# DZIENNIK URZĘDOWY
## SŁUŻBY OCHRONY PAŃSTWA

Warszawa, dnia 30 listopada 2020 r.

Poz. 17




**ZARZĄDZENIE NR 18/2020**
**KOMENDANTA SŁUŻBY OCHRONY PAŃSTWA**

z dnia 27 listopada 2020 r.

**w sprawie polityki ochrony danych osobowych w Służbie Ochrony Państwa**

Na podstawie art. 31 ust. 4 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) oraz art. 24 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz L 127 z 23.05.2018, str. 2), w związku z art. 10 ust. 1 i art. 61 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2020 r. poz. 384, 695 i 1610), zarządza się, co następuje:

Rozdział 1
**Przepisy ogólne**

**§ 1.** 1. Zarządzenie określa politykę ochrony danych osobowych w Służbie Ochrony Państwa, w tym zasady organizacji i ochrony danych osobowych przetwarzanych w SOP, których administratorem jest Komendant SOP, zgodnie z obowiązującymi przepisami prawa oraz polskimi i europejskimi normami technicznymi dotyczącymi zarządzania bezpieczeństwem, w tym bezpieczeństwem systemów teleinformatycznych służących do przetwarzania danych osobowych.

2. Przepisami prawa, o których mowa w ust. 1, są w szczególności przepisy:

1) 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”;
2) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
3) ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, zwanej dalej „ustawą DODO”;
4) ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa;
5) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 maja 2018 r. w sprawie przetwarzania informacji przez Służbę Ochrony Państwa (Dz. U. poz. 1069 i z 2020 r. poz. 888).

3. Stosowanie przepisów zarządzenia powinno następować w sposób zapewniający jednolitość systemu ochrony danych osobowych i wdrożenie niezbędnych mechanizmów zabezpieczających te dane w procesie przetwarzania w każdej postaci, zarówno w sposób niezautomatyzowany (tradycyjny), jak i zautomatyzowany (elektroniczny), w tym przez uwzględnienie systemu zarządzania bezpieczeństwem informacji w Służbie Ochrony Państwa określonego odrębnymi przepisami.

4. W sprawach nieuregulowanych w zarządzeniu, jeżeli nie postanowiono inaczej, mają zastosowanie przepisy prawa powszechnie obowiązującego dotyczące ochrony danych osobowych, w szczególności określone w ust. 2.

**§ 2.** 1. Zarządzenie stosuje się do funkcjonariuszy i pracowników SOP oraz osób mających dostęp do danych osobowych przetwarzanych w SOP na zlecenie Komendanta SOP jako Administratora, niezależnie od podstawy prawnej wykonywania zadań, z którymi wiąże się przetwarzanie danych osobowych.

2. Zarządzenie stosuje się do przetwarzania danych osobowych w sposób niezautomatyzowany (tradycyjny), jak i zautomatyzowany (elektroniczny), w tym danych osobowych udostępnianych SOP przez organy, służby lub inne podmioty na podstawie przepisów prawa, postanowień umów lub porozumień, we wszelkiego rodzaju rejestrach, skorowidzach, kartotekach, wykazach, listach, księgach, a także w systemach informatycznych służących do przetwarzania danych osobowych użytkowanych w SOP, w tym zapisanych na zewnętrznych informatycznych nośnikach danych.

3. W przypadku, gdy z innych przepisów obowiązujących w SOP wynikają odmienne od zawartych w zarządzeniu uregulowania dotyczące ochrony danych osobowych, użytkownicy stosują te przepisy, które zapewniają wyższy poziom ochrony danych osobowych.

