UCHWAŁA nr **OSPR.011.5.2026**
z dnia **23 września** roku
Zarządu Ochotniczej Straży Pożarnej Rydułtowy

o przyjęciu Polityki Ochrony Danych Osobowych oraz zasad bezpieczeństwa przetwarzania danych osobowych w Ochotniczej Straży Pożarnej Rydułtowy

Na podstawie właściwych postanowień Statutu Ochotniczej Straży Pożarnej Rydułtowy, w związku z art. 5, art. 6, art. 9, art. 12–22, art. 24, art. 25, art. 28, art. 29, art. 30, art. 32–36 oraz art. 37–39 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, zwanego dalej „RODO", ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz ustawą z dnia 17 grudnia 2021 r. o ochotniczych strażach pożarnych, mając na względzie konieczność zapewnienia zgodnego z prawem, rzetelnego, przejrzystego i bezpiecznego przetwarzania danych osobowych przez Ochotniczą Straż Pożarną Rydułtowy, Zarząd Ochotniczej Straży Pożarnej Rydułtowy uchwala, co następuje:

§1. **Polityka Ochrony Danych Osobowych**

1. Przyjmuje się „Politykę Ochrony Danych Osobowych Ochotniczej Straży Pożarnej Rydułtowy", zwaną dalej „Polityką", określającą organizacyjne, proceduralne i techniczne zasady ochrony danych osobowych przetwarzanych przez Ochotniczą Straż Pożarną Rydułtowy.
2. Polityka określa w szczególności:
    a. zasady i podstawy przetwarzania danych osobowych;
    b. organizację systemu ochrony danych osobowych;
    c. zakres odpowiedzialności osób uczestniczących w przetwarzaniu danych osobowych;
    d. zasady nadawania, zmiany, zawieszania i cofania upoważnień do przetwarzania danych osobowych;
    e. zasady zabezpieczenia dokumentacji papierowej i elektronicznej;
    f. zasady ochrony danych przetwarzanych w systemach teleinformatycznych;
    g. zasady przetwarzania danych w Centralnej Bazie Danych Ochotniczej Straży Pożarnej – CBDOSP;
    h. zasady przetwarzania danych członków OSP, członków Młodzieżowej Drużyny Pożarniczej, rodziców i opiekunów prawnych, kandydatów na członków, byłych członków, pracowników, współpracowników, kontrahentów i innych osób;
    i. zasady przetwarzania szczególnych kategorii danych osobowych;
    j. zasady udostępniania i powierzania danych osobowych;
    k. zasady wykonywania praw osób, których dane dotyczą;
    l. zasady postępowania w przypadku naruszenia ochrony danych osobowych;
    m. zasady prowadzenia analizy ryzyka i oceny skutków dla ochrony danych;
    n. zasady retencji, archiwizacji, brakowania i niszczenia danych;
    o. zasady kontroli przestrzegania przepisów o ochronie danych osobowych;
    p. zasady odpowiedzialności osób dopuszczonych do przetwarzania danych.
3. Przepisy Polityki stosuje się do danych przetwarzanych:
    a. w postaci papierowej;

b. w postaci elektronicznej;
c. w systemach teleinformatycznych;
d. na urządzeniach przenośnych;
e. na nośnikach danych;
f. w korespondencji elektronicznej;
g. w systemach i usługach świadczonych przez podmioty zewnętrzne;
h. w materiałach fotograficznych, filmowych i dźwiękowych;
i. w innych zbiorach i formach umożliwiających identyfikację osoby fizycznej.

§2. **Stosowanie polityki Ochrony Danych Osobowych**

1. Polityka ma zastosowanie do wszystkich członków OSP Rydułtowy oraz innych osób, którym powierzono wykonywanie czynności wiążących się z dostępem do danych osobowych przetwarzanych przez OSP Rydułtowy.
2. Obowiązek przestrzegania Polityki dotyczy w szczególności:
    a. członków Zarządu OSP;
    b. członków Komisji Rewizyjnej – w zakresie danych niezbędnych do wykonywania jej statutowych kompetencji;
    c. członków Jednostki Operacyjno-Technicznej;
    d. opiekunów Młodzieżowej Drużyny Pożarniczej;
    e. Inspektora Ochrony Małoletnich;
    f. Kwatermistrza;
    g. osób prowadzących dokumentację członkowską;
    h. osób prowadzących księgowość i dokumentację finansową;
    i. administratorów oraz użytkowników CBDOSP;
    j. osób posiadających dostęp do poczty elektronicznej, serwerów, urządzeń lub systemów OSP;
    k. osób wykonujących czynności na rzecz OSP na podstawie umowy, porozumienia, upoważnienia lub innego tytułu prawnego.
3. Uzyskanie dostępu do danych osobowych jest dopuszczalne wyłącznie w zakresie wynikającym z powierzonych obowiązków i przyznanych uprawnień.
4. Pełnienie funkcji w OSP nie powoduje samoistnie powstania prawa dostępu do wszystkich danych osobowych przetwarzanych przez OSP.

§3. **Osoby dopuszczone do przetwarzania danych osobowych**

1. Zobowiązuje się wszystkie osoby dopuszczone do przetwarzania danych osobowych do zapoznania się z niniejszą Polityką oraz przestrzegania jej postanowień.
2. Osoba dopuszczona do przetwarzania danych jest obowiązana w szczególności:
    a. przetwarzać dane wyłącznie w granicach udzielonego upoważnienia;
    b. zachowywać dane w poufności;
    c. chronić dane przed utratą, zniszczeniem, zmianą, nieuprawnionym ujawnieniem lub dostępem;
    d. stosować ustanowione środki bezpieczeństwa;
    e. niezwłocznie zgłaszać stwierdzone lub podejrzewane naruszenia ochrony danych;
    f. nie wykorzystywać danych uzyskanych w związku z działalnością OSP do celów prywatnych.

3. Obowiązek zachowania poufności jest bezterminowy i trwa również po:
    a. ustaniu członkostwa w OSP;
    b. odwołaniu z pełnionej funkcji;
    c. wygaśnięciu upoważnienia;
    d. zakończeniu współpracy;
    e. zakończeniu wykonywania określonych czynności na rzecz OSP.

§4. **Wykonanie uchwały**

1. Wykonanie niniejszej uchwały powierza się Prezesowi Zarządu OSP Rydułtowy oraz pozostałym członkom Zarządu w zakresie wynikającym z podziału kompetencji.
2. Zarząd zapewnia warunki organizacyjne i techniczne umożliwiające stosowanie Polityki.
3. Osoby odpowiedzialne za poszczególne obszary działalności OSP są obowiązane zapewnić stosowanie Polityki w podległym im zakresie.
4. Wdrożenie nowego procesu, ewidencji, systemu teleinformatycznego, modułu CBDOSP albo istotna zmiana dotychczasowego sposobu przetwarzania danych wymaga uwzględnienia zasad ochrony danych osobowych określonych w niniejszej uchwale.

§5. **Przegląd polityki ochrony danych osobowych**

1. Polityka podlega przeglądowi:
    a. nie rzadziej niż raz na 12 miesięcy;
    b. po istotnej zmianie przepisów prawa;
    c. po istotnej zmianie sposobu przetwarzania danych;
    d. po wdrożeniu systemu lub rozwiązania mogącego istotnie wpływać na bezpieczeństwo danych;
    e. po poważnym naruszeniu ochrony danych;
    f. w przypadku stwierdzenia podczas kontroli potrzeby zmiany przyjętych zabezpieczeń.
2. Przegląd nie musi skutkować zmianą Polityki, jeżeli przeprowadzona analiza potwierdzi jej aktualność i adekwatność.
3. Fakt przeprowadzenia przeglądu powinien zostać udokumentowany.

§6. **Postanowienia końcowe**

1. Traci moc wcześniejsza regulacja wewnętrzna OSP Rydułtowy dotycząca ochrony danych osobowych w zakresie, w jakim jest sprzeczna z niniejszą uchwałą.
2. Upoważnienia, oświadczenia, rejestry i procedury wydane przed wejściem w życie niniejszej uchwały zachowują moc, o ile są zgodne z jej postanowieniami.
3. Zarząd dokonuje przeglądu dotychczasowych upoważnień i dostępów do systemów informatycznych w terminie 60 dni od dnia wejścia w życie uchwały.
4. Uchwała wchodzi w życie z dniem jej podjęcia.

PREZES OSP
/Jerzy Salwiczek/

SEKRETARZ OSP
/Karol Weingart/

Załącznik nr 1
do Uchwały nr OSPR.011.5.2026
Zarządu Ochotniczej Straży Pożarnej Rydułtowy z dnia 23 września 2026 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH OCHOTNICZEJ STRAŻY POŻARNEJ RYDUŁTOWY

Rozdział I
Przepisy ogólne

§1. **Przedmiot Polityki**

1. Polityka Ochrony Danych Osobowych Ochotniczej Straży Pożarnej Rydułtowy, zwana dalej „Polityką", określa zasady organizacji, przetwarzania, zabezpieczania i nadzorowania danych osobowych przetwarzanych przez Ochotniczą Straż Pożarną Rydułtowy.
2. Polityka stanowi podstawowy wewnętrzny akt regulujący ochronę danych osobowych w OSP Rydułtowy.
3. Postanowienia Polityki stosuje się do wszystkich procesów przetwarzania danych osobowych wykonywanych przez OSP, niezależnie od:
    a. rodzaju danych;
    b. kategorii osób, których dane dotyczą;
    c. miejsca przetwarzania;
    d. sposobu utrwalenia danych;
    e. rodzaju wykorzystywanego systemu teleinformatycznego;
    f. rodzaju nośnika informacji.
4. Politykę stosuje się odpowiednio również do procesów przetwarzania realizowanych na rzecz OSP przez podmioty zewnętrzne, z uwzględnieniem zakresu odpowiedzialności wynikającego z przepisów prawa oraz zawartych umów.

§2. **Cele Polityki**

1. Celem Polityki jest zapewnienie zgodnego z prawem, rzetelnego, przejrzystego i bezpiecznego przetwarzania danych osobowych.
2. Polityka służy w szczególności zapewnieniu:
    a. poszanowania praw i wolności osób fizycznych;
    b. zgodności procesów przetwarzania z RODO oraz właściwymi przepisami prawa krajowego;
    c. poufności danych;
    d. integralności danych;
    e. dostępności danych;
    f. odporności systemów i usług przetwarzania;
    g. rozliczalności działań podejmowanych przez OSP;
    h. odpowiedniego poziomu bezpieczeństwa informacji;
    i. właściwego podziału kompetencji i odpowiedzialności;
    j. skutecznego reagowania na naruszenia ochrony danych.
3. Ochronę danych osobowych uwzględnia się na każdym etapie organizacji działalności OSP.

§3. **Zakres stosowania Polityki**

1. Politykę stosuje się do danych przetwarzanych:
    a. w postaci papierowej;
    b. w postaci elektronicznej;
    c. w CBDOSP;
    d. w innych systemach teleinformatycznych;
    e. w poczcie elektronicznej;
    f. na komputerach;
    g. na urządzeniach przenośnych;
    h. na elektronicznych nośnikach danych;
    i. w dokumentacji fotograficznej;
    j. w materiałach audiowizualnych;
    k. w nagraniach dźwiękowych;
    l. w kopiach zapasowych;
    m. w archiwum;
    n. w dokumentacji roboczej;
    o. w innych formach umożliwiających identyfikację osoby fizycznej.
2. Polityka obejmuje cały cykl życia danych, od momentu ich pozyskania do chwili ich zgodnego z prawem:
    1. usunięcia;
    2. zniszczenia;
    3. anonimizacji;
    4. przekazania do archiwizacji;
    5. przekazania innemu uprawnionemu podmiotowi.

§4. **Obszary przetwarzania danych**

1. Ochronie na zasadach określonych w Polityce podlegają dane przetwarzane w szczególności w:
    a. dokumentacji członkowskiej;
    b. aktach osobowych członków;
    c. Kartach personalnych członków prowadzonych w CBDOSP;
    d. dokumentacji Młodzieżowej Drużyny Pożarniczej;
    e. dokumentacji Jednostki Operacyjno-Technicznej;
    f. dokumentacji działań ratowniczych i innych działań OSP;
    g. dokumentacji szkoleniowej;
    h. dokumentacji dotyczącej kwalifikacji, badań i uprawnień;
    i. dokumentacji Zarządu;
    j. dokumentacji Komisji Rewizyjnej;
    k. dokumentacji Sekretariatu;
    l. książce korespondencji;
    m. ewidencji spraw;
    n. Dzienniku Urzędowym OSP;
    o. dokumentacji finansowo-księgowej;
    p. ewidencji składek członkowskich;
    q. dokumentacji magazynowej;
    r. dokumentacji dotyczącej pojazdów i wyposażenia;
    s. systemie CBDOSP;

t. poczcie elektronicznej;
u. serwisach internetowych i mediach społecznościowych prowadzonych przez OSP;
v. archiwum i dokumentacji przeznaczonej do brakowania.

2. Wyliczenie określone w ust. 1 nie ma charakteru zamkniętego.

§ 5. Zasada powszechności ochrony

1. Ochrona danych osobowych obowiązuje niezależnie od miejsca wykonywania czynności przetwarzania.
2. Dane podlegają ochronie również w przypadku ich czasowego przetwarzania:
   a. poza siedzibą OSP;
   b. podczas działań ratowniczych;
   c. podczas ćwiczeń;
   d. podczas zawodów;
   e. podczas zbiórek MDP;
   f. podczas wydarzeń organizowanych przez OSP;
   g. w czasie wykonywania czynności służbowych z wykorzystaniem urządzeń mobilnych.
3. Wyniesienie dokumentacji lub nośnika zawierającego dane osobowe poza miejsce jego zwykłego przechowywania wymaga istnienia uzasadnionej potrzeby wynikającej
   z wykonywanych zadań oraz zastosowania odpowiednich zabezpieczeń.

§ 6. Zasada ograniczonego dostępu

1. Dostęp do danych osobowych przysługuje wyłącznie osobom, dla których jest on niezbędny do prawidłowego wykonywania powierzonych obowiązków.
2. Dostęp do danych ogranicza się:
   a. przedmiotowo – do niezbędnych kategorii danych;
   b. funkcjonalnie – do niezbędnych operacji na danych;
   c. organizacyjnie – do właściwego obszaru działalności;
   d. czasowo – do okresu wykonywania określonych obowiązków.
3. Przy określaniu zakresu dostępu stosuje się zasadę najmniejszych niezbędnych uprawnień.
4. Techniczna możliwość uzyskania dostępu do danych nie stanowi uprawnienia do ich przeglądania, kopiowania, wykorzystywania lub udostępniania.

§ 7. Zasada poufności

1. Każda osoba posiadająca dostęp do danych osobowych jest obowiązana zachować je w poufności.
2. Obowiązek poufności obejmuje również:
   a. sposób organizacji zabezpieczeń;
   b. dane uwierzytelniające;
   c. informacje o uprawnieniach użytkowników;
   d. informacje o stwierdzonych podatnościach systemów;
   e. informacje o naruszeniach ochrony danych, jeżeli ich ujawnienie nie jest wymagane przepisami prawa.

3. Obowiązek zachowania poufności trwa bezterminowo, również po ustaniu członkostwa, funkcji, upoważnienia lub współpracy z OSP.

§ 8. Odpowiedzialność za własne działania

1. Każda osoba dopuszczona do przetwarzania danych odpowiada za wykonywanie czynności zgodnie z zakresem udzielonego upoważnienia oraz obowiązującymi procedurami.
2. Zabronione jest:
    a. udostępnianie własnego konta innej osobie;
    b. korzystanie z konta innego użytkownika;
    c. udostępnianie hasła;
    d. wykonywanie operacji na polecenie osoby nieuprawnionej;
    e. obchodzenie zabezpieczeń technicznych;
    f. świadome ukrywanie naruszenia ochrony danych;
    g. wykorzystywanie danych do celów prywatnych.
3. Użytkownik nie może usprawiedliwiać nieuprawnionej operacji wyłącznie faktem, że system technicznie umożliwił jej wykonanie.

Rozdział II
Definicje i zasady interpretacyjne

§ 9. Definicje podstawowe

1. Ilekroć w Polityce jest mowa o:
    a. **OSP** – należy przez to rozumieć Ochotniczą Straż Pożarną Rydułtowy;
    b. **Administratorze** – należy przez to rozumieć OSP Rydułtowy w zakresie procesów, w których OSP samodzielnie albo wspólnie z innym podmiotem ustala cele i sposoby przetwarzania danych osobowych;
    c. **Zarządzie** – należy przez to rozumieć Zarząd OSP Rydułtowy;
    d. **RODO** – należy przez to rozumieć rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.;
    e. **danych osobowych** – należy przez to rozumieć wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
    f. **osobie, której dane dotyczą** – należy przez to rozumieć osobę fizyczną, której dotyczą przetwarzane dane osobowe;
    g. **przetwarzaniu** – należy przez to rozumieć operację lub zestaw operacji wykonywanych na danych osobowych, niezależnie od tego, czy odbywają się w sposób zautomatyzowany;
    h. **zbiorze danych** – należy przez to rozumieć uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów;
    i. **danych szczególnych kategorii** – należy przez to rozumieć dane osobowe określone w art. 9 ust. 1 RODO;
    j. **osobie upoważnionej** – należy przez to rozumieć osobę dopuszczoną przez Administratora do przetwarzania danych w określonym zakresie;
    k. **użytkowniku** – należy przez to rozumieć osobę korzystającą z systemu teleinformatycznego OSP na podstawie przyznanych jej uprawnień;

l. **odbiorcy** – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, z uwzględnieniem zasad wynikających z RODO;
m. **podmiocie przetwarzającym** – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot przetwarzający dane osobowe w imieniu Administratora;
n. **naruszeniu ochrony danych osobowych** – należy przez to rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych;
o. **incydencie bezpieczeństwa** – należy przez to rozumieć zdarzenie mogące mieć niekorzystny wpływ na poufność, integralność lub dostępność informacji;
p. **systemie teleinformatycznym** – należy przez to rozumieć zespół współpracujących urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie lub przesyłanie danych;
q. **CBDOSP** – należy przez to rozumieć Centralną Bazę Danych Ochotniczej Straży Pożarnej, stanowiącą system teleinformatyczny wykorzystywany przez OSP Rydułtowy;
r. **MDP** – należy przez to rozumieć Młodzieżową Drużynę Pożarniczą działającą przy OSP Rydułtowy;
s. **JOT OSP** – należy przez to rozumieć Jednostkę Operacyjno-Techniczną OSP Rydułtowy;
t. **dokumentacji** – należy przez to rozumieć wszelkie dokumenty, rejestry, ewidencje, akta, pliki i inne nośniki informacji zawierające dane osobowe;
u. **nośniku danych** – należy przez to rozumieć urządzenie albo przedmiot umożliwiający zapis lub przechowywanie informacji;
v. **retencji** – należy przez to rozumieć okres, przez który dane lub dokumentacja są przechowywane;
w. **brakowaniu** – należy przez to rozumieć udokumentowany proces kwalifikowania i niszczenia dokumentacji, której okres przechowywania upłynął;
x. **anonimizacji** – należy przez to rozumieć nieodwracalne przekształcenie danych w sposób uniemożliwiający identyfikację osoby fizycznej;
y. **pseudonimizacji** – należy przez to rozumieć przetwarzanie danych w taki sposób, aby nie można było ich przypisać konkretnej osobie bez użycia dodatkowych informacji;
z. **analizie ryzyka** – należy przez to rozumieć proces identyfikowania, analizowania i oceny ryzyka dla praw i wolności osób fizycznych;
aa. **ocenie skutków dla ochrony danych** – należy przez to rozumieć ocenę, o której mowa w art. 35 RODO.

2. Pojęcia niezdefiniowane w Polityce interpretuje się zgodnie z RODO, właściwymi przepisami prawa krajowego oraz znaczeniem przyjętym w innych obowiązujących aktach wewnętrznych OSP, o ile nie pozostaje ono w sprzeczności z przepisami prawa.

