Warszawa, dnia 25 czerwca 2020 r.

Poz. 6

Z A R Z Ą D Z E N I E

M I N I S T R A Ś R O D O W I S K A [1)]

z dnia 25 czerwca 2020 r.

w sprawie wprowadzenia Polityki Ochrony Danych Osobowych

Na podstawie art. 24 ust. 1 i 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 r., str. 1) zarządza się, co następuje:

§ 1. W Ministerstwie Środowiska wprowadza się do stosowania Politykę Ochrony Danych Osobowych, zwaną dalej „Polityką", stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Polityka jest dokumentem określającym zadania służące realizacji zasady zapewnienia poufności, integralności, dostępności, rozliczalności przetwarzanych danych osobowych oraz ochronie prawa osób, których dane dotyczą w Ministerstwie Środowiska.

§ 3. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

MINISTER ŚRODOWISKA

Michał Woś

[1)] Minister Środowiska kieruje działem administracji rządowej – środowisko, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 20 marca 2020 r. w sprawie szczegółowego zakresu działania Ministra Środowiska (Dz. U. poz. 494).

Załącznik
do zarządzenia
Ministra Środowiska
z dnia 25 czerwca 2020 r.(poz. 6)

POLITYKA OCHRONY DANYCH OSOBOWYCH

Rozdział 1

Przepisy ogólne

§ 1. Przetwarzanie danych osobowych w Ministerstwie Środowiska, zwanym dalej „MŚ", jest dopuszczalne tylko w przypadkach i na warunkach określonych w rozporządzeniu 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.), zwanego dalej „RODO", a także zgodnie z Polityką Ochrony Danych Osobowych, zwaną dalej „Polityką".

§ 2. Użyte w Polityce określenia oznaczają:

1) Administrator Danych Osobowych – Ministra Środowiska;
2) Inspektor Ochrony Danych - osobę wyznaczoną na podstawie art. 37 ust. 1 lit. a RODO, w szczególności, w celu monitorowania przestrzegania RODO innych przepisów Unii Europejskiej lub państw członkowskich oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie danych osobowych;
3) Administrator Bezpieczeństwa Systemów Informatycznych - pracownika wyznaczonego do kontroli przestrzegania ochrony danych osobowych w systemach teleinformatycznych;
4) Administrator Systemów Informatycznych - osobę nadzorującą całość lub część systemu informatycznego, w którym przetwarzane są dane osobowe;
5) dane osobowe - dane osobowe w rozumieniu art. 4 pkt 1 RODO;
6) ewidencja - ewidencję osób upoważnionych do przetwarzania danych osobowych w MŚ;
7) EZD - aplikację służącą do elektronicznego obiegu dokumentacji;
8) hasło - ciąg znaków literowych, cyfrowych lub innych znanych jedynie osobie uprawnionej do pracy w systemie informatycznym;

9) identyfikator - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
10) kierujący komórką organizacyjną - dyrektora departamentu lub biura, a także szefa Gabinetu Politycznego Ministra albo osoby ich zastępujące;
11) komórka organizacyjna - departament, biuro oraz Gabinet Polityczny Ministra;
12) osoba nieupoważniona - osobę nieposiadającą upoważnienia do przetwarzania danych osobowych w zakresie niezbędnym do wykonania czynności;
13) osoba upoważniona - osobę przetwarzającą dane osobowe, w tym również za pomocą systemu informatycznego lub sieci teleinformatycznej, w ramach wykonywanych zadań służbowych w zakresie określonym w upoważnieniu;
14) pracownik - osobę zatrudnioną w MŚ, stażystę, wolontariusza, praktykanta lub osobę świadczącą usługi na podstawie umów cywilnoprawnych na rzecz MŚ;
15) przetwarzanie danych osobowych - przetwarzanie w rozumieniu art. 4 pkt 2 RODO;
16) rejestr czynności przetwarzania - rejestr czynności przetwarzania w rozumieniu art. 30 RODO;
17) zbiór danych - zbiór danych w rozumieniu art. 4 pkt 6 RODO.

Rozdział 2

Organizacja systemu bezpieczeństwa przetwarzania danych osobowych

§ 3. Za prawidłowość przetwarzania danych osobowych i ich ochronę w MŚ odpowiada Administrator Danych Osobowych, Inspektor Ochrony Danych, w zakresie określonym w art. 39 RODO, a także w zakresie określonym w Polityce bezpieczeństwa: kierujący komórkami organizacyjnymi w MŚ, Administrator Bezpieczeństwa Systemów Informatycznych, Administratorzy Systemów Informatycznych i pozostali pracownicy.

§ 4. Administrator Danych Osobowych zapewnia zgodnie z art. 38 RODO organizacyjną odrębność Inspektora Ochrony Danych.

§ 5. 1. Inspektor Ochrony Danych realizuje zadania określone w art. 39 RODO

2. Inspektor Ochrony Danych w ramach wykonywania zadań z zakresu ochrony danych osobowych podlega bezpośrednio Ministrowi Środowiska.

3. Zadania Inspektora Ochrony Danych podczas jego nieobecności wykonuje osoba wskazana przez Administratora Danych Osobowych posiadająca wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych.

§ 6. 1. Administrator Bezpieczeństwa Systemów Informatycznych:

1) współpracuje z Inspektorem Ochrony Danych w zakresie opracowania i aktualizowania Polityki Ochrony Danych Osobowych oraz formularza szacowania ryzyka przetwarzania danych osobowych;
2) zapewnia, stosownie do potrzeb, zabezpieczenia w systemie informatycznym i kontroli funkcjonowania informatycznych mechanizmów ochrony danych osobowych.

2. Wykonawcami Polityki w zakresie bezpieczeństwa systemów informatycznych są Administrator Bezpieczeństwa Systemów Informatycznych i Administratorzy Systemów Informatycznych.

