lub proponowanych środków w celu zaradzenia naruszeniu ochrony danych osobowych lub zminimalizowania jego ewentualnych negatywnych skutków.
8. Wzór raportu z naruszenia ochrony danych załącznik nr 6 do niniejszej Polityki.
9. Wzór rejestru naruszeń ochrony danych stanowi załącznik nr 7 do niniejszej Polityki.
10. Inspektor Ochrony Danych Osobowych niezwłocznie przekazuje raport, o którym mowa powyżej, Administratorowi danych.
11. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki - w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
12. Zgłoszenie, o którym mowa w ust. 10 powyżej, musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

13. Jeżeli zgłoszenia do organu nadzoru nie da się udzielić jednorazowo, należy go udzielać sukcesywnie bez zbędnej zwłoki.
14. Jeśli zdarzenie ma charakter przestępstwa, sprawa kierowana jest do organów ścigania.
15. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, chyba że:
    a) wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
    b) zastosowano następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
    c) wymagałoby ono niewspółmiernie dużego wysiłku; w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
16. Zawiadomienie, o którym mowa w ust. 14 powyżej, powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej następujące informacje:
    a) imię i nazwisko oraz dane kontaktowe IOD,
    b) opis możliwych konsekwencji naruszenia ochrony danych osobowych,
    c) opis środków zastosowane lub proponowane przez Administratora danych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
17. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Administratora Danych, IOD, ASI oraz osób wyznaczonych przez Administratora danych.
18. Analiza powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.
19. Inspektor Ochrony Danych Osobowych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Wzór rejestru naruszeń ochrony danych stanowi załącznik nr 7 do niniejszej Polityki.

VI. Postanowienia końcowe

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, przepisów o ochronie danych osobowych.

2. Integralną część niniejszej Procedury przetwarzania stanowią następujące załączniki:
   a) Załącznik nr 1 – Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe u ADO
   b) Załącznik nr 2 – Wzór Rejestru Czynności Przetwarzania Danych,
   c) Załącznik nr 3 – Wzór upoważnienia do przetwarzania danych osobowych,
   d) Załącznik nr 4 – Ewidencja osób upoważnionych do przetwarzania danych osobowych w Organizacji.
   e) Załącznik nr 5 – Wzór umowy powierzenia przetwarzania danych,
   f) Załącznik nr 6 – Wzór raportu z naruszenia ochrony danych rejestru naruszeń ochrony danych
   g) Załącznik nr 7 – Wzór rejestru naruszeń ochrony danych.

Załącznik nr 1 do Polityki Ochrony Danych Osobowych:

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowych w Organizacji

Lp.	Lokalizacja – adres i numer budynku	Nazwa pomieszczenia/ przeznaczenie	Zabezpieczenie pomieszczenia
1	ul. …….	Pomieszczenie Zarządu ……..	- dostęp do budynku tylko dla upoważnionych osób (domofon kodowany) - budynek posiada system telewizji dozorowej z rejestracją - budynek posiada system alarmowy - każde z pomieszczeń zamykane jest na klucz
2	ul. ……	Pomieszczenie Księgowości	- dostęp do budynku tylko dla upoważnionych osób (domofon kodowany) - budynek pilnowany przez portiera oraz system telewizji dozorowej z rejestracją - pomieszczenie posiada system alarmowy - pomieszczenie jest zamykane na klucz
3			

Załącznik nr 2 do Polityki Ochrony Danych Osobowych:

Wzór Rejestru Czynności Przetwarzania Danych

(na osobnej karcie A3)

Załącznik nr 3 do Polityki Ochrony Danych Osobowych:

Wzór upoważnienia do przetwarzania danych osobowych

Warszawa, ……r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej RODO, niniejszym upoważniam:
Panią/Pana ……..
do przetwarzania danych osobowych w Stowarzyszeniu/Fundacji ……. z siedzibą w ……., ul. ……, …….. (zwanym/zwaną dalej Stowarzyszeniem/Fundacją) w następującym zakresie:

A. Okres upoważnienia:

• na okres trwania stosunku pracy w Stowarzyszeniu/Fundacji

B. Zakres upoważnienia:

- dane przetwarzane na nośnikach papierowych
- system informatyczny oraz urządzenia wchodzące w jego skład
- dane osobowe objęte:
  a) Zbiorem …… (TAK/NIE) *
  b) Zbiorem …… (TAK/NIE) *
  c) Zbiorem ……. (TAK/NIE) *
  d) Zbiorem …….. (TAK/NIE) *

(podgląd danych *, wprowadzanie danych *, opracowywanie danych *, zmienianie danych *)

……..