§ 10. Dokumentacja zawierająca dane osobowe

1. Za dokumentację zawierającą dane osobowe uważa się każdy dokument lub zbiór informacji pozwalający bezpośrednio albo pośrednio zidentyfikować osobę fizyczną.
2. Dokumentację, o której mowa w ust. 1, stanowią w szczególności:
    a. dokumenty papierowe;
    b. formularze;
    c. wnioski;
    d. deklaracje;
    e. oświadczenia;
    f. rejestry;
    g. ewidencje;
    h. protokoły;
    i. uchwały i zarządzenia, jeżeli zawierają dane osobowe;
    j. pliki tekstowe;
    k. arkusze kalkulacyjne;
    l. pliki PDF;
    m. skany;
    n. fotografie dokumentów;
    o. wiadomości poczty elektronicznej;
    p. załączniki do wiadomości;
    q. eksporty z CBDOSP;
    r. kopie zapasowe;
    s. fotografie osób;
    t. nagrania audiowizualne;
    u. nagrania dźwiękowe.
3. Ochronie podlegają również dokumenty:
    a. robocze;
    b. tymczasowe;
    c. niepodpisane;
    d. znajdujące się w trakcie opracowywania;
    e. przeznaczone do późniejszego usunięcia.
4. Wykonanie fotografii lub skanu dokumentu stanowi operację przetwarzania danych osobowych i jest dopuszczalne wyłącznie, jeżeli jest niezbędne do realizacji określonego zadania.

§ 11. Dane wymagające podwyższonego poziomu ochrony

1. Szczególnej ochronie podlegają dane osobowe, których utrata, ujawnienie, zmiana albo nieuprawnione wykorzystanie może powodować zwiększone ryzyko naruszenia praw lub wolności osoby fizycznej.
2. Do danych, o których mowa w ust. 1, zalicza się w szczególności:
    a. dane szczególnych kategorii określone w art. 9 RODO;
    b. dane dotyczące zdrowia;
    c. dane małoletnich;
    d. numer PESEL;
    e. serię i numer dokumentu tożsamości;
    f. dane dotyczące rachunków bankowych;

g. dane uwierzytelniające;
h. informacje dotyczące sytuacji rodzinnej;
i. dane umożliwiające kradzież lub wykorzystanie tożsamości;
j. zestawienia obejmujące znaczny zakres informacji o określonej osobie.

3. Dane określone w ust. 2 mogą być udostępniane wewnątrz OSP wyłącznie osobom, których zakres obowiązków uzasadnia dostęp do tych danych.
4. Jeżeli wykonanie określonego zadania nie wymaga ujawnienia pełnego zakresu danych, należy zastosować ograniczenie zakresu informacji, pseudonimizację, anonimizację albo inną odpowiednią metodę minimalizacji.

§ 12. Zasady interpretacji uprawnień

1. Uprawnienia do przetwarzania danych interpretuje się ściśle.
2. W razie wątpliwości, czy określona osoba posiada uprawnienie do:
   a. uzyskania danych;
   b. przeglądania danych;
   c. modyfikowania danych;
   d. eksportowania danych;
   e. drukowania danych;
   f. przekazywania danych;
   g. usuwania danych – należy wstrzymać wykonanie czynności do czasu wyjaśnienia zakresu uprawnienia.
3. Dostęp do funkcji systemu teleinformatycznego nie jest równoznaczny z uprawnieniem do wykorzystania wszystkich danych dostępnych za pomocą tej funkcji.
4. W przypadku kolizji pomiędzy wygodą organizacyjną a koniecznością zapewnienia ochrony danych należy zastosować rozwiązanie zapewniające odpowiedni poziom ochrony praw i wolności osób fizycznych.

Rozdział III
Podstawowe zasady przetwarzania danych osobowych

§ 13. Zasada zgodności z prawem, rzetelności i przejrzystości

1. Dane osobowe przetwarza się zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą.
2. Każdy proces przetwarzania powinien posiadać:
   a. określony cel;
   b. odpowiednią podstawę prawną;
   c. ustalony zakres danych;
   d. określony krąg osób uprawnionych;
   e. określone zasady przechowywania;
   f. odpowiednie zabezpieczenia.
3. Niedopuszczalne jest tworzenie procesu przetwarzania, którego celu nie można jasno określić.
4. Administrator powinien być w stanie wykazać podstawowe założenia procesu przetwarzania.

§ 14. Zasada ograniczenia celu

1. Dane zbiera się w konkretnych, wyraźnych i prawnie uzasadnionych celach.
2. Danych nie wolno dalej przetwarzać w sposób niezgodny z celami, dla których zostały pozyskane, chyba że dalsze przetwarzanie jest zgodne z prawem.
3. Przed wykorzystaniem istniejących danych do nowego celu należy ustalić w szczególności:
    a. związek pomiędzy pierwotnym i nowym celem;
    b. kontekst pozyskania danych;
    c. charakter danych;
    d. możliwe konsekwencje dalszego przetwarzania;
    e. zastosowane zabezpieczenia;
    f. istnienie właściwej podstawy prawnej.
4. Zabronione jest wykorzystywanie danych członków OSP do prywatnych celów członków organów OSP lub innych osób.

§ 15. Zasada minimalizacji danych

1. Zakres przetwarzanych danych ogranicza się do danych adekwatnych, stosownych i niezbędnych do realizacji określonego celu.
2. Przed wprowadzeniem nowego pola w formularzu, ewidencji albo CBDOSP należy ustalić:
    a. cel jego utworzenia;
    b. podstawę prawną;
    c. niezbędność pozyskiwanej informacji;
    d. przewidywany okres przechowywania;
    e. krąg osób posiadających dostęp.
3. Nie należy pozyskiwać danych:
    a. wyłącznie dlatego, że mogą być przydatne w przyszłości;
    b. z przyzwyczajenia organizacyjnego;
    c. wyłącznie dlatego, że formularz technicznie umożliwia ich wpisanie;
    d. w zakresie szerszym niż niezbędny.
4. Jeżeli określony cel może zostać osiągnięty przy użyciu mniejszej ilości danych, należy zastosować rozwiązanie ograniczające ich zakres.

§ 16. Zasada prawidłowości danych

1. Dane osobowe powinny być prawidłowe i w razie potrzeby aktualizowane.
2. Osoby odpowiedzialne za prowadzenie dokumentacji podejmują rozsądne działania w celu:
    a. sprostowania danych nieprawidłowych;
    b. uzupełnienia danych niekompletnych, jeżeli jest to niezbędne;
    c. usunięcia danych nieprawidłowych, jeżeli ich sprostowanie nie jest właściwym rozwiązaniem;
    d. oznaczenia danych, których prawidłowość jest przedmiotem wyjaśnienia.
3. Użytkownik CBDOSP, który stwierdzi nieprawidłowość danych, powinien:
    a. dokonać korekty, jeżeli posiada odpowiednie uprawnienia i wiarygodną podstawę do ustalenia prawidłowej treści; albo
    b. przekazać informację osobie odpowiedzialnej za prowadzenie danego zakresu danych.

4. Niedopuszczalne jest dokonywanie zmian w dokumentacji w sposób uniemożliwiający ustalenie pierwotnej treści, jeżeli przepisy prawa albo charakter dokumentacji wymagają zachowania historii zmian.

§ 17. Zasada ograniczenia przechowywania

1. Dane przechowuje się w formie umożliwiającej identyfikację osoby nie dłużej, niż jest to niezbędne do celów, dla których dane są przetwarzane.
2. Okres przechowywania ustala się z uwzględnieniem:
    a. przepisów prawa;
    b. celu przetwarzania;
    c. zasad archiwizacji;
    d. obowiązującej w OSP instrukcji kancelaryjnej;
    e. Jednolitego Rzeczowego Wykazu Akt, jeżeli znajduje zastosowanie;
    f. terminów przedawnienia roszczeń;
    g. konieczności zabezpieczenia praw OSP lub osoby, której dane dotyczą.
3. Dane nie mogą być przechowywane bezterminowo wyłącznie na podstawie założenia, że mogą być kiedyś potrzebne.
4. Po upływie właściwego okresu dane podlegają:
    a. usunięciu;
    b. zniszczeniu;
    c. anonimizacji; albo
    d. dalszemu przechowywaniu, jeżeli istnieje ku temu odrębna podstawa.

§ 18. Zasada integralności i poufności

1. Dane przetwarza się w sposób zapewniający odpowiednie bezpieczeństwo.
2. Stosowane zabezpieczenia powinny chronić dane w szczególności przed:
    a. nieuprawnionym dostępem;
    b. nieuprawnionym ujawnieniem;
    c. przypadkową utratą;
    d. zniszczeniem;
    e. uszkodzeniem;
    f. nieuprawnioną modyfikacją;
    g. nieuprawnionym kopiowaniem;
    h. nieuprawnionym przesłaniem;
    i. utratą dostępności.
3. Dobór zabezpieczeń powinien uwzględniać:
    a. charakter danych;
    b. zakres przetwarzania;
    c. kontekst przetwarzania;
    d. cele przetwarzania;
    e. prawdopodobieństwo wystąpienia zagrożenia;
    f. możliwe skutki naruszenia;
    g. aktualny stan wiedzy technicznej;
    h. koszty wdrożenia odpowiednich środków.

§ 19. Zasada rozliczalności

1. Administrator jest obowiązany nie tylko przestrzegać zasad ochrony danych, lecz również być w stanie wykazać ich przestrzeganie.
2. W celu realizacji zasady rozliczalności prowadzi się odpowiednią dokumentację obejmującą w szczególności:
    a. Politykę;
    b. rejestr upoważnień;
    c. rejestr czynności przetwarzania – w zakresie wymaganym prawem;
    d. rejestr naruszeń;
    e. dokumentację analiz ryzyka;
    f. dokumentację ocen skutków dla ochrony danych, jeżeli są wymagane;
    g. dokumentację powierzenia przetwarzania;
    h. dokumentację realizacji praw osób;
    i. dokumentację szkoleń;
    j. dokumentację kontroli;
    k. dokumentację przeglądów uprawnień;
    l. dokumentację przeglądów Polityki.
3. Dokumentacja powinna umożliwiać ustalenie podstawowych okoliczności podejmowania istotnych decyzji dotyczących ochrony danych.

§ 20. Zasada ochrony danych w fazie projektowania

1. Ochronę danych osobowych uwzględnia się już na etapie projektowania nowego procesu, rozwiązania organizacyjnego albo systemu teleinformatycznego.
2. Przed wdrożeniem nowego rozwiązania należy ocenić w szczególności:
    a. zakres przetwarzanych danych;
    b. niezbędność ich przetwarzania;
    c. sposób uwierzytelniania użytkowników;
    d. zakres uprawnień;
    e. możliwość rejestrowania istotnych operacji;
    f. sposób wykonywania kopii bezpieczeństwa;
    g. zasady retencji;
    h. możliwość bezpiecznego usunięcia danych;
    i. ryzyko nieuprawnionego ujawnienia;
    j. sposób reagowania na incydenty.
3. Postanowienia ust. 1 i 2 stosuje się w szczególności do:
    a. nowych modułów CBDOSP;
    b. nowych formularzy;
    c. nowych rejestrów;
    d. nowych usług internetowych;
    e. nowych urządzeń wykorzystywanych do przetwarzania danych;
    f. integracji CBDOSP z innymi systemami.

§ 21. Zasada domyślnej ochrony danych

1. Systemy i procesy powinny być skonfigurowane w sposób zapewniający, aby domyślnie przetwarzane były wyłącznie dane niezbędne do konkretnego celu.

2. Domyślne ustawienia powinny ograniczać:
    a. zakres zbieranych danych;
    b. zakres ich przetwarzania;
    c. okres przechowywania;
    d. liczbę osób posiadających dostęp;
    e. zakres widoczności danych.
3. Nowo utworzone konto użytkownika powinno posiadać najniższy zakres uprawnień wystarczający do realizacji powierzonych zadań.
4. Rozszerzenie uprawnień powinno następować dopiero po ustaleniu uzasadnionej potrzeby.

Rozdział IV
Podstawy prawne przetwarzania danych

§ 22. Obowiązek ustalenia podstawy prawnej

1. Każdy proces przetwarzania danych osobowych musi posiadać właściwą podstawę prawną.
2. Podstawę prawną ustala się przed rozpoczęciem przetwarzania.
3. Ustalenie podstawy powinno uwzględniać:
    a. cel przetwarzania;
    b. kategorię danych;
    c. kategorię osób;
    d. charakter relacji pomiędzy OSP a osobą;
    e. przepisy szczególne regulujące działalność OSP.
4. Niedopuszczalne jest wskazywanie zgody jako automatycznej podstawy każdego procesu przetwarzania.

§ 23. Przetwarzanie danych zwykłych

1. Dane osobowe inne niż dane szczególnych kategorii przetwarza się, jeżeli zachodzi co najmniej jedna z przesłanek określonych w art. 6 ust. 1 RODO.
2. W zależności od charakteru procesu podstawą może być w szczególności:
    a. zgoda osoby;
    b. niezbędność do wykonania umowy lub podjęcia działań przed jej zawarciem;
    c. wykonanie obowiązku prawnego;
    d. ochrona żywotnych interesów osoby fizycznej;
    e. wykonanie zadania realizowanego w interesie publicznym, jeżeli odpowiednia podstawa wynika z prawa;
    f. prawnie uzasadniony interes realizowany przez Administratora albo stronę trzecią, z zastrzeżeniem warunków określonych w RODO.
3. Wybór podstawy prawnej powinien odpowiadać rzeczywistemu charakterowi procesu.
4. Nie należy zmieniać podstawy prawnej wyłącznie w celu obejścia wymagań związanych z pierwotnie przyjętą podstawą.

§ 24. Zgoda na przetwarzanie danych

1. Jeżeli podstawę przetwarzania stanowi zgoda, musi ona być:
    a. dobrowolna;
    b. konkretna;
    c. świadoma;
    d. jednoznaczna.
2. Administrator powinien być w stanie wykazać, że zgoda została udzielona.
3. Treść zgody powinna być sformułowana w sposób jasny i zrozumiały.
4. Zgoda nie może być domniemana z:
    a. milczenia;
    b. braku sprzeciwu;
    c. wcześniej zaznaczonego pola;
    d. samego członkostwa w OSP;
    e. samego udziału w wydarzeniu, jeżeli charakter przetwarzania wymaga odrębnej zgody.
5. Osoba powinna mieć możliwość wycofania zgody w dowolnym momencie.
6. Wycofanie zgody powinno być równie łatwe jak jej udzielenie.
7. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem.

§ 25. Przetwarzanie szczególnych kategorii danych

1. Przetwarzanie szczególnych kategorii danych jest co do zasady zabronione, chyba że zachodzi jedna z przesłanek określonych w art. 9 ust. 2 RODO.
2. Przed rozpoczęciem przetwarzania takich danych należy ustalić:
    a. podstawę wynikającą z art. 9 ust. 2 RODO;
    b. w razie potrzeby podstawę wynikającą z prawa krajowego;
    c. niezbędny zakres danych;
    d. osoby uprawnione do dostępu;
    e. szczególne zabezpieczenia;
    f. okres przechowywania.
3. Dostęp do szczególnych kategorii danych powinien być ograniczony bardziej rygorystycznie niż dostęp do zwykłych danych członkowskich.
4. Dokumentacja zawierająca dane szczególnych kategorii nie może być udostępniana wszystkim członkom Zarządu, Komisji Rewizyjnej, JOT OSP lub innym osobom wyłącznie z uwagi na pełnioną funkcję.
5. Każdorazowo decydują rzeczywista potrzeba dostępu, zakres kompetencji oraz podstawa prawna.

§ 26. Dane dotyczące zdrowia i zdolności do wykonywania zadań

1. Informacje dotyczące zdrowia członków OSP przetwarza się wyłącznie w zakresie niezbędnym do realizacji określonego zgodnego z prawem celu.
2. Jeżeli dla realizacji zadania wystarczająca jest informacja o:
    a. posiadaniu aktualnego badania;
    b. terminie ważności badania;
    c. zdolności albo braku zdolności do wykonywania określonych czynności – nie należy gromadzić szerszej dokumentacji medycznej, jeżeli jej posiadanie nie jest wymagane przepisami prawa.

3. W CBDOSP należy w miarę możliwości ograniczać zakres danych dotyczących zdrowia do informacji niezbędnych do zarządzania uprawnieniami i terminami.
4. Dokumentów zawierających szczegółowe informacje medyczne nie należy udostępniać osobom, dla których wystarczająca jest informacja o aktualności określonego uprawnienia lub zdolności.

Rozdział V
Administrator danych i organizacja systemu ochrony danych

§ 27. Administrator danych osobowych

1. Administratorem danych osobowych jest Ochotnicza Straż Pożarna Rydułtowy w zakresie, w którym samodzielnie ustala cele i sposoby przetwarzania danych osobowych.
2. Status Administratora ustala się na podstawie rzeczywistego charakteru danego procesu, a nie wyłącznie na podstawie nazwy dokumentu, systemu lub podmiotu przechowującego dane.
3. W przypadku gdy cele i sposoby przetwarzania są wspólnie ustalane z innym podmiotem, należy ocenić, czy zachodzi współadministracja w rozumieniu art. 26 RODO.
4. W przypadku przetwarzania danych w imieniu innego administratora należy ustalić właściwe zasady powierzenia przetwarzania.

§ 28. Reprezentowanie Administratora

1. Administrator wykonuje swoje obowiązki poprzez właściwe organy OSP zgodnie ze Statutem, uchwałami oraz przyjętym podziałem kompetencji.
2. Zarząd OSP zapewnia organizacyjne warunki wykonywania obowiązków Administratora.
3. Podejmowanie czynności w imieniu Administratora nie zwalnia osoby wykonującej daną czynność z obowiązku przestrzegania Polityki.
4. Decyzje o szczególnym znaczeniu dla systemu ochrony danych powinny być odpowiednio dokumentowane.

§ 29. Zadania Zarządu OSP

1. Do zadań Zarządu w zakresie ochrony danych należy w szczególności:
    a. ustanawianie wewnętrznych zasad ochrony danych;
    b. zapewnienie odpowiednich środków organizacyjnych i technicznych;
    c. zatwierdzanie istotnych zmian systemu ochrony danych;
    d. zapewnienie okresowej oceny ryzyka;
    e. zapewnienie przeglądów uprawnień;
    f. zapewnienie reagowania na naruszenia;
    g. zapewnienie realizacji praw osób, których dane dotyczą;
    h. nadzorowanie powierzania przetwarzania danych;
    i. zapewnienie szkoleń osób upoważnionych;
    j. zapewnienie okresowego przeglądu Polityki.
2. Zarząd może powierzyć wykonywanie określonych czynności poszczególnym osobom, jednak powierzenie czynności nie może prowadzić do niejasności w zakresie odpowiedzialności.

3. Podział obowiązków powinien być udokumentowany w sposób umożliwiający ustalenie osoby odpowiedzialnej za dany obszar.

§ 30. Obowiązki Prezesa Zarządu

1. Prezes Zarządu koordynuje wykonywanie przez Zarząd zadań dotyczących organizacji ochrony danych osobowych, z uwzględnieniem kompetencji pozostałych członków Zarządu.
2. Do jego zadań należy w szczególności:
    a. zapewnienie wykonywania uchwał Zarządu dotyczących ochrony danych;
    b. inicjowanie przeglądów systemu ochrony danych;
    c. zapewnienie podjęcia działań w przypadku istotnego naruszenia;
    d. zapewnienie współdziałania osób odpowiedzialnych za poszczególne obszary;
    e. przedstawianie Zarządowi spraw wymagających jego rozstrzygnięcia.
3. Prezes nie uzyskuje z tytułu pełnionej funkcji nieograniczonego prawa do dostępu do wszystkich danych osobowych.
4. Dostęp Prezesa do określonych danych powinien odpowiadać zakresowi wykonywanych kompetencji i rzeczywistej potrzebie.