§ 7. 1. Kierujący komórką organizacyjną, w zakresie ochrony danych osobowych, w kierowanej komórce organizacyjnej:

1) realizuje zadania wynikające z Polityki;
2) wdraża oraz nadzoruje przestrzeganie Polityki;
3) organizuje i nadzoruje funkcjonowanie systemu zabezpieczeń danych osobowych;
4) wykonuje, we współpracy z Inspektorem Ochrony Danych, w imieniu Administratora Danych Osobowych, realizację obowiązków, o których mowa w art. 14-21 RODO;
5) informuje Inspektora Ochrony Danych o:
   a) nieprawidłowościach i naruszeniu ochrony danych osobowych,
   b) zmianach w zakresie, sposobie lub rodzaju przetwarzania danych osobowych,
   c) planowanym przetwarzaniu danych osobowych w zakresie innym niż wskazany w rejestrze czynności przetwarzania, m.in. w przypadku projektowania nowych rozwiązań informatycznych, w celu wdrożenia rozwiązań spełniających wymogi RODO oraz chroniących prawa osób, których dane dotyczą, o których mowa w art. 25 RODO,
   d) potrzebie przeszkolenia podległych pracowników w zakresie przetwarzania danych osobowych;
6) wykonuje zalecenia Administratora Danych Osobowych i Inspektora Ochrony Danych;
7) regularnie dokonuje przeglądu upoważnień do przetwarzania danych osobowych w celu zapewnienia ich aktualności;
8) podejmuje decyzje dotyczące sposobu przetwarzania danych osobowych;
9) występuje do Administratora Danych Osobowych, po zasięgnięciu opinii Inspektora Ochrony Danych, o uzyskanie zgody na przekazanie danych osobowych do państwa

trzeciego, które zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych;

10) przekazuje projekty umów dotyczących przetwarzania danych osobowych, w tym powierzenia przetwarzania danych osobowych do zaopiniowania:
    a) Inspektorowi Ochrony Danych oraz w przypadku przetwarzania danych osobowych w systemach informatycznych - Administratorowi Bezpieczeństwa Systemów Informatycznych,
    b) kierującemu Departamentem Prawnym.

2. Pracownicy MŚ:

1) przestrzegają przepisów RODO, przepisów regulujących ochronę danych osobowych oraz postanowienia Polityki;
2) składają oświadczenia o:
    a) zachowaniu w tajemnicy danych osobowych,
    b) zapoznaniu się z przepisami RODO, regulującymi ochronę danych osobowych oraz Polityką;
3) przetwarzają dane osobowe zgodnie z celem, dla którego zostały one zebrane;
4) zgłaszają Inspektorowi Ochrony Danych zdarzenia związane z bezpieczeństwem danych osobowych;
5) biorą udział w sprawdzeniu, o którym mowa w § 9 ust. 1, w tym umożliwiają Inspektorowi Ochrony Danych przeprowadzenie czynności w toku sprawdzenia.

3. Oświadczenia, o których mowa w ust. 2 pkt 2, dołączane są do akt pracowników.

§ 8. Do zadań Administratorów Systemów Informatycznych należy wykonanie czynności technicznej polegającej na nadawaniu oraz odbieraniu uprawnień do systemów informatycznych, w których przetwarzane są dane osobowe, prowadzenie ewidencji nadanych uprawnień oraz nadzorowanie działania tych systemów.

Rozdział 3

Testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych

§ 9. 1. Inspektor Ochrony Danych uczestniczy w testowaniu, mierzeniu i ocenianiu skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych poprzez sprawdzenia, zgodnie z planem sprawdzeń, zwanym dalej „planem".

2. Plan, opracowany w komórce organizacyjnej właściwej do spraw ochrony danych osobowych, jest przedstawiany Administratorowi Danych Osobowych, nie później niż dwa tygodnie przed dniem rozpoczęcia okresu objętego planem, z wyłączeniem sprawdzeń, o których mowa w ust. 7. Plan obejmuje co najmniej jedno sprawdzenie.

3. W sprawdzeniu, o którym mowa w ust. 1, biorą udział osoby upoważnione do przetwarzania danych osobowych, a w przypadku sprawdzenia danych osobowych przetwarzanych w systemie informatycznym - Administrator Systemu Informatycznego oraz w uzasadnionych przypadkach także Administrator Bezpieczeństwa Systemów Informatycznych.

4. Plan określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń planowych oraz sposób i zakres ich dokumentowania.

5. Nie później niż 14 dni przed dniem planowanego sprawdzenia, informuje się kierujących komórkami organizacyjnymi o terminie przeprowadzenia sprawdzenia.

6. Dokumentuje się czynności przeprowadzone w toku sprawdzenia, w zakresie niezbędnym do przedstawienia wyników testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

7. W przypadku sprawdzeń nieprzewidzianych w planie, w sytuacji powzięcia wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia, informuje się Administratora Danych Osobowych, o tym fakcie, a ten zleca przeprowadzenie sprawdzenia doraźnego.

8. W ciągu 30 dni od dnia zakończenia sprawdzenia, sporządza się sprawozdanie i przekazuje się je Administratorowi Danych Osobowych.

Rozdział 4

Udzielanie upoważnień do przetwarzania danych osobowych i ewidencja osób upoważnionych

§ 10. Udzielając dostępu do przetwarzania danych osobowych stosuje się zasadę wiedzy koniecznej polegającą na dostępie do danych niezbędnych do wykonywania służbowych obowiązków.

§ 11. 1. Dostęp do danych osobowych mają osoby uprawnione na podstawie imiennego pisemnego upoważnienia do przetwarzania danych osobowych, z zastrzeżeniem ust. 2.

