Regulamin Ochrony Danych Osobowych

odeka
OŚRODEK DOSKONALENIA KADR

Ośrodek Doskonalenia Kadr SIMP
Firma Franszyzingowa Henryk Wojciechowski,
Ul. Toruńska 286, 85-880 Bydgoszcz

Niniejszy regulamin opracowany do celów szkoleniowych stanowi wyciąg najistotniejszych zapisów zawartych w Polityce Bezpieczeństwa. Obowiązuje pracowników etatowych oraz współpracowników (użytkowników), mających upoważnienia do przetwarzania danych osobowych

1 Informacje ogólne.

Informacje ogólne

Dokument jest zgodny z następującymi aktami prawnymi:

Rozporządzeniem 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 (dalej: RODO);

Ustawą z 10 maja 2018 r. o ochronie danych osobowych (Dz. U z 2018 r. poz. 1000)

Wprowadzenie Polityki bezpieczeństwa ochrony danych osobowych reguluje zasady przetwarzania danych osobowych w **ODEKA** reprezentowanego przez **Właściciela** jako „Administrator Danych AD".

Podstawowe definicje:

1. **System teleinformatyczny (STI)** - zespół współpracujących ze sobą według określonych reguł urządzeń, oprogramowania, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
2. **Ryzyko** - prawdopodobieństwo, że określone zagrożenie w połączeniu z podatnością doprowadzi do utraty lub zniszczenia zasobów;
3. **Dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
4. **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie, które można podzielić na dwie grupy:
5. **Ograniczenie przetwarzania** - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
6. **Profilowanie** - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej,

zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

7. **Pseudonimizacja** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
8. **Zbiór danych** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
9. **Administrator Danych (AD)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych – Właściciel ODEKA.
10. **Inspektor Ochrony Danych (IOD)** – osoba powołana przez administratora na podstawie kwalifikacji i doświadczenia odpowiadająca za przestrzeganie procedur w zakresie danych osobowych i zgłoszona do Urzędu Ochrony Danych;
11. **Administrator Systemu Informatycznego (ASI) / Informatyk** - wyznaczony pracownik lub firma zewnętrzna realizująca obsługę IT ODEKA, odpowiedzialny za realizację zadań związanych z zarządzaniem systemem informatycznym, w tym za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów infrastruktury informatycznej oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, a także ich utratą;
12. **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
13. **Zgoda osoby, której dane dotyczą** - oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
14. **Naruszenie ochrony danych osobowych** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
15. **Dane biometryczne** - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
16. **Dane dotyczące zdrowia** - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
17. **Pracownik** – oznacza osobę zatrudnioną w ODEKA niezależnie od podstawy prawnej zatrudnienia (umowa o pracę, umowa cywilno-prawna). Za pracownika uważa się też: praktykanta, stażystę, wolontariusza

Zakres obowiązywania Polityki bezpieczeństwa:

1. Dokument ten dotyczy wszystkich pracowników, a także innych osób mających dostęp do danych osobowych (np. wolontariuszy, stażystów, praktykantów, pracowników firm zewnętrznych realizujących prace w ODEKA).
2. Dokument ma zastosowanie do wszystkich informacji zawierających dane osobowe niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej).
3. Dokument ten dotyczy również wszystkich systemów informatycznych zlokalizowanych w budynkach ODEKA oraz systemów mobilnych będących własnością ODEKA.
4. Polityka jest dokumentem ogólnym w stosunku do dokumentów szczególnych, mających na celu ochronę danych osobowych, do których stosuje się procedury im przypisane.

Podstawy prawne przetwarzania danych osobowych:

Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy spełniony zostanie, co najmniej jeden warunek:

a. osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych,
b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
c. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ODEKA.
d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
e. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym,
f. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ODEKA, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Zasady bezpiecznego użytkowania sprzętu IT

1. Sprzęt IT służący do przetwarzania zbioru danych osobowych składa się z komputerów stacjonarnych oraz przenośnych , serwera, drukarek.
2. Użytkownik zobowiązany jest korzystać ze sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.
3. Użytkownik zobowiązany jest do zabezpieczenia sprzętu IT przed dostępem osób nieupoważnionych a w szczególności zbiorów danych osobowych, które są zainstalowane w komputerze.

4. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
5. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

Podstawowe prawa osób do danych osoby, której dane dotyczą

Prawo do sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych:

a. które są nieprawidłowe,
b. uzupełnienia niekompletnych danych osobowych.

Prawo do sprostowania danych realizowane jest z uwzględnieniem art. 16 RODO.

Prawo do usunięcia danych (prawo do bycia zapomnianym)

1. Osoba, której dane dotyczą, może żądać na podstawie art. 17 RODO w formie wyraźnego oświadczenia usunięcia danych osobowych jej dotyczących, wskazując przedmiotowy zakres żądania.
2. ODEKA ustali okresy przechowywania danych, uwzględniając okres nie dłuższy, niż jest to niezbędne dla celów, w których dane są przetwarzane oraz okres dla przechowywania danych w celach archiwalnych lub statystycznych.
3. ODEKA może przechowywać dane po osiągnięciu pierwotnych celów przetwarzania, pod warunkiem, że ich dalsze przechowywanie znajduje podstawę prawną.

Prawo do ograniczenia przetwarzania danych osobowych

1. Żądanie ograniczenia przetwarzania danych wynika z art. 19 RODO powinno być złożone w formie wyraźnego oświadczenia wskazującego przedmiotowy zakres żądania.
2. Ograniczenie przetwarzania danych ODEKA może realizować w szczególności poprzez ich pseudonimizację.
3. ODEKA może dodatkowo, w celu ograniczenia przetwarzania danych osobowych, w szczególności:
   a. czasowo przenieść wybrane dane osobowe do innego systemu przetwarzania,
   b. uniemożliwić użytkownikowi dostęp do wybranych danych,
   c. czasowo usunąć ze strony internetowej opublikowane dane,
   d. ograniczyć środkami technicznymi przetwarzanie w zautomatyzowanych zbiorach danych w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane.
4. ODEKA może przechowywać dane osobowe, co do których zostało zgłoszone żądanie ograniczenia przetwarzania.

5. Realizacja żądania ograniczenia przetwarzania danych nie powoduje zaprzestania przetwarzania, które jest niezbędne do wykonania obowiązków wynikających z przepisów prawa, zaleceń lub rekomendacji Organu nadzorczego.

Sankcje za naruszenie zasad ochrony danych osobowych:

1. Nieprzestrzeganie zasad zawartych w dokumentach Polityki Bezpieczeństwa, jest naruszeniem obowiązków pracowniczych wynikających w szczególności z Kodeksu Pracy i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie do odpowiedzialności wynikającej z przepisów prawa lub umów.
2. Naruszenie zasad ochrony danych osobowych może spowodować pociągnięcie do odpowiedzialności karnej wynikającej z przepisów:
    a. ustawy o ochronie danych osobowych;
    b. RODO;
    c. kodeksu karnego dot. przestępstw przeciwko ochronie informacji;
    d. przepisów chroniących tajemnice zawodowe.

3. Odpowiedzialność dyscyplinarna lub karna nie zwalnia od dochodzenia roszczeń cywilno – prawnych wynikających z RODO, ustawy o ochronie danych osobowych oraz kodeksu cywilnego

2 Zasady korzystania z oprogramowania

1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi, którego właścicielem jest ODEKA.
2. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na sprzęcie IT na swoje własne potrzeby ani na potrzeby osób trzecich.
3. Instalowanie jakiegokolwiek oprogramowania na sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną.
4. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im za pośrednictwem ASI przez ODEKA. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych prywatnie płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.
5. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną.
6. W przypadku naruszenia któregokolwiek z powyższych postanowień ASI ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie

3 Zasady korzystania z internetu

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.