Załącznik nr 4 do Polityki Ochrony Danych Osobowych:

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH
Stowarzyszenie/Fundacja

PRACOWNICY:

L.p.	Imię	Nazwisko	zakres upoważnienia	Uwagi
1				
2				
3				
4				
5				
6				

ZLECENIOBIORCY

1			dane na nośnikach papierowych, zbiór internetowy	Umowa zlecenia
2			dane na nośnikach papierowych, zbiór internetowy	Umowa zlecenia
3			dane na nośnikach papierowych, zbiór internetowy	Umowa zlecenia

Załącznik nr 5 do Polityki Ochrony Danych Osobowych:

Wzór umowy powierzania przetwarzania danych osobowych

Przykładowy wzór umowy powierzenia stanowi Załącznik nr 1 do niniejszego Kodeksu

Załącznik nr 6 do Polityki Ochrony Danych Osobowych:

Wzór raportu naruszeń ochrony danych

STOWARZYSZENIE/ FUNDACJA z siedzibą w przy ul. ……., wpisane pod numerem …… do Rejestru Przedsiębiorców a także stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz publicznych zakładów opieki zdrowotnej, prowadzonego przez Sąd Rejonowy …… w ……, Wydział XI Gospodarczy, posiadający REGON: ……., NIP: ……..

RAPORT Z NARUSZENIA OCHRONY DANYCH

Miejsce……Data ……. Godzina ……

1. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem *(imię, nazwisko, stanowisko służbowe):*
……..
……..

2. Czas i lokalizacja zdarzenia *(numer pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):*
……
……

3. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:
……
……

4. Kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie:
……
……

5. Podjęte działania:
……
……

6. Wstępna ocena przyczyn wystąpienia naruszenia:
……..
……

7. Możliwe konsekwencje naruszenia ochrony danych osobowych:
……..

……

8. Postępowanie wyjaśniające i naprawcze *(w tym opis zastosowanych lub proponowanych środków w celu zaradzenia naruszeniu ochrony danych osobowych lub zminimalizowania jego ewentualnych negatywnych skutków)*:

……..

……

…… ……..

(podpis pracownika) (data i podpis IOD)

Załącznik nr 7 do Polityki Ochrony Danych Osobowych:

Wzór rejestru naruszeń ochrony danych

(na osobnej karcie A3)

Załącznik nr 4 - Wzór Instrukcji zarządzania systemami informatycznymi

INSTRUKCJA ZARZADZANIA SYSTEMAMI INFORMATYCZNYMI PRZETWARZAJĄCYMI DANE OSOBOWE

1. Postanowienia ogólne

Niniejsza Instrukcja Zarządzania Systemami Informatycznymi Organizacji …. *(zwanej dalej ADO*) jest dokumentem regulującym zasady oraz procedury zarządzania i administrowania systemami informatycznymi ADO. Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych, w szczególności zaś osoby pełniące funkcje:

1) Inspektora Ochrony Danych (IOD);
2) Administratora Systemów Informatycznych (ASI);
3) bezpośrednich przełożonych osób przetwarzających dane osobowe;
4) inne osoby wskazane przez Inspektora Ochrony Danych, w tym osoby z podmiotów zewnętrznych współpracujące z ADO i współuczestniczące w procesie przetwarzania danych osobowych.

2. Podstawa prawna

1) ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).Dz.U.UE.L.2016.119.1 z dnia 2016.05.04. (RODO),
2) ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku (tj.: Dz. U. 2018 poz. 1000).