§ 31. Osoby odpowiedzialne za obszary przetwarzania

1. Osoba odpowiedzialna za określony obszar działalności OSP odpowiada w zakresie powierzonych obowiązków za prawidłową organizację przetwarzania danych w tym obszarze.
2. Do obowiązków takiej osoby należy w szczególności:
    a. przestrzeganie zasady minimalizacji;
    b. zapewnienie prawidłowości dokumentacji;
    c. ograniczanie dostępu do osób uprawnionych;
    d. zgłaszanie potrzeby zmiany uprawnień;
    e. zgłaszanie naruszeń i nieprawidłowości;
    f. przestrzeganie okresów przechowywania;
    g. współpraca przy realizacji praw osób;
    h. współpraca przy kontroli i analizie ryzyka.
3. Powierzenie prowadzenia dokumentacji nie uprawnia do dowolnego wykorzystywania zawartych w niej informacji.

§ 32. Administrator systemu CBDOSP

1. Osobie odpowiedzialnej za techniczne utrzymanie CBDOSP mogą zostać przyznane uprawnienia administracyjne niezbędne do zapewnienia prawidłowego funkcjonowania systemu.
2. Uprawnienia administracyjne służą wyłącznie realizacji zadań technicznych i organizacyjnych.
3. Administrator systemu nie może wykorzystywać technicznej możliwości dostępu do danych w celu niezwiązanym z wykonywaniem powierzonych zadań.
4. Do jego obowiązków może należeć w szczególności:
    a. zarządzanie kontami;
    b. techniczne zarządzanie rolami;
    c. zapewnienie wykonywania kopii bezpieczeństwa;

d. wdrażanie aktualizacji;
e. usuwanie podatności;
f. analiza technicznych incydentów;
g. zapewnienie dostępności systemu;
h. prowadzenie albo zabezpieczanie logów;
i. współpraca przy odtwarzaniu danych;
j. blokowanie kont w przypadkach przewidzianych Polityką.

5. Szczegółowe zasady bezpieczeństwa CBDOSP określają dalsze przepisy Polityki.

§ 33. Obowiązek współdziałania

1. Wszystkie osoby uczestniczące w przetwarzaniu danych są obowiązane współdziałać w celu zapewnienia zgodności przetwarzania z prawem.
2. Obowiązek współdziałania obejmuje w szczególności:
   a. udzielanie niezbędnych informacji;
   b. przekazywanie dokumentacji;
   c. zgłaszanie zmian w procesach;
   d. zgłaszanie nowych kategorii danych;
   e. zgłaszanie potrzeby utworzenia lub usunięcia kont;
   f. uczestnictwo w wyjaśnianiu incydentów;
   g. wykonywanie działań naprawczych;
   h. udział w przeglądach uprawnień.
3. Zabronione jest zatajenie informacji o zdarzeniu mogącym mieć wpływ na bezpieczeństwo danych.

Rozdział VI
Upoważnienia do przetwarzania danych osobowych

§ 34. Zasada dostępu na podstawie upoważnienia

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające odpowiednie umocowanie i działające w zakresie powierzonych obowiązków.
2. Jeżeli dla zapewnienia rozliczalności przyjęto system imiennych upoważnień, osoba powinna otrzymać upoważnienie przed rozpoczęciem samodzielnego przetwarzania danych.
3. Upoważnienie powinno określać co najmniej:
   a. osobę upoważnioną;
   b. zakres danych albo obszar przetwarzania;
   c. dopuszczalne czynności;
   d. datę nadania;
   e. okres obowiązywania, jeżeli jest ograniczony;
   f. podmiot lub osobę nadającą upoważnienie.
4. Upoważnienie może mieć postać:
   1. papierową;
   2. elektroniczną;
   3. wpisu w prowadzonym w sposób rozliczalny systemie uprawnień – jeżeli możliwe jest wykazanie jego zakresu i okresu obowiązywania.

§ 35. Zakres upoważnienia

1. Zakres upoważnienia ustala się odpowiednio do rzeczywistych obowiązków osoby.
2. Upoważnienie może obejmować w szczególności prawo do:
    a. odczytu danych;
    b. wprowadzania danych;
    c. modyfikowania danych;
    d. zatwierdzania danych;
    e. drukowania;
    f. eksportowania;
    g. udostępniania uprawnionym odbiorcom;
    h. archiwizowania;
    i. usuwania danych;
    j. zarządzania uprawnieniami innych użytkowników.
3. Uprawnienia szczególnie wrażliwe, w szczególności do:
    a. masowego eksportu;
    b. usuwania danych;
    c. zarządzania użytkownikami;
    d. zmiany uprawnień;
    e. dostępu do danych szczególnych kategorii – powinny być ograniczone do niezbędnego minimum.
4. Upoważnienie nie może być interpretowane rozszerzająco.

§ 36. Rejestr osób upoważnionych

1. Prowadzi się rejestr osób upoważnionych do przetwarzania danych, jeżeli taki model upoważnień został przyjęty przez Administratora.
2. Rejestr powinien umożliwiać ustalenie co najmniej:
    a. imienia i nazwiska osoby;
    b. zakresu upoważnienia;
    c. daty nadania;
    d. daty zmiany;
    e. daty cofnięcia lub wygaśnięcia;
    f. osoby lub organu zatwierdzającego uprawnienie.
3. Rejestr może być prowadzony w CBDOSP.
4. Historia upoważnień powinna być zachowywana w zakresie niezbędnym do wykazania, kto posiadał dostęp do danych w określonym czasie.

§ 37. Zmiana zakresu upoważnienia

1. Zmiana obowiązków osoby wymaga oceny aktualności posiadanych przez nią uprawnień.
2. Uprawnienia, które przestały być niezbędne, podlegają niezwłocznemu cofnięciu.
3. Niedopuszczalne jest pozostawianie rozszerzonych uprawnień:
    a. z przyzwyczajenia;
    b. na wypadek ewentualnej przyszłej potrzeby;
    c. z uwagi na wcześniejsze pełnienie funkcji;
    d. wyłącznie ze względu na długość członkostwa w OSP.
4. Zmiana uprawnień w CBDOSP powinna odpowiadać zmianie rzeczywistego zakresu obowiązków.

§ 38. Cofnięcie i wygaśnięcie upoważnienia

1. Upoważnienie podlega cofnięciu albo wygasa w szczególności:
    a. po ustaniu członkostwa, jeżeli dostęp był związany z członkostwem;
    b. po odwołaniu z funkcji;
    c. po zakończeniu wykonywania określonego zadania;
    d. po zakończeniu współpracy;
    e. po zmianie zakresu obowiązków;
    f. w przypadku stwierdzenia braku dalszej potrzeby dostępu.
2. W przypadku ustania podstawy dostępu należy niezwłocznie:
    1. zablokować lub usunąć właściwe konto;
    2. odebrać klucze, karty lub inne środki dostępu;
    3. odebrać dokumentację;
    4. odebrać nośniki danych;
    5. ustalić, czy osoba posiada kopie danych poza systemami OSP;
    6. zabezpieczyć dane związane z prowadzonymi przez nią sprawami.
3. Cofnięcie upoważnienia nie uchyla obowiązku zachowania poufności.

§ 39. Okresowy przegląd uprawnień

1. Uprawnienia do danych podlegają okresowej weryfikacji.
2. Przegląd przeprowadza się:
    a. nie rzadziej niż raz na 12 miesięcy;
    b. po zmianach składu Zarządu;
    c. po zmianie zakresów obowiązków;
    d. po istotnej reorganizacji systemu;
    e. po stwierdzeniu naruszenia związanego z nieprawidłowym zakresem dostępu.
3. Przegląd powinien obejmować co najmniej:
    a. aktywne konta;
    b. role użytkowników;
    c. uprawnienia administracyjne;
    d. dostęp do danych szczególnych kategorii;
    e. możliwość eksportowania danych;
    f. dostęp do dokumentacji papierowej;
    g. dostęp do poczty i zasobów współdzielonych.
4. Wyniki przeglądu podlegają udokumentowaniu.

Rozdział VII
Dokumentacja członkowska i akta osobowe członków OSP

§ 40. Zasady prowadzenia dokumentacji członkowskiej

1. OSP prowadzi dokumentację członkowską w zakresie niezbędnym do:
    a. przyjmowania członków;
    b. prowadzenia ewidencji członków;
    c. wykonywania praw i obowiązków wynikających z członkostwa;
    d. dokumentowania przebiegu członkostwa;
    e. wykonywania obowiązków wynikających z przepisów prawa;
    f. realizacji postanowień Statutu OSP;

g. zapewnienia prawidłowej organizacji działalności OSP;
h. dokumentowania kwalifikacji, uprawnień i powierzonych funkcji;
i. wykonywania innych prawnie uzasadnionych zadań związanych z działalnością OSP.

2. Zakres dokumentacji członkowskiej powinien być dostosowany do statusu członka oraz rzeczywistych potrzeb wynikających z jego udziału w działalności OSP.
3. Niedopuszczalne jest gromadzenie w aktach osobowych informacji niemających związku z członkostwem, wykonywanymi funkcjami, obowiązkami lub innym zgodnym z prawem celem przetwarzania.
4. Dokumentacja członkowska może być prowadzona:
   a. w postaci papierowej;
   b. w postaci elektronicznej;
   c. równolegle w obu postaciach, jeżeli jest to uzasadnione organizacją dokumentacji.
5. W przypadku równoległego prowadzenia dokumentacji należy dążyć do ograniczenia tworzenia zbędnych kopii tych samych danych.

§ 41. Akta osobowe członka OSP

1. Dla członka OSP prowadzi się dokumentację członkowską zgodnie z obowiązującymi aktami wewnętrznymi OSP.
2. Akta osobowe powinny umożliwiać udokumentowanie przebiegu członkostwa w zakresie wymaganym przez przepisy prawa, Statut OSP oraz akty wewnętrzne OSP.
3. W aktach mogą znajdować się w szczególności:
   a. deklaracja członkowska;
   b. dokumenty dotyczące przyjęcia w poczet członków;
   c. dokumenty dotyczące zmian rodzaju lub statusu członkostwa;
   d. dokumenty dotyczące pełnionych funkcji;
   e. dokumenty dotyczące kwalifikacji i uprawnień;
   f. dokumenty dotyczące szkoleń;
   g. dokumenty dotyczące odznaczeń i wyróżnień;
   h. dokumenty dotyczące odpowiedzialności organizacyjnej, jeżeli ich przechowywanie jest uzasadnione i zgodne z prawem;
   i. dokumenty dotyczące ustania członkostwa;
   j. inne dokumenty, których przechowywanie jest niezbędne dla realizacji określonego zgodnego z prawem celu.
4. Dokument zawierający zakres danych szerszy niż potrzebny powinien być przechowywany tylko wtedy, gdy istnieje ku temu odpowiednia podstawa i rzeczywista potrzeba.
5. W przypadku gdy wystarczające jest przechowywanie informacji o fakcie posiadania określonego dokumentu lub uprawnienia, należy rozważyć ograniczenie zakresu przechowywanych danych.

§ 42. Karta personalna członka w CBDOSP

1. Elektroniczną formę ewidencji danych członkowskich stanowi Karta personalna członka prowadzona w CBDOSP.
2. Karta personalna może obejmować w szczególności dane dotyczące:
   a. identyfikacji członka;

b. danych kontaktowych;
c. członkostwa;
d. pełnionych funkcji;
e. przydziału organizacyjnego;
f. udziału w JOT OSP;
g. wyszkolenia;
h. kwalifikacji;
i. uprawnień;
j. przebiegu służby w OSP;
k. odznaczeń i wyróżnień;
l. wydanego wyposażenia i umundurowania;
m. udziału w działaniach i ćwiczeniach – jeżeli jest to przewidziane funkcjonalnością systemu;
n. innych informacji niezbędnych do prawidłowego prowadzenia dokumentacji członkowskiej.

3. Zakres pól Karty personalnej powinien podlegać okresowej ocenie pod kątem:
   a. niezbędności;
   b. aktualności;
   c. zgodności z celem;
   d. prawidłowości podstawy prawnej.
4. Utworzenie technicznej możliwości wprowadzenia określonego rodzaju danych do Karty personalnej nie oznacza automatycznie, że dane te powinny być gromadzone dla każdego członka.
5. Dostęp do poszczególnych części Karty personalnej powinien być różnicowany odpowiednio do roli użytkownika.

§ 43. Numer identyfikacyjny członka

1. Członkowi może zostać nadany wewnętrzny numer identyfikacyjny służący prowadzeniu ewidencji w CBDOSP i dokumentacji OSP.
2. Wewnętrzny numer identyfikacyjny powinien być stosowany w procesach, w których nie jest konieczne posługiwanie się numerem PESEL albo innym powszechnym identyfikatorem.
3. W miarę możliwości wewnętrzny identyfikator członka należy wykorzystywać w:
   a. ewidencjach technicznych;
   b. kodach kreskowych;
   c. dokumentach wewnętrznych;
   d. powiązaniach pomiędzy modułami CBDOSP;
   e. innych procesach, w których pełny identyfikator ustawowy nie jest potrzebny.
4. Numer identyfikacyjny członka nie powinien ujawniać informacji szczególnych dotyczących osoby.

§ 44. Aktualizacja danych członkowskich

1. Dane zawarte w dokumentacji członkowskiej powinny być aktualizowane w zakresie niezbędnym dla realizacji celów ich przetwarzania.

2. Członek powinien zgłaszać zmiany danych mających znaczenie dla prowadzenia dokumentacji OSP, jeżeli obowiązek taki wynika z przepisów, Statutu albo właściwych aktów wewnętrznych.
3. Osoba dokonująca aktualizacji powinna zweryfikować, czy:
    a. posiada uprawnienie do zmiany danych;
    b. istnieje wiarygodna podstawa dokonania zmiany;
    c. aktualizacja nie prowadzi do nieuzasadnionego usunięcia danych historycznych.
4. Dane historyczne istotne dla udokumentowania przebiegu członkostwa mogą być zachowywane, jeżeli istnieje podstawa dalszego ich przechowywania.

§ 45. Dostęp do dokumentacji członkowskiej

1. Dostęp do dokumentacji członkowskiej posiadają wyłącznie osoby, których obowiązki uzasadniają taki dostęp.
2. Zakres dostępu powinien odpowiadać rodzajowi wykonywanych czynności.
3. Osoba uprawniona do wglądu w część dokumentacji nie uzyskuje automatycznie prawa dostępu do całych akt osobowych członka.
4. W szczególności należy ograniczyć dostęp do:
    a. numerów PESEL;
    b. danych dotyczących zdrowia;
    c. danych dokumentów tożsamości;
    d. danych bankowych;
    e. prywatnych danych kontaktowych;
    f. dokumentacji zawierającej informacje wymagające zwiększonej ochrony.
5. Udostępnienie dokumentacji wewnątrz OSP powinno następować w zakresie niezbędnym do wykonania konkretnego zadania.

§ 46. Dokumentacja po ustaniu członkostwa

1. Ustanie członkostwa nie powoduje automatycznego usunięcia wszystkich danych dotyczących byłego członka.
2. Po ustaniu członkostwa dokonuje się oceny:
    a. które dane powinny zostać zachowane;
    b. w jakim celu;
    c. przez jaki okres;
    d. na jakiej podstawie;
    e. kto powinien zachować do nich dostęp.
3. Dane potrzebne wyłącznie do bieżącej obsługi aktywnego członkostwa powinny zostać usunięte lub ograniczone, gdy ustanie podstawa ich dalszego przetwarzania.
4. Dane stanowiące część dokumentacji historycznej, finansowej, archiwalnej lub niezbędnej do ustalenia, dochodzenia albo obrony roszczeń mogą być przechowywane przez odpowiedni okres.
5. Konto byłego członka w systemach OSP podlega zablokowaniu lub usunięciu niezwłocznie po ustaniu podstawy dostępu.

Rozdział VIII
Centralna Baza Danych Ochotniczej Straży Pożarnej – CBDOSP

§ 47. Status i przeznaczenie CBDOSP

1. CBDOSP stanowi podstawowy system teleinformatyczny służący wspomaganiu prowadzenia ewidencji, dokumentacji i procesów organizacyjnych OSP Rydułtowy.
2. CBDOSP może służyć w szczególności do prowadzenia:
    a. Kart personalnych;
    b. ewidencji członków;
    c. dokumentacji MDP;
    d. dokumentacji Zarządu;
    e. dokumentacji Komisji Rewizyjnej;
    f. dokumentacji Sekretariatu;
    g. ewidencji korespondencji;
    h. dokumentacji magazynowej;
    i. dokumentacji sprzętu i umundurowania;
    j. ewidencji szkoleń;
    k. ewidencji odznaczeń;
    l. dokumentacji dotyczącej działań operacyjnych;
    m. kalendarza i terminów;
    n. dokumentacji finansowej – w zakresie przewidzianym funkcjonalnością systemu;
    o. innych procesów zatwierdzonych do realizacji w systemie.
3. Wprowadzenie danych do CBDOSP nie zmienia celu ani podstawy prawnej ich przetwarzania.
4. CBDOSP nie może być wykorzystywany do gromadzenia informacji niezwiązanych z działalnością OSP.

§ 48. Indywidualne konta użytkowników

1. Dostęp do CBDOSP odbywa się za pomocą indywidualnego konta użytkownika.
2. Zabrania się:
    a. tworzenia wspólnych kont dla kilku osób, chyba że wyjątkowa funkcjonalność techniczna nie pozwala na inne rozwiązanie i przeprowadzona analiza dopuszcza taki sposób działania;
    b. udostępniania danych logowania;
    c. korzystania z konta innego użytkownika;
    d. umożliwiania osobie trzeciej wykonywania czynności na aktywnej sesji użytkownika;
    e. zapisywania hasła w miejscu dostępnym dla osób nieuprawnionych.
3. Operacje wykonane z użyciem indywidualnego konta mogą być przypisywane użytkownikowi tego konta w zakresie wynikającym z prowadzonej dokumentacji i logów systemowych.
4. Użytkownik jest obowiązany niezwłocznie zgłosić:
    1. podejrzenie ujawnienia hasła;
    2. nieautoryzowane logowanie;
    3. nieznane operacje wykonane na koncie;
    4. utratę urządzenia posiadającego aktywną sesję;
    5. inne okoliczności mogące świadczyć o przejęciu konta.

§ 49. Nadawanie konta w CBDOSP

1. Konto w CBDOSP tworzy się wyłącznie dla osoby, która posiada uzasadnioną potrzebę korzystania z systemu.
2. Przed aktywacją konta ustala się:
    a. tożsamość użytkownika;
    b. podstawę przyznania dostępu;
    c. właściwą rolę;
    d. zakres modułów;
    e. zakres operacji;
    f. potrzebę dostępu do danych wymagających zwiększonej ochrony.
3. Nie należy nadawać dostępu do całego systemu, jeżeli do wykonania obowiązków wystarczający jest dostęp do określonego modułu.
4. Przyznanie funkcji administratora systemu wymaga szczególnego uzasadnienia.
5. Konto nie powinno być aktywowane przed spełnieniem wymagań organizacyjnych przewidzianych dla danego rodzaju dostępu.

§ 50. Role i poziomy uprawnień w CBDOSP

1. CBDOSP powinien stosować system ról i uprawnień odpowiadający strukturze organizacyjnej i zakresowi obowiązków użytkowników.
2. Uprawnienia mogą być różnicowane w szczególności według:
    a. modułu;
    b. rodzaju danych;
    c. prawa odczytu;
    d. prawa dodawania;
    e. prawa edycji;
    f. prawa zatwierdzania;
    g. prawa usuwania;
    h. prawa drukowania;
    i. prawa eksportowania;
    j. prawa zarządzania użytkownikami.
3. Użytkownik powinien otrzymywać wyłącznie uprawnienia niezbędne do wykonywania jego obowiązków.
4. System powinien w miarę możliwości technicznych uniemożliwiać użytkownikowi wykonywanie operacji wykraczających poza przyznany zakres.
5. Funkcjonalność techniczna nie zastępuje obowiązku działania zgodnie z udzielonym upoważnieniem.