2. W szczególnie uzasadnionym przypadku, do czasu uzyskania pisemnego upoważnienia do przetwarzania danych osobowych, o którym mowa w ust. 1, dostęp do danych osobowych

mogą mieć osoby, którym Administrator Danych Osobowych udzielił ustnego upoważnienia na wniosek kierującego komórką organizacyjną MŚ.

3. W przypadku określonym w ust. 2 kierujący komórką organizacyjną MŚ, zobowiązany jest niezwłocznie mailowo poinformować o tym fakcie Inspektora Ochrony Danych oraz wystąpić o udzielenie pisemnego upoważnienia do przetwarzania danych osobowych zgodnie z § 12.

§ 12. 1. Upoważnienie do przetwarzania danych osobowych jest udzielane przez Administratora Danych Osobowych bądź osobę przez niego wskazaną.

2. Do złożenia wniosku o udzielenie upoważnienia przez Administratora Danych Osobowych jest zobowiązany właściwy kierujący komórką organizacyjną w MŚ, w której zatrudniony jest pracownik objęty wnioskowaniem, zastępca kierującego, bądź osoba przez niego upoważniona.

3. Upoważnienie do przetwarzania danych osobowych, z wyłączeniem przypadku, o którym mowa w ust. 5, jest udzielane na podstawie wniosku, zatwierdzonego przez kierującego komórką organizacyjną w MŚ, z zastrzeżeniem ust. 4. Wzór wniosku stanowi załącznik nr 1 do Polityki.

4. W przypadku konieczności udzielenia upoważnienia osobie niebędącej pracownikiem MŚ, wniosek, o którym mowa w ust. 2, zatwierdza kierujący komórką organizacyjną w MŚ, właściwą do realizacji zadania związanego z przetwarzaniem danych osobowych.

5. Administrator Danych Osobowych lub osoba przez niego wskazana udziela upoważnienia do przetwarzania danych osobowych bez wniosku członkom Kierownictwa MŚ, Inspektorowi Danych Osobowych oraz może udzielić upoważnienia do przetwarzania danych osobowych bez wniosku kierownikom komórek organizacyjnych w MŚ i ich zastępcom.

6. Wzór upoważnienia do przetwarzania danych osobowych określa załącznik nr 2 do niniejszej Polityki.

§ 13. 1. W przypadku upoważnienia do przetwarzania danych osobowych w systemie informatycznym, komórka organizacyjna w MŚ przekazuje do Administratora Systemów Informatycznych upoważnienie, o którym mowa w § 12 ust. 1 w celu założenia konta w systemie informatycznym. Administrator Systemu Informatycznego tworzy indywidualne konto użytkownika oraz nadaje identyfikator i hasło. Hasło do systemu informatycznego jest przekazywane przy uruchomieniu konta bezpośrednio użytkownikowi.

2. Administrator Systemu Informatycznego, który nadawał identyfikator osobie upoważnionej po udzieleniu upoważnienia, otrzymuje potwierdzenie tego faktu na skrzynkę mailową lub za pomocą EZD.

3. Właściwy Administrator Systemu Informatycznego po otrzymaniu informacji o udzieleniu upoważnienia, o którym mowa w ust. 2, wydaje osobie upoważnionej identyfikator oraz hasło do konta.

§ 14. 1. Upoważnienie traci moc w przypadku:

1) rozwiązania umowy o pracę;
2) przeniesienia pracownika do innej komórki organizacyjnej MŚ;
3) wygaśnięcia upoważnienia wydanego na czas określony.

2. W przypadkach innych, niż określone w ust. 1, odebranie upoważnienia do przetwarzania danych osobowych odbywa się na wniosek, którego wzór określa załącznik nr 3 do niniejszej Polityki lub na podstawie opinii Inspektora Ochrony Danych.

3. W przypadku upoważnienia do przetwarzania danych osobowych w systemie informatycznym, przekazuje się stosowną informację Administratorowi Systemu Informatycznego, w celu odebrania dostępu do zasobów informatycznych.

4. W przypadku, gdy upoważnienie traci moc na podstawie przesłanek określonych w ust. 1 pkt 1-2, informację o konieczności odebrania dostępu do zasobów informatycznych pozyskiwana jest przez Administratorów Systemu Informatycznego poprzez bazę kadrowo – płacową MŚ.

5. Informuje się właściwego kierującego komórką organizacyjną w MŚ lub pracownika, a w przypadku systemów informatycznych Administratora Systemu Informatycznego o udzielonym upoważnieniu oraz dokonuje stosownych zmian w ewidencji osób upoważnionych do przetwarzania danych osobowych.

§ 15. Prawo dostępu do danych osobowych w systemie informatycznym mogą mieć wyłącznie osoby, którym udzielono upoważnienia do przetwarzania danych osobowych.

§ 16. 1. Cofnięcie upoważnienia do przetwarzania danych osobowych powoduje cofnięcie tego prawa w trybie natychmiastowym.

2. W sytuacji, o której mowa w ust. 1, informuje się kierującego komórką organizacyjną w MŚ o tym fakcie.

3. Prawo dostępu przyznane osobom upoważnionym do danych osobowych przetwarzanych w systemie informatycznym, którzy nie są pracownikami MŚ, ma charakter czasowy i może być przyznane na okres odpowiadający wykonywanemu zadaniu.

§ 17. 1. Upoważnienia do przetwarzania danych osobowych oraz wnioski o cofnięcie upoważnienia są przechowywane w komórce organizacyjnej właściwej w sprawach ochrony danych osobowych.

2. Komórka organizacyjna właściwa w sprawach ochrony danych osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Ewidencja zawiera następujące dane:

1) nazwisko i imię osoby upoważnionej;
2) nazwę komórki organizacyjnej, w której osoba jest zatrudniona lub wykonuje oznaczone czynności na rzecz MŚ lub nazwę instytucji, w imieniu której wykonuje czynności;
3) identyfikator;
4) datę udzielenia lub cofnięcia upoważnienia do przetwarzania danych osobowych oraz zakres upoważnienia do przetwarzania danych osobowych.