3. Zakres Instrukcji

Niniejsza Instrukcja zawiera między innymi:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemów;
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5) sposób, miejsce i okres przechowywania:
   a) elektronicznych nośników informacji zawierających dane osobowe
   b) kopii zapasowych, o których mowa w pkt 14
6) sposób zabezpieczenia systemów informatycznych przed działalnością szkodliwego oprogramowania;

7) monitorowanie dostępu do danych, w tym sposób realizacji wymogu odnotowywania przez systemy informatyczne informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia;
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

4. Definicje

1) ***Administrator Danych Osobowych (ADO)*** – Organizacja z siedzibą w … przy ul …; zwana dalej Administratorem lub ADO.
2) ***Inspektor Ochrony Danych Osobowych (IOD)*** – osoba wyznaczona przez Administratora danych na podstawie art. 37 RODO, realizująca zadania przewidziane w Rozporządzeniu oraz inne obowiązki powierzone przez administratora danych).
3) ***Administrator Systemów Informatycznych (ASI)*** – wyznaczony przez Administratora Danych Osobowych pracownik bądź współpracownik zatrudniony na Stanowisku Informatyk lub współpracujący z Administratorem Danych Osobowych w zakresie wykonywania czynności informatycznych, odpowiedzialny za wdrożenie i stosowanie zasad bezpieczeństwa systemów informatycznych, zobowiązany do stosowania technicznych i organizacyjnych środków ochrony przewidzianych w systemach informatycznych.
4) ***Użytkownik systemu*** – osoba posiadająca upoważnienie do wprowadzania i przetwarzania danych w systemie informatycznym w zakresie wskazanym w upoważnieniu.
5) ***Podmiot zewnętrzny*** – osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, z którą ADO zawarła umowę o powierzeniu do przetwarzania danych osobowych lub inną, na podstawie której możliwy jest dostęp i przetwarzanie danych osobowych.
6) ***Dane osobowe*** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
7) ***Przetwarzanie danych*** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
8) ***Polityka Ochrony Danych Osobowych*** – polityka ochrony danych osobowych obowiązująca przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich procesach przetwarzania danych osobowych w związku i w celach związanych z działalnością ADO.
9) ***Instrukcja*** – niniejszy dokument.
10) ***Rejestr czynności przetwarzania danych osobowych***, zwany dalej ***Rejestrem*** – rejestr określony w art. 30 RODO, w którym odnotowywane są m.in. cele przetwarzania dla poszczególnych czynności przetwarzania, opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych; kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych.

11) ***Hasło*** – ciąg znaków literowych, cyfrowych lub innych specjalnych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
12) ***Identyfikator użytkownika*** – ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym.
13) ***Sieć LAN*** – sieć lokalna umożliwiająca połączenie komputerów, serwerów i innych urządzeń sieciowych przy wykorzystaniu aktywnych i pasywnych elementów sieci.
14) ***Sieć publiczna (Internet)*** – sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych
15) ***Chmura –*** *model przetwarzania danych opartych na użytkowaniu usług dostarczonych przez wewnętrzny dział lub zewnętrznego dostawcę.*
16) ***System informatyczny*** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania m.in. danych osobowych.
17) ***Integralność*** – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
18) ***Rozliczalność*** – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
19) ***Niezaprzeczalność*** – brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.
3) ***RODO –*** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Dz.U.UE.L.2016.119.1 z dnia 2016.05.04. (RODO),
20) ***Ustawa*** – ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku (Dz. U. 2018 poz. 1000).

5. **Poziom bezpieczeństwa**

Poziom bezpieczeństwa systemów informatycznych przetwarzających dane osobowe określono jako wysoki.

6. **Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej**

Zabezpieczenia odnoszą się do:

1) technicznych środków zabezpieczenia komputerów przed skutkami awarii zasilania,
    a. Zastosowano urządzenia do podtrzymywania zasilania (UPS)
2) opisu infrastruktury sieci informatycznej, w której użytkowane są komputery wykorzystywane do przetwarzania danych osobowych,
    a. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje na użytkowanie oprogramowania komputerowego;
3) sprzętowych i programowych środków ochrony przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji,

a. Lokalizacja urządzeń komputerowych (komputerów , terminali, drukarek) uniemożliwia osobom niepowołanym (w szczególności gościom, osobom nieupoważnionym) dostęp do nich;
b. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora oraz hasła;
c. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
d. Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.