**§ 3.** Użyte w zarządzeniu określenia i skróty oznaczają:

1) Administrator – Komendanta Służby Ochrony Państwa;

2) AS/LAS (Administrator Systemu/Lokalny Administrator Systemu) – osobę lub zespół osób wyznaczonych przez Administratora, które odpowiadają za funkcjonowanie i bezpieczeństwo systemów i sieci teleinformatycznych służących do przetwarzania danych osobowych, przy czym AS wyznacza się dla systemów własnych SOP, a LAS wyznacza się dla innych systemów;

3) dane osobowe – dane, o których mowa w art. 4 pkt 1 RODO;

4) IOD (Inspektor Ochrony Danych) – osobę wyznaczoną przez Administratora i bezpośrednio mu podległą;

5) kierownik SKO – osobę wyznaczoną do kierowania SKO lub jego zastępcę;

6) osoba upoważniona – osobę posiadającą upoważnienie do przetwarzania danych osobowych;

7) RCP – rejestr czynności przetwarzania danych osobowych, w którym są zawarte informacje, o których mowa w art. 30 ust. 1 RODO oraz art. 35 ust. 2 ustawy DODO;

8) SKO – komórkę organizacyjną SOP, która podlega bezpośrednio Komendantowi SOP lub jego zastępcy;

9) SOP – Służbę Ochrony Państwa;

10) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

11) Zarządzający – kierownika komórki organizacyjnej wykonującego zadania Administratora.

## Rozdział 2
## Organizacja zarządzania ochroną danych

**§ 4.** Do zadań Administratora należy:

1) wdrażanie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych odbywało się zgodnie z przepisami dotyczącymi ochrony danych osobowych i aby móc wykazać, że warunek ten jest spełniony;

2) wyznaczenie IOD oraz zapewnienie IOD środków i organizacyjnej odrębności, niezbędnych do niezależnego wykonywania przez niego zadań;

3) wyznaczenie Zarządzającego;

4) powoływanie oraz odwoływanie AS/LAS na podstawie odrębnych przepisów;

5) wspieranie IOD w wypełnianiu przez niego zadań przez zapewnienie środków niezbędnych do wykonania tych zadań, dostęp do danych osobowych i operacji przetwarzania oraz do podnoszenia przez niego wiedzy fachowej;

6) wdrażanie polityki ochrony danych osobowych oraz dokumentów związanych z ochroną danych osobowych, w szczególności instrukcji, procedur i algorytmów postępowania.

**§ 5.** Do zadań Zarządzającego należy:

1) nadzorowanie wdrażania środków technicznych i organizacyjnych, które powinny zapewniać ochronę przetwarzanych danych osobowych, w szczególności przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów dotyczących ochrony danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

2) wydawanie oraz cofanie upoważnień do przetwarzania danych osobowych, na wniosek kierowników SKO;

3) prowadzenie ewidencji osób upoważnionych;

4) udostępnianie informacji w ramach wykonywania obowiązku informacyjnego;

5) podejmowanie działań mających na celu ułatwienie osobie, której dane dotyczą, wykonywania przysługujących jej praw, o których mowa w art. 15 RODO oraz art. 22–25 i 29 ustawy DODO, oraz udzielanie informacji w takiej samej postaci w jakiej wniesiono wniosek;

6) opracowanie dokumentów powiązanych z polityką ochrony danych osobowych, w szczególności instrukcji, procedur i algorytmów postępowania;

7) bieżący przegląd środków technicznych i organizacyjnych pod kątem potrzeby ich uaktualnienia;

8) prowadzenie RCP;

9) przeprowadzanie wszelkich czynności służących wyjaśnieniu okoliczności naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych;

10) prowadzenie rejestru incydentów bezpieczeństwa związanych z przetwarzaniem danych osobowych;

11) dokonywanie oceny, o której mowa w art. 35 RODO i art. 37 ustawy DODO.

**§ 6.** Zakres, tryb i sposób realizacji zadań IOD określają odrębne przepisy.

**§ 7.** Do zadań AS/LAS należy:

1) zarządzanie, na podstawie odrębnych przepisów, systemami teleinformatycznymi służącymi do przetwarzania danych osobowych;

2) konfigurowanie urządzeń składowych systemów teleinformatycznych służących do przetwarzania danych osobowych, zgodnie z obowiązującą dokumentacją;

3) zarządzanie kontami i uprawnieniami użytkowników;

4) umożliwienie Zarządzającemu prowadzenia elektronicznej ewidencji zarządzanych kont użytkowników;

5) wykonywanie kopii konfiguracji systemu operacyjnego;

6) zapewnienie ochrony antywirusowej systemów informatycznych służących do przetwarzania danych osobowych oraz ich bieżącej aktualizacji;

7) współpracę w opracowywaniu i aktualizacji dokumentacji dotyczącej ochrony danych osobowych;

8) współpracę z Zarządzającym w zakresie obsługi incydentów bezpieczeństwa danych osobowych przetwarzanych w sposób zautomatyzowany.