§ 51. Uwierzytelnianie użytkowników

1. Dostęp do CBDOSP wymaga uwierzytelnienia użytkownika.
2. Dane uwierzytelniające mają charakter poufny.
3. Hasło powinno:
    a. być znane wyłącznie użytkownikowi;
    b. być odpowiednio odporne na odgadnięcie;
    c. nie stanowić oczywistego połączenia danych użytkownika;
    d. nie być przekazywane innym osobom;
    e. zostać niezwłocznie zmienione w przypadku podejrzenia jego ujawnienia.

4. Jeżeli system umożliwia zastosowanie uwierzytelniania wieloskładnikowego, zasadność jego wdrożenia ocenia się w szczególności dla:
    1. kont administratorów;
    2. dostępu zdalnego;
    3. kont posiadających dostęp do szczególnych kategorii danych;
    4. kont posiadających możliwość masowego eksportu danych.
5. Mechanizmy uwierzytelniania powinny być okresowo oceniane w ramach analizy ryzyka.

§ 52. Sesja użytkownika i zabezpieczenie stanowiska

1. Użytkownik jest obowiązany chronić aktywną sesję CBDOSP przed wykorzystaniem przez osobę nieuprawnioną.
2. W przypadku czasowego opuszczenia stanowiska użytkownik powinien:
    a. zablokować urządzenie; albo
    b. zakończyć sesję, jeżeli wymagają tego okoliczności.
3. Po zakończeniu pracy użytkownik powinien wylogować się z systemu.
4. CBDOSP powinien, jeżeli jest to technicznie uzasadnione, stosować automatyczne zakończenie lub blokowanie nieaktywnej sesji.
5. Zabrania się pozostawiania aktywnego konta na ogólnodostępnym komputerze bez nadzoru.

§ 53. Rejestrowanie operacji w CBDOSP

1. CBDOSP powinien zapewniać rejestrowanie operacji w zakresie odpowiednim do ryzyka i charakteru przetwarzanych danych.
2. Rejestracji mogą podlegać w szczególności:
    a. logowania;
    b. nieudane próby logowania;
    c. utworzenie konta;
    d. zmiana roli;
    e. zmiana uprawnień;
    f. dodanie danych;
    g. istotna modyfikacja danych;
    h. usunięcie danych;
    i. eksport danych;
    j. inne operacje o podwyższonym znaczeniu dla bezpieczeństwa.
3. Logi systemowe służą w szczególności:
    a. zapewnieniu bezpieczeństwa;
    b. wykrywaniu nieprawidłowości;
    c. wyjaśnianiu incydentów;
    d. zapewnieniu rozliczalności;
    e. ustalaniu przyczyn błędów technicznych.
4. Dostęp do logów posiadają wyłącznie osoby uprawnione.
5. Logi nie mogą być wykorzystywane do celów niezwiązanych z bezpieczeństwem, rozliczalnością, obsługą techniczną lub innym zgodnym z prawem celem.

§ 54. Drukowanie danych z CBDOSP

1. Wydruk z CBDOSP stanowi dokument podlegający ochronie odpowiednio do zakresu zawartych w nim danych.
2. Wydruk powinien obejmować wyłącznie dane niezbędne do realizacji celu, dla którego został wygenerowany.
3. Użytkownik wykonujący wydruk odpowiada za:
    a. zasadność jego wykonania;
    b. odebranie wydruku z urządzenia;
    c. zabezpieczenie przed dostępem osób nieuprawnionych;
    d. właściwe wykorzystanie;
    e. przechowywanie;
    f. bezpieczne zniszczenie zbędnego egzemplarza.
4. Wydruki zawierające dane osobowe nie mogą pozostawać bez nadzoru w urządzeniu drukującym.
5. Nie należy wykonywać dodatkowych kopii wydruku, jeżeli nie jest to niezbędne.

§ 55. Eksport danych z CBDOSP

1. Eksport danych z CBDOSP do pliku może być wykonywany wyłącznie w uzasadnionym celu.
2. Dotyczy to w szczególności eksportu do:
    a. XLSX;
    b. CSV;
    c. PDF;
    d. plików tekstowych;
    e. innych formatów umożliwiających dalsze przetwarzanie.
3. Eksport powinien obejmować możliwie najmniejszy niezbędny zakres danych.
4. Plik po wyeksportowaniu powinien:
    a. być przechowywany w bezpiecznej lokalizacji;
    b. posiadać ograniczony dostęp;
    c. być zabezpieczony odpowiednio do charakteru danych;
    d. zostać usunięty po ustaniu potrzeby jego przechowywania, chyba że istnieje podstawa dalszej retencji.
5. Zabrania się systematycznego eksportowania danych w celu tworzenia prywatnej lub niezatwierdzonej równoległej bazy członków.
6. Plik pobrany na urządzenie użytkownika nie przestaje podlegać Polityce.

§ 56. Usuwanie i modyfikowanie danych w CBDOSP

1. Usuwanie danych w CBDOSP może następować wyłącznie przez osobę posiadającą odpowiednie uprawnienie.
2. Przed usunięciem należy w razie potrzeby ustalić:
    a. podstawę usunięcia;
    b. wpływ usunięcia na inne moduły;
    c. obowiązujący okres retencji;
    d. znaczenie danych dla dokumentacji historycznej;
    e. możliwość występowania obowiązku archiwizacji;
    f. konieczność zachowania śladu operacji.

3. Dane nie mogą być usuwane w celu:
    a. ukrycia błędu;
    b. ukrycia nieprawidłowości;
    c. uniemożliwienia kontroli;
    d. usunięcia dowodu wykonanej operacji;
    e. obejścia zasad archiwizacji.
4. Jeżeli charakter dokumentacji wymaga zachowania historii, korekta powinna następować w sposób umożliwiający odtworzenie przebiegu zmian.
5. Operacje usunięcia danych o istotnym znaczeniu powinny podlegać odpowiedniej rozliczalności.

§ 57. Kopie bezpieczeństwa CBDOSP

1. Dla danych CBDOSP stosuje się odpowiednie mechanizmy wykonywania kopii bezpieczeństwa.
2. Organizacja kopii bezpieczeństwa powinna uwzględniać:
    a. częstotliwość wykonywania kopii;
    b. zakres danych;
    c. miejsce przechowywania;
    d. ochronę przed nieuprawnionym dostępem;
    e. ochronę przed utratą wraz z systemem podstawowym;
    f. okres przechowywania;
    g. możliwość skutecznego odtworzenia danych.
3. Dostęp do kopii bezpieczeństwa powinien być ograniczony do osób odpowiedzialnych za ich utrzymanie i odtwarzanie.
4. Kopia bezpieczeństwa nie może być traktowana jako bezterminowe archiwum wszystkich danych.
5. Zasady usuwania danych z kopii zapasowych powinny uwzględniać techniczne właściwości systemu oraz obowiązujące okresy rotacji kopii.
6. Skuteczność procesu odtwarzania danych powinna być okresowo weryfikowana.

§ 58. Aktualizacje i bezpieczeństwo CBDOSP

1. CBDOSP powinien być utrzymywany w sposób ograniczający ryzyko wykorzystania znanych podatności.
2. W szczególności należy zapewnić:
    a. instalowanie uzasadnionych aktualizacji bezpieczeństwa;
    b. usuwanie stwierdzonych podatności;
    c. kontrolę zmian w systemie;
    d. ograniczenie dostępu do środowiska produkcyjnego;
    e. zabezpieczenie danych podczas prac serwisowych;
    f. weryfikację wpływu istotnych zmian na ochronę danych.
3. Dane rzeczywistych członków nie powinny być wykorzystywane w środowisku testowym, jeżeli test może zostać przeprowadzony na danych fikcyjnych lub odpowiednio zanonimizowanych.
4. Jeżeli wykorzystanie rzeczywistych danych w testach jest wyjątkowo niezbędne, należy:
    a. ustalić podstawę i cel takiego działania;
    b. ograniczyć zakres danych;

c. ograniczyć krąg osób posiadających dostęp;
d. zastosować odpowiednie zabezpieczenia;
e. usunąć dane po zakończeniu testu, jeżeli nie istnieje podstawa dalszego przechowywania.

§ 59. Ciągłość działania CBDOSP

1. OSP podejmuje odpowiednie działania służące zapewnieniu dostępności danych i możliwości odtworzenia dostępu do nich po wystąpieniu incydentu.
2. Przy organizacji ciągłości działania należy uwzględniać w szczególności:
   a. awarię serwera;
   b. awarię bazy danych;
   c. uszkodzenie plików;
   d. utratę dostępu do hostingu;
   e. działanie złośliwego oprogramowania;
   f. przypadkowe usunięcie danych;
   g. utratę danych uwierzytelniających;
   h. niedostępność osoby posiadającej uprawnienia administracyjne.
3. Procedury odtworzeniowe powinny zapewniać możliwość ustalenia:
   1. zakresu utraconych danych;
   2. momentu wystąpienia awarii;
   3. dostępnych kopii;
   4. zakresu możliwego odtworzenia;
   5. ewentualnego wpływu zdarzenia na prawa i wolności osób fizycznych.
4. Awaria CBDOSP mogąca prowadzić do naruszenia poufności, integralności lub dostępności danych podlega również ocenie jako potencjalne naruszenie ochrony danych.

Rozdział IX
Dane małoletnich i dokumentacja Młodzieżowej Drużyny Pożarniczej

§ 60. Szczególna ochrona danych małoletnich

1. Dane osobowe członków MDP podlegają szczególnej ochronie z uwagi na status osób małoletnich.
2. Przetwarzając dane członków MDP, należy w szczególności:
   a. ograniczać zakres danych do niezbędnego minimum;
   b. stosować podwyższone środki organizacyjne;
   c. ograniczać krąg osób posiadających dostęp;
   d. uwzględniać wiek i dojrzałość małoletniego;
   e. przekazywać informacje dotyczące przetwarzania w sposób jasny i zrozumiały;
   f. odpowiednio uwzględniać rolę rodziców lub opiekunów prawnych;
   g. zachować szczególną ostrożność przy publikowaniu danych i wizerunku.
3. Fakt członkostwa dziecka w MDP nie stanowi podstawy do nieograniczonego przetwarzania jego danych.

§ 61. Dokumentacja członka MDP

1. Dla członka MDP może być prowadzona dokumentacja niezbędna do organizacji jego członkostwa i udziału w działalności MDP.
2. Dokumentacja może obejmować w szczególności:
   a. dane identyfikacyjne;
   b. dane kontaktowe;
   c. datę urodzenia;
   d. informacje o członkostwie;
   e. dane rodziców lub opiekunów prawnych w zakresie niezbędnym do kontaktu i wykonywania obowiązków organizacyjnych;
   f. dokumenty wymagane dla uczestnictwa w określonych przedsięwzięciach;
   g. ewidencję udziału w zbiórkach;
   h. ewidencję udziału w zawodach, wyjazdach i wydarzeniach;
   i. informacje o przyznanych wyróżnieniach;
   j. informacje niezbędne do zapewnienia bezpieczeństwa małoletniego – w zakresie posiadającym właściwą podstawę prawną.
3. Nie należy pozyskiwać informacji o sytuacji rodzinnej małoletniego w zakresie wykraczającym poza rzeczywistą potrzebę wynikającą z działalności MDP.
4. Dokumentacja MDP powinna być oddzielona organizacyjnie lub logicznie od dokumentacji dostępnej dla ogółu członków OSP.

§ 62. Dane rodziców i opiekunów prawnych

1. Dane rodziców lub opiekunów prawnych członka MDP mogą być przetwarzane w zakresie niezbędnym do:
   a. organizacji członkostwa małoletniego;
   b. wykonywania obowiązków informacyjnych;
   c. uzyskiwania wymaganych oświadczeń lub zgód;
   d. kontaktu w sprawach organizacyjnych;
   e. kontaktu w sytuacjach wymagających pilnego działania;
   f. organizacji wyjazdów, zawodów i innych przedsięwzięć.
2. Dane kontaktowe rodziców lub opiekunów nie mogą być wykorzystywane do prywatnych celów osób prowadzących MDP.
3. Udostępnienie danych kontaktowych innemu rodzicowi lub osobie trzeciej wymaga istnienia odpowiedniej podstawy.
4. Listy kontaktowe nie powinny być rozpowszechniane pomiędzy rodzicami, jeżeli realizacja celu nie wymaga ujawnienia danych wszystkich osób.

§ 63. Dostęp do danych MDP

1. Dostęp do dokumentacji MDP przysługuje wyłącznie osobom, dla których jest on niezbędny do wykonywania powierzonych zadań.
2. Zakres dostępu może obejmować w szczególności:
   a. właściwych członków Zarządu;
   b. Inspektora Ochrony Małoletnich – w zakresie wynikającym z powierzonych mu zadań;
   c. opiekunów MDP – w zakresie koniecznym do organizacji działalności drużyny;
   d. osoby wykonujące określone zadania administracyjne;

e. inne osoby, jeżeli istnieje właściwa podstawa dostępu.

3. Pełnienie funkcji w OSP nie daje automatycznego prawa do przeglądania dokumentacji MDP.
4. Uprawnienia do modułu MDP w CBDOSP powinny być nadawane oddzielnie i podlegać okresowej weryfikacji.

§ 64. Informacje dotyczące bezpieczeństwa małoletniego

1. Informacje dotyczące szczególnych potrzeb małoletniego mogą być przetwarzane wyłącznie w zakresie niezbędnym do zapewnienia jego bezpieczeństwa i prawidłowej organizacji określonej aktywności oraz przy istnieniu właściwej podstawy prawnej.
2. Jeżeli do zapewnienia bezpieczeństwa wystarcza informacja praktyczna, nie należy udostępniać szerszego zakresu dokumentacji.
3. Opiekunowi odpowiedzialnemu za określone wydarzenie przekazuje się wyłącznie informacje, których znajomość jest rzeczywiście niezbędna.
4. Informacje, o których mowa w ust. 1, nie mogą:
    a. być omawiane w obecności osób nieuprawnionych;
    b. być publikowane w grupach komunikacyjnych;
    c. być umieszczane w ogólnodostępnych zestawieniach;
    d. być wykorzystywane w celu innym niż ten, dla którego zostały pozyskane.

§ 65. Ewidencja obecności na zbiórkach MDP

1. OSP może prowadzić ewidencję obecności członków MDP na zbiórkach oraz innych zajęciach.
2. Ewidencja powinna obejmować wyłącznie dane niezbędne do:
    a. potwierdzenia uczestnictwa;
    b. prowadzenia dokumentacji działalności MDP;
    c. zapewnienia bezpieczeństwa uczestników;
    d. sporządzania wymaganych zestawień.
3. Jeżeli obecność jest rejestrowana za pomocą identyfikatora, kodu kreskowego albo innego rozwiązania technicznego, należy dążyć do tego, aby sam identyfikator nie ujawniał zbędnych danych małoletniego.
4. System rejestracji obecności nie może służyć do nieuzasadnionego śledzenia aktywności małoletniego poza działalnością MDP.

§ 66. Wyjazdy, zawody i wydarzenia MDP

1. Przy organizacji wyjazdu, zawodów, obozu, uroczystości albo innego wydarzenia z udziałem członków MDP przetwarza się wyłącznie dane niezbędne do organizacji i bezpiecznego przeprowadzenia przedsięwzięcia.
2. Listy uczestników powinny zawierać zakres informacji odpowiedni do celu ich wykorzystania.
3. Dokument przeznaczony dla:
    a. organizatora;
    b. przewoźnika;
    c. opiekuna;
    d. ubezpieczyciela;

e. innego odbiorcy – powinien obejmować wyłącznie dane niezbędne danemu odbiorcy.
4. Niedopuszczalne jest stosowanie jednej pełnej listy zawierającej wszystkie zgromadzone dane w każdym celu organizacyjnym.
5. Po zakończeniu przedsięwzięcia zbędne kopie robocze list podlegają bezpiecznemu usunięciu lub zniszczeniu.

§ 67. Wizerunek członków MDP

1. Wykonywanie, utrwalanie i rozpowszechnianie wizerunku członków MDP wymaga każdorazowego uwzględnienia właściwych przepisów prawa, celu wykorzystania materiału oraz praw i interesów małoletniego.
2. Jeżeli rozpowszechnianie wizerunku wymaga zezwolenia, powinno ono określać w sposób odpowiednio jasny zakres i cel wykorzystania.
3. Przy publikowaniu materiałów należy unikać ujawniania wraz z wizerunkiem nadmiernego zakresu informacji o małoletnim.
4. W szczególności nie należy bez uzasadnionej potrzeby łączyć publicznie:
   a. pełnego imienia i nazwiska;
   b. dokładnej daty urodzenia;
   c. adresu;
   d. prywatnych danych kontaktowych;
   e. informacji dotyczących zdrowia;
   f. informacji dotyczących sytuacji rodzinnej – z fotografią małoletniego.
5. Materiały naruszające godność, prywatność albo mogące przedstawiać małoletniego w nieodpowiednim kontekście nie mogą być publikowane niezależnie od istnienia technicznej możliwości publikacji.

§ 68. Ochrona danych MDP w komunikacji elektronicznej

1. Komunikacja elektroniczna dotycząca MDP powinna być organizowana w sposób ograniczający nieuzasadnione ujawnianie danych małoletnich oraz ich rodziców lub opiekunów.
2. W szczególności należy:
   a. ograniczać publikowanie list członków;
   b. ograniczać przekazywanie danych kontaktowych w grupach;
   c. weryfikować odbiorców przed wysłaniem dokumentacji;
   d. nie przesyłać danych szczególnych kategorii w otwartych grupach komunikacyjnych;
   e. usuwać zbędne załączniki zawierające dane po zakończeniu ich wykorzystania.
3. Utworzenie grupy komunikacyjnej nie oznacza, że każdy jej uczestnik jest uprawniony do otrzymywania wszystkich danych dotyczących innych członków MDP.
4. Przy masowej korespondencji elektronicznej należy odpowiednio chronić adresy odbiorców przed nieuzasadnionym ujawnieniem.

§ 69. Ustanie członkostwa w MDP

1. Po ustaniu członkostwa w MDP dokonuje się przeglądu danych małoletniego.
2. Dane potrzebne wyłącznie do bieżącej organizacji uczestnictwa powinny zostać usunięte albo ograniczone po ustaniu celu ich przetwarzania.
3. Dokumentacja posiadająca znaczenie:
    a. organizacyjne;
    b. dowodowe;
    c. finansowe;
    d. archiwalne;
    e. historyczne – może być przechowywana przez okres właściwy dla danej kategorii dokumentacji, jeżeli istnieje odpowiednia podstawa.
4. Dostęp byłych opiekunów MDP do dokumentacji podlega cofnięciu niezwłocznie po ustaniu podstawy dostępu.

Rozdział X
Wizerunek, materiały fotograficzne i działalność informacyjna OSP

§ 70. Zasady przetwarzania wizerunku

1. Utrwalanie, przechowywanie i rozpowszechnianie wizerunku osób fizycznych odbywa się z poszanowaniem przepisów o ochronie danych osobowych, przepisów dotyczących ochrony wizerunku oraz dóbr osobistych.
2. Przed rozpowszechnieniem wizerunku należy ustalić w szczególności:
    a. cel publikacji;
    b. podstawę prawną przetwarzania danych osobowych;
    c. czy rozpowszechnienie wizerunku wymaga zezwolenia na podstawie właściwych przepisów;
    d. zakres informacji publikowanych razem z wizerunkiem;
    e. krąg potencjalnych odbiorców;
    f. możliwe skutki publikacji dla osoby przedstawionej.
3. Fakt członkostwa w OSP nie oznacza automatycznej zgody na nieograniczone utrwalanie i rozpowszechnianie wizerunku.
4. Zgoda na wykorzystanie wizerunku, jeżeli jest wymagana, powinna być odpowiednio konkretna i umożliwiać ustalenie zakresu dopuszczonego wykorzystania.
5. Materiałów fotograficznych nie należy wykorzystywać w sposób mogący naruszać godność, dobre imię lub prywatność przedstawionej osoby.

