|  |  |  |  |
| --- | --- | --- | --- |
| **Formularz dla podmiotu przetwarzającego dane osobowe ……………………** | | | |
| Instrukcja wypełniania formularza:   1. Podmiot, wobec którego planowane jest powierzenie przetwarzania danych osobowych / któremu powierzono przetwarzanie danych osobowych w ramach ww. zbioru, wypełnia kolumny pn. *Odpowiedź* oraz *Uwagi*. 2. W przypadku wypełniania przez podmiot formularza po powierzeniu mu przetwarzania danych osobowych, treść niektórych pytań, odpowiadających tej sytuacji, zawarto w przypisie. 3. W części pn. *Ocena zgodności i rekomendacje* administrator danych osobowych może zgłosić podmiotowi, któremu planuje powierzyć przetwarzanie danych osobowych / któremu powierzył przetwarzanie danych osobowych, pewne zalecenia i rekomendacje (bez oficjalnie wiążącego ich charakteru), mające na celu poprawę stopnia bezpieczeństwa przetwarzanych danych poprzez modyfikację stosowanych środków technicznych i organizacyjnych. | | | |
| **lp.** | **PYTANIE** | **ODPOWIEDŹ** (tak / nie / nie dotyczy) | **UWAGI** (dodatkowe informacje) |
| **KWESTIE OGÓLNE** | | | |
| 1. | Czy podmiot przetwarzający powołał w swojej jednostce Inspektora Ochrony danych (IOD) lub inną osobę do wykonywania zadań związanych z ochroną danych osobowych? |  |  |
| 2. | Czy podmiotowi do zrealizowania umowy, która zostanie/została zawarta z administratorem, niezbędne jest przetwarzanie danych osobowych? |  |  |
| 3 | Proszę wskazać w uwagach kategorie danych, których przetwarzanie jest niezbędne do zrealizowania umowy, która zostanie/została zawarta z administratorem/podmiotem przetwarzającym[[1]](#footnote-1). | **Kategorie danych przetwarzanych w ramach realizacji umowy:**   * **Dane identyfikacyjne (np. imię, nazwisko, PESEL, numer dowodu osobistego),** * **Dane kontaktowe (np. adres e-mail, numer telefonu, adres zamieszkania).** |  |
| 4. | Czy podmiot przetwarzający posiada doświadczenie w przetwarzaniu danych osobowych w imieniu innych administratorów? |  |  |
| 5. | Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania (zgodnie z art. 30 ust. 2 RODO) w związku z przetwarzaniem danych osobowych powierzonych przez innych administratorów? Jakie elementy zawiera przedmiotowy rejestr. |  | Podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania. Rejestr zawiera następujące elementy:   * Dane kontaktowe podmiotu przetwarzającego oraz inspektora ochrony danych. * Kategorie przetwarzania danych wykonywanych na zlecenie administratorów. * Informacje o ewentualnych transferach danych do państw trzecich i zastosowanych zabezpieczeniach. |
| **PROCEDURY** | | | |
| 6. | Czy podmiot przetwarzający posiada procedury w obszarze bezpieczeństwa informacji w tym ochrony danych osobowych? Czy te procedury umożliwiają realizację obowiązków podmiotu przetwarzającego zapewniające realizację art. 32 RODO? Jakie to procedury? |  |  |
| 7. | Czy te procedury zapewniają realizację przez podmiot przetwarzający art. 28 RODO ? W jakim zakresie nie realizują postanowień art. 28 RODO? |  |  |
| 8. | Czy podmiot przetwarzający stosuje w swojej działalności zasady *privacy by design* oraz *privacy by default*? |  |  |
| 9. | Czy zastosowano środki kontroli dostępu fizycznego na terenie budynku lub budynków podmiotu przetwarzającego, gdzie realizowana będzie umowa z administratorem? |  |  |
| 10. | Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona), bądź dostęp ten jest szczegółowo nadzorowany? |  |  |
| 11. | Czy podmiot przetwarzający stosuje odpowiednie zabezpieczenia w systemach informatycznych, w których będą przetwarzane dane osobowe w ramach umowy? W uwagach należy wskazać, jakie zabezpieczenia są stosowane, lub odwołać się do dokumentów regulujących tę kwestię. |  |  |
| 12. | Czy każdy pracownik otrzymuje imienny identyfikator do systemów informatycznych? |  |  |
| 13. | Czy systemy informatyczne podmiotu przetwarzającego wymuszają okresową zmianę haseł? |  |  |
| 14. | Czy pracownicy zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób? |  |  |
| 15. | Czy podmiot przetwarzający zainstalował i uaktualnia oprogramowanie antywirusowe w komputerach lub systemach IT używanych do przetwarzania powierzonych mu danych osobowych? |  |  |