4) sprzętowych i programowych środków ochrony poufności danych przesyłanych drogą elektroniczną ,
   a. Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
5) sprzętowych i programowych środków ochrony przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych,
   a. Zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak m.in. wirusy, robaki, trojany, rootkit, backdoor, keylogger, ransomware, inne;
   b. Użyto urządzeń dostępowych do Internetu z kontrolą ruchu sieciowego oraz wykrywaniem i blokowaniem ataków (Firewall z IPS)..

7. **Zabezpieczenia baz danych i oprogramowania przetwarzającego dane osobowe**

Opis technicznych i programowych środków bezpieczeństwa zastosowanych w procedurach, aplikacjach i programach oraz innych narzędziach programowych wykorzystywanych do przetwarzania danych osobowych.

1) Dostęp do zbioru danych osobowych (do baz danych i do programów) wymaga uwierzytelnienia z wykorzystaniem identyfikatora oraz hasła.
2) Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych oraz ustalono wymagania dotyczące samego hasła, takie jak: minimalna długość hasła, użycie dużych i małych liter, użycie cyfr, użycie znaków specjalnych.
3) Zastosowano mechanizm blokady dostępu po 3 próbach nieudanego logowania się.
4) Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
5) Zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych.
6) Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
7) Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
8) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

9) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika (automatyczny wygaszacz ekranu po 15 minutach)
10) Zastosowano system antywirusowy na stanowiskach, na których przetwarzane są dane osobowe.
11) Zastosowano automatyczne aktualizacje systemów operacyjnych oraz innego oprogramowania – jeśli producent oprogramowania to umożliwia.

8. **Procedura dostępu podmiotów zewnętrznych**

Celem procedury jest zapewnienie bezpiecznego przetwarzania danych osobowych przez podmioty zewnętrzne, gdy cel i zakres tego przetwarzania określa Administrator Danych.

1) ADO prowadzi rejestr podmiotów zewnętrznych, którym udostępnia dane osobowe oraz podmiotów, którym powierzono przetwarzanie danych osobowych w formie usługi zewnętrznej.
2) ADO udostępnia dane osobowe będące w jego obszarze fizycznym podmiotom zewnętrznym w oparciu o umowę poufności bądź oświadczenia o zobowiązaniu do zachowania poufności. Podmiot zewnętrzny zobowiązany jest do zachowania poufności udostępnionych danych i przetwarzania ich zgodnie z celem umowy zawartej z ADO.
3) ADO powierza dane osobowe do przetwarzania w formie usługi zewnętrznej podmiotom zewnętrznym w oparciu o umowę powierzenia przetwarzania danych.

9. **Procedura korzystania z Internetu**

1) Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2) Zabrania się samodzielnego instalowania oprogramowania bez zgody ASI
3) Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. .
4) Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie ściągnięte z Internetu i przez niego zainstalowane.
5) Zabrania się wchodzenia bądź logowania się na stronach internetowych, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym przez prawo.
6) Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
7) Dla zapamiętywania haseł należy stosować program typu „menedżer haseł”.
8) Należy korzystać wyłącznie z przeglądarek posiadających odpowiednie opcje zabezpieczeń.
9) W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka, protokół https).

10. **Procedura korzystania z poczty elektronicznej**

1) Przesyłanie informacji poza ADO może odbywać się tylko przez osoby do tego upoważnione przez ADO lub IOD.

2) W przypadku przesyłania informacji wrażliwych wewnątrz ADO bądź wszelkich danych osobowych poza ADO należy wykorzystywać mechanizmy kryptograficzne (pakowanie i zabezpieczanie hasłem wysyłanych plików lub podpis elektroniczny).
3) Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
4) Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
5) Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
6)
7) Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.