§ 71. Dokumentowanie działalności OSP

1. OSP może dokumentować swoją działalność w formie fotografii, materiałów audiowizualnych oraz innych zapisów, jeżeli odbywa się to zgodnie z prawem.
2. Dokumentowanie może dotyczyć w szczególności:
    a. uroczystości;
    b. ćwiczeń;
    c. szkoleń;
    d. zawodów;
    e. wydarzeń społecznych;
    f. działalności MDP;

g. zebrań i wydarzeń organizacyjnych;
h. działań ratowniczych – z uwzględnieniem szczególnych ograniczeń wynikających z charakteru zdarzenia;
i. historii OSP.

3. Osoba wykonująca dokumentację fotograficzną w imieniu OSP powinna ograniczać utrwalanie informacji niezwiązanych z celem dokumentacji.
4. Szczególnej ostrożności wymaga utrwalanie:
   a. osób poszkodowanych;
   b. osób małoletnich;
   c. wnętrz prywatnych nieruchomości;
   d. dokumentów;
   e. tablic rejestracyjnych, jeżeli ich publikacja nie jest uzasadniona;
   f. ekranów urządzeń zawierających dane;
   g. innych informacji mogących naruszać prywatność osoby.

§ 72. Publikowanie materiałów w Internecie

1. Przed opublikowaniem materiału w Internecie należy ocenić zakres ujawnianych danych.
2. Publikacja powinna ograniczać się do informacji niezbędnych do realizacji celu informacyjnego, promocyjnego, edukacyjnego, dokumentacyjnego lub historycznego.
3. Zabrania się publikowania bez odpowiedniej podstawy w szczególności:
   a. numerów PESEL;
   b. adresów zamieszkania;
   c. prywatnych numerów telefonów;
   d. prywatnych adresów poczty elektronicznej;
   e. danych dokumentów tożsamości;
   f. informacji dotyczących zdrowia;
   g. danych finansowych;
   h. dokumentów zawierających podpisy, jeżeli ich publikacja nie jest konieczna;
   i. danych uwierzytelniających;
   j. informacji objętych obowiązkiem poufności.
4. Przed publikacją fotografii dokumentu należy zweryfikować całą widoczną treść, w tym tło, załączniki, podpisy, numery identyfikacyjne i inne dane.
5. Publikacja materiału w Internecie powinna być traktowana jako potencjalne udostępnienie go nieograniczonemu kręgowi odbiorców.

§ 73. Media społecznościowe OSP

1. Oficjalne profile OSP w mediach społecznościowych mogą być prowadzone wyłącznie przez osoby upoważnione.
2. Dostęp administracyjny do profili powinien być ograniczony do niezbędnej liczby osób.
3. Dane dostępowe do oficjalnych profili nie mogą być przekazywane osobom nieuprawnionym.
4. W przypadku zmiany osoby odpowiedzialnej za prowadzenie profilu należy:
   a. odebrać dotychczasowy dostęp;
   b. zmienić dane uwierzytelniające, jeżeli jest to niezbędne;

c. zweryfikować listę aktywnych administratorów;
d. zabezpieczyć ciągłość dostępu OSP do profilu.

5. Osoba publikująca materiał odpowiada za dokonanie przed publikacją podstawowej weryfikacji, czy materiał nie zawiera danych, których ujawnienie jest niedopuszczalne.
6. Prywatny profil członka OSP nie staje się oficjalnym kanałem OSP wyłącznie dlatego, że publikowane są na nim informacje dotyczące działalności jednostki.

§ 74. Materiały archiwalne i kronikarskie

1. OSP może prowadzić dokumentację kronikarską i historyczną dotyczącą działalności jednostki.
2. Przy kwalifikowaniu materiałów do trwałego zachowania należy uwzględnić:
   a. ich znaczenie historyczne;
   b. wartość dokumentacyjną;
   c. zakres zawartych danych;
   d. prawa i wolności osób;
   e. możliwość ograniczenia zakresu danych;
   f. obowiązujące przepisy dotyczące archiwizacji.
3. Cel historyczny nie uzasadnia automatycznie trwałego przechowywania każdego dokumentu zawierającego dane osobowe.
4. W przypadku udostępniania materiałów historycznych należy każdorazowo ocenić zakres danych podlegających ujawnieniu.

Rozdział XI
Sekretariat, korespondencja i dokumentacja urzędowa OSP

§ 75. Ochrona danych w Sekretariacie

1. Sekretariat OSP prowadzi dokumentację zgodnie z zasadami ochrony danych, instrukcją kancelaryjną oraz innymi właściwymi aktami wewnętrznymi.
2. Organizacja Sekretariatu powinna zapewniać w szczególności:
   a. rejestrowanie dokumentacji w odpowiednim zakresie;
   b. ograniczenie dostępu;
   c. zabezpieczenie dokumentów;
   d. możliwość ustalenia lokalizacji dokumentacji;
   e. przestrzeganie zasad retencji;
   f. właściwe przekazywanie dokumentacji do archiwizacji;
   g. bezpieczne brakowanie.
3. Dokumentacja nie może pozostawać bez nadzoru w miejscach dostępnych dla osób nieuprawnionych.
4. Dokumenty robocze podlegają ochronie na takich samych zasadach jak dokumenty ostateczne, jeżeli zawierają dane osobowe.

§ 76. Korespondencja przychodząca

1. Korespondencję przychodzącą zawierającą dane osobowe przetwarza się wyłącznie w zakresie niezbędnym do jej rejestracji, dekretacji, rozpatrzenia i archiwizacji.
2. Osoba przyjmująca korespondencję nie może ujawniać jej treści osobom, których udział w prowadzeniu sprawy nie jest niezbędny.

3. Jeżeli korespondencja:
    a. została oznaczona jako przeznaczona do rąk określonej osoby;
    b. zawiera dane wymagające podwyższonej ochrony;
    c. dotyczy sprawy wymagającej ograniczonego dostępu – należy zastosować sposób postępowania odpowiedni do charakteru przesyłki.
4. Rejestr korespondencji powinien zawierać wyłącznie dane niezbędne do identyfikacji przesyłki i prowadzenia sprawy.

§ 77. Korespondencja wychodząca

1. Przed wysłaniem korespondencji należy zweryfikować:
    a. prawidłowość odbiorcy;
    b. prawidłowość adresu;
    c. zakres danych;
    d. kompletność i właściwość załączników;
    e. zasadność przekazania danych danemu odbiorcy.
2. W przypadku korespondencji elektronicznej należy dodatkowo sprawdzić:
    a. adres poczty elektronicznej;
    b. listę odbiorców;
    c. pola DW i UDW;
    d. nazwy i zawartość załączników;
    e. potrzebę zastosowania dodatkowego zabezpieczenia.
3. Dokument zawierający dane innej osoby niż adresat nie może zostać wysłany bez uprzedniej weryfikacji zasadności ujawnienia tych danych.
4. Błędne wysłanie korespondencji podlega ocenie jako potencjalne naruszenie ochrony danych.

§ 78. Poczta elektroniczna

1. Służbowa poczta elektroniczna powinna być wykorzystywana zgodnie z jej przeznaczeniem.
2. Przy przetwarzaniu danych za pośrednictwem poczty elektronicznej należy:
    a. weryfikować adres odbiorcy;
    b. ograniczać liczbę odbiorców;
    c. stosować pole UDW, jeżeli ujawnienie adresów pomiędzy odbiorcami nie jest uzasadnione;
    d. ograniczać zakres danych w treści wiadomości;
    e. zabezpieczać załączniki, jeżeli wymaga tego ryzyko;
    f. usuwać zbędne kopie wiadomości zgodnie z zasadami retencji.
3. Zabrania się automatycznego przekierowywania całej służbowej korespondencji na prywatną skrzynkę pocztową bez zatwierdzonej potrzeby i oceny bezpieczeństwa.
4. Przesłanie dokumentu na własną prywatną skrzynkę w celu wygodniejszego wykonania pracy jest niedopuszczalne, jeżeli nie zostało przewidziane jako zatwierdzony sposób przetwarzania.

§ 79. Książka korespondencji i ewidencja spraw

1. Książka korespondencji oraz ewidencja spraw powinny zawierać dane niezbędne do zapewnienia prawidłowego obiegu dokumentacji.
2. Opis sprawy nie powinien zawierać nadmiernego zakresu danych osobowych.

3. Jeżeli wystarczające jest użycie:
    a. numeru sprawy;
    b. numeru dokumentu;
    c. skróconego przedmiotu sprawy;
    d. wewnętrznego identyfikatora – należy unikać umieszczania dodatkowych danych osobowych w widokach zbiorczych.
4. Dostęp do pełnej treści dokumentu może być bardziej ograniczony niż dostęp do informacji o istnieniu sprawy.

§ 80. Dziennik Urzędowy OSP

1. Dziennik Urzędowy OSP prowadzony w CBDOSP może zawierać uchwały, zarządzenia, regulaminy, procedury i inne akty wewnętrzne.
2. Przed umieszczeniem dokumentu w Dzienniku Urzędowym należy ustalić:
    a. czy dokument zawiera dane osobowe;
    b. czy zakres danych jest niezbędny;
    c. jaki krąg użytkowników powinien posiadać dostęp;
    d. czy dokument może być udostępniony publicznie;
    e. czy przed publikacją konieczna jest anonimizacja.
3. Umieszczenie dokumentu w Dzienniku Urzędowym OSP nie oznacza automatycznie, że dokument powinien być dostępny dla wszystkich użytkowników CBDOSP.
4. Dokumenty zawierające dane wymagające ograniczonego dostępu powinny posiadać odpowiednio ograniczone uprawnienia.
5. Wersja publiczna dokumentu może różnić się od wersji wewnętrznej poprzez anonimizację albo ograniczenie danych.

§ 81. Dokumentacja Zarządu OSP

1. Dokumentacja Zarządu podlega ochronie odpowiednio do charakteru zawartych w niej danych.
2. Protokoły posiedzeń powinny zawierać dane osobowe wyłącznie w zakresie niezbędnym do rzetelnego udokumentowania przebiegu posiedzenia oraz podjętych rozstrzygnięć.
3. W protokole nie należy zamieszczać nadmiernie szczegółowych informacji dotyczących:
    a. zdrowia;
    b. sytuacji rodzinnej;
    c. prywatnych okoliczności członka;
    d. innych informacji wymagających zwiększonej ochrony – jeżeli dla udokumentowania sprawy wystarczające jest użycie bardziej ogólnego sformułowania.
4. Załączniki zawierające szczegółowe dane mogą podlegać bardziej ograniczonemu dostępowi niż sam protokół.
5. Publikacja uchwały lub protokołu wymaga odrębnej oceny zakresu danych podlegających ujawnieniu.

§ 82. Dokumentacja Komisji Rewizyjnej

1. Komisja Rewizyjna może uzyskiwać dostęp do danych osobowych w zakresie niezbędnym do wykonywania statutowych kompetencji kontrolnych.
2. Uprawnienie kontrolne nie oznacza nieograniczonego prawa do kopiowania całych zbiorów danych.
3. Jeżeli cel kontroli można osiągnąć poprzez:
    a. wgląd;
    b. zestawienie ograniczone;
    c. dane zanonimizowane;
    d. dane pseudonimizowane;
    e. próbę dokumentacji – należy rozważyć zastosowanie rozwiązania ograniczającego zakres przetwarzania.
4. Członkowie Komisji są obowiązani zachować poufność danych uzyskanych w związku z kontrolą.
5. Materiał dowodowy dołączany do dokumentacji kontroli powinien zawierać wyłącznie zakres danych niezbędny do udokumentowania ustalenia.
6. Zbędne kopie dokumentacji wykonane na potrzeby kontroli podlegają usunięciu lub zniszczeniu po ustaniu potrzeby ich przechowywania.

Rozdział XII
Dokumentacja finansowa, składki i rozliczenia

§ 83. Dane w dokumentacji finansowo-księgowej

1. Dane osobowe zawarte w dokumentacji finansowo-księgowej przetwarza się w zakresie niezbędnym do:
    a. prowadzenia rachunkowości;
    b. dokumentowania operacji finansowych;
    c. wykonywania obowiązków podatkowych;
    d. rozliczania należności i zobowiązań;
    e. rozliczania członków;
    f. dokumentowania składek;
    g. wykonywania obowiązków wynikających z przepisów prawa;
    h. ustalania, dochodzenia lub obrony roszczeń.
2. Dostęp do pełnej dokumentacji finansowej powinien być ograniczony do osób wykonujących zadania uzasadniające taki dostęp.
3. Dane finansowe nie mogą być wykorzystywane do celów niezwiązanych z gospodarką finansową OSP.

§ 84. Ewidencja składek członkowskich

1. OSP może prowadzić ewidencję należnych i zapłaconych składek członkowskich.
2. Ewidencja może zawierać w szczególności:
    a. identyfikator członka;
    b. imię i nazwisko;
    c. okres, którego dotyczy składka;
    d. wysokość należności;
    e. datę zapłaty;
    f. status rozliczenia;

g. informacje niezbędne do identyfikacji płatności.
3. Informacje o zaległościach członka nie powinny być publicznie ujawniane.
4. Zestawienia składek powinny być udostępniane wyłącznie osobom, których obowiązki uzasadniają taki dostęp.
5. Jeżeli dla określonego celu wystarcza informacja zbiorcza, nie należy ujawniać danych poszczególnych członków.

§ 85. Rachunki bankowe i płatności

1. Dane rachunków bankowych osób fizycznych podlegają zwiększonej ochronie.
2. Dane te mogą być przetwarzane wyłącznie w zakresie niezbędnym do:
   a. wykonania płatności;
   b. przyjęcia płatności;
   c. rozliczenia operacji;
   d. prowadzenia księgowości;
   e. wykonania obowiązku prawnego;
   f. ustalenia, dochodzenia lub obrony roszczeń.
3. Dokumentów bankowych nie należy udostępniać w całości, jeżeli dla danego celu wystarczające jest ograniczone zestawienie.
4. Dane uwierzytelniające do bankowości elektronicznej nie mogą być umieszczane w CBDOSP, dokumentach ogólnych ani przekazywane osobom nieuprawnionym.

§ 86. Darczyńcy, kontrahenci i osoby współpracujące

1. Dane darczyńców, kontrahentów i innych osób współpracujących z OSP przetwarza się wyłącznie w zakresie wynikającym z właściwego celu.
2. Dane mogą być przetwarzane w szczególności w celu:
   a. zawarcia i wykonania umowy;
   b. prowadzenia rozliczeń;
   c. dokumentowania darowizny;
   d. prowadzenia korespondencji;
   e. wykonywania obowiązków podatkowych i rachunkowych;
   f. ustalenia, dochodzenia lub obrony roszczeń.
3. Dane osób reprezentujących kontrahenta oraz jego pracowników powinny być ograniczone do zakresu niezbędnego dla współpracy.
4. Dane kontaktowe uzyskane w związku z określoną współpracą nie powinny być wykorzystywane do innych celów bez właściwej podstawy.

Rozdział XIII
Dane związane z działalnością operacyjną OSP

§ 87. Dokumentacja działalności operacyjnej

1. Dane osobowe związane z działalnością operacyjną OSP przetwarza się wyłącznie w zakresie wynikającym z właściwych zadań, przepisów prawa oraz potrzeb dokumentacyjnych.
2. Dokumentacja może obejmować dane dotyczące w szczególności:
   a. członków uczestniczących w działaniu;
   b. składu zastępu;
   c. pełnionych funkcji;

d. czasu udziału w działaniu;
e. wykorzystanych pojazdów i sprzętu;
f. rodzaju zdarzenia;
g. miejsca zdarzenia;
h. innych informacji wymaganych dla prawidłowego udokumentowania działalności.

3. Zakres danych osób innych niż członkowie OSP powinien być ograniczony do informacji, których przetwarzanie jest rzeczywiście uzasadnione.
4. CBDOSP nie powinien służyć do tworzenia nieuzasadnionych baz danych osób poszkodowanych, świadków lub właścicieli nieruchomości.

§ 88. Dane członków JOT OSP

1. W zakresie niezbędnym do organizacji gotowości operacyjnej mogą być przetwarzane informacje dotyczące spełniania przez członka warunków wymaganych do udziału w działaniach.
2. W widokach operacyjnych należy preferować informacje o:
   a. aktualności wymaganego badania;
   b. aktualności szkolenia;
   c. posiadaniu wymaganych uprawnień;
   d. zdolności do udziału w działaniu – zamiast ujawniania szczegółowych danych źródłowych, jeżeli nie są one potrzebne użytkownikowi.
3. Informacja o braku zdolności do udziału w działaniu nie powinna ujawniać przyczyny medycznej osobom, które nie potrzebują tej informacji.
4. Dostęp do dokumentów źródłowych powinien być bardziej ograniczony niż dostęp do informacji o spełnianiu wymagań operacyjnych.

§ 89. Materiały ze zdarzeń i ochrona osób trzecich

1. Materiały powstałe podczas działań ratowniczych lub innych zdarzeń mogą zawierać dane osób trzecich wymagające szczególnej ostrożności.
2. Dotyczy to w szczególności:
   a. osób poszkodowanych;
   b. osób zmarłych;
   c. członków ich rodzin;
   d. świadków;
   e. właścicieli i użytkowników nieruchomości;
   f. uczestników zdarzeń drogowych;
   g. osób małoletnich.
3. Dokumentacja fotograficzna lub audiowizualna wykonana podczas zdarzenia nie może być traktowana jako materiał przeznaczony automatycznie do publikacji.
4. Przed wykorzystaniem materiału do celów informacyjnych należy ocenić, czy nie ujawnia on w szczególności:
   a. wizerunku osoby znajdującej się w sytuacji naruszającej jej prywatność lub godność;
   b. danych dotyczących zdrowia;
   c. dokumentów osobistych;
   d. danych widocznych na ekranach lub formularzach;
   e. informacji pozwalających ustalić szczegóły sytuacji osobistej osoby;

f. innych danych, których publiczne ujawnienie byłoby nieproporcjonalne.

5. Pierwszeństwo ma ochrona praw i godności osób, których dotyczy zdarzenie, przed interesem polegającym wyłącznie na atrakcyjności publikowanego materiału.

Rozdział XIV
Udostępnianie danych osobowych

§ 90. Ogólne zasady udostępniania danych

1. Dane osobowe mogą być udostępniane innemu podmiotowi wyłącznie w przypadku istnienia podstawy prawnej oraz w zakresie niezbędnym do realizacji określonego celu.
2. Przed udostępnieniem danych należy ustalić w szczególności:
    a. tożsamość lub status odbiorcy;
    b. cel żądania;
    c. podstawę prawną udostępnienia;
    d. zakres danych niezbędnych do realizacji celu;
    e. właściwy sposób przekazania danych;
    f. potrzebę udokumentowania udostępnienia.
3. Sam fakt zwrócenia się przez inny podmiot o przekazanie danych nie stanowi wystarczającej podstawy do ich udostępnienia.
4. W przypadku wątpliwości dotyczących zasadności żądania dane nie powinny być przekazywane do czasu wyjaśnienia podstawy i zakresu udostępnienia.
5. Dane przekazuje się w możliwie najmniejszym zakresie pozwalającym zrealizować zgodny z prawem cel.

§ 91. Weryfikacja wniosku o udostępnienie danych

1. Wniosek o udostępnienie danych powinien umożliwiać ustalenie:
    a. podmiotu występującego z wnioskiem;
    b. osoby działającej w jego imieniu, jeżeli ma to zastosowanie;
    c. celu żądania;
    d. podstawy prawnej;
    e. zakresu żądanych danych;
    f. osoby lub kategorii osób, których dane dotyczą.
2. Jeżeli wniosek jest nieprecyzyjny, obejmuje nadmierny zakres danych albo nie pozwala ustalić podstawy żądania, OSP może wystąpić o jego doprecyzowanie.
3. Weryfikacja żądania powinna być przeprowadzona przed udostępnieniem danych.
4. Nie należy przekazywać całych akt, baz danych lub Kart personalnych, jeżeli do realizacji celu wystarcza:
    a. określona informacja;
    b. zaświadczenie;
    c. wyciąg;
    d. kopia konkretnego dokumentu;
    e. ograniczone zestawienie danych.

