Załącznik nr 1
do zarządzenia nr 14/2019
z dnia 17 grudnia 2019 rok

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

1. Inne jednostki ochrony przeciwpożarowej, przetwarzające dane w SWD PSP są zobowiązane do:

1) Dopuszczania do pracy w SWD PSP wyłącznie osób spełniających minimalne wymagania odnośnie bezpieczeństwa osobowego określone w dziale IV.1. załącznika nr 2 do zarządzenia;
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 oraz UODO;
10) Przestrzegania obowiązujących przepisów i procedur wewnętrznych.

2. Inne jednostki ochrony przeciwpożarowej są również obowiązane do przestrzegania minimalnych wymagań dotyczących realizacji zadań w zakresie:

1) Zbierania danych, opisanym w pkt I.1 załącznika nr 2 do zarządzenia;
2) Utrwalania danych, opisanym w pkt I.2 a–b oraz g–l załącznika nr 2 do zarządzenia;
3) Przekazywania danych za pomocą środków łączności, opisanym w pkt I.3. c-d załącznika nr 2 do zarządzenia;
4) Usuwania danych, opisanym w pkt I.9 załącznika nr 2 do zarządzenia;
5) Zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, opisanym w pkt IV.5 c-d załącznika nr 2 do zarządzenia;
6) Zasad napraw urządzeń teleinformatycznych, opisanym w pkt IV.7 załącznika nr 2 do zarządzenia;
7) Zabezpieczenia przed dostępem fizycznym do obszaru przetwarzania, opisanym w pkt IV.8 załącznika nr 2 do zarządzenia;
8) Postępowania w sytuacji naruszeń praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych, opisanym w pkt IV.9 załącznika nr 2 do zarządzenia.