Rozdział 5

Zasady przetwarzania danych osobowych

§ 18. 1. Inspektor Ochrony Danych w porozumieniu z kierującymi komórkami organizacyjnymi w MŚ oraz Administratorem Bezpieczeństwa Systemów Informatycznych opracowuje i aktualizuje Rejestr czynności przetwarzania danych osobowych.

2. Dane osobowe są przetwarzane w MŚ tylko i wyłącznie na zasadach określonych w RODO.

3. Dane osobowe w MŚ przetwarzane są wyłącznie w przypadkach, gdy jest to niezbędne do:

1) wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
2) wypełnienia obowiązku prawnego ciążącego na administratorze;
3) ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
4) wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

§ 19. 1. Kierujący komórkami organizacyjnymi, w których zbierane są dane osobowe informują osoby, których te dane dotyczą o:

1) adresie siedziby MŚ;
2) danych kontaktowych Inspektora Ochrony Danych;
3) celach przetwarzania danych osobowych oraz podstawie prawnej przetwarzania;
4) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
5) gdy ma to zastosowanie - zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
6) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;
7) prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
8) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO - prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
9) prawie wniesienia skargi do organu nadzorczego;
10) tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
11) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;
12) celu innym niż cel, w którym dane osobowe zostały zebrane chyba, że przepisy szczególne stanowią inaczej.

2. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, osobę, której dotyczą te dane, należy poinformować ponadto o źródle danych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych.

3. Zasady określone w ust. 1 i 2 nie mają zastosowania w przypadku, gdy:

1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania;
2) osoba, której dane dotyczą, posiada informacje określone w ust. 1 lub 2.

§ 20. 1. Dane osobowe przetwarzane w MŚ są przechowywane przez okres wynikający z obowiązujących przepisów kancelaryjnych w MŚ.

2. Dane osobowe kandydatów do pracy w MŚ zawarte w ofertach zgłaszanych w odpowiedzi na ogłoszenia o naborze na wolne stanowiska pracy oraz staż, praktykę lub wolontariat są przechowywane przez co najmniej 3 miesiące od dnia zakończenia rekrutacji.

3. Po upływie terminu, o którym mowa w ust. 1 i 2, dokumenty zawierające dane osobowe kandydatów do pracy są niszczone zgodnie z § 25.

Rozdział 6

Postępowanie w sytuacji naruszenia ochrony danych osobowych lub ich bezpieczeństwa.

§ 21. 1. Pracownicy MŚ oraz wszystkie osoby, którym zlecono prace związane z dostępem do danych osobowych obowiązane są do natychmiastowego zgłaszania Inspektorowi Ochrony Danych, w każdy możliwy sposób, każdego naruszenia ochrony danych osobowych lub zdarzeń/incydentów będących naruszeniem bezpieczeństwa danych osobowych lub mających wpływ na bezpieczeństwo danych osobowych lub zaistnienia sytuacji, która może wskazywać na naruszenie bezpieczeństwa danych osobowych, w tym w szczególności w zakresie:

1) zabezpieczeń:
   a) systemu informatycznego,
   b) pomieszczeń, kartotek lub szaf, w których znajdują się nośniki danych osobowych;
2) stanu urządzeń, zawartości zbioru danych, ujawnienia metody pracy, sposobu działania programu.

2. Zdarzeniem będącym naruszeniem bezpieczeństwa danych osobowych jest w szczególności:

1) nieautoryzowany dostęp do danych osobowych;
2) nieuprawniona ingerencja w systemie informatycznym;
3) nieautoryzowana modyfikacja lub zniszczenie danych osobowych;
4) udostępnienie danych osobowych podmiotom nieupoważnionym;
5) niezgodne z prawem ujawnienie danych osobowych;

6) pozyskiwanie danych osobowych z nielegalnych źródeł.

3. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

1) niewłaściwe zabezpieczenie:
   a) fizyczne pomieszczeń, urządzeń i dokumentów,
   b) sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
2) nieprzestrzeganie zasad ochrony danych osobowych przez użytkowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

4. Do typowych incydentów bezpieczeństwa danych osobowych należą:

1) zdarzenia losowe:
   a) zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   b) wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych);
2) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

5. Do czasu przybycia Inspektora Ochrony Danych pracownicy MŚ oraz wszystkie osoby, którym zlecono prace związane z dostępem do danych osobowych obowiązane są do:

1) powstrzymania się od rozpoczęcia lub kontynuowania pracy, jak również do podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;
2) zabezpieczenia elementów systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom trzecim;
3) podjęcia wszelkich niezbędnych działań w celu zapobieżenia dalszym zagrożeniom.

6. W przypadku uzyskania informacji o naruszeniu ochrony danych osobowych lub zdarzeniu/incydencie będącym naruszeniem bezpieczeństwa danych osobowych lub mającym wpływ na bezpieczeństwo danych osobowych, Inspektor Ochrony Danych przeprowadza sprawdzenie zgodnie z § 9 ust. 1, w szczególności w celu:

1) minimalizacji negatywnych skutków zdarzenia losowego;
2) wyjaśnienia okoliczności zdarzenia losowego;
3) zabezpieczenia dowodów zdarzenia losowego;

4) umożliwienia dalszego bezpiecznego przetwarzania danych osobowych.

7. Osoba, która dokonała zgłoszenia, o którym mowa w ust. 1 lub osoba, która przetwarza dane osobowe, o którym mowa w zgłoszeniu, podejmuje wraz z Inspektorem Ochrony Danych niezbędne czynności w celu udokumentowania naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

8. W przypadku, gdy w opinii Inspektora Ochrony Danych zgłoszenie narusza ochronę danych osobowych i skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, Inspektor Ochrony Danych powiadamia bez zbędnej zwłoki Administratora Danych Osobowych, który - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu.