11. **Procedura nadawania uprawnień do przetwarzania danych osobowych.**

Procedura opisuje zasady: przyznawania, modyfikacji i usuwania uprawnień użytkownika do przetwarzania zbiorów w systemie informatycznym lub w wersji papierowej. Celem procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych osobowych i utraty ich poufności przez osoby nieupoważnione.

a. Zarządzane uprawnieniami użytkowników

1) Przyznanie, zmiana lub cofniecie uprawnień użytkownika do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym realizowane jest na pisemne zlecenie przełożonego bądź osoby upoważnionej przez ADO. Informacja o zleceniu przekazywana jest IOD w formie pisemnej bądź elektronicznej. W przypadku zlecenia nadania bądź zmiany uprawnień (m.in. z powodu zatrudnienia nowej osoby lub zmiany stanowiska pracy), IOD zobowiązany jest do sprawdzenia, czy użytkownik:
    a. odbył szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych,
    b. będzie przetwarzał dane osobowe w zakresie i celu określonym w Polityce ochrony danych osobowych i w niniejszej Instrukcji zarządzania.
2) Po akceptacji zlecenia przez IOD, przełożony lub osoba upoważniona przez ADO przekazuje go bezpośrednio ASI bądź osobie upoważnionej przez ADO celem nadania identyfikatora oraz uprawnień użytkownika w systemie informatycznym.
3) Cofnięcie uprawnień użytkownikowi polega na wyrejestrowaniu go z systemu przez ASI na zlecenie IOD, przełożonego bądź osoby upoważnionej przez ADO. Każdorazowo ASI bądź ADO powinien zawiadomić o tym IOD w formie pisemnej lub elektronicznej.
4) Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielony innej osobie.
5) ADO odpowiada za przechowywanie i aktualizację wszystkich Upoważnień.
6) ADO opowiada za prowadzenie rejestru Upoważnień.
7) IOD nadzoruje rejestr osób upoważnionych przez ADO.

b. Zarządzanie uprawnieniami administratorów

1) ASI jest powoływany przez Zarząd ADO.

2) ASI zobowiązany jest do bieżącej pracy na koncie z ograniczonymi uprawnieniami. Użycie konta z pełnymi uprawnieniami administratora systemu dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.
3) Hasło administratora systemu znane jest tylko ASI odpowiedzialnemu za dany system.
4) W przypadkach awaryjnych (w szczególności nieobecność administratora) hasło może być przekazane osobie zastępującej ASI.
5) Po ustaniu sytuacji awaryjnej Administrator jest zobowiązany do zmiany hasła.

12. **Metody i środki uwierzytelnienia**

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

a. Ogólne zasady postępowania z hasłami

1) ASI informuje w formie elektronicznej użytkownika o nadaniu pierwszego hasła do systemu.
2) Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
3) Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
4) Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
5) Użytkownik zobowiązany jest do cyklicznej – wymuszanej przez system – zmiany hasła.
6) Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
7) W przypadku podejrzenia utraty poufności hasła, należy niezwłocznie zmienić je na nowe.

b. Hasła do sieci i serwera oraz programów przetwarzających dane osobowe

1) Hasło dostępu (do serwera / sieci) składa się z co najmniej 8 znaków.
2) Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3) Zmiana hasła odbywa się nie rzadziej niż raz na 90 dni i jest wymuszana przez system.

c. Hasła do programów przetwarzających dane osobowe

1) Hasło dostępu do programów:……. składa się z co najmniej 8 znaków.
2) Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3) Zmiana hasła odbywa się nie rzadziej niż raz na 90 dni.
4) Zmiana hasła jest wymuszana automatycznie.

d. Hasła administratora

1) Hasło administratora składa się co najmniej z 8 znaków.
2) Administrator systemu zobowiązany jest zmieniać swoje hasło nie rzadziej niż co 60 dni.
3) W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

13. **Procedura rozpoczęcia, zawieszenia i zakończenia pracy**

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

1) Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
2) Użytkownik jest zobowiązany do powiadomienia IOD oraz ASI o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
3) W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi.
4) Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (w szczególności klientom, osobom nieupoważnionym) wglądu do danych wyświetlanych na monitorach komputerowych – zgodnie z tzw. *polityką czystego ekranu*.
5) Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni – po upływie 5 minut system automatycznie aktywuje wygaszacz.
6) Po zakończeniu pracy, użytkownik zobowiązany jest:
   a) wylogować się z systemu informatycznego oraz wyłączyć sprzęt komputerowy.
   b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki , na których mogą znajdować się dane osobowe.