§ 92. Udostępnianie danych organom i instytucjom publicznym

1. Dane osobowe mogą być udostępniane uprawnionym organom i instytucjom publicznym w zakresie wynikającym z przepisów prawa.

2. Dotyczy to w szczególności żądań pochodzących od:
    a. sądów;
    b. prokuratury;
    c. Policji;
    d. Państwowej Straży Pożarnej;
    e. organów administracji publicznej;
    f. organów podatkowych;
    g. organów kontroli;
    h. innych podmiotów posiadających ustawowe uprawnienie do uzyskania określonych danych.
3. Przed udostępnieniem danych należy zweryfikować zakres kompetencji podmiotu występującego z żądaniem, jeżeli nie wynika on jednoznacznie z treści wniosku lub przepisów prawa.
4. Nie należy rozszerzać zakresu odpowiedzi ponad zakres wynikający z podstawy prawnej i treści żądania.
5. Jeżeli charakter sprawy tego wymaga, fakt udostępnienia danych podlega odnotowaniu.

§ 93. Udostępnianie danych jednostkom ochrony przeciwpożarowej i podmiotom współpracującym

1. Przekazywanie danych Państwowej Straży Pożarnej, innym ochotniczym strażom pożarnym, właściwej gminie, Związkowi Ochotniczych Straży Pożarnych Rzeczypospolitej Polskiej lub innym podmiotom współpracującym z OSP następuje wyłącznie w zakresie właściwym dla określonego zadania.
2. Fakt współpracy pomiędzy podmiotami nie stanowi samodzielnej podstawy do swobodnej wymiany wszystkich posiadanych danych.
3. Każdorazowo należy określić:
    a. cel przekazania;
    b. podstawę prawną;
    c. zakres danych;
    d. role podmiotów uczestniczących w przetwarzaniu.
4. W przypadku cyklicznego przekazywania danych zasady takiego przekazywania powinny zostać odpowiednio udokumentowane.

§ 94. Udostępnianie danych wewnątrz OSP

1. Przekazanie danych pomiędzy członkami organów, osobami funkcyjnymi, komórkami organizacyjnymi lub użytkownikami CBDOSP stanowi operację przetwarzania i wymaga istnienia uzasadnionej potrzeby.
2. Członek Zarządu nie uzyskuje automatycznie dostępu do wszystkich danych wyłącznie z tytułu członkostwa w Zarządzie.
3. Członek Komisji Rewizyjnej uzyskuje dostęp do danych w zakresie niezbędnym do wykonywania konkretnych kompetencji kontrolnych.
4. Opiekun MDP uzyskuje dostęp do danych członków MDP wyłącznie w zakresie niezbędnym do wykonywania powierzonych zadań.
5. Kwatermistrz uzyskuje dostęp do danych członków w zakresie niezbędnym do:
    a. wydawania sprzętu;
    b. wydawania umundurowania;

c. prowadzenia ewidencji;
d. rozliczania zwrotów;
e. wykonywania innych powierzonych obowiązków gospodarczych.

6. Osoba posiadająca uprawnienie do określonego modułu CBDOSP nie może wykorzystywać dostępnych w nim informacji do celu niezwiązanego z powierzonymi obowiązkami.

§ 95. Sposób przekazywania danych

1. Dane osobowe przekazuje się w sposób odpowiedni do ich charakteru oraz poziomu ryzyka.
2. W zależności od okoliczności stosuje się w szczególności:
   a. osobiste przekazanie dokumentacji;
   b. przesyłkę rejestrowaną;
   c. służbową pocztę elektroniczną;
   d. odpowiednio zabezpieczony plik;
   e. system teleinformatyczny zapewniający właściwy poziom bezpieczeństwa;
   f. inny zatwierdzony sposób przekazania.
3. Przed wysłaniem danych należy zweryfikować odbiorcę.
4. W przypadku danych wymagających zwiększonej ochrony należy rozważyć zastosowanie:
   1. szyfrowania;
   2. zabezpieczenia pliku hasłem;
   3. odrębnego kanału przekazania hasła;
   4. ograniczenia czasu dostępności;
   5. potwierdzenia odbioru.
5. Zabezpieczenia dobiera się proporcjonalnie do ryzyka.

Rozdział XV
Powierzenie przetwarzania i współpraca z podmiotami zewnętrznymi

§ 96. Powierzenie przetwarzania danych

1. Jeżeli podmiot zewnętrzny przetwarza dane osobowe w imieniu OSP, należy ustalić, czy zachodzi powierzenie przetwarzania w rozumieniu art. 28 RODO.
2. Powierzenie przetwarzania wymaga odpowiedniego uregulowania stosunku pomiędzy OSP a podmiotem przetwarzającym.
3. Przed powierzeniem danych należy ocenić, czy podmiot zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych.
4. Powierzenie nie może prowadzić do obniżenia poziomu ochrony danych.
5. Podmiot przetwarzający może przetwarzać dane wyłącznie w zakresie wynikającym z udokumentowanych instrukcji Administratora, z zastrzeżeniem przypadków przewidzianych prawem.

§ 97. Umowa powierzenia przetwarzania

1. Umowa lub inny instrument prawny regulujący powierzenie powinien spełniać wymagania art. 28 RODO.
2. Powinien określać w szczególności:
   a. przedmiot przetwarzania;

b. czas trwania;
c. charakter przetwarzania;
d. cel przetwarzania;
e. rodzaj danych;
f. kategorie osób, których dane dotyczą;
g. prawa i obowiązki Administratora;
h. obowiązki podmiotu przetwarzającego.

3. Umowa powinna odpowiednio regulować:
   a. poufność;
   b. bezpieczeństwo;
   c. korzystanie z dalszych podmiotów przetwarzających;
   d. pomoc przy realizacji praw osób;
   e. pomoc w obsłudze naruszeń;
   f. zwrot lub usunięcie danych;
   g. możliwość wykazania zgodności;
   h. zasady audytu lub uzyskiwania informacji o stosowanych zabezpieczeniach.

§ 98. Usługi hostingowe i utrzymanie systemów

1. Korzystanie z hostingu, serwera, usługi kopii bezpieczeństwa, poczty elektronicznej albo innej usługi informatycznej wymaga ustalenia roli dostawcy względem przetwarzanych danych.
2. Przy wyborze dostawcy należy uwzględnić w szczególności:
   a. zakres przetwarzanych danych;
   b. miejsce ich przechowywania;
   c. stosowane zabezpieczenia;
   d. zasady wykonywania kopii bezpieczeństwa;
   e. możliwość korzystania z podwykonawców;
   f. procedury reagowania na incydenty;
   g. zasady zwrotu i usuwania danych po zakończeniu usługi.
3. Dostawca nie może otrzymywać szerszego dostępu do danych niż wynika to z charakteru świadczonej usługi.
4. Dostęp serwisowy do CBDOSP powinien być odpowiednio kontrolowany i ograniczony.

§ 99. Rejestr podmiotów przetwarzających

1. OSP prowadzi wykaz podmiotów, którym powierzono przetwarzanie danych, jeżeli takie podmioty występują.
2. Wykaz powinien umożliwiać ustalenie co najmniej:
   a. nazwy podmiotu;
   b. rodzaju świadczonej usługi;
   c. zakresu powierzonych danych;
   d. kategorii osób;
   e. daty rozpoczęcia współpracy;
   f. dokumentu regulującego powierzenie;
   g. informacji o zakończeniu powierzenia.
3. Wykaz powinien być aktualizowany w przypadku rozpoczęcia, zmiany lub zakończenia współpracy.

§ 100. Zakończenie współpracy z podmiotem zewnętrznym

1. Po zakończeniu współpracy należy ustalić sposób postępowania z danymi powierzonymi podmiotowi zewnętrznemu.
2. W zależności od obowiązujących ustaleń i przepisów dane powinny zostać:
    a. zwrócone;
    b. usunięte;
    c. odpowiednio zabezpieczone do czasu upływu obowiązku ich przechowywania.
3. OSP powinno w miarę potrzeby uzyskać potwierdzenie wykonania obowiązków dotyczących usunięcia lub zwrotu danych.
4. Należy również odebrać lub wyłączyć:
    a. konta;
    b. dostęp serwisowy;
    c. klucze API;
    d. inne środki technicznego dostępu – jeżeli były wykorzystywane podczas współpracy.

§ 101. Przekazywanie danych poza Europejski Obszar Gospodarczy

1. Przed wykorzystaniem usługi mogącej powodować przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej należy ustalić, czy transfer jest zgodny z rozdziałem V RODO.
2. Ocena powinna obejmować w szczególności:
    a. miejsce przetwarzania;
    b. podstawę transferu;
    c. zakres danych;
    d. charakter usługi;
    e. stosowane zabezpieczenia.
3. Niedopuszczalne jest wdrożenie usługi wyłącznie na podstawie jej popularności lub bezpłatnego charakteru bez oceny konsekwencji dla ochrony danych.
4. Postanowienia niniejszego paragrafu stosuje się odpowiednio do usług chmurowych, komunikacyjnych i innych usług internetowych.

Rozdział XVI
Prawa osób, których dane dotyczą

§ 102. Zasady realizacji praw osób

1. OSP zapewnia realizację praw osób, których dane dotyczą, zgodnie z RODO.
2. W zależności od podstawy i okoliczności przetwarzania osobie mogą przysługiwać w szczególności:
    a. prawo dostępu do danych;
    b. prawo sprostowania danych;
    c. prawo usunięcia danych;
    d. prawo ograniczenia przetwarzania;
    e. prawo do przenoszenia danych;
    f. prawo sprzeciwu;
    g. prawa związane ze zautomatyzowanym podejmowaniem decyzji, jeżeli taki proces występuje.

3. Zakres poszczególnych praw ustala się zgodnie z przesłankami i wyjątkami przewidzianymi w RODO.
4. OSP nie może zapewniać osobie prawa szerszego ani węższego niż wynikające z właściwych przepisów.

§ 103. Przyjmowanie żądań

1. Żądanie dotyczące realizacji praw może zostać złożone w sposób umożliwiający Administratorowi zapoznanie się z jego treścią.
2. Żądanie powinno zostać niezwłocznie przekazane osobie odpowiedzialnej za jego obsługę.
3. Osoba, która otrzymała żądanie, nie może:
    a. pozostawić go bez dalszego biegu;
    b. samodzielnie odmówić jego realizacji bez odpowiedniej analizy;
    c. usuwać danych objętych żądaniem w celu uniknięcia jego realizacji.
4. Datę otrzymania żądania należy ustalić w sposób umożliwiający kontrolę terminu odpowiedzi.

§ 104. Weryfikacja tożsamości wnioskodawcy

1. Przed udostępnieniem danych należy posiadać uzasadnioną pewność co do tożsamości osoby składającej żądanie.
2. W przypadku uzasadnionych wątpliwości można zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości.
3. Zakres danych wymaganych do weryfikacji nie może być nadmierny.
4. Nie należy rutynowo żądać kopii dokumentu tożsamości, jeżeli tożsamość można skutecznie potwierdzić w mniej ingerujący sposób.
5. Dane pozyskane wyłącznie w celu weryfikacji tożsamości nie powinny być wykorzystywane do innych celów.

§ 105. Prawo dostępu do danych

1. Osoba może żądać potwierdzenia, czy dotyczące jej dane są przetwarzane, oraz uzyskać informacje i kopię danych w zakresie wynikającym z RODO.
2. Przy realizacji prawa dostępu należy chronić prawa i wolności innych osób.
3. Przed przekazaniem kopii dokumentacji należy zweryfikować, czy zawiera ona dane:
    a. innych członków;
    b. małoletnich;
    c. świadków;
    d. kontrahentów;
    e. innych osób trzecich.
4. Jeżeli jest to niezbędne, dane osób trzecich powinny zostać odpowiednio ograniczone lub zanonimizowane.
5. Prawo dostępu nie oznacza automatycznego prawa do otrzymania kopii każdego dokumentu w niezmienionej postaci, jeżeli informacje wymagane prawem można prawidłowo przekazać w inny sposób.

§ 106. Sprostowanie, usunięcie i ograniczenie przetwarzania

1. Żądanie sprostowania danych podlega weryfikacji pod kątem prawidłowości informacji.
2. Dane nieprawidłowe powinny zostać sprostowane bez zbędnej zwłoki, jeżeli zachodzą ku temu przesłanki.
3. Żądanie usunięcia danych wymaga ustalenia, czy nie istnieje podstawa ich dalszego przechowywania.
4. Dane nie podlegają usunięciu wyłącznie dlatego, że osoba tego żąda, jeżeli obowiązek lub prawo dalszego przetwarzania wynika z właściwych przepisów lub przesłanek RODO.
5. Jeżeli zachodzą przesłanki ograniczenia przetwarzania, należy zastosować odpowiednie rozwiązanie organizacyjne lub techniczne zapobiegające wykonywaniu niedopuszczalnych operacji na danych.
6. W CBDOSP ograniczenie przetwarzania może być realizowane odpowiednio przez:
    a. oznaczenie rekordu;
    b. ograniczenie uprawnień;
    c. przeniesienie danych do obszaru o ograniczonym dostępie;
    d. inne rozwiązanie zapewniające skuteczne ograniczenie.

§ 107. Terminy realizacji żądań

1. Żądania osób realizuje się bez zbędnej zwłoki, z zachowaniem terminów określonych w art. 12 RODO.
2. Bieg terminu powinien być monitorowany od chwili otrzymania żądania.
3. Jeżeli z uwagi na skomplikowany charakter żądania lub liczbę żądań konieczne jest przedłużenie terminu, osoba powinna zostać poinformowana zgodnie z RODO.
4. Informacja o przedłużeniu powinna zawierać przyczyny opóźnienia.
5. Obsługa żądania powinna zostać odpowiednio udokumentowana.

§ 108. Rejestr żądań osób

1. OSP prowadzi rejestr żądań dotyczących realizacji praw osób, jeżeli jest to uzasadnione potrzebą zapewnienia rozliczalności.
2. Rejestr może obejmować:
    a. numer sprawy;
    b. datę wpływu;
    c. rodzaj żądania;
    d. sposób weryfikacji tożsamości;
    e. osobę odpowiedzialną za obsługę;
    f. datę odpowiedzi;
    g. sposób rozstrzygnięcia;
    h. informację o przedłużeniu terminu;
    i. inne informacje niezbędne do wykazania prawidłowej obsługi.
3. Rejestr nie powinien zawierać pełnych kopii dokumentacji, jeżeli do wykazania sposobu realizacji żądania wystarczają informacje ewidencyjne.

Rozdział XVII
Obowiązek informacyjny

§ 109. Realizacja obowiązku informacyjnego

1. OSP realizuje obowiązki informacyjne wynikające z art. 13 i 14 RODO w przypadkach, w których przepisy te mają zastosowanie.
2. Informacje przekazuje się w sposób:
    a. zwięzły;
    b. przejrzysty;
    c. zrozumiały;
    d. łatwo dostępny;
    e. napisany jasnym i prostym językiem.
3. Szczególną uwagę należy zwrócić na sposób przekazywania informacji małoletnim.
4. Klauzule informacyjne powinny odpowiadać rzeczywistemu procesowi przetwarzania i nie mogą być stosowane mechanicznie do wszystkich procesów.

§ 110. Treść klauzul informacyjnych

1. Klauzula informacyjna powinna zawierać informacje wymagane odpowiednio przez art. 13 albo art. 14 RODO.
2. Przy opracowaniu klauzuli należy w szczególności prawidłowo ustalić:
    a. tożsamość Administratora;
    b. dane kontaktowe;
    c. cele przetwarzania;
    d. podstawy prawne;
    e. odbiorców lub kategorie odbiorców;
    f. informacje dotyczące ewentualnych transferów poza Europejski Obszar Gospodarczy;
    g. okres przechowywania albo kryteria jego ustalania;
    h. prawa osoby;
    i. prawo wniesienia skargi do organu nadzorczego;
    j. źródło danych, jeżeli dane nie zostały pozyskane od osoby;
    k. informacje dotyczące zautomatyzowanego podejmowania decyzji, jeżeli ma ono zastosowanie.
3. Klauzula nie powinna wskazywać podstaw prawnych, które w rzeczywistości nie mają zastosowania do danego procesu.
4. Zmiana procesu przetwarzania wymaga oceny aktualności właściwej klauzuli informacyjnej.

§ 111. Klauzule informacyjne stosowane przez OSP

1. OSP może stosować odrębne klauzule informacyjne w szczególności dla:
    a. członków OSP;
    b. kandydatów na członków;
    c. byłych członków;
    d. członków MDP;
    e. rodziców i opiekunów prawnych;
    f. kontrahentów;
    g. darczyńców;

h. uczestników wydarzeń;
i. osób kontaktujących się z OSP;
j. osób składających korespondencję;
k. osób korzystających z serwisów internetowych OSP;
l. innych kategorii osób, jeżeli charakter procesu tego wymaga.

2. Dopuszczalne jest stosowanie warstwowych klauzul informacyjnych, jeżeli zapewniają osobie łatwy dostęp do pełnego zakresu wymaganych informacji.
3. Aktualne wzory klauzul powinny być przechowywane w sposób umożliwiający ich stosowanie przez osoby odpowiedzialne za dany proces.

§ 112. Dokumentowanie spełnienia obowiązku informacyjnego

1. OSP powinno być w stanie wykazać, że obowiązek informacyjny został prawidłowo zrealizowany.
2. W zależności od procesu może to nastąpić w szczególności przez:
   a. podpis na formularzu;
   b. potwierdzenie elektroniczne;
   c. zapis w systemie;
   d. udokumentowanie przekazania klauzuli;
   e. opublikowanie informacji w odpowiednim miejscu, jeżeli taki sposób jest zgodny z prawem;
   f. zastosowanie innego rozliczalnego mechanizmu.
3. Potwierdzenie zapoznania się z klauzulą informacyjną nie jest zgodą na przetwarzanie danych.
4. Klauzula informacyjna nie powinna zawierać sformułowania sugerującego, że osoba „wyraża zgodę na RODO" albo wyraża zgodę na przetwarzanie, jeżeli podstawą procesu nie jest zgoda.

Rozdział XVIII
Incydenty i naruszenia ochrony danych osobowych

§ 113. Obowiązek zgłaszania incydentów

1. Każda osoba przetwarzająca dane osobowe w związku z działalnością OSP jest obowiązana niezwłocznie zgłosić zdarzenie, które:
   a. spowodowało naruszenie ochrony danych;
   b. mogło spowodować naruszenie ochrony danych;
   c. wskazuje na możliwość nieuprawnionego dostępu do danych;
   d. może prowadzić do utraty poufności, integralności lub dostępności danych.
2. Obowiązek zgłoszenia istnieje również wtedy, gdy osoba zgłaszająca:
   a. nie zna pełnego zakresu zdarzenia;
   b. nie jest pewna, czy doszło do naruszenia;
   c. samodzielnie usunęła bezpośrednią przyczynę zdarzenia;
   d. uważa, że zdarzenie nie spowodowało szkody.
3. Osoba zgłaszająca nie powinna samodzielnie przesądzać, czy zdarzenie wymaga zgłoszenia organowi nadzorczemu.
4. Zgłoszenie wewnętrzne powinno nastąpić bez zbędnej zwłoki po stwierdzeniu zdarzenia.

§ 114. Zdarzenia wymagające zgłoszenia wewnętrznego

1. Zgłoszeniu podlegają w szczególności:
    a. wysłanie wiadomości do niewłaściwego odbiorcy;
    b. wysłanie niewłaściwego załącznika;
    c. ujawnienie adresów poczty elektronicznej nieuprawnionym odbiorcom;
    d. utrata dokumentacji;
    e. utrata telefonu, komputera albo nośnika zawierającego dane;
    f. kradzież urządzenia;
    g. nieuprawnione wejście do CBDOSP;
    h. podejrzenie przejęcia konta;
    i. ujawnienie hasła;
    j. dostęp użytkownika do danych wykraczających poza jego uprawnienia;
    k. nieuprawniony eksport danych;
    l. przypadkowe usunięcie danych;
    m. zniszczenie dokumentacji przed upływem właściwego okresu;
    n. opublikowanie danych w Internecie bez właściwej podstawy;
    o. nieuprawnione ujawnienie danych członka MDP;
    p. pozostawienie dokumentów w miejscu dostępnym dla osób nieuprawnionych;
    q. przekazanie dokumentacji niewłaściwej osobie;
    r. działanie złośliwego oprogramowania mogące mieć wpływ na dane;
    s. inne zdarzenie mogące naruszyć bezpieczeństwo danych.
2. Katalog określony w ust. 1 ma charakter otwarty.