**§ 8.** 1. Administrator Materiałów Kryptograficznych zarządza materiałami kryptograficznymi wykorzystywanymi w procesie przetwarzania informacji, w tym danych osobowych.

2. Administratora Materiałów Kryptograficznych wyznacza Administrator.

**§ 9.** Kierownik SKO:

1) wnioskuje do Zarządzającego o wydanie lub cofnięcie upoważnienia do przetwarzania danych osobowych;

2) wskazuje w karcie opisu stanowiska służby lub pracy procesy przetwarzania z RCP, do których ma dostęp osoba upoważniona na danym stanowisku służbowym;

3) przekazuje Zarządzającemu informacje o incydentach, anomaliach, zauważonych ryzykach lub podatnościach w procesie przetwarzania danych osobowych;

4) bierze udział we wdrożeniu mechanizmów bezpieczeństwa przetwarzanych danych osobowych przez opiniowanie i ocenę możliwości zastosowania środków bezpieczeństwa;

5) wnioskuje o uruchomienie systemu teleinformatycznego lub pojedynczych stacji roboczych i o wydanie zgody na przetwarzanie danych osobowych w sieciach i systemach informatycznych służących do przetwarzania danych osobowych;

6) dokonuje weryfikacji danych osobowych w terminach określonych przez przepisy szczególne, lecz nie rzadziej niż co 10 lat od dnia zebrania, uzyskania, pobrania lub aktualizacji danych;

7) zapewnia, w zakresie danych osobowych przetwarzanych na podstawie przepisów ustawy DODO, realizację zadań o których mowa w art. 19 oraz art. 20 ustawy DODO;

8) zapewnia, aby dane osobowe były przetwarzane zgodnie z zasadami odkreślonymi w art. 5 RODO;

9) prowadzi dokumentację dotyczącą realizacji czynności związanych z przetwarzaniem danych osobowych;

10) na podstawie zawartych umów, powierza przetwarzanie danych osobowych innemu podmiotowi przetwarzającemu;

11) zawiadamia Zarządzającego o planowaniu utworzenia nowego, modyfikacji lub usunięcia procesu przetwarzania danych osobowych;

12) udziela informacji, określonych przez Zarządzającego, niezbędnych do przeprowadzenia oceny, o której mowa w art. 35 RODO i art. 37 ustawy DODO;

13) umożliwia Zarządzającemu przeprowadzanie wszelkich czynności służących do wyjaśnienia okoliczności naruszenia lub podejrzenia naruszenia.

**§ 10.** Kierownik komórki organizacyjnej SOP właściwej do spraw teleinformatyki lub osoba go zastępująca:

1) wydaje zgody na użycie w systemach informatycznych służących do przetwarzania danych osobowych systemów operacyjnych, jeżeli jest to wymagane na podstawie odrębnych przepisów;

2) zapewnia obsługę incydentów bezpieczeństwa związanych z przetwarzaniem danych osobowych w sposób zautomatyzowany;

3) nadzoruje zadania realizowane przez AS/LAS;

4) dokonuje bieżących przeglądów środków technicznych i organizacyjnych pod kątem ich uaktualniania;

5) prowadzi ewidencję operacji przetwarzania danych osobowych w zautomatyzowanych systemach przetwarzania;

6) obsługuje naruszenia i gromadzi dokumentację o przypadkach naruszenia ochrony danych osobowych do celów kontrolnych.