9. Inspektor Ochrony Danych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania art. 33 RODO.

10. Inspektor Ochrony Danych zawiadamia osoby, których dane dotyczą, o naruszeniu ochrony danych osobowych zgodnie z art. 34 RODO.

Rozdział 7

Udzielanie informacji o przetwarzanych danych osobowych oraz ich udostępnianie

§ 22. 1. Osobie, której dane są przetwarzane w MŚ, informacji udziela właściwy kierujący komórką organizacyjną w MŚ we współpracy z Inspektorem Ochrony Danych, w sposób określony w RODO.

2. W przypadku wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem RODO lub są zbędne do realizacji celu, dla którego je zebrano, kierujący komórką organizacyjną w MŚ jest obowiązany w szczególności do ich uzupełnienia, uaktualnienia, sprostowania, usunięcia lub ograniczenia przetwarzania.

§ 23. 1. Biuro Dyrektora Generalnego udostępnia dane osobowe pracowników MŚ niezbędne do potwierdzenia zatrudnienia pracownika, wskazanej przez tego pracownika instytucji lub osobie fizycznej, wyłącznie w przypadkach kiedy osoba, której dotyczy potwierdzenie, wyrazi na to pisemną zgodę.

2. Biuro Dyrektora Generalnego udostępnia dane osobowe pracowników MŚ bez pisemnej zgody pracowników, jeżeli jest to niezbędne do zrealizowania uprawnień lub spełnienia obowiązku wynikającego z przepisów ustaw.

3. Wzór zgody stanowi załącznik nr 4 do niniejszej Polityki.

Rozdział 8

Zasady powierzenia przetwarzania danych osobowych podmiotowi przetwarzającemu

§ 24. 1. Administrator Danych Osobowych lub inne osoby upoważnione mogą powierzyć przetwarzanie danych osobowych innemu podmiotowi na zasadach określonych w art. 28 RODO.

2. Projekt umowy powierzenia przetwarzania danych osobowych jest przekazywany do zaopiniowania:

1) Inspektorowi Ochrony Danych;
2) Administratorowi Bezpieczeństwa Systemów Informatycznych - w przypadku, gdy przedmiotem umowy są dane osobowe przetwarzane w systemach informatycznych;
3) kierującemu Departamentem Prawnym.

3. Przed zawarciem umowy powierzenia przetwarzania danych osobowych nie można udostępniać podmiotowi danych osobowych.

Rozdział 9

Usuwanie danych osobowych

§ 25. 1. Dane osobowe usuwa się poprzez:

1) zniszczenie nośników, w tym w szczególności dokumentów papierowych, płyt wielokrotnego zapisu przy użyciu niszczarek;
2) trwałe usunięcie danych osobowych z nośników je zawierających.

2. Usuwanie, o którym mowa w ust. 1, jest przeprowadzane przez:

1) osobę wyznaczoną przez kierującego komórką organizacyjną w MŚ upoważnioną do przetwarzania danych osobowych podlegających zniszczeniu;
2) podmiot, z którym została zawarta umowa, o której mowa w art. 28 RODO;
3) Administratora Systemu Informatycznego, w przypadku danych osobowych, o których mowa w art. 25 ust. 1 pkt 3 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) po otrzymaniu informacji od Inspektora Ochrony Danych Osobowych.

3. Z czynności zniszczenia danych osobowych należy sporządzić protokół. Wzór protokołu stanowi załącznik nr 5 do niniejszej Polityki.

4. Protokół, o którym mowa w ust. 3, kierujący komórką organizacyjną w MŚ przechowuje w aktach sprawy przez okres przechowywania tych akt, a jego kopię przekazuje do wiadomości Inspektora Ochrony Danych.

5. Przepisów ust. 1 i 3 nie stosuje się do niszczenia bieżących kopii roboczych informacji.

6. Nie należy sporządzać protokołu, o którym mowa w ust. 3, w przypadku, gdy niszczeniu ulegają dane osobowe korespondencyjne ze zbioru danych osobowych - Korespondencja.

Rozdział 10

Techniczne środki ochrony danych osobowych

§ 26. 1. Dane osobowe mogą być przetwarzane w MŚ wyłącznie w pomieszczeniach odpowiednio zabezpieczonych przed nieuprawnionym dostępem.

2. W przypadku, gdy kierujący komórką organizacyjną lub pracownik MŚ stwierdzą, że pomieszczenia, w których są przetwarzane dane osobowe nie zapewniają odpowiedniego zabezpieczenia przed nieuprawnionym dostępem, zgłaszają ten fakt Inspektorowi Ochrony Danych.

3. Zabrania się przetwarzania danych osobowych poza siedzibą MŚ, z wyjątkiem danych osobowych znajdujących się na nośnikach mobilnych oraz sprzęcie przenośnym, z zastrzeżeniem ust. 4.

4. Przetwarzanie danych osobowych, poza siecią MŚ, dopuszczalne jest na sprzęcie służbowym.

Rozdział 11

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem w systemach informatycznych

§ 27. 1. Hasło do systemu informatycznego nie może być powszechnie używanymi słowami.

2. Użytkownik systemu informatycznego jest obowiązany zachować hasło w poufności, nawet po utracie przez nie ważności oraz do niezwłocznej zmiany tego hasła, gdy zostało ono ujawnione.

3. Zabronione jest zapisywanie hasła w sposób jawny oraz przekazywanie go innym osobom.

4. Hasło jest zmieniane w sposób automatyczny. W przypadku braku wymuszenia zmiany hasła przez system informatyczny, użytkownik systemu informatycznego jest obowiązany zmieniać hasło samodzielnie w terminie nie dłuższym niż co 60 dni.