§ 115. Treść zgłoszenia incydentu

1. Zgłoszenie powinno, w miarę dostępnych informacji, zawierać:
    a. datę i godzinę stwierdzenia zdarzenia;
    b. datę i godzinę jego wystąpienia, jeżeli jest znana;
    c. opis zdarzenia;
    d. miejsce wystąpienia;
    e. system, dokument lub urządzenie, którego dotyczy zdarzenie;
    f. kategorie danych;
    g. kategorie osób, których dane dotyczą;
    h. przybliżoną liczbę osób;
    i. informację o możliwych odbiorcach danych;
    j. działania podjęte bezpośrednio po stwierdzeniu zdarzenia.
2. Brak części informacji nie może powodować opóźnienia zgłoszenia.
3. Informacje uzupełniające przekazuje się po ich ustaleniu.

§ 116. Natychmiastowe działania zabezpieczające

1. Po stwierdzeniu incydentu należy, w zakresie możliwym i bezpiecznym, podjąć działania ograniczające jego skutki.
2. Działania mogą obejmować w szczególności:
    a. zmianę hasła;
    b. zablokowanie konta;
    c. zakończenie aktywnych sesji;
    d. odebranie błędnie przesłanej wiadomości, jeżeli jest to technicznie możliwe;

e. zwrócenie się do nieuprawnionego odbiorcy o usunięcie danych;
f. odłączenie zagrożonego urządzenia od sieci;
g. zabezpieczenie dokumentacji;
h. cofnięcie błędnie nadanych uprawnień;
i. ograniczenie dostępu do określonego modułu;
j. wykonanie zabezpieczającej kopii informacji technicznych niezbędnych do wyjaśnienia zdarzenia.

3. Działania nie mogą prowadzić do nieuzasadnionego zniszczenia dowodów potrzebnych do wyjaśnienia zdarzenia.

§ 117. Zabezpieczenie informacji o incydencie

1. Informacje niezbędne do ustalenia przebiegu incydentu powinny zostać zabezpieczone.
2. Zabezpieczeniu mogą podlegać w szczególności:
   a. logi systemowe;
   b. historia logowania;
   c. historia zmian uprawnień;
   d. kopie wiadomości;
   e. informacje o przesłanych załącznikach;
   f. dokumentacja papierowa;
   g. dane dotyczące urządzeń;
   h. informacje od użytkowników;
   i. inne materiały pozwalające ustalić przebieg zdarzenia.
3. Dostęp do dokumentacji incydentu powinien być ograniczony do osób uczestniczących w jego wyjaśnianiu.
4. Dokumentacji incydentu nie należy modyfikować w sposób uniemożliwiający ustalenie rzeczywistego przebiegu zdarzenia.

§ 118. Ocena zdarzenia

1. Każde zgłoszone zdarzenie podlega ocenie w celu ustalenia, czy stanowi naruszenie ochrony danych osobowych.
2. W ramach oceny ustala się w szczególności:
   a. czy doszło do naruszenia bezpieczeństwa;
   b. czy zdarzenie dotyczy danych osobowych;
   c. czy doszło do naruszenia poufności;
   d. czy doszło do naruszenia integralności;
   e. czy doszło do naruszenia dostępności;
   f. jakie osoby i dane zostały objęte zdarzeniem;
   g. jakie mogą być jego konsekwencje.
3. Fakt, że dane zostały odzyskane albo nieuprawniony odbiorca zadeklarował ich usunięcie, nie powoduje automatycznie, że zdarzenie przestaje być naruszeniem.
4. Wynik oceny powinien zostać udokumentowany.

§ 119. Ocena ryzyka naruszenia praw i wolności osób

1. W przypadku stwierdzenia naruszenia dokonuje się oceny ryzyka dla praw i wolności osób fizycznych.

2. Przy ocenie uwzględnia się w szczególności:
    a. rodzaj naruszenia;
    b. charakter danych;
    c. zakres danych;
    d. liczbę osób;
    e. możliwość identyfikacji osób;
    f. szczególne kategorie danych;
    g. dane małoletnich;
    h. możliwe konsekwencje finansowe;
    i. możliwość kradzieży tożsamości;
    j. możliwość dyskryminacji;
    k. możliwość naruszenia dobrego imienia lub prywatności;
    l. charakter odbiorcy danych;
    m. zastosowane zabezpieczenia;
    n. możliwość skutecznego ograniczenia skutków.
3. Ocena nie może ograniczać się wyłącznie do liczby osób objętych naruszeniem.
4. Naruszenie dotyczące jednej osoby może powodować wysokie ryzyko, jeżeli charakter danych lub możliwe konsekwencje są szczególnie poważne.

§ 120. Zgłoszenie naruszenia organowi nadzorczemu

1. Jeżeli naruszenie może powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator dokonuje zgłoszenia właściwemu organowi nadzorczemu zgodnie z art. 33 RODO.
2. Zgłoszenia dokonuje się bez zbędnej zwłoki, a w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia przez Administratora.
3. Jeżeli zgłoszenie następuje po upływie 72 godzin, dołącza się wyjaśnienie przyczyn opóźnienia.
4. Decyzja o dokonaniu albo niedokonaniu zgłoszenia powinna zostać udokumentowana.
5. Osoba, która spowodowała albo wykryła naruszenie, nie podejmuje samodzielnie decyzji o zgłoszeniu go organowi nadzorczemu, chyba że posiada wyraźne umocowanie do działania w imieniu Administratora.

§ 121. Treść zgłoszenia do organu nadzorczego

1. Zgłoszenie powinno zawierać informacje wymagane przez art. 33 RODO.
2. W szczególności należy:
    a. opisać charakter naruszenia;
    b. wskazać, w miarę możliwości, kategorie i przybliżoną liczbę osób;
    c. wskazać, w miarę możliwości, kategorie i przybliżoną liczbę rekordów danych;
    d. wskazać dane kontaktowe osoby, od której można uzyskać więcej informacji;
    e. opisać możliwe konsekwencje naruszenia;
    f. opisać środki zastosowane lub proponowane w celu zaradzenia naruszeniu i ograniczenia jego skutków.
3. Jeżeli wszystkich informacji nie można udzielić jednocześnie, mogą być one przekazywane sukcesywnie, bez dalszej nieuzasadnionej zwłoki, zgodnie z RODO.

§ 122. Zawiadomienie osoby o naruszeniu

1. Jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osoby fizycznej, Administrator zawiadamia tę osobę bez zbędnej zwłoki, chyba że zachodzi wyjątek przewidziany w art. 34 RODO.
2. Zawiadomienie powinno być sformułowane jasnym i prostym językiem.
3. Zawiadomienie powinno zawierać co najmniej informacje wymagane przez RODO, w tym:
    a. opis charakteru naruszenia;
    b. dane kontaktowe umożliwiające uzyskanie dalszych informacji;
    c. opis możliwych konsekwencji;
    d. opis środków zastosowanych lub proponowanych w celu ograniczenia skutków.
4. Przy formułowaniu zawiadomienia należy, jeżeli jest to zasadne, wskazać działania, które osoba może podjąć w celu ograniczenia własnego ryzyka.

§ 123. Rejestr naruszeń ochrony danych

1. OSP prowadzi rejestr naruszeń ochrony danych osobowych.
2. W rejestrze dokumentuje się wszystkie stwierdzone naruszenia, niezależnie od tego, czy zostały zgłoszone organowi nadzorczemu.
3. Rejestr powinien umożliwiać ustalenie w szczególności:
    a. numeru zdarzenia;
    b. daty wystąpienia;
    c. daty stwierdzenia;
    d. charakteru naruszenia;
    e. kategorii danych;
    f. kategorii osób;
    g. możliwych konsekwencji;
    h. przeprowadzonej oceny ryzyka;
    i. podjętych środków;
    j. informacji o zgłoszeniu organowi nadzorczemu;
    k. informacji o zawiadomieniu osób;
    l. sposobu zakończenia sprawy.
4. Dokumentacja powinna umożliwiać organowi nadzorczemu zweryfikowanie przestrzegania wymagań dotyczących naruszeń.

§ 124. Analiza przyczyn i działania naprawcze

1. Po opanowaniu naruszenia dokonuje się, w zakresie odpowiednim do charakteru zdarzenia, analizy jego przyczyn.
2. Analiza powinna służyć ustaleniu:
    a. bezpośredniej przyczyny zdarzenia;
    b. przyczyn organizacyjnych;
    c. ewentualnych braków technicznych;
    d. ewentualnych braków proceduralnych;
    e. potrzeby dodatkowego szkolenia;
    f. potrzeby zmiany zakresu uprawnień;
    g. potrzeby zmiany systemu lub procedury.

3. Działania naprawcze mogą obejmować w szczególności:
    a. zmianę konfiguracji systemu;
    b. zmianę procedury;
    c. ograniczenie uprawnień;
    d. aktualizację oprogramowania;
    e. dodatkowe zabezpieczenia;
    f. szkolenie;
    g. zmianę organizacji pracy;
    h. aktualizację analizy ryzyka.
4. Zamknięcie incydentu nie powinno następować przed ustaleniem, czy wymagane są działania zapobiegające jego ponownemu wystąpieniu.

Rozdział XIX
Zarządzanie ryzykiem dla ochrony danych osobowych

§ 125. Obowiązek zarządzania ryzykiem

1. OSP stosuje podejście oparte na ryzyku przy doborze środków ochrony danych osobowych.
2. Analiza ryzyka służy ustaleniu odpowiednich środków technicznych i organizacyjnych.
3. Analiza uwzględnia ryzyko dla praw i wolności osób fizycznych, a nie wyłącznie ryzyko organizacyjne dla OSP.
4. Poziom zabezpieczeń powinien odpowiadać charakterowi, zakresowi, kontekstowi i celom przetwarzania.

§ 126. Przeprowadzanie analizy ryzyka

1. Analizę ryzyka przeprowadza się:
    a. okresowo;
    b. przed wdrożeniem istotnego nowego procesu;
    c. przed wdrożeniem rozwiązania technologicznego mogącego istotnie wpływać na ochronę danych;
    d. po poważnym naruszeniu;
    e. po istotnej zmianie sposobu przetwarzania;
    f. w przypadku stwierdzenia nowych zagrożeń.
2. Analiza powinna obejmować w szczególności:
    a. proces;
    b. kategorie osób;
    c. kategorie danych;
    d. wykorzystywane systemy;
    e. źródła zagrożeń;
    f. istniejące zabezpieczenia;
    g. prawdopodobieństwo wystąpienia zdarzenia;
    h. możliwe konsekwencje;
    i. poziom ryzyka;
    j. wymagane działania.
3. Analiza powinna być dokumentowana w sposób pozwalający ustalić podstawowe założenia dokonanej oceny.

§ 127. Identyfikacja zagrożeń

1. W analizie ryzyka uwzględnia się zagrożenia związane z działaniem człowieka, technologią, organizacją pracy i zdarzeniami zewnętrznymi.
2. Uwzględnia się w szczególności:
    a. błąd użytkownika;
    b. niewłaściwe nadanie uprawnień;
    c. utratę dokumentu;
    d. utratę urządzenia;
    e. kradzież;
    f. ujawnienie hasła;
    g. phishing;
    h. złośliwe oprogramowanie;
    i. nieuprawniony dostęp;
    j. awarię sprzętu;
    k. awarię serwera;
    l. uszkodzenie bazy danych;
    m. błędną aktualizację;
    n. utratę kopii bezpieczeństwa;
    o. nieuprawnione usunięcie danych;
    p. nieuprawnioną publikację;
    q. niewłaściwe brakowanie dokumentacji;
    r. niewłaściwe działanie podmiotu przetwarzającego;
    s. zagrożenia wynikające z pracy poza siedzibą.
3. Katalog zagrożeń powinien być aktualizowany wraz ze zmianą sposobu działania OSP.

§ 128. Postępowanie z ryzykiem

1. Po ustaleniu poziomu ryzyka określa się sposób postępowania.
2. Działania mogą polegać w szczególności na:
    a. zmniejszeniu ryzyka przez wdrożenie zabezpieczeń;
    b. zmianie procesu;
    c. ograniczeniu zakresu danych;
    d. ograniczeniu liczby osób posiadających dostęp;
    e. skróceniu okresu przechowywania;
    f. zastosowaniu pseudonimizacji;
    g. zastosowaniu szyfrowania;
    h. rezygnacji z określonego sposobu przetwarzania, jeżeli ryzyka nie można odpowiednio ograniczyć.
3. Akceptacja ryzyka powinna następować świadomie i na odpowiednim poziomie organizacyjnym.
4. Nie można uznawać wysokiego ryzyka za zaakceptowane wyłącznie dlatego, że usunięcie jego przyczyny jest organizacyjnie niewygodne.

§ 129. Ocena skutków dla ochrony danych

1. Jeżeli dany rodzaj przetwarzania, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przed rozpoczęciem

przetwarzania przeprowadza się ocenę skutków dla ochrony danych zgodnie z art. 35 RODO.

2. Przy ustalaniu obowiązku przeprowadzenia oceny uwzględnia się:
    a. charakter procesu;
    b. skalę przetwarzania;
    c. zakres danych;
    d. szczególne kategorie danych;
    e. dane małoletnich;
    f. stosowanie nowych technologii;
    g. możliwość systematycznego monitorowania osób;
    h. inne czynniki zwiększające ryzyko.
3. Oceny nie przeprowadza się mechanicznie dla każdego procesu, lecz w przypadkach wynikających z RODO i przeprowadzonej analizy.

§ 130. Treść i wynik oceny skutków

1. Ocena skutków powinna zawierać elementy wymagane przez art. 35 RODO, w szczególności:
    a. systematyczny opis planowanych operacji przetwarzania;
    b. cele przetwarzania;
    c. ocenę niezbędności i proporcjonalności;
    d. ocenę ryzyka dla praw i wolności osób;
    e. środki planowane w celu zaradzenia ryzyku;
    f. zabezpieczenia i mechanizmy mające zapewnić ochronę danych.
2. Jeżeli w wyniku oceny stwierdzono ryzyko wymagające dodatkowych środków, proces nie powinien zostać wdrożony bez podjęcia odpowiednich działań.
3. Jeżeli mimo planowanych zabezpieczeń przetwarzanie powodowałoby wysokie ryzyko, którego Administrator nie może ograniczyć odpowiednimi środkami, należy rozważyć obowiązek uprzednich konsultacji z organem nadzorczym zgodnie z art. 36 RODO.
4. Ocena skutków podlega ponownemu przeglądowi, jeżeli zmienia się ryzyko związane z danym procesem.

Rozdział XX
Bezpieczeństwo fizyczne i teleinformatyczne

§ 131. Zabezpieczenie pomieszczeń i dokumentacji

1. Pomieszczenia, w których przetwarzane są dane osobowe, zabezpiecza się odpowiednio do rodzaju dokumentacji, zakresu danych oraz ryzyka związanego z dostępem osób nieuprawnionych.
2. Dokumentacja papierowa zawierająca dane osobowe powinna być przechowywana w sposób ograniczający dostęp osób nieuprawnionych.
3. Dokumentacja wymagająca zwiększonej ochrony powinna być przechowywana w zamykanych szafach, pomieszczeniach lub innych odpowiednio zabezpieczonych miejscach.
4. Klucze oraz inne środki dostępu do miejsc przechowywania dokumentacji mogą być powierzane wyłącznie osobom posiadającym uzasadnioną potrzebę dostępu.

5. Zabrania się pozostawiania dokumentacji:
    a. na ogólnodostępnych stołach;
    b. w pomieszczeniach dostępnych dla osób postronnych;
    c. w niezabezpieczonych pojazdach;
    d. w miejscach umożliwiających swobodne fotografowanie lub kopiowanie;
    e. w innych miejscach stwarzających nieuzasadnione ryzyko ujawnienia.
6. Po zakończeniu pracy dokumentacja powinna zostać umieszczona w miejscu przeznaczonym do jej bezpiecznego przechowywania.

§ 132. Zabezpieczenie komputerów i urządzeń

1. Komputery, telefony, tablety oraz inne urządzenia wykorzystywane do przetwarzania danych OSP powinny posiadać zabezpieczenia odpowiednie do zakresu przetwarzanych informacji.
2. Stosuje się w szczególności:
    a. zabezpieczenie dostępu do urządzenia;
    b. aktualizacje systemu i oprogramowania;
    c. ochronę przed złośliwym oprogramowaniem – odpowiednio do rodzaju urządzenia i ryzyka;
    d. automatyczne blokowanie ekranu po okresie bezczynności, jeżeli jest dostępne;
    e. ograniczenie instalowania nieautoryzowanego oprogramowania;
    f. inne środki wynikające z analizy ryzyka.
3. Użytkownik nie może wyłączać zabezpieczeń urządzenia bez uzasadnionej potrzeby i właściwego uprawnienia.
4. Urządzenia posiadające dostęp do CBDOSP powinny być chronione przed użyciem przez osoby nieuprawnione.
5. W przypadku utraty urządzenia posiadającego dostęp do danych OSP użytkownik jest obowiązany niezwłocznie zgłosić zdarzenie zgodnie z procedurą obsługi incydentów.

§ 133. Hasła i inne dane uwierzytelniające

1. Hasła, kody dostępu, klucze uwierzytelniające oraz inne dane umożliwiające dostęp do systemów OSP mają charakter poufny.
2. Zabrania się:
    a. przekazywania własnego hasła innej osobie;
    b. żądania od innego użytkownika podania jego hasła;
    c. przechowywania hasła w miejscu ogólnodostępnym;
    d. przesyłania hasła otwartym kanałem, jeżeli można zastosować bezpieczniejszy sposób;
    e. używania danych uwierzytelniających innej osoby.
3. Hasło powinno posiadać poziom złożoności odpowiedni do chronionego zasobu i aktualnego ryzyka.
4. W przypadku podejrzenia ujawnienia hasła należy niezwłocznie:
    a. zmienić hasło;
    b. zgłosić zdarzenie, jeżeli mogło dojść do nieuprawnionego dostępu;
    c. zweryfikować aktywne sesje, jeżeli system posiada taką możliwość.

5. Dla kont o podwyższonych uprawnieniach stosuje się, jeżeli jest to technicznie możliwe i adekwatne do ryzyka, dodatkowe mechanizmy uwierzytelniania.

§ 134. Nośniki danych

1. Nośniki zawierające dane osobowe powinny być wykorzystywane wyłącznie w uzasadnionych przypadkach.
2. Do nośników zalicza się w szczególności:
    a. pamięci USB;
    b. dyski zewnętrzne;
    c. karty pamięci;
    d. płyty optyczne;
    e. inne urządzenia umożliwiające zapis danych.
3. Przy korzystaniu z nośnika należy:
    a. ograniczyć zakres zapisanych danych;
    b. zabezpieczyć nośnik przed utratą;
    c. ograniczyć dostęp osób nieuprawnionych;
    d. stosować szyfrowanie, jeżeli wynika to z poziomu ryzyka;
    e. usunąć dane po ustaniu potrzeby ich przechowywania.
4. Nieznany nośnik nie powinien być podłączany do urządzenia wykorzystywanego do przetwarzania danych OSP bez oceny bezpieczeństwa.
5. Nośnik przeznaczony do likwidacji powinien zostać wyczyszczony lub fizycznie zniszczony w sposób uniemożliwiający odtworzenie danych.