**§ 11.** 1. Do przetwarzania danych osobowych mogą być dopuszczeni funkcjonariusze i pracownicy SOP, którzy spełniają łącznie następujące warunki:

1) realizują zadania służbowe wymagające przetwarzania danych osobowych;

2) odbyli szkolenie z zakresu ochrony danych osobowych;

3) zobowiązali się do zachowania w poufności przetwarzanych danych osobowych;

4) zapoznali się z przepisami dotyczącymi ochrony danych osobowych, w szczególności z niniejszym zarządzeniem;

5) posiadają upoważnienie do przetwarzania danych osobowych.

2. Wydanie upoważnienia do przetwarzania danych osobowych osobie, która spełnia warunki określone w ust. 1 pkt 1–4, następuje przez złożenie przez Zarządzającego podpisu pod formułą „Upoważniam” na wniosku kierownika SKO. Wzór wniosku o wydanie upoważnienia do przetwarzania danych osobowych, będącego po podpisaniu przez Zarządzającego upoważnieniem, jest określony w załączniku nr 1 do zarządzenia.

3. Do wniosku, o którym mowa w ust. 2, dołącza się podpisane przez osobę wskazaną we wniosku oświadczenie o spełnieniu warunków określonych w ust. 1 pkt 2–4. Wzór oświadczenia jest określony w załączniku nr 2 do zarządzenia.

4. Upoważnienie oraz oświadczenie, o których mowa w ust. 2 i 3, włącza się do akt osobowych osoby upoważnionej.

**§ 12.** Osoba upoważniona jest obowiązana:

1) znać sposób postępowania z danymi osobowymi w czasie wykonywania obowiązków służbowych;

2) przetwarzać dane osobowe w sposób zgodny z prawem i zakresem posiadanego upoważnienia;

3) dołożyć szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane osobowe są przetwarzane;

4) chronić wszelkie nośniki zawierające dane osobowe, w tym informatyczne nośniki danych, przed dostępem do nich przez osoby nieupoważnione oraz przed utratą, uszkodzeniem lub zniszczeniem;

5) zabezpieczyć dane osobowe przed ich udostępnieniem lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem, w szczególności po zakończeniu służby lub pracy;

6) w przypadku przekazywania dokumentów zawierających dane osobowe postępować zgodnie z przepisami kancelaryjnymi dotyczącymi obiegu dokumentów w SOP;

7) informować Zarządzającego oraz przełożonych o przypadkach naruszenia zasad bezpieczeństwa przetwarzania danych osobowych, przyczynach ich powstania, podjętych działaniach mających na celu zapobieżenie powstaniu szkód, w tym w szczególności utraty poufności, integralności i dostępności danych osobowych oraz propozycjach mających na celu wyeliminowanie zagrożenia dla bezpieczeństwa danych osobowych w przyszłości;

8) uczestniczyć w szkoleniach z zakresu ochrony danych osobowych, do odbycia których została wyznaczona;

9) udzielić wszelkiej pomocy Zarządzającemu oraz IOD w czasie prowadzenia przez nich monitoringu zgodności przetwarzania danych z przepisami dotyczącymi ochrony danych osobowych oraz czynności służących wyjaśnieniu okoliczności naruszeniea lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych.

**§ 13.** 1. Upoważnienie do przetwarzania danych osobowych może zostać cofnięte w przypadku:

1) istotnego naruszenia przez osobę upoważnioną obowiązków określonych w § 12;

2) wszczęcia postępowania dyscyplinarnego, w którym osoba upoważniona jest obwinionym lub rozpoczęcia czynności wyjaśniających, w toku których nie zachodzą wątpliwości co do popełnienia przewinienia dysyplinarnego przez osobę upoważnioną;

3) zawieszenia osoby upoważnionej w czynnościach służbowych.

2. Cofnięcie upoważnienia do przetwarzania danych osobowych następuje przez złożenie przez Zarządzającego podpisu pod formułą „Cofam upoważnienie” na wniosku kierownika SKO. Wzór wniosku o cofnięcie upoważnienia do przetwarzania danych osobowych jest określony w załączniku nr 3 do zarządzenia.