2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą administratora systemu informatycznego i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”
7. Korzystanie z internetu dla celów prywatnych jest zabronione i nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność systemu informatycznego.
8. Przy korzystaniu z internetu, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego
9. W zakresie dozwolonym przepisami prawa, Właściciel za pośrednictwem IOD lub innych upoważnionych osób lub podmiotów, zastrzega sobie prawo kontrolowania sposobu korzystania przez użytkownika z internetu pod kątem wyżej opisanych zasad.
10. Ponadto, w uzasadnionym zakresie, Właściciel ODEKA zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika w internecie.
11. ASI na wniosek Właściciela lub osób przez niego upoważnionych może również blokować dostęp do niektórych treści dostępnych przez internet.

4 Zasady korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza ODEKA może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania informacji podlegających ochronie prawnej bądź danych osobowych poza ODEKA należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny) lub kompresje plików (dokumentów) z zabezpieczeniem hasłem przesyłanym do adresata innym kanałem łączności.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata
8. Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę, który może zainfekować komputer groźnym wirusem umożliwiającym kradzież danych osobowych lub otwierania załączników o podejrzanej treści, do fałszywych e-maili, w których hakerzy mogą podszyć się pod znanego nadawcę.
6. Nie należy otwierać stron internetowych wskazanych hiperlinkami w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych.
7. Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji ozagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.
8. Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze.
9. Użytkownicy powinni okresowo kasować niepotrzebne maile.
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”.
11. Mail jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
12. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności i prawa autorskiego.
13. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

5 Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie ASI lub osobę upoważnioną.

6 Nadawanie uprawnień do przetwarzania danych osobowych

Kierownicy komórek organizacyjnych, korzystający z sieci komputerowej, odpowiedzialni są za analizę celowości uruchomienia stanowiska, za przygotowanie i przekazanie wniosków o skonfigurowanie stanowiska oraz przydzielenie lub zlikwidowanie konta użytkownikowi, a także zapoznanie podległych im pracowników z treścią zawartą w tej polityce.

1. Utworzenie konta:
   a. Wniosek o założenie / zmianę konta osoba uprawniona przekazuje lub wysyła do Inspektora Ochrony Danych (lub osoby koordynującej ochronę danych z upoważnienia AD).
   b. Następnie wniosek po weryfikacji jest przekazywany Administratorowi Systemu Informatycznego / Informatykowi, który ustanawia parametry konta.
   c. W przypadku negatywnej weryfikacji, wniosek jest odsyłany wnioskodawcy z określeniem przyczyny uniemożliwiającej założenia konta.

d. Administrator Systemu Informatycznego ma prawo zablokować dostęp do funkcji i zasobów systemu w przypadku stwierdzenia niewłaściwego, niezgodnego z treścią wniosku wykorzystywania stanowiska roboczego.

2. Zmiany na koncie:
   a. W przypadku zmiany danych podanych we wniosku osoba bezpośrednio zainteresowana jest zobowiązana złożyć nowy wniosek do AD niezwłocznie od wystąpienia zdarzenia powodującego zmianę.
   b. AD informuje ASI oraz IDO o potrzebie likwidacji konta niezwłocznie od wystąpienia zdarzenia powodującego likwidację konta.
   c. Inspektor Ochrony Danych (lub osoba koordynująca ochronę danych z upoważnienia AD) przekazuje wniosek Administratorowi Systemu Informatycznego.
   d. W przypadku negatywnego rozpatrzenia wniosku, Administrator Systemu Informatycznego, udziela wnioskodawcy odpowiedź z określeniem przyczyny, uniemożliwiającej realizację wniosku.
   e. Administrator Systemu Informatycznego sprawdza wniosek a następnie przekazuje zaakceptowany wniosek do akt osobowych oraz ustala z użytkownikiem nazwę konta.
   f. Administrator Systemu Informatycznego na podstawie wniosku zakłada konto lub zmienia parametry konta i przekazuje użytkownikowi wszystkie dane niezbędne do korzystania z niego, w tym hasło do pierwszego zalogowania.
   g. W przypadku likwidacji konta, Administrator Systemu Informatycznego blokuje konto niezwłocznie lub w terminie podanym we wniosku.
   h. Ostateczne usunięcie konta może nastąpić nie wcześniej niż 12 m-cy po zablokowaniu konta.
   i. Administrator Systemu Informatycznego dokonuje końcowej konfiguracji poczty elektronicznej na komputerze użytkownika (jeżeli wniosek tego dotyczy) i innych niezbędnych elementów potrzebnych użytkownikowi do wykonywania zadań.
   j. Administrator Systemu Informatycznego ma prawo zablokować konto, w przypadku stwierdzenia niewłaściwego, niezgodnego z treścią wniosku wykorzystywania konta.