§ 135. Praca poza siedzibą OSP

1. Przetwarzanie danych poza siedzibą OSP jest dopuszczalne wyłącznie w zakresie uzasadnionym wykonywanym zadaniem.
2. Osoba przetwarzająca dane poza siedzibą powinna w szczególności:
    a. chronić ekran przed wglądem osób postronnych;
    b. chronić dokumenty papierowe;
    c. nie pozostawiać urządzeń i dokumentów bez nadzoru;
    d. korzystać z bezpiecznych sposobów dostępu do systemów;
    e. ograniczać tworzenie lokalnych kopii;
    f. zwrócić dokumentację po zakończeniu zadania.
3. Szczególnej ostrożności wymaga przetwarzanie danych:
    a. w pojeździe;
    b. podczas wyjazdu;
    c. podczas zawodów;
    d. podczas ćwiczeń;
    e. podczas zbiórek MDP;
    f. podczas wydarzeń publicznych;
    g. w miejscu zamieszkania użytkownika.
4. Dokumentacja OSP nie powinna być przechowywana w miejscu zamieszkania użytkownika dłużej, niż jest to rzeczywiście konieczne do wykonania konkretnego zadania.

§ 136. Prywatne urządzenia użytkowników

1. Przetwarzanie danych OSP na prywatnym urządzeniu może następować wyłącznie w zakresie dopuszczonym przez zasady organizacyjne OSP i przy zapewnieniu odpowiedniego poziomu bezpieczeństwa.
2. W przypadku dopuszczenia prywatnego urządzenia użytkownik jest obowiązany zapewnić w szczególności:
    a. zabezpieczenie dostępu do urządzenia;
    b. aktualność oprogramowania;
    c. ochronę przed dostępem innych użytkowników urządzenia;
    d. usuwanie lokalnych kopii danych po ustaniu potrzeby ich wykorzystania;
    e. zgłoszenie utraty lub przejęcia urządzenia, jeżeli mogło ono umożliwiać dostęp do danych OSP.
3. Zabrania się przechowywania trwałych kopii baz danych CBDOSP na prywatnych urządzeniach bez wyraźnie uzasadnionej i zatwierdzonej potrzeby.
4. Korzystanie z prywatnego urządzenia nie zwalnia użytkownika z obowiązków wynikających z niniejszej Polityki.

Rozdział XXI
Retencja, archiwizacja, brakowanie i niszczenie danych

§ 137. Ustalanie okresów przechowywania

1. Dane osobowe przechowuje się przez okres nie dłuższy, niż jest to niezbędne dla celów, dla których są przetwarzane, chyba że dalsze przechowywanie wynika z przepisów prawa lub istnieje inna właściwa podstawa.
2. Przy ustalaniu okresu przechowywania uwzględnia się w szczególności:
    a. przepisy prawa;
    b. cel przetwarzania;
    c. rodzaj dokumentacji;
    d. instrukcję kancelaryjną;
    e. właściwy rzeczowy wykaz akt, jeżeli znajduje zastosowanie;
    f. obowiązki rachunkowe i podatkowe;
    g. terminy przedawnienia roszczeń;
    h. uzasadnione potrzeby archiwalne;
    i. prawa i wolności osób.
3. Niedopuszczalne jest przyjmowanie zasady bezterminowego przechowywania wszystkich danych wyłącznie z powodu technicznej możliwości ich zachowania.
4. Okresy retencji powinny być możliwe do ustalenia dla podstawowych kategorii dokumentacji.

§ 138. Przegląd danych i dokumentacji

1. Dokumentacja powinna podlegać okresowemu przeglądowi pod kątem dalszej zasadności przechowywania.
2. Przegląd obejmuje w szczególności:
    a. dokumentację papierową;
    b. dane w CBDOSP;
    c. załączniki elektroniczne;
    d. eksporty danych;

e. dokumenty robocze;
f. nośniki danych;
g. dokumentację byłych członków;
h. dokumentację zakończonych spraw.

3. W wyniku przeglądu dokumentacja może zostać:
   a. pozostawiona do dalszego przechowywania;
   b. przekazana do archiwum;
   c. zanonimizowana;
   d. przeznaczona do brakowania;
   e. usunięta lub zniszczona zgodnie z właściwą procedurą.
4. Przegląd powinien uwzględniać zakaz niszczenia dokumentacji, która jest potrzebna w związku z trwającym postępowaniem, kontrolą, sporem lub obowiązkiem prawnym.

§ 139. Archiwizacja dokumentacji

1. Dokumentacja przeznaczona do dalszego przechowywania podlega archiwizacji zgodnie z zasadami obowiązującymi w OSP.
2. Archiwizacja powinna zapewniać:
   a. możliwość identyfikacji dokumentacji;
   b. zachowanie integralności;
   c. ochronę przed utratą;
   d. ochronę przed nieuprawnionym dostępem;
   e. możliwość odnalezienia dokumentu;
   f. kontrolę okresu przechowywania.
3. Przekazanie dokumentacji do archiwum nie oznacza, że może ona być przechowywana bezterminowo.
4. Dostęp do dokumentacji archiwalnej powinien odpowiadać jej charakterowi oraz aktualnej potrzebie dostępu.

§ 140. Brakowanie dokumentacji

1. Dokumentacja, której okres przechowywania upłynął i która nie posiada podstawy dalszego przechowywania, podlega brakowaniu zgodnie z właściwą procedurą.
2. Brakowanie powinno być przeprowadzone w sposób uporządkowany i rozliczalny.
3. Przed zatwierdzeniem brakowania należy ustalić, czy dokumentacja:
   a. nie podlega dalszemu obowiązkowi przechowywania;
   b. nie jest potrzebna w związku z postępowaniem;
   c. nie jest objęta kontrolą;
   d. nie posiada uzasadnionej wartości archiwalnej;
   e. nie jest potrzebna do ustalenia, dochodzenia lub obrony roszczeń.
4. Z brakowania może zostać sporządzony protokół określający co najmniej zakres dokumentacji oraz sposób jej zniszczenia lub usunięcia.
5. Jeżeli brakowanie jest prowadzone za pośrednictwem CBDOSP, system powinien zapewniać odpowiednią rozliczalność tej operacji.

§ 141. Niszczenie dokumentacji papierowej i elektronicznej

1. Dokumentację papierową zawierającą dane osobowe niszczy się w sposób uniemożliwiający lub odpowiednio utrudniający odtworzenie zawartych w niej informacji.
2. Dokumentów zawierających dane osobowe nie należy wyrzucać w stanie czytelnym do ogólnodostępnych pojemników na odpady.
3. Dane elektroniczne usuwa się z uwzględnieniem:
    a. rodzaju nośnika;
    b. możliwości odtworzenia danych;
    c. charakteru informacji;
    d. dostępnych metod bezpiecznego usuwania.
4. W przypadku przekazania niszczenia dokumentacji podmiotowi zewnętrznemu należy odpowiednio uregulować zasady postępowania z danymi i zweryfikować sposób realizacji usługi.

Rozdział XXII
Szkolenia, nadzór i kontrola przestrzegania Polityki

§ 142. Szkolenia z zakresu ochrony danych

1. Osoby przetwarzające dane powinny posiadać wiedzę odpowiednią do zakresu wykonywanych zadań.
2. Szkolenie lub instruktaż przeprowadza się w szczególności:
    a. przed rozpoczęciem wykonywania zadań wymagających dostępu do danych;
    b. po istotnej zmianie przepisów lub procedur;
    c. po wdrożeniu istotnych nowych funkcjonalności;
    d. jeżeli analiza incydentów wskazuje na potrzebę dodatkowego szkolenia;
    e. okresowo – odpowiednio do poziomu ryzyka.
3. Zakres szkolenia powinien być dostosowany do funkcji uczestnika.
4. Szkolenie użytkownika CBDOSP powinno obejmować co najmniej zasady:
    a. logowania;
    b. ochrony konta;
    c. korzystania z przyznanych uprawnień;
    d. eksportowania i drukowania danych;
    e. zgłaszania incydentów;
    f. zachowania poufności.
5. Przeprowadzenie szkolenia może podlegać udokumentowaniu.

§ 143. Kontrola przestrzegania Polityki

1. Przestrzeganie niniejszej Polityki podlega okresowej kontroli.
2. Kontrola może obejmować w szczególności:
    a. prawidłowość upoważnień;
    b. zakres uprawnień w CBDOSP;
    c. aktywne konta użytkowników;
    d. sposób przechowywania dokumentacji;
    e. realizację zasad retencji;
    f. rejestr naruszeń;
    g. realizację praw osób;

h. umowy powierzenia;
i. kopie bezpieczeństwa;
j. sposób niszczenia dokumentacji;
k. zgodność rzeczywistych procesów z przyjętymi procedurami.

3. Kontrola powinna być prowadzona z poszanowaniem zasady minimalizacji danych.
4. Osoba kontrolująca uzyskuje dostęp wyłącznie do danych niezbędnych do przeprowadzenia kontroli.
5. Wyniki kontroli oraz wymagane działania naprawcze powinny być odpowiednio dokumentowane.

§ 144. Obowiązek współpracy podczas kontroli

1. Osoby odpowiedzialne za poszczególne obszary przetwarzania są obowiązane współpracować przy kontroli przestrzegania Polityki.
2. W szczególności są obowiązane:
   a. udzielać zgodnych z prawdą informacji;
   b. udostępniać niezbędną dokumentację w granicach kompetencji osoby kontrolującej;
   c. wyjaśniać sposób realizacji procesów;
   d. informować o stwierdzonych nieprawidłowościach;
   e. realizować zatwierdzone działania naprawcze.
3. Niedopuszczalne jest ukrywanie naruszenia lub usuwanie informacji w celu uniemożliwienia ustalenia rzeczywistego stanu.

§ 145. Nieprawidłowości i działania naprawcze

1. Stwierdzone nieprawidłowości podlegają ocenie pod kątem ich znaczenia i ryzyka.
2. Działanie naprawcze powinno określać w miarę potrzeby:
   a. stwierdzoną nieprawidłowość;
   b. wymagany sposób jej usunięcia;
   c. osobę odpowiedzialną;
   d. termin realizacji;
   e. sposób weryfikacji wykonania.
3. Nieprawidłowość powodująca bezpośrednie i poważne zagrożenie dla bezpieczeństwa danych powinna być usunięta niezwłocznie.
4. Jeżeli nieprawidłowość doprowadziła lub mogła doprowadzić do naruszenia ochrony danych, stosuje się również przepisy Rozdziału XVIII.

Rozdział XXIII
Inspektor Ochrony Danych i koordynacja ochrony danych

§ 146. Ocena obowiązku wyznaczenia Inspektora Ochrony Danych

1. OSP dokonuje oceny, czy w świetle art. 37 RODO zachodzą przesłanki powodujące obowiązek wyznaczenia Inspektora Ochrony Danych.
2. Ocena powinna uwzględniać rzeczywisty charakter, zakres i skalę działalności OSP oraz wykonywanych operacji przetwarzania.
3. Sam fakt przetwarzania danych osobowych przez OSP nie oznacza automatycznie obowiązku wyznaczenia Inspektora Ochrony Danych.

4. W przypadku zmiany zakresu działalności albo sposobu przetwarzania ocena powinna zostać ponowiona.
5. Wynik oceny może zostać udokumentowany dla celów rozliczalności.

§ 147. Wyznaczenie Inspektora Ochrony Danych

1. Jeżeli powstanie obowiązek wyznaczenia Inspektora Ochrony Danych albo OSP podejmie decyzję o jego dobrowolnym wyznaczeniu, jego status, zadania i warunki wykonywania funkcji określa się zgodnie z art. 37–39 RODO.
2. Inspektor powinien posiadać odpowiednią wiedzę fachową z zakresu prawa i praktyk ochrony danych.
3. Inspektor wykonuje zadania w sposób niezależny, zgodnie z wymaganiami RODO.
4. Administrator zapewnia Inspektorowi warunki niezbędne do prawidłowego wykonywania jego zadań.
5. Dane kontaktowe Inspektora podlegają udostępnieniu i zgłoszeniu w zakresie wymaganym prawem.

§ 148. Koordynacja ochrony danych w przypadku niewyznaczenia Inspektora

1. Jeżeli OSP nie jest obowiązana do wyznaczenia Inspektora Ochrony Danych i nie wyznaczy go dobrowolnie, Zarząd może powierzyć określone zadania organizacyjne w zakresie ochrony danych wyznaczonej osobie lub osobom.
2. Osoba taka może posługiwać się określeniem „Koordynator ds. ochrony danych osobowych” albo innym określeniem niewprowadzającym w błąd co do statusu wynikającego z RODO.
3. Koordynator nie jest Inspektorem Ochrony Danych w rozumieniu art. 37–39 RODO, chyba że został formalnie wyznaczony na tę funkcję.
4. Do zadań Koordynatora może należeć w szczególności:
    1. prowadzenie dokumentacji ochrony danych;
    2. koordynowanie obsługi żądań osób;
    3. prowadzenie rejestru naruszeń;
    4. wspieranie analizy ryzyka;
    5. organizowanie przeglądów uprawnień;
    6. przygotowywanie projektów procedur;
    7. koordynowanie szkoleń;
    8. wspieranie Zarządu przy ocenie zgodności procesów.
5. Powierzenie zadań Koordynatorowi nie przenosi na niego odpowiedzialności Administratora.

Rozdział XXIV
Odpowiedzialność i przepisy końcowe

§ 149. Odpowiedzialność za przestrzeganie Polityki

1. Każda osoba posiadająca dostęp do danych osobowych w związku z działalnością OSP jest obowiązana przestrzegać niniejszej Polityki w zakresie dotyczącym wykonywanych przez nią zadań.
2. Naruszenie zasad ochrony danych może skutkować, odpowiednio do okoliczności:
    a. cofnięciem lub ograniczeniem uprawnień;
    b. cofnięciem upoważnienia do przetwarzania danych;

c. odebraniem dostępu do CBDOSP;
d. zastosowaniem środków przewidzianych w Statucie lub innych aktach wewnętrznych;
e. podjęciem innych działań wymaganych przepisami prawa.

3. Przy ocenie zdarzenia uwzględnia się w szczególności:
   a. charakter naruszenia;
   b. zakres danych;
   c. stopień zagrożenia dla osób;
   d. umyślność lub nieumyślność działania;
   e. działania podjęte w celu ograniczenia skutków;
   f. wcześniejsze naruszenia;
   g. stopień współpracy przy wyjaśnianiu zdarzenia.
4. Niezwłoczne i rzetelne zgłoszenie własnego błędu powinno być uwzględnione przy ocenie sposobu postępowania z danym zdarzeniem.
5. Odpowiedzialność wewnętrzna pozostaje bez uszczerbku dla odpowiedzialności wynikającej z powszechnie obowiązujących przepisów prawa.

§ 150. Przegląd, aktualizacja i stosowanie Polityki

1. Niniejsza Polityka podlega przeglądowi nie rzadziej niż raz w roku oraz każdorazowo, gdy zachodzą okoliczności mogące mieć istotny wpływ na ochronę danych osobowych.
2. Przegląd przeprowadza się w szczególności w przypadku:
   a. zmiany przepisów prawa;
   b. zmiany Statutu OSP mającej wpływ na procesy przetwarzania;
   c. wdrożenia nowego systemu teleinformatycznego;
   d. istotnej rozbudowy CBDOSP;
   e. uruchomienia nowego modułu CBDOSP;
   f. istotnej zmiany zakresu przetwarzanych danych;
   g. zmiany podmiotu świadczącego usługi hostingowe lub inne istotne usługi informatyczne;
   h. wystąpienia poważnego naruszenia ochrony danych;
   i. stwierdzenia istotnych nieprawidłowości podczas kontroli;
   j. zmiany sposobu prowadzenia dokumentacji członkowskiej;
   k. zmiany organizacji działalności MDP;
   l. innych zmian mających znaczenie dla bezpieczeństwa danych.
3. Przegląd powinien obejmować ocenę:
   a. aktualności Polityki;
   b. zgodności rzeczywistych procesów z dokumentacją;
   c. aktualności podstaw prawnych;
   d. adekwatności środków bezpieczeństwa;
   e. aktualności zakresów uprawnień;
   f. prawidłowości okresów retencji;
   g. aktualności umów powierzenia;
   h. skuteczności procedur reagowania na incydenty;
   i. potrzeby aktualizacji dokumentów wykonawczych.
4. Zmiany Polityki wymagają przyjęcia w sposób właściwy dla aktów wewnętrznych OSP.

5. W przypadku zmiany Polityki należy zapewnić, aby osoby, których obowiązki obejmują zmieniony zakres, zostały poinformowane o zmianach w sposób odpowiedni do ich znaczenia.
6. Dokumenty, formularze, procedury, rejestry oraz rozwiązania teleinformatyczne funkcjonujące w OSP powinny być sukcesywnie dostosowywane do niniejszej Polityki.
7. W zakresie nieuregulowanym niniejszą Polityką stosuje się:
    a. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679;
    b. przepisy krajowe dotyczące ochrony danych osobowych;
    c. przepisy dotyczące ochotniczych straży pożarnych;
    d. inne przepisy właściwe dla określonego procesu;
    e. Statut OSP;
    f. pozostałe akty wewnętrzne OSP, o ile nie pozostają w sprzeczności z niniejszą Polityką.
8. W razie sprzeczności pomiędzy postanowieniem dokumentu wewnętrznego a bezwzględnie obowiązującym przepisem prawa pierwszeństwo ma przepis prawa.
9. Integralną część systemu ochrony danych osobowych OSP stanowią dokumenty wykonawcze ustanowione na podstawie niniejszej Polityki.
10. Politykę stosuje się od dnia wejścia w życie Uchwały Zarządu OSP Rydułtowy, do której stanowi ona Załącznik nr 1.

Załącznik nr 2
do Uchwały nr OSPR.011.5.2026 Zarządu Ochotniczej Straży Pożarnej Rydułtowy z dnia 23 września 2026 r.

Rydułtowy, 23.09.2026r.
(miejscowość, data)

UPOWAŻNIENIE
do przetwarzania danych osobowych nr: …….. / 20 ……

Na podstawie:

- §34 ust.1 w związku z §41 i §42 załącznika nr 1 do Uchwały nr OSPR.011.5.2026 z dnia 23 września 2026 o przyjęciu Polityki Ochrony Danych Osobowych oraz zasad bezpieczeństwa przetwarzania danych osobowych w Ochotniczej Straży Pożarnej Rydułtowy,
- art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 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), zwane dalej RODO.

upoważniam Panią/Pana:

(Imię i nazwisko upoważnionego)

pełniącą/-ego obowiązki na stanowisku/-ach:

(nazwy stanowisk pełnienia obowiązków)

OCHOTNICZA STRAŻ POŻARNA RYDUŁTOWY, 44-280 Rydułtowy, ul. Traugutta 270
(nazwa jednostki OSP w której upoważniony pełnieni służbę oraz adres)

Identyfikator:
(wypełnia się jedynie w przypadku, gdy dane przetwarzane są w systemie teleinformatycznym)

do przetwarzania danych osobowych w ramach następujących kategorii czynności przetwarzania:

- **dostęp do danych osobowych zgodnie z zajmowanym stanowiskiem i powierzonym zakresem obowiązków bądź pełnionymi funkcjami oraz bezpośrednio wynikających z powiązanymi z nimi merytorycznie kategoriami czynności przetwarzania danych osobowych**

Okres trwania upoważnienia:

- **od dnia wystawienia na czas pełnienia obowiązków na wskazanym/-ch stanowisku/-ach**
(okres obowiązywania upoważnienia, np. od dnia wystawienia do chwili ustania pełnienia obowiązków na wskazanym stanowisku)

(data i podpis osoby upoważnionej)

(podpis i pieczęć administratora danych osobowych)

Wykonano w 2 egz.:
1) Akta osobowe osoby upoważnionej
2) a/a

Załącznik nr 3
do Uchwały nr OSPR.011.5.2026
Zarządu Ochotniczej Straży Pożarnej Rydułtowy z dnia 23 września 2026 r.

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

l.p.	Nr upoważnienia	Imię i nazwisko	Zakres upoważnienia	Dostęp do CBDOSP	Data wydania upoważnienia	Data cofnięcia upoważnienia
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						