3. Cofnięcie upoważnienia włącza się do akt osobowych osoby upoważnionej.

Rozdział 3

**Dokumentowanie przetwarzania danych osobowych**

**§ 14.** Zarządzający dokumentuje przetwarzanie danych osobowych przez prowadzenie:

1) RCP;

2) wykazu zbiorów danych oraz opis ich struktury;

3) ewidencji osób upoważnionych do przetwarzania danych osobowych;

4) wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe;

5) rejestru incydentów bezpieczeństwa związanych z przetwarzaniem danych osobowych.

**§ 15.** IOD dokumentuje przeprowadzanie szkoleń przez prowadzenie ewidencji osób przeszkolonych z zakresu ochrony danych osobowych.

Rozdział 4

**Zarządzanie ryzykiem bezpieczeństwa danych osobowych**

**§ 16.** 1. Zakres i sposób zarządzania ryzykiem powinien zapewnić odpowiedni stopień bezpieczeństwa danych osobowych odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych. Określając czy stopień bezpieczeństwa jest odpowiedni uwzględnia się przede wszystkim ryzyko wiążące się z przetwarzaniem danych osobowych, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

2. W ramach zarządzania ryzykiem dokonuje się identyfikacji zagrożeń, szacowania poziomu ich ryzyka, oceny ryzyka oraz opracowania i wdrożenia planu minimalizacji ryzyka w stosunku do ryzyk o najwyższym poziomie. Opracowany plan minimalizacji ryzyka przed wdrożeniem przedstawia się Administratorowi do akceptacji.

3. Szczegółowy sposób zarządzania ryzykiem określają odrębne przepisy w sprawie metodyki zarządzania ryzykiem w systemie zarządzania bezpieczeństwem informacji w Służbie Ochrony Państwa.

Rozdział 5

**Bezpieczeństwo przetwarzania danych osobowych**

**§ 17.** Zapewnienie bezpieczeństwa danych osobowych polega na zapewnieniu poufności, integralności, dostępności i rozliczalności na poziomie wymaganym przez przepisy prawa, regulacje wewnętrzne SOP i standardy wynikające z międzynarodowych norm.

**§ 18.** Środki ochrony powinny być zróżnicowane odpowiednio do poziomu zagrożeń wynikających z wymaganego stopnia bezpieczeństwa, z uwzględnieniem możliwości finansowych i organizacyjnych SOP oraz przepisów prawa.

**§ 19.** 1. Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania danych osobowych wymienionych w wykazie obszarów przetwarzania danych osobowych oraz w miejscach realizacji ustawowych zadań przez funkcjonariuszy i pracowników SOP.

2. Wykaz, o którym mowa w ust. 1, opracowuje i w miarę potrzeb aktualizuje Zarządzający oraz zatwierdza Administrator.

3. W przypadku przetwarzania danych osobowych poza obszarami, o których mowa w ust. 1, osoba upoważniona jest obowiązana do ochrony danych osobowych przed utratą, ujawnieniem, zniszczeniem lub uszkodzeniem.

4. Przetwarzanie danych osobowych powinno odbywać się w sposób i w miejscu zapewniającym odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem za pomocą odpowiednich środków technicznych lub organizacyjnych.

5. W przypadku przetwarzania danych osobowych w strefach ochronnych stosuje się środki techniczne i organizacyjne zgodnie z planem ochrony informacji niejawnych.

6. Pomieszczenie, w którym odbywa się przetwarzanie danych osobowych, powinno być zabezpieczone przed dostępem osób nieuprawnionych przez czas nieobecności w nim osób upoważnionych.

7. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym odbywa się przetwarzanie danych osobowych, jest dopuszczalne jedynie w obecności osoby upoważnionej lub za zgodą Administratora.

8. Klucze do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, powinny być przechowywane i wydawane zgodnie z procedurą opisaną w planach ochrony informacji niejawnych SOP.