5. Hasło składa się z co najmniej 8 znaków, w tym dużych i małych liter oraz z cyfr lub znaków specjalnych. W haśle nie może być zawarty w szczególności: identyfikator, imię lub nazwisko, stanowisko, symbol lub nazwa komórki organizacyjnej użytkownika systemu informatycznego, przewidywalna sekwencja znaków, w tym „QWERTY", „12345678".

6. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. AnnaOOl, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

§ 28. 1. Dane osobowe znajdujące się na nośnikach służących do zapisu i przechowywania informacji, np. zewnętrznych dyskach twardych, pamięciach przenośnych flash, płytach wielokrotnego zapisu, przed udostępnieniem osobom upoważnionym należy zabezpieczyć nadając hasło w programie 7-zip lub w innym równoważnym programie i zapisać w formacie zgodnym z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247).

2. Dane osobowe udostępniane przy pomocy poczty elektronicznej należy przed wysłaniem zabezpieczyć nadając hasło w programie 7-zip lub w innym równoważnym programie i zapisać w formacie zgodnym z Krajowymi Ramami Interoperacyjności (np. zip).

3. Hasła do zabezpieczonych plików należy przekazać odbiorcy pliku ustnie lub innym kanałem komunikacyjnym niż zabezpieczony plik.

4. Przepisów ust. 2 można nie stosować w przypadku udostępniania danych osobowych przy pomocy poczty elektronicznej wewnątrz MŚ z zastrzeżeniem, że podczas wysyłania użytkownik skorzysta z opcji „szyfruj".

§ 29. Dostęp użytkowników systemu informatycznego do wewnętrznych systemów informatycznych, do których nadano im uprawnienia jest możliwy przy zastosowaniu, w szczególności:

1) szyfrowanego tunelem VPN do dedykowanych aplikacji;
2) reguł zdefiniowanych na firewallu MŚ podczas dostępu do poczty elektronicznej.

§ 30. 1. W MŚ stosuje się zabezpieczenia kryptograficzne w celu zapewnienia poufności, integralności, autentyczności i niezaprzeczalności danych przetwarzanych w systemach informatycznych oraz uwierzytelnienia użytkowników, w szczególności:

1) tunele VPN;
2) dostęp do poczty elektronicznej bazujący na protokole SSL;
3) zabezpieczenia kryptograficzne sprzętu komputerowego przenośnego i nośników informacji wynoszonych poza siedzibę MŚ.

2. W sieci VPN eksploatowanej przez MŚ jest stosowane zarządzanie kluczami kryptograficznymi bazujące na certyfikatach.

Rozdział 12

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego

§ 31. 1. Użytkownik systemu informatycznego loguje się do systemu informatycznego przetwarzającego dane osobowe z użyciem identyfikatora i hasła.

2. Użytkownik systemu informatycznego jest obowiązany powiadomić kierującego komórką organizacyjną o próbach logowania się do systemu informatycznego osoby nieupoważnionej, jeżeli system to sygnalizuje. Kierujący komórką organizacyjną powiadamia o tym Administratora Systemu Informatycznego oraz Inspektora Ochrony Danych.

3. Użytkownik systemu informatycznego jest obowiązany do stosowania polityki czystego ekranu, polegającej na uniemożliwieniu osobom niepowołanym - osobom, które nie posiadają upoważnienia do przetwarzania danych osobowych - wglądu do danych osobowych wyświetlanych na monitorach komputerowych.

4. Opuszczając na określony czas stanowisko pracy, użytkownik systemu informatycznego jest obowiązany wywołać blokowany hasłem wygaszacz ekranu, zablokować system lub wylogować się z systemu.

5. Po zakończeniu pracy, użytkownik systemu informatycznego jest obowiązany wylogować się z systemu informatycznego, ewentualnie wyłączyć sprzęt komputerowy oraz

stosować politykę czystego biurka dla dokumentów - wydruków z systemu informatycznego oraz nośników - zawierających dane z systemu informatycznego.

Rozdział 13

Procedury tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 32. 1. W MŚ tworzone są kopie bezpieczeństwa wszystkich systemów, w których przetwarzane są dane osobowe wraz ze środowiskiem.

2. Administrator Systemu Informatycznego przygotowuje i aktualizuje plan wykonywania kopii zapasowych. Plan ten zatwierdza Administrator Bezpieczeństwa Systemów Informatycznych. Częstotliwość oraz zakres wykonywanych kopii zapasowych ustalany jest adekwatnie do celów MŚ i znaczenia archiwizowanych danych dla MŚ w porozumieniu z komórkami organizacyjnymi.

3. Administrator Bezpieczeństwa Systemów Informatycznych lub osoba przez niego wyznaczona prowadzi i aktualizuje rejestr planów wykonywania kopii zapasowych.

§ 33. 1. Kopie całościowe wykonywane są z częstotliwością nie mniejszą niż 90-dniową.

2. Kopie przyrostowe mogą być sporządzane na streamerze, serwerze (mirror), pamięci przenośnej flash lub dysku wymiennym.

3. W przypadku, gdy kopia zapasowa jest wykonywana po raz pierwszy, wymagane jest wykonanie kopii pełnej (całościowej).

4. Każdą kopię należy czytelnie opisać co do zawartości i daty sporządzenia.

5. Dostęp do kopii mają Administrator Bezpieczeństwa Systemów Informatycznych, Administratorzy Systemów Informatycznych oraz pracownicy wyznaczeni przez Administratora Bezpieczeństwa Systemów Informatycznych.

6. Administrator Systemu Informatycznego lub osoba wyznaczona przez Administratora Bezpieczeństwa Systemów Informatycznych w przypadku systemów, dla których nie został wyznaczony Administrator Systemu Informatycznego jest obowiązany do sporządzenia kopii oraz weryfikacji ich poprawności i możliwości ponownego odtworzenia.

7. Niszczenie kopii odbywa się poprzez trwałe fizyczne zniszczenie nośnika lub nieodwracalne usunięcie danych z nośnika z użyciem specjalnego oprogramowania.

