Zarządzenie Nr 04/18
Dyrektora OSiR w Hajnówce
z dnia 27 lipca 2018 r.

w sprawie przyjęcia Polityki ochrony danych osobowych w Ośrodku Sportu i Rekreacji w Hajnówce.

Na podstawie § 5 ust. 2 Regulaminu Organizacyjnego Ośrodka Sportu i Rekreacji w Hajnówce, z dnia 3 grudnia 2012 roku, zarządzam co następuje:

§ 1

Przyjmuje się Politykę ochrony danych osobowych stanowiącą załącznik do niniejszego Zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
mgr Mirosław Awksentiuk

Załącznik
do zarządzenia Dyrektora nr 04/18
Ośrodek Sportu i Rekreacji w Hajnówce
z 27 lipca 2018 r.
w sprawie przyjęcia polityki ochrony danych osobowych

POLITYKA
OCHRONY DANYCH OSOBOWYCH
Ośrodek Sportu i Rekreacji w Hajnówce

Spis treści:

PODSTAWY PRAWNE

§1

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 (ogólne rozporządzenie o ochronie danych).
2. Ustawa z 10 maja 2018 r. o ochronie danych osobowych.

PODSTAWOWE POJĘCIA

§2

1. Administrator – w tym dokumencie jest rozumiany, jako Ośrodek Sportu i Rekreacji w Hajnówce.
2. RODO – w tym dokumencie rozumiane jako rozporządzenie 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)
3. Polityka – w tym dokumencie jest rozumiana jako „Polityka ochrony danych osobowych" obowiązująca u Administratora.
4. Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Administratora (Dyrektora) do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez RODO. IOD powołany jest zarządzeniem Administratora.
5. Użytkownik – osoba upoważniona do przetwarzania danych osobowych. Użytkownikiem może być osoba zatrudniona, wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, porozumienia wolontarystycznego, odbywająca staż.

Cele i zasady funkcjonowania polityki ochrony danych osobowych

§3

Realizując Politykę ochrony danych osobowych informacji zapewnia się ich:

1) poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom;
2) integralność – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany;
3) dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot;
4) rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom;
5) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;
6) niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne;
7) niezawodność – zamierzone zachowania i skutki są spójne;
8) minimalizacji – zbierania jak najmniej danych osobowych i tylko takich jakie są wymagane do realizacji zadań Administratora.

§4

Polityka ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, to jest:

1) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone OSiR;
2) naruszeń przepisów prawa oraz innych regulacji;
3) utraty lub obniżenia reputacji OSiR;
4) strat finansowych ponoszonych w wyniku nałożonych kar.

§5

Realizując politykę w zakresie ochrony danych osobowych Administrator dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

1) przetwarzane zgodnie z prawem,
2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
3) merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów

§6

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem.
Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety, smartfony, telefony, karty pamięci, dyski zewnętrzne, sprzęt do nagrywania itp.
2. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
3. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych.
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
a) wylogować się z systemu informatycznego, a jeśli to wymagane - następnie wyłączyć sprzęt komputerowy,
b) zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe.
7. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
8. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien trwale zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive młotkiem).
9. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez internet zobowiązani są do stosowania zasad bezpieczeństwa.
10. Niedozwolone jest zabezpieczanie służbowych telefonów komórkowych przez użytkowników

blokadami posługującymi się danymi biometrycznymi (np. odciskiem palca, twarzą). Możliwymi do zastosowania zabezpieczeniami są m.in. kod PIN oraz wzór blokady.

Zarządzanie uprawnieniami

§7

1. Każdy użytkownik z dostępem do danych osobowych (np. na swoim komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
2. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonych i przy realizacji informatyków.
3. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień administratora.
4. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest zatem umożliwianie innym osobom praca na koncie innego użytkownika.

Polityka haseł

§8

1. Hasła powinny składać się z m.in. 8 znaków.
2. Hasła powinny zawierać małe i duże litery cyfry i znaki specjalne.
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami.
4. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.
5. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
6. W przypadku ujawnienia hasła – należy natychmiast go zmienić.
7. Hasła muszą być zmieniane co 30 dni.
8. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
9. W przypadku przetwarzania danych we własnych systemach informatycznych (m.in. adresach mailowych w wykupionej domenie, stronach internetowych, aplikacjach) należy stosować uwierzytelnianie co najmniej dwustopniowe (np. podanie loginu oraz hasła + hasła wysłanego wiadomością na podany wcześniej numer telefonu / adres email).

