Odpowiedzialność i zadania innych niż PSP jednostek ochrony przeciwpożarowej mających dostęp do SWD PSP

Inne jednostki ochrony przeciwpożarowej, które zostaną dopuszczone do przetwarzania

danych w SWD PSP, na mocy odrębnych przepisów, są zobowiązane do:

1. Dopuszczania do pracy w SWD PSP wyłącznie osób spełniających minimalne wymogi odnośnie bezpieczeństwa osobowego. Oznacza to, że każda osoba mająca przetwarzać dane, które będą trafiały do SWD PSP powinna: posiadać imienne upoważnienie pisemne do przetwarzania danych osobowych wydane przez właściwego administratora, podpisać oświadczenie o poufności zawierające dodatkowo informację o zapoznaniu się z procedurami, przepisami i instrukcjami oraz zobowiązanie do ich przestrzegania, odbyć szkolenie obejmujące zasady przetwarzania w systemach teleinformatycznych oraz ochrony danych osobowych. Dodatkowo każda osoba mająca przetwarzać dane w SWD PSP powinna dodatkowo: posiadać dokument zatwierdzony przez administratora, upoważniający do przetwarzania danych w systemie teleinformatycznym łączące jego nazwę oraz nazwę użytkownika, pod którą dozwolone jest przetwarzanie danych dla danej osoby.
2. Prowadzenia i aktualizowania ewidencji osób upoważnionych do przetwarzania danych osobowych w SWD PSP.
3. Prowadzenia szkoleń dla użytkowników w zakresie bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych.
4. Regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
5. Zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, w tym tworzenia zabezpieczeń technicznych, ograniczeń dostępu fizycznego i zdalnego, przestrzegania zasad zarządzania - administrowania, zarządzania użytkownikami i uprawnieniami w odniesieniu do sieci oraz stacji roboczych i oprogramowania końcowego.
6. Zapewnienia rozliczalności operacji przetwarzania.
7. Zgłaszania naruszeń i przeprowadzania postępowań po ich stwierdzeniu.
8. Wykonania obowiązku informacyjnego oraz udostępnienia treści uzgodnień strażakom i innym osobom z własnych jednostek, których dane dotyczą.
9. Zapewnienia współpracy z IOD z właściwej jednostki PSP oraz UODO.
10. Zapewnienia przestrzegania obowiązujących przepisów i procedur wewnętrznych przez własnych członków i pracowników.

Dodatkowo inne jednostki ochrony przeciwpożarowej, są również obowiązane do

przestrzegania minimalnych wymogów bezpieczeństwa dotyczących przetwarzania

danych osobowych w SWD PSP w zakresie:

1. Zbierania danych, tj.:

a. osoby pozyskujące dane powinny spełniać minimalne wymogi odnośnie bezpieczeństwa osobowego opisane powyżej.

2. Utrwalania danych, tj.:
   a. Dane zbierane w związku z prowadzonymi działaniami ratowniczymi mogą być pierwotnie utrwalane na nośnikach tradycyjnych – papierowych, skąd niezwłocznie przenoszone są do SWD PSP. Dane utrwalone w formie papierowej (notatki odręcznej) powinny zostać zniszczone, po ich skutecznym przeniesieniu do SWD PSP, chyba, że zostały lub będą włączone do akt sprawy. Odpowiedzialność za te czynności spoczywa na osobie pierwotnie utrwalającej dane;
   b. Wyjątek mogą stanowić notatniki KDR i notatniki dyżurnego stanowiska kierowania/punktu alarmowego (dyżurnego), które podlegają rejestracji wiążącej notatnik z konkretną osobą odpowiedzialną. Notatniki te podlegają niszczeniu do 3 miesięcy po upływie roku kalendarzowego, w którym zostały wytworzone. Dokumentacja w postaci notatników KDR i dyżurnych powinna być odpowiednio chroniona przed dostępem osób nieupoważnionych;
   c. Dokumentacja multimedialna (audio, zdjęcia i wideo) powinna być wykonywana za pomocą sprzętu służbowego przez osoby spełniające minimalne wymogi odnośnie bezpieczeństwa osobowego;
   d. Użycie sprzętu prywatnego do wykonywania dokumentacji multimedialnej dozwolone jest wyłącznie za wiedzą i zgodą właściwego administratora;
   e. Zabrania się wykorzystywania ogólnie dostępnych systemów informatycznych, w tym mediów społecznościowych w celu przetwarzania dokumentacji ze zdarzenia, a zwłaszcza dokumentacji multimedialnej (audio, zdjęcia, wideo);
   f. Podczas zgrywania materiałów z urządzeń w celu ich dalszego przetwarzania, należy dokonać ich przeglądu pod kątem niezbędności ich przechowywania oraz adekwatności zawartości w odniesieniu do celu, jakim jest dokumentowanie działań ratowniczych;
   g. Systemy informatyczne, służące do przechowywania materiałów multimedialnych powinny spełniać wymogi bezpieczeństwa analogiczne jak określone dla SWD PSP;
   h. Administrator może zdecydować o wykorzystaniu wybranej dokumentacji multimedialnej do celów związanych z działalnością informacyjną oraz do działań związanych z zapobieganiem powstawania i rozprzestrzeniania się pożarów, klęsk żywiołowych lub innych miejscowych zagrożeń w ramach prewencji społecznej.
3. Przekazywania danych za pomocą środków łączności, tj.:
   a. Przekazując i przyjmując dane w formie informacji ustnej, za pomocą środków łączności, należy zawsze mieć na względzie ochronę danych osobowych; nie wolno robić tego w obecności osób nieupoważnionych;
   b. Zabronione jest przekazywanie za pomocą niekodowanych środków łączności informacji, które umożliwiają zidentyfikowanie konkretnych osób, w tym obejmujących szczególne kategorie danych osobowych, o których mowa w art. 9 ust 1 RODO.
4. Usuwania danych, tj.: usunięcie danych z SWD PSP może nastąpić wyłącznie w przypadkach określonych w art. 17 RODO, na pisemny wniosek osoby, której dane dotyczą lub z inicjatywy administratora.

5. Zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, tj.:
    a. W zakresie funkcjonowania stacji roboczych i oprogramowania końcowego:
        - urządzenia muszą być zlokalizowane w pomieszczeniach spełniających wymogi bezpieczeństwa fizycznego dla przetwarzania danych osobowych,
        - sprzęt oraz oprogramowanie na nim używane musi być wyposażone w zabezpieczenia przed nieautoryzowanym dostępem zdalnym w postaci: login i hasło oraz odseparowany od sieci publicznej przy pomocy zapory sieciowej,
        - wymagana jest praca użytkowników pod indywidualnym identyfikatorem,
        - dopuszczalna jest praca na wspólnym loginie w stanowiskach kierowania/punktach alarmowych pod warunkiem zapewnienia innego mechanizmu rozliczalności operacji przetwarzania danych,
        - wskazane jest rozdzielenie uprawnień użytkownika od uprawnień administracyjnych i technicznych.
    b. W zakresie przetwarzania w formie papierowej:
        - kopie papierowe z danymi osobowymi muszą być przechowywane w zamykanych na klucz szafach, szufladach lub sejfach,
        - obowiązuje tzw. „zasada czystego biurka”, czyli niepozostawianie dokumentów z danymi osobowymi w trakcie nieobecności w pomieszczeniu bez odpowiedniego ich zabezpieczenia,
        - dopuszcza się przechowywanie danych osobowych w niezamykanych szafach lub regałach tylko w pomieszczeniu archiwum lub pomieszczeniu do przechowywania informacji niejawnych zabezpieczonym zgodnie z odrębnymi przepisami.
6. Zasad napraw urządzeń teleinformatycznych, tj.:
    a. Urządzenia teleinformatyczne powinny być oddawane do naprawy po usunięciu z nich nośników pamięci zawierających dane osobowe lub po trwałym skasowaniu tych danych;
    b. W przypadku, gdy naprawa dotyczy samego nośnika, a nie jest możliwe usunięcie z niego danych, administrator jest zobowiązany podpisać umowę powierzenia przetwarzania danych osobowych z podmiotem dokonującym naprawy.
7. Zabezpieczenia przed dostępem fizycznym do obszaru przetwarzania, tj.:
    a. Administrator definiuje obszar, w którym dozwolone jest przetwarzanie danych osobowych oraz zasady przebywania w nim osób postronnych, nieupoważnionych do przetwarzania danych;
    b. Administrator określa zasady dostępu do pomieszczeń i obszarów, gdzie są przetwarzane dane osobowe, które zapewniają poufność przetwarzanych danych oraz rozliczalność w zakresie osób w nich przebywających;
    c. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób dopuszczonych do danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym;
    d. Przetwarzanie danych osobowych poza wyznaczonymi pomieszczeniami i obszarami powinno się odbywać wyłącznie na polecenie administratora lub osoby przez niego upoważnionej, przy zachowaniu adekwatnym do ryzyka,

zasad i procedur bezpieczeństwa. Procedury te powinny być co najmniej tak skuteczne jak stosowane do wyznaczonych pomieszczeń i obszarów.

8. Postępowania w sytuacji naruszeń praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych, tj.:
   a. Administrator po stwierdzeniu lub uzyskaniu informacji o naruszeniu ochrony danych osobowych powinien:
      - przystąpić do identyfikacji rodzaju zdarzenia, a w szczególności do określenia skali zniszczeń, dostępu do danych osobowych itp.,
      - powiadomić właściwego IOD, a także przekazać mu wszelkie niezbędne informacje do realizacji jego obowiązków,
      - podjąć odpowiednie kroki w celu zminimalizowania szkód i rozmiarów zdarzenia oraz zabezpieczenia przed usunięciem śladów zdarzenia,
      - opisać zdarzenie w prowadzonej dokumentacji naruszeń (również takie, które nie wymaga zgłoszenia do UODO),
      - w terminie 72 godzin przesłać do UODO zgłoszenie naruszenia ochrony danych osobowych, jeżeli skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych,
      - zgodne z art. 34 RODO, bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą o naruszeniu, jeżeli skutkowało ono dużym ryzykiem naruszenia praw i wolności osób fizycznych.
   b. W przypadku zdarzenia mającego związek z systemem informatycznym należy dodatkowo:
      - dokonać szczegółowej analizy systemu w celu potwierdzenia lub wykluczenia faktu naruszenia,
      - wygenerować, wydrukować dokumenty, raporty lub zestawienia, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrując je datą i podpisem,
      - w razie konieczności dokonać fizycznego odłączenia urządzenia, segmentu sieci, które mogły umożliwiać dostęp do bazy danych osobowych osobie nieupoważnionej,
      - wylogować użytkownika podejrzewanego o naruszenie ochrony danych osobowych,
      - dokonać zmiany haseł na kontach, poprzez które uzyskano nielegalny dostęp,
      - przywrócić normalne działanie systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, przywrócić ją z ostatniej kopii awaryjnej z zachowaniem środków ostrożności przed ponownym dostępem tą samą drogą przez osobę nieupoważnioną.