7 Polityka haseł

1. Użytkownicy stanowisk roboczych są zobowiązani zapoznać się z „Polityką Bezpieczeństwa” oraz chronić przed nieuprawnionym wykorzystaniem wszelkie znane im lub będące w ich posiadaniu dane umożliwiające dostęp do danych osobowych przetwarzanych w sieci informatycznej.
2. Oznacza to m.in. zakaz ujawniania haseł umożliwiających dostęp do kont lub innych zasobów, np. do plików zawierających hasła, klucze szyfrujące, itp.
3. Po otrzymaniu od Administratora Systemu Informatycznego haseł umożliwiających dostęp do konta użytkownik powinien niezwłocznie zmienić te hasła na inne, znane tylko sobie.
4. Hasła powinny spełniać następujące wymagania:

a. minimalna długość hasła powinna wynosić 8 znaków;
b. hasło powinno zawierać duże i małe litery, znaki specjalne oraz cyfry;
c. nie należy używać wyrazów występujących we wszelkiego rodzaju słownikach, nawet jeśli zostaną uzupełnione innymi znakami;
d. nie należy też używać żadnych wyrazów lub liczb występujących w danych personalnych użytkownika;
e. nie należy używać haseł wynikających z układu klawiatury (np.: qwerty);
f. hasło nie może się powtarzać.

5. Hasła nie wolno udostępniać.
6. Nie dopuszcza się zmiany loginu.
7. Niedopuszczalne jest zapisywanie haseł na kartkach przyklejonych do monitora, klawiatury czy biurka.
8. Hasło należy zmieniać co najmniej raz na trzy miesiące o ile nie zastosowano metod autentyfikacji biometrycznej.
9. Posługiwanie się danymi identyfikującymi lub uwierzytelniającymi należącymi do innego użytkownika w celu dostępu do zasobów sieci komputerowej na jego konto lub podejmowania jakichkolwiek innych działań w jego imieniu jest zabronione.

8 Korzystanie z przenośnych komputerów służbowych, nośników i innego sprzętu mobilnego poza siedzibą ODEKA

1. Przemieszczanie nośników lub sprzętu mobilnego zawierających dane osobowe poza pomieszczenia, w których są one przetwarzane, wymaga stosowania środków ochrony gwarantujących ich zabezpieczenie przed nieuprawnionym dostępem i ich ujawnianiem.
2. Na użytkowniku nośnika lub sprzętu mobilnego użytkowanego poza siedzibą ODEKA spoczywa obowiązek jego ochrony. W szczególności zabrania się pozostawiania bez opieki sprzętu mobilnego i nośników w miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nimi skutecznego nadzoru.
3. Za utratę lub zniszczenie nośnika lub sprzętu mobilnego powierzonego do pracy odpowiada dany użytkownik, któremu sprzęt został powierzony. Zaistnienie takiego zdarzenia użytkownik zgłasza do bezpośredniego przełożonego.
4. W przypadku, gdy na sprzęcie mobilnym lub nośniku przetwarzane są dane osobowe należy dodatkowo poinformować ASI / IOD.
5. W zawiadomieniu użytkownik, poza informacjami ogólnymi, podaje okoliczności utraty sprzętu mobilnego lub nośnika oraz zakres utraconych danych osobowych lub informacji wraz z podaniem ich znaczenia dla ODEKA.
6. Sprzęt mobilny podlega szczególnej ochronie. Jego używanie poza siedzibą ODEKA musi mieć uzasadnienie w realizowanych przez użytkownika zadaniach.
7. Zgodę na użytkowanie sprzętu mobilnego poza siedzibą ODEKA wydaje AD na pisemny wniosek przełożonego pracownika użytkującego sprzęt mobilny po zaopiniowaniu wniosku przez ASI.
8. ASI dookreśla okres na jaki sprzęt jest wynoszony oraz odpowiada za jego zwrot w określonym terminie.