| 16. | Czy oprogramowanie, używane w podmiocie przetwarzającym, posiada licencję i jest na bieżąco aktualizowane? |  |  |
| 17. | Czy dyski komputerów przenośnych używane przez podmiot przetwarzający są szyfrowane? |  |  |
| 18. | W jaki sposób są zabezpieczone urządzenia mobilne, używane w podmiocie przetwarzającym? Czy są one zabezpieczone co najmniej hasłem, czy posiadają aktualny program antywirusowy? W jaki sposób zabezpieczony jest przesył danych? |  |  |
| 19. | Czy urządzenia mobilne posiadają skonfigurowaną kontrolę dostępu? |  |  |
| 20. | Czy wobec urządzeń mobilnych stosuje się techniki kryptograficzne? |  |  |
| 21. | Czy na urządzeniach mobilnych zainstalowano oprogramowania antywirusowe? |  |  |
| **PRACOWNICY** | | | |
| 22. | Czy podmiot przetwarzający wdrożył i realizuje szkolenie dla pracowników nowozatrudnionych (przed przystąpieniem do wykonywania przez nich obowiązków związanych z przetwarzaniem danych osobowych) z ochrony danych osobowych i wewnętrznych procedur w tym zakresie? |  |  |
| 23. | Czy podmiot przetwarzający nadaje pracownikom upoważnienia do przetwarzania danych osobowych i dopuszcza do czynności przetwarzania jedynie osoby, które otrzymały takie upoważnienia? Czy został określony w szczególności zakres przetwarzanych przez te osoby danych? |  |  |
| 24. | Czy podmiot przetwarzający zobowiązuje pracowników do stosowania obowiązujących w jego jednostce procedur w obszarze ochrony danych osobowych i weryfikuje ich stosowanie? Należy wskazać w uwagach, w jaki sposób potwierdzane jest to zobowiązanie, oraz jak odbywa się weryfikacja jego realizacji. |  |  |
| 25. | Czy pracownicy podmiotu przetwarzającego, którzy przetwarzają dane osobowe, zostali zobowiązani do zachowania ich w tajemnicy ? |  |  |
| 26. | Czy pracownicy przetwarzający dane osobowe w formie papierowej zabezpieczają je przed dostępem do nich osób nieuprawnionych? Jakie narzędzia i procedury bezpieczeństwa stosowane są w tym obszarze? |  |  |
| **INNE** | | | |
| 27. | Czy podmiot przetwarzający prowadzi rejestr naruszeń ochrony danych osobowych? |  |  |
| 28. | Czy podmiot przetwarzający posiada wdrożone mechanizmy identyfikacji oraz oceny i notyfikacji naruszeń ochrony danych osobowych? |  |  |
| 29. | Czy podmiot przetwarzający posiada regulacje w zakresie zapewnienia ciągłości działania? |  |  |
| 30. | Czy w przypadku incydentu w zakresie danych osobowych zapewniono możliwość szybkiego przywrócenia danych i dostępu do nich? |  |  |
| 31. | Czy podmiot przetwarzający dokonał oszacowania ryzyka przetwarzania danych osobowych i czy w jego wyniku konieczne okazało się sporządzenie oceny skutków dla ochrony danych (DPIA)? |  |  |
| 32. | Czy i w jaki sposób podmiot przetwarzający zapewnia realizację praw osób, których dane dotyczą? Czy posiada w tym zakresie ustalone procedury postępowania? |  |  |
| 33. | Czy dostawca posiada certyfikaty w zakresie bezpieczeństwa informacji lub wdrożył system zarządzenia bezpieczeństwa informacji? |  |  |
| 34. | Jeżeli dostawca dokonuje transferów danych do państw poza EOG, to czy zapewniony jest mechanizm legalizujący taki transfer? |  |  |
| 35. | Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 RODO? |  |  |
| 36. | Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych? |  |  |
| 37. | Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? |  |  |
| 38. | Czy zapewniono fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez organizację od tych, które należą do innych organizacji? |  |  |
| 39. | Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |  |  |
| 40. | Jaki przyjęto zakres oraz częstotliwość tworzenia kopii zapasowych? |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **OCENA ZGODNOŚCI Z RODO PRZEDSTAWIONYCH PRZEZ PODMIOT PRZETWARZAJACY INFORMACJI**  **ORAZ EWENTUALNE ZALECENIA I REKOMENDACJE ZE STRONY ADMINISTRATORA** | | | |
|  | | | |

1. W przypadku wypełniania formularza przed podpisaniem umowy powierzenia, zakres danych planowanych do powierzenia powinien być ograniczony do takich danych, które są niezbędne do zrealizowania celu zawieranej umowy . W przypadku wypełniania formularza po zawarciu umowy powierzenia, należy wziąć pod uwagę zakres danych powierzonych do przetwarzania - w uwagach można wskazać, że przetwarzany będzie jedynie ten zakres danych. [↑](#footnote-ref-1)