8. Administrator Systemu Informatycznego, przed wykonaniem kopii zapasowej, o ile ma to zastosowanie, testuje nośniki, na których zapisane będą dane osobowe, pod względem poprawności ich działania.

Rozdział 14

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

§ 34. 1. Do typowych nośników informacji należą: pamięci przenośne flash, przenośne twarde dyski, płyty z możliwością zapisu danych, przenośne komputery osobiste.

2. Użytkownicy systemu informatycznego są obowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników po ustaniu celu ich przetwarzania na nośnikach informacji.

3. Nośniki należy przechowywać w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczyć je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).

§ 35. Zabrania się przekazywania nośników z nieusuniętymi danymi osobowymi podmiotom lub osobom zewnętrznym (kontrola dostępu osób reprezentujących podmioty zewnętrzne do elektronicznych nośników informacji jest określana w umowie z tymi podmiotami).

§ 36. Zabrania się pozostawiania nośników dostępnych dla osób nieupoważnionych (polityka czystego biurka).

§ 37. 1. Nośniki używane w MŚ powinny być przechowywane zgodnie z zaleceniami producenta.

2.W przypadku ryzyka pogorszenia się stanu nośnika informacji (w tym nośników z kopiami zapasowymi), na którym przechowywane są istotne, wciąż wykorzystywane dane, Administrator Systemu Informatycznego odpowiedzialny za przechowywanie danego nośnika dokonuje przeniesienia danych na nowy nośnik.

3. W przypadku konieczności transportu nośników informacji (w tym kopii zapasowych) należy korzystać z własnego transportu, nadzorowanego przez pracowników MŚ oraz bezpiecznie pakować sprzęt i nośniki, zgodnie z zaleceniami producenta w celu zapewnienia ochrony przez wpływem czynników środowiskowych.

§ 38. 1. Kopie zapasowe, w przypadku, gdy wykonywane są na odrębnych nośnikach, przechowywane są, o ile jest to możliwe, w innym pomieszczeniu niż serwerownia, w sejfie lub w szafie zamykanej na klucz lub w innych ustalonych w planie, odizolowanych od ingerencji zewnętrznej miejscach.

2. W przypadku kopii zapasowych danych osobowych mających szczególną wartość dla organizacji wykonuje się wielokrotne kopie, na oddzielnych nośnikach, które przechowywane są w różnych lokalizacjach, w celu zmniejszenia możliwości utraty istotnych informacji. Ponadto wszystkie kopie zapasowe, o ile to możliwe, przechowywane są w innych lokalizacjach niż dane, z których zostały wykonane.

3. Kopie zapasowe mające szczególną wartość dla organizacji należy przechowywać w miejscach, które minimalizują możliwość ich utraty w przypadku wystąpienia zdarzeń losowych mogących je zniszczyć (np. powódź, pożar, itp.).

4. Za przechowywane kopie zapasowe odpowiedzialny jest Administrator Systemu Informatycznego.

5. Kopie zapasowe przechowywane są przez okres minimum 30 dni.

6. Dostęp do kopii zapasowych jest ograniczony jedynie dla Administratora Bezpieczeństwa Systemów Informatycznych lub kierującego komórką organizacyjną oraz Administratora Systemu Informatycznego danego systemu. W razie potrzeby udostępnienia kopii systemu innemu użytkownikowi systemu informatycznego, kierujący komórką organizacyjną występuje z wnioskiem o zgodę do Administratora Bezpieczeństwa Systemów Informatycznych.

7. W przypadku kopii zapasowej systemu informatycznego pracującego tylko w jednej komórce organizacyjnej, decyzję może podjąć kierujący komórką organizacyjną.

8. Udostępnienie informacji odtworzonych z kopii zapasowej odbywa się pod nadzorem Administratora Systemu Informatycznego obsługującego dany system.

Rozdział 15

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

§ 39. 1. Sieci lokalne MŚ są odpowiednio zarządzane i nadzorowane, aby ochronić je przed zagrożeniami oraz utrzymywać bezpieczeństwo systemów teleinformatycznych i urządzeń sieciowych. Przesyłanie danych pomiędzy lokacjami MŚ, przez sieć publiczną, odbywa się bezpiecznymi kanałami szyfrowania w technologii VPN.

2. Na stacjach roboczych, przenośnych komputerach osobistych, serwerach oraz bramkach pocztowych zainstalowano system antywirusowy wykrywający aplikacje lub

skrypty, których celem jest złośliwe, szkodliwe bądź przestępcze działanie mogące naruszyć poufność, integralność lub dostępność informacji.

3. Otwieranie stron www przez użytkowników systemu informatycznego jest monitorowane a dostęp do wybranych stron zablokowany (np. stron służących do rozrywki, gier sieciowych lub hazardu).

4. Żadne oprogramowanie oraz nośniki danych nie mogą być użyte bez wcześniejszego sprawdzenia przy pomocy odpowiedniego oprogramowania antywirusowego.

Rozdział 16

Sposób realizacji wymogów odnotowania informacji o odbiorcach

§ 40. Użytkownik systemu informatycznego jest obowiązany do odnotowywania w systemie:

1) źródła danych w przypadku zebrania tych danych nie od osoby, której dane dotyczą;
2) informacji o odbiorcach, dacie i zakresie udostępnienia.

§ 41. Nowotworzone systemy informatyczne powinny spełniać wymagania określone w RODO.

Rozdział 17

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

§ 42. 1. Niezbędne procedury eksploatacyjne systemów informatycznych MŚ są udokumentowane, utrzymywane i udostępniane użytkownikom systemu informatycznego. w miarę potrzeby Administrator Bezpieczeństwa Systemów Informatycznych zleca, a Administrator Systemu Informatycznego opracowuje dodatkowe procedury.