**§ 20.** 1. Wydruki i nośniki informatyczne, z wyjątkiem dysków twardych zamontowanych w komputerach stacjonarnych i laptopach, zawierające dane osobowe należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.

2. Wydruki próbne lub uszkodzone należy niszczyć w niszczarkach, z uwzględnieniem przepisów dotyczących obiegu informacji w SOP.

Rozdział 6
**Zarządzanie incydentami**

**§ 21.** 1. Incydenty związane z bezpieczeństwem przetwarzanych danych osobowych są wykrywane i rejestrowane w celu ich zidentyfikowania i zapobiegania ich wystąpieniu w przyszłości, z wykorzystaniem w szczególności takich środków jak:

1) strefy ochronne I, II i III;

2) elektroniczny system kontroli dostępu „KANTECH”;

3) systemy kamer CCTV;

4) systemy alarmowe;

5) oprogramowanie antywirusowe;

6) firewall sprzętowy lub programowy;

7) dzienniki zdarzeń systemów informatycznych służących do przetwarzania danych osobowych;

8) dzienniki zdarzeń oprogramowania antywirusowego oraz firewall;

9) sprawdzenia realizowane przez AS/LAS;

10) szkolenia użytkowników.

2. Dzienniki zdarzeń systemów informatycznych służących do przetwarzania danych osobowych, oprogramowania antywirusowego oraz firewall są przechowywane przez co najmniej 90 dni.

3. Dzienniki zdarzeń urządzeń firewall są przechowywane przez co najmniej 30 dni.

**§ 22.** Incydenty związane z naruszeniem lub podejrzeniem naruszenia bezpieczeństwa przetwarzania danych osobowych wykryte podczas sprawdzeń są obsługiwane przez AS/LAS we współpracy z Zarządzającym.

**§ 23.** 1. Osoba upoważniona, w przypadku zaistnienia zdarzenia związanego z naruszeniem lub podejrzeniem naruszenia bezpieczeństwa przetwarzania danych osobowych, jest obowiązana niezwłocznie zgłosić to zdarzenie Zarządzającemu oraz powiadomić swojego bezpośredniego przełożonego. Zgłoszenie potwierdza się w notatce służbowej zawierającej opis stwierdzonych naruszeń, z którą zapoznaje się bezpośredni przełożony oraz IOD.

2. Zarządzający, w porozumieniu z IOD, przeprowadza wszelkie czynności służące wyjaśnieniu okoliczności naruszenia lub podejrzenia naruszenia oraz wskazuje sposoby usunięcia skutków naruszenia i zapobieżenia powstania takiego zdarzenia w przyszłości.

3. Zarządzający, w porozumieniu z IOD, sporządzając protokół z przeprowadzonych czynności, określa osobę lub osoby odpowiedzialne za naruszenie bezpieczeństwa przetwarzania danych osobowych z jednoczesnym wskazaniem jakie normy i w jaki sposób zostały naruszone. Protokół z przeprowadzonych czynności Zarządzający przedstawia Administratorowi.

4. Szczegółowe procedury zarządzania incydentami określają odrębne przepisy.

Rozdział 7
**Zbiory danych osobowych**

**§ 24.** 1. Zarządzający opracowuje i aktualizuje:

1) wykaz zbiorów danych osobowych oraz opis ich struktury;

2) RCP.

2. Dokumenty wymienione w ust. 1 zatwierdza Administrator.

3. Wykaz zbiorów danych osobowych oraz RCP Zarządzający przekazuje do opublikowania przez AS/LAS w systemie teleinformatycznym BASTION.

Rozdział 8
**Przepisy dostosowujące i końcowe**

**§ 25.** Kierownicy SKO zapoznają funkcjonariuszy oraz pracowników SOP mających dostęp do danych osobowych przetwarzanych w SOP z przepisami zarządzenia.

**§ 26.** Upoważnienia do przetwarzania danych osobowych wydane przed dniem wejścia w życie niniejszego zarządzenia zachowują ważność.

**§ 27.** Karty opisu stanowiska służby lub pracy sporządzone i podpisane przez funkcjonariuszy lub pracowników przed dniem wejścia w życie niniejszego zarządzenia zachowują ważność.