9. W przypadku sprzętu mobilnego, w którym przetwarza się dane osobowe dodatkowo potrzebna jest zgoda IOD.
10. Wszelkie dane osobowe przechowywane w sprzęcie mobilnym lub nośniku, które pracują poza siedzibą ODEKA muszą być zaszyfrowane.
11. Każdy użytkownik, któremu powierzono urządzenie przenośne, przed rozpoczęciem użytkowania go poza siedzibą ODEKA, obowiązany jest do wystąpienia do wydziału odpowiedzialnego za utrzymanie i bezpieczeństwo systemu informatycznego z wnioskiem o zapewnienie środków techniczno - organizacyjnych gwarantujących poufność i integralność przetwarzanych informacji. Do środków tych zalicza się w szczególności ochronę antywirusową.
12. Używanie sprzętu komputerowego poza siedzibą ODEKA obliguje użytkownika do stosowania odpowiednich zabezpieczeń, takich jak np. zamykanie szafki, polityka czystego biurka i ekranu, zabezpieczenia dostępu do komputera, uniemożliwienie dostępu do sprzętu osób postronnym (w tym rodzinie, dzieciom).

9 Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe

1. Elektroniczne nośniki, to: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu flash.
2. Nośniki z danymi osobowymi wynoszone poza ODEKA muszą być zaszyfrowane.
3. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe, należy dokonać jego fizycznego zniszczenia lub trwałego usunięcia znajdujących się na nim danych.
4. Przekazywanie nośników z danymi osobowymi powinno być przeprowadzane z uwzględnieniem zasad bezpieczeństwa. Adresat powinien zostać powiadomiony o przesyłce, zaś nadawca powinien sporządzić kopię przesyłanych danych. Adresat powinien powiadomić nadawcę o otrzymaniu przesyłki. Jeżeli nadawca nie otrzymał potwierdzenia, zaś adresat twierdzi, że nie otrzymał przesyłki, użytkownik będący nadawcą powinien poinformować o zaistniałej sytuacji administratora bezpieczeństwa informacji

10 Postępowanie z danymi osobowymi w wersji papierowej

1. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione (użytkownicy) oraz kierownicy właściwych komórek organizacyjnych.
2. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.
3. Użytkownicy są zobowiązani do stosowania „polityki czystego biurka”. Polega ona na zabezpieczaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.
4. Użytkownicy zobowiązani są do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie.
5. Użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

11 Zapewnienie poufności danych osobowych

1. Użytkownik zobowiązany jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych lub zadań zleconych przez Właściciela – AD.
2. Użytkownik zobowiązany jest do niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem o ile nie są one ogólno-dostępne.
3. Użytkownik zobowiązany jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym.

12 Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego lub Inspektora Ochrony Danych (IOD).
2. Do typowych incydentów w obszarze bezpieczeństwa danych osobowych należy:
    a. Niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
    b. Niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
    c. Nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek);

3. Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:
    a. Stwierdzono naruszenie zabezpieczenia systemu ochrony danych osobowych;
    b. Stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

4. Osoba, która stwierdziła lub uzyskała informację wskazującą na naruszenie ochrony tego zbioru/ bazy danych zobowiązana jest do niezwłocznego:

    a. Zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu;
    b. Jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania;
    c. Powiadomienia o tym fakcie ASI

Rejestr Uchybień i Zagrożeń oraz postępowanie osób funkcyjnych.