2. Przeglądy i konserwacje systemów informatycznych są dokonywane zgodnie z planem lub wytycznymi producentów przez serwis komputerowy MŚ lub podmioty zewnętrzne.

3. Naprawa/konserwacja/serwis sprzętu komputerowego i programów, wykonywane przez podmiot zewnętrzny, powinny odbywać się pod ścisłym nadzorem osób upoważnionych.

4. Administratorzy Systemów Informatycznych okresowo wykonują przeglądy uprawnień użytkowników w celu wykrycia i usunięcia nieaktywnych kont pracowników, którzy zostali zwolnieni lub zakończyli pracę, staż, praktykę, wolontariat.

§ 43. 1. Zmiany w systemach informatycznych podlegają kontroli. Po dokonaniu zmian przeprowadzane są testy i przeglądy aplikacji, aby uzyskać pewność, że wprowadzone zmiany nie mają niekorzystnego wpływu na funkcjonalność, wydajność i bezpieczeństwa systemów informatycznych MŚ.

2. Administrator Bezpieczeństwa Systemów Informatycznych nadzoruje i monitoruje prace rozwojowe nad oprogramowaniem powierzone dostawcom zewnętrznym.

3. Administrator Systemów Informatycznych jest obowiązany do uzyskiwania aktualnych informacji o technicznych podatnościach dotyczących wykorzystywanych przez MŚ systemów informatycznych oraz szacowania stopnia ich narażenia.

Rozdział 18

Odpowiedzialność

§ 44. Nieprzestrzeganie zasad zawartych w Polityce stanowi naruszenie obowiązków pracowniczych, co może skutkować odpowiedzialnością dyscyplinarną lub inną odpowiedzialnością wynikającą z przepisów prawa.

Załączniki
do Polityki Ochrony Danych
Osobowych

Załącznik Nr 1

W Z Ó R

. . . . . .
(identyfikator koszulki)*)

WNIOSEK Kierującego komórką organizacyjną

do przetwarzania danych osobowych w Ministerstwie Środowiska

w systemie: ☐ informatycznym /☐ nieinformatycznym**),

Pani/ Pan: .....

(imię i nazwisko osoby, której ma być udzielone upoważnienie)

nazwa komórki organizacyjnej: .....
zakres dostępu: .....

(należy sprecyzować zakres upoważnienia poprzez wskazanie kategorii danych, rodzaju czynności lub operacji oraz podać nazwę systemu informatycznego i zakres dostępu do tego systemu)

okres obowiązywania upoważnienia***):.....

☐

Data:	Podpis wnioskodawcy kierującego komórką organizacyjną w MŚ

*) -należy wypełnić w przypadku braku pisma przewodniego
**) - właściwe zaznaczyć
***) - należy wskazać datę od której należy udzielić upoważnienia oraz wskazać ewentualną datę końcową

Załącznik Nr 2

W Z Ó R

. . . . . .
(nr upoważnienia)

Warszawa, dnia …… 2020 r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH
W MINISTERSTWIE ŚRODOWISKA

Na podstawie art. 29 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 r., str. 1, z późn. zm.).

Upoważniam

Panią/Pana…….
realizującą/ego obowiązki służbowe w ……..

Ministerstwa Środowiska

do przetwarzania, w ramach pełnionych obowiązków służbowych, danych osobowych
……
…….
(zakres danych/nazwa systemu)
Sposób przetwarzania danych: system tradycyjny, stanowisko komputerowe, mieszany*)

Miejsce przetwarzania danych: w obszarze, poza obszarem*)

Zakres przetwarzania danych: zbieranie, kopiowanie, usuwanie, wprowadzanie, utrwalanie, przechowywanie, zmienianie, odczyt, udostępnianie, bez ograniczeń*)

Upoważnienie wygasa z chwilą rozwiązania umowy o pracę, zakończenia oddelegowania, stażu lub praktyki albo w przypadku zmiany stanowiska pracy*).

Jednocześnie potwierdzam czynności dokonywane we wskazanym powyżej zakresie przez **Panią/Pana ……** od dnia …….....

*) – niewłaściwe skreślić

……
z up. Administratora Danych Osobowych

Załącznik Nr 3

W Z Ó R

. . . . . .
(identyfikator koszulki)*)

WNIOSEK
Kierującego komórką organizacyjną

o odebranie upoważnienia

do przetwarzania danych osobowych w Ministerstwie Środowiska

w systemie: ☐ informatycznym / ☐ nieinformatycznym**),

Pani/Pan: .....

(imię i nazwisko osoby, której ma być odebrane upoważnienie)

Nazwa komórki organizacyjnej:……nr upoważnienia:…….

Data:	Podpis wnioskodawcy Kierującego komórką organizacyjną

Data:	Akceptacja Administratora Danych Osobowych na odebranie upoważnienia:

*) – należy wypełnić w przypadku braku pisma przewodniego
**) – właściwe zaznaczyć

Załącznik Nr 4

W Z Ó R
Warszawa, dnia…….

Zgoda na potwierdzenie zatrudnienia

Ja niżej podpisany(a) ..... ……..wyrażam zgodę na potwierdzenie mojego zatrudnienia następującym instytucjom/osobom fizycznym*):

……...
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...

……..
podpis pracownika

*) - niepotrzebne skreślić

Załącznik Nr 5

W Z Ó R

PROTOKÓŁ ZNISZCZENIA

danych osobowych

W dniu ..... 20 ..... roku zostały zniszczone przez pana/panią..... ……: (imię i nazwisko oraz stanowisko służbowe)

* następujące nośniki:……..zawierające dane osobowe przetwarzane w związku z ..... za okres.....

* dane osobowe, poprzez ich trwałe usunięcie, przetwarzane w związku z .... za okres.....

……

Podpis osoby niszczącej dane osobowe

*) - niepotrzebne skreślić