**§ 28.** Traci moc zarządzenie nr 20/2019 Komendanta Służby Ochrony Państwa z dnia 14 czerwca 2019 r. w sprawie polityki ochrony danych osobowych w Służbie Ochrony Państwa (Dz. Urz. SOP poz. 25).

**§ 29.** Zarządzenie wchodzi w życie z dniem następującym po dniu podpisania.

Komendant Służby Ochrony Państwa
mjr SOP Paweł Olszewski

Załączniki do zarządzenia nr 18/2020 Komendanta
Służby Ochrony Państwa z dnia 27 listopada 2020 r.

**Załącznik nr 1**

WZÓR WNIOSKU O WYDANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

**Upoważniam**

_____
(pieczęć i podpis osoby upoważniającej)

_____
(data wydania upoważnienia)

_____
(numer upoważnienia)

Warszawa, dnia _____

## WNIOSEK

### o wydanie upoważnienia do przetwarzania danych osobowych

Na podstawie art. 70a ust. 2 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2020 r. poz. 384, z późn. zm.) oraz art. 41 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) oraz art. 32 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) wnoszę o wydanie

_____
(stopień, imię i nazwisko)

upoważnienia do przetwarzania danych osobowych, w formie papierowej oraz w formie elektronicznej w ramach nadanych dostępów do systemów informatycznych, zgodnie z zakresem określonym w karcie opisu stanowiska służby lub pracy upoważnianego, na okres do dnia jego cofnięcia albo do ustania stosunku pracy lub służby upoważnionego.

_____
(kierownik komórki organizacyjnej SOP)

**Załącznik nr 2**

WZÓR OŚWIADCZENIA O SPEŁNIENIU WARUNKÓW DO UZYSKANIA UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Warszawa, dnia _____

_____
(stopień, imię i nazwisko)

_____
(komórka organizacyjna)

_____
(nr tel. służbowego)

**O Ś W I A D C Z E N I E**

Zgodnie z art. 70a ust. 2 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2020 r. poz. 384, z późn. zm.) oraz art. 41 ust. 3 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) zobowiązuję się do przetwarzania danych osobowych zgodnie z upoważnieniem oraz oświadczam, że zostałem przeszkolony, zapoznałem się, rozumiem i będę przestrzegać obowiązków wynikających w szczególności z przepisów:

- ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2020 r. poz. 384, z poźn. zm.);
- ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
- ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125);
- rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.);
- rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 maja 2018 r. w sprawie przetwarzania informacji przez Służbę Ochrony Państwa (Dz. U. poz. 1069 i z 2020 r. poz. 888);
- aktów prawa wewnętrznego Służby Ochrony Państwa z zakresu ochrony danych osobowych.

Ponadto zobowiązuję się do:

- zapewnienia bezpieczeństwa danych osobowych, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem;
- zachowania udostępnionych mi danych osobowych oraz sposobów ich zabezpieczenia w poufności w trakcie służby lub pracy, a także po jej ustaniu.

_____
(podpis funkcjonariusza lub pracownika)

**Załącznik nr 3**

WZÓR WNIOSKU O COFNIĘCIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Warszawa, dnia _____.

**Cofam upoważnienie**

_____
(pieczęć i podpis osoby upoważnionej)

_____
(data cofnięcia upoważnienia)

_____
(numer upoważnienia)

**WNIOSEK**

**o cofnięcie upoważnienia do przetwarzania danych osobowych**

Na podstawie art. 70a ust. 2 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2020 r. poz. 384, z późn. zm.) oraz art. 41 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) oraz art. 32 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) wnoszę o cofnięcie

_____
(stopień, imię i nazwisko)

upoważnienia do przetwarzania danych osobowych, w formie papierowej oraz w formie elektronicznej:

– od dnia _____ ,
(data cofnięcia upoważnienia)

– z powodu _____ .
(wpisać powód cofnięcia upoważnienia)

_____
(kierownik komórki organizacyjnej SOP)