14. **Procedura tworzenia kopii zapasowych**

a. Tworzenie kopii bezpieczeństwa.

1) Kopie zapasowe danych tworzone są automatycznie raz na dobę (po zakończeniu pracy przez użytkowników).
2) Kopie sporządzane są na zewnętrznym urządzeniu lub udostępnionym zasobie sieciowym
3) Kopie całościowe przechowywane są przez 5 lat,
4) Dostęp do kopii mają: ASI.
5) Kopie przechowywane są w innym pomieszczeniu niż pomieszczenie, w którym znajduje się serwer,
6) ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

15. **Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków**

Procedura określa sposób postępowania z nośnikami danych osobowych takimi jak: twarde dyski, płyty CD/DVD/BR, pendrive, telefony komórkowe, pamięci typu „flash", karty pamięci, na których znajdują się dane osobowe celem zabezpieczenia ich przez niszczeniem, kradzieżą, dostępem osób nieupoważnionych.

a. Zabezpieczenie elektronicznych nośników informacji

1) Nośniki danych w tym sprzęt komputerowy, systemy informatyczne oraz kopie bezpieczeństwa, są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
2) Zabrania się wynoszenia poza obszar … wymiennych nośników informacji a w szczególności twardych dysków z zapisanymi danymi osobowymi bez zgody ADO.
3) W sytuacji przekazywania nośników z danymi osobowymi poza obszar ADO należy stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce,
    b. nadawca powinien sporządzić kopię przesyłanych danych,
    c. dane przed wysłaniem powinny zostać zaszyfrowane (np. korzystając z klucza publicznego odbiorcy)
    d. stosować bezpieczne koperty depozytowe,
    e. przesyłkę należy przesyłać przez kuriera
    f. adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.
4) W wypadku potrzeby wyniesienia urządzenia przenośnego (np. laptop, tablet, pendrive) zawierającego dane osobowe, lub inne informacje chronione, urządzenie takie powinno być odpowiednio zabezpieczone, a dane zaszyfrowane.
5) Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania (chyba, że z powodu odrębnych przepisów należy je zachować na dłużej).
6) Podlegające likwidacji uszkodzone lub przestarzałe nośniki, a w szczególności twarde dyski z danymi osobowymi, są komisyjnie niszczone w sposób fizyczny.
7) Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski z danymi osobowymi, powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar ADO.

b. Zabezpieczenie kopii zapasowych

Zabezpieczenie kopii zapasowych opisane jest w procedurach tworzenia kopii zapasowych.

c. Zabezpieczenie dokumentów i wydruków

1) Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie zgodnie z zasadami określonymi w Polityce ochrony danych osobowych obowiązującej u ADO.
2) Za bezpieczeństwo dokumentów i wydruków odpowiedzialne są osoby je przetwarzające oraz kierownicy właściwych działów bądź osoby nadzorujące na zlecenie ADO poszczególne działy, a w szczególności odpowiadają za:
    a. zamykanie dokumentów na klucz w szafach, biurkach, sejfach podczas nieobecności w pomieszczeniach lub po zakończeniu pracy (tzw. polityka czystego biurka).
    b. niszczenie dokumentów i tymczasowych wydruków w niszczarce, niezwłocznie po ustaniu celu ich przetwarzania.
    c. niepozostawianie wydruków i ksero na urządzeniach lub w ich okolicy bez nadzoru.

16. **Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi**

a. Ochrona antywirusowa

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (m.in. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe.

1) Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada ASI, w tym za zapewnienie odpowiedniej ilości licencji dla użytkowników.
2) System antywirusowy zainstalowano na komputerach
3) System antywirusowy zapewnia ochronę: poczta, przeglądarki internetowe, ruch sieciowy, pamięci masowe i przenośne.
4) Program antywirusowy skanuje automatycznie pliki przychodzące na pocztę elektroniczną każdego użytkownika.
5) ASI zapewnia stałą aktywność programu antywirusowego. Tzn. program antywirusowy musi być aktywny podczas pracy wszystkich systemów informatycznych przetwarzających dane osobowe. Aktualizacja definicji wirusów odbywa się automatycznie przez system.
6) W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić ASI.
7) System antywirusowy zapewnia automatyczną aktualizację sygnatur wirusów i innych zagrożeń.

b. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej.

1) Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ASI.
2) Stosowany jest firewall zabezpieczający sieć lokalną oraz systemy przed nieautoryzowanym dostępem, jak również monitorujący i filtrujący ruch wejściowy i wyjściowy z sieci
3) Firewall posiada mechanizmy wykrywania oraz przeciwdziałania atakom (IDS/IPS)
4) Sieć bezprzewodową zabezpieczono szyfrowaniem WPA2 oraz WPA3 (na nowszych urządzeniach).
5) Zastosowano mechanizmy monitorujące przeglądanie Internetu przez użytkowników. Uwzględniają one analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania.

17. **Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych**

1) Odbiorcą danych jest każdy, komu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców (art. 4 pkt 9 RODO).
2) System przetwarzający dane osobowe udostępniane odbiorcom musi umożliwiać rejestrację:

a. nazwy jednostki organizacyjnej lub imienia i nazwiska osoby, której udostępniono dane,
b. zakresu udostępnianych danych
c. daty udostępnienia.

3) Dane osobowe udostępnia się:
   a. osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa,
   b. pozostałym osobom lub podmiotom, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.
4) Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej.
5) Zgody na udostępnienie danych udziela ADO, po zasięgnięciu opinii IOD.
6) Odnotowanie w *Rejestrze wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora* informacji o udostępnieniu danych (komu, zakresie, dacie) powinno nastąpić niezwłocznie po udostępnieniu danych.
7) Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego lub wyciągu z rejestru papierowego a raport przekazywany jest tej osobie.

18. **Procedura wykonywania przeglądów i konserwacji**

Celem procedury jest zapewnienie ciągłości działania systemów informatycznych przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.

a. Przeglądy i konserwacje systemu informatycznego i aplikacji

1) ASI odpowiada za bezawaryjną pracę systemu IT, w szczególności: stacji roboczych, aplikacji serwerowych, baz danych, poczty email.
2) Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI, jednak nie rzadziej, niż raz w roku.
3) Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
4) ASI odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków.
5) ASI odpowiada za sprawdzanie poprawności działania systemu IT, w szczególności: stacji roboczych, serwera, drukarek, baz danych, poczty email.
6) ASI odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
7) Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
8) Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nieposiadające upoważnień do przetwarzania danych muszą być wykonywane pod nadzorem osób upoważnionych.

9) Przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren ADO, należy:
    a. wymontować nośniki z danymi osobowymi,
    b. trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania
    c. nadzorować proces naprawy przez osobę upoważnioną przez administratora systemu, gdy nie ma możliwości usunięcia danych z nośnika.

b. Aktualizacje oprogramowania

1) ASI odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów co do bezpieczeństwa i stabilności nowych wersji.
2) ASI odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.

Załącznik nr 5 - Wzór oświadczenia o przystąpieniu do kodeku postępowania

Warszawa, dnia ……

Konfederacja Inicjatyw
Pozarządowych Rzeczypospolitej Polskiej”
z siedzibą w Warszawie, przy ul. S. Jaracza 10/1
00-378 Warszawa

……..
nazwa organizacji społecznej
……
adres
……

Oświadczenie o przystąpieniu do Kodeksu

Działając w imieniu organizacji …….. z siedzibą w ……, przy ulicy …….oświadczam/y, iż organizacja ……..przystępuje do Kodeksu Dobrych Praktyk w zakresie przetwarzania danych osobowych w organizacjach społecznych i zobowiązuje się do jego przetwarzania.

.....
miejscowość, data

……
podpisy osób upoważnionych do reprezentacji