Kod uchybienia lub zagrożenia	Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne	Postępowanie w przypadku uchybienia lub zagrożenia
1	Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru.	Należy zabezpieczyć dane osobowe oraz powiadomić IOD. IOD sporządza protokół uchybienia.
2	Komputer nie jest zabezpieczony hasłem.	Należy zabezpieczyć dane osobowe oraz powiadomić IOD. IOD sporządza protokół uchybienia.
3	Dostęp do danych osobowych mają osoby nieposiadające upoważnienia.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD. IOD sporządza protokół uchybienia.
4	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym.	Należy powiadomić IOD, który sprawdza za pośrednictwem ASI system uwierzytelniania oraz sprawdza, czy nie doszło do kradzieży lub zniszczenia danych. IOD sporządza protokół uchybienia.
5	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych.	Należy nie dopuścić do kradzieży danych i powiadomić IOD. IOD za pośrednictwem ASI zabezpiecza nośnik danych. IOD sporządza protokół zagrożenia. Należy powiadomić Policję.
6	Próba kradzieży danych osobowych w formie papierowej.	Należy nie dopuścić do kradzieży danych i powiadomić IOD. IOD lub osoba które otrzymała o powyższym informacje zabezpiecza dane. IOD sporządza protokół zagrożenia. Należy powiadomić Policję.
7	Nieuprawniony dostęp do danych osobowych w formie papierowej.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD. IOD sporządza protokół uchybienia.
8	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu.	Należy powiadomić IOD. Osoba odpowiedzialna zabezpiecza pomieszczenie. IOD sporządza protokół uchybienia.
9	Próba włamania do pomieszczenia/budynku.	Należy zabezpieczyć dowody i powiadomić IOD. IOD lub osoba upoważniona sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. IOD sporządza protokół zagrożenia. Należy powiadomić Policję.
10	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania.	Należy zrobić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych, firewall. IOD za pośrednictwem ASI ocenia, czy nie doszło do utraty danych osobowych i sporządza protokół uchybienia lub zagrożenia.
11	Brak aktywnego oprogramowania antywirusowego.	Należy powiadomić ASI. ASI aktualizuje lub nabywa oprogramowanie antywirusowe. IOD sporządza protokół uchybienia.
12	Zniszczenie lub modyfikacja danych osobowych w formie papierowej.	Należy zabezpieczyć dowody i powiadomić IOD. IOD lub osoba upoważniona sprawdza stan uszkodzeń, zabezpiecza dowody. IOD sporządza protokół zagrożenia.
13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym.	Należy zabezpieczyć dowody i powiadomić ASI. ASI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia IOD. IOD sporządza protokół zagrożenia.
14	Uszkodzenie komputerów, nośników danych.	Należy powiadomić ASI. ASI ocenia w wyniku czego doszło do zniszczenia i przywraca dane z kopii zapasowej. ASI powiadamia IOD, który sporządza protokół zagrożenia.
15	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ASI. IOD sporządza protokół uchybienia.
16	Zdarzenia losowe.	Należy oszacować powstałe starty i sporządzić protokół zagrożenia lub uchybienia.

13 Postępowanie dyscyplinarne

1. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
2. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

OŚWIADCZENIE

***dot*.:** zapoznania się z Regulaminem

Oświadczam, że zostałem zapoznany z Regulaminem.
Niezastosowanie się do postanowień przez pracowników niniejszego regulaminu stanowi ciężkie naruszenie obowiązków pracowniczych określonych w art. 100 § 2 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy. Ponadto zarówno w odniesieniu do pracowników ODEKA jak i osób współpracujących powoduje odpowiedzialność cywilno-prawną i karną określoną w przepisach prawa, w szczególności w ustawie o ochronie danych osobowych (art. 107) oraz Kodeksie karnym (art. 266).

L.P.	Imię i nazwisko	Data zapoznania	Podpis

L.P.	Imię i nazwisko	Data zapoznania	Podpis

L.P.	Imię i nazwisko	Data zapoznania	Podpis

L.P.	Imię i nazwisko	Data zapoznania	Podpis

L.P.	Imię i nazwisko	Data zapoznania	Podpis

L.P.	Imię i nazwisko	Data zapoznania	Podpis

L.P.	Imię i nazwisko	Data zapoznania	Podpis