Zabezpieczenie dokumentacji papierowej z danymi osobowymi

§9

1. Pracownicy są zobowiązani do stosowania tzw. „Polityki czystego biurka". Polega ona na zabezpieczaniu (zamykaniu) dokumentów w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na

zewnątrz, np., na terenach publicznych miejskich lub w lesie.
5. W przypadku braku stosownego uprawnienia przewidzianego w obowiązujących przepisach prawa, zabrania się tworzenia oraz przechowywania kopii dokumentów publicznych (np. dowodu osobistego, prawa jazdy) pod rygorem odpowiedzialności karnej przewidzianej w ustawie z dnia 22 listopada 2018 r. o dokumentach publicznych.

Zasady wynoszenia nośników z danymi poza organizację

§10

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora.
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
4. Należy korzystać ze sprawdzonych firm kurierskich (musi zostać zawarta umowa powierzenia przetwarzania danych osobowych).
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.

Zasady korzystania z internetu

§11

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 osoby upoważnionej do administrowania infrastrukturą IT 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:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

Zasady korzystania z poczty elektronicznej

§12

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko

przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązują minimum 4 znaki: litery i cyfry 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. Nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy.
6. Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy.
7. Należy zgłaszać administratorowi przypadki podejrzanych emaili.
8. Użytkownicy nie powinni rozsyłać „niezawodowych" emaili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 230 osób.
9. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!
10. Użytkownicy powinni okresowo kasować niepotrzebne maile.
11. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
12. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
13. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
14. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
15. Użytkownik bez zgody Administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Administratora, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

Ochrona antywirusowa

§13

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Administratora.

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

§14

1. Konserwacja baz danych i oprogramowania przeprowadzana jest przez Administratora Systemu.
2. Konserwacja sprzętu komputerowego przeprowadzana jest przez Administratora Systemu lub firmę zewnętrzną.
3. W przypadku awarii sprzętu, na którym znajdują się dane osobowe w zależności od uszkodzenia następuje:
   a) naprawa na miejscu pod nadzorem Administratora Systemu,
   b) demontowanie dysku i zabezpieczenie u Administratora Systemu na czas naprawy,
   c) przegrywanie danych przez Administratora Systemu na inny nośniki usunięcia danych z przekazywanego do naprawy sprzętu.
4. W przypadku przekazania komputerów innemu użytkownikowi lub jednostce organizacyjnej, dane z dysków twardych są usuwane przez Administratora Systemu w sposób uniemożliwiający ich odtworzenie.
5. W przypadku złomowania sprzętu komputerowego, nośniki informacji (dyski twarde) są fizycznie niszczone przez Administratora Systemu.

Procedura tworzenia kopii zapasowych

§15

1. Kopie całościowe sporządzane są raz w miesiącu.
2. Kopie sporządzane są na płytach dyskach zewnętrznych lub płycie DVD/CD.
3. Każda nośnik jest opisany datą jej sporządzenia.
4. Kopie zapasowe przechowywane są tak długo jak wymagają tego przepisy prawa.
5. Dostęp do kopii mają osoby upoważnione przez administratora.
6. Kopie przechowywane są miejscu zabezpieczonym na terenie siedziby Administratora.

Procedura napraw w serwisach zewnętrznych

§16

1. Komputery przeznaczone do naprawy należy wysyłać bez dysków a urządzenia mobilne bez kart pamięci.
2. W przypadku naprawy sprzętu z danymi osobowymi na nośniku należy je wpierw trwale usunąć z użyciem specjalistycznego oprogramowania
3. W przypadku naprawy sprzętu z danymi osobowymi na nośniku trzeba zawrzeć umowę powierzenia przetwarzania danych osobowych.
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła.
5. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta.

Regulamin użytkowania komputerów przenośnych

§17

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z zasadami użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.
2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Administratora, Użytkownik zobowiązany jest do ich przechowywania

na dysku szyfrowanym, zabezpieczonym co najmniej 8 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).

3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny,

o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Administratora.

4. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych (IOD), zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.

5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:

a) zaleca się przenoszenie go w specjalnym futerale. Dobrym sposobem na zmylenie potencjalnego złodzieja jest przenoszenie komputera przenośnego w zwykłej teczce-aktówce. Sugeruje to przenoszenie dokumentów

a ukrywa fakt transportu komputera przenośnego.

b) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru. W chwili obecnej złodzieje dysponują aparaturą umożliwiającą wykrywanie nawet ukrytych komputerów przenośnych.

c) podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod tylnym siedzeniem kierowcy. Zabrania się przewożenia go np. na siedzeniach, co może skutkować kradzieżą na skrzyżowaniach, przejściach dla pieszych lub w korkach.

6. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp

7. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach

8. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.

9. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Procedura postępowania na wypadek wystąpienia naruszenia ochrony danych

§18

1. Procedura została opracowana w celu zapewnienia sprawnego oraz prawidłowego reagowania na wystąpienie naruszenia ochrony danych. Ma ona zastosowanie do wszelkich danych osobowych przetwarzanych przez Administratora zarówno w jego siedzibie, jak i poza nią.
2. Katalog przykładowych zagrożeń i naruszeń, jakie mogą wystąpić w związku z przetwarzaniem danych znajduje się w załączniku nr 6 do polityki ochrony danych osobowych.
3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Administratora bądź osób przez niego upoważnionych o przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych. Zawiadomienie ma nastąpić bez zbędnej zwłoki, ale w przeciągu 24 godzin od zaistnienia sytuacji.
4. Osoba, która stwierdzi fakt naruszenia ma obowiązek podjąć działania niezbędne do

powstrzymania skutków naruszenia oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn i skutków naruszenia.

5. Administrator podejmuje działania w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków.
6. Administrator przeprowadza analizę pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych (§19). W przypadku stwierdzenia:
   a) braku lub niskiego prawdopodobieństwa wystąpienia ryzyka Administrator zwolniony jest z obowiązku powiadamiania Prezesa UODO oraz osoby, której dane dotyczą o naruszeniu. Wnioski z przeprowadzonej analizy należy odnotować w wewnętrznym rejestrze naruszeń.
   b) wysokiego prawdopodobieństwa wystąpienia ryzyka Administrator ma obowiązek:
      - bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych zgodnie z zasadą przejrzystości. Należy uważać, aby nie wykorzystywać kanału kontaktowego, który w wyniku naruszenia przestał być bezpieczny. Zasadą jest powiadamianie bezpośrednie (np. e-mail, SMS), natomiast gdy wymagałoby to niewspółmiernie dużego wysiłku Administrator powiadamia o naruszeniu komunikatem publicznym lub podobnym środkiem, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane o naruszeniu w równie skuteczny sposób;
      - bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zawiadomić organ nadzorczy (Prezesa UODO). W przypadku nieposiadania przez Administratora w terminie wyznaczonym do udzielenia zgłoszenia wszystkich wymaganych informacji dotyczących naruszenia, zgłoszenie należy sukcesywnie uzupełniać podając przyczyny opóźnienia.
7. Naruszenia związane z atakami phishingowymi Administrator zgłasza również przez stronę www.incydent.cert.pl.

Analiza wystąpienia ryzyka naruszenia praw i wolności osób fizycznych

§19

1. Administrator „stwierdza" naruszenie, kiedy ma on wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, które doprowadziło do naruszenia ochrony danych.
2. Konsekwencją stwierdzenia naruszenia jest konieczność przeprowadzenia analizy pod kątem ryzyka naruszenia praw lub wolności osób, których dane dotyczą. – od tego zależy czy naruszenie będzie podlegało zgłoszeniu do Prezesa UODO.
3. Administrator dokonuje analizy każdorazowo w odniesieniu do konkretnego naruszenia.
4. W ocenie ryzyka naruszenia praw i wolności osób fizycznych konieczne jest uwzględnienie:
   a) powagi zdarzenia tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą
   b) prawdopodobieństwa wystąpienia tego zdarzenia będącego skutkiem naruszenia.
5. Stopień dotkliwości w przypadku zmaterializowania się zagrożenia należy oceniać z perspektywy osób, których dane są przetwarzane.
6. Dla poziomu potencjalnego ryzyka może mieć znaczenie fakt posiadania przez Administratora wiedzy, że dane osobowe znajdują się w rękach osób, których zamiary są nieznane lub które mogą mieć złe intencje.
7. Nie jest konieczne, aby ryzyko się zmaterializowało (by faktycznie doszło do naruszenia). Należy ocenić prawdopodobieństwo zaistnienia szkody w przypadku danego zdarzenia.

8. W przypadku jakichkolwiek wątpliwości Administrator powinien zgłosić naruszenie, nawet jeśli taka ostrożność mogłaby się okazać nadmierna.
9. Ryzyko naruszenia praw lub wolności osób fizycznych powstaje, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Szkodami takimi są np.:
   a) dyskryminacja,
   b) kradzież tożsamości lub oszustwo dotyczące tożsamości,
   c) nadużycia finansowe,
   d) straty finansowe,
   e) nieuprawnione cofniecie pseudonimizacji,
   f) utrata poufności danych osobowych chronionych tajemnicą zawodową,
   g) naruszenie dobrego imienia
   h) lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej.
10. Jeżeli naruszenie dotyczy danych osobowych ujawniających:
   a) pochodzenie etniczne,
   b) poglądy polityczne,
   c) przekonania religijne lub światopoglądowe,
   d) przynależność do związków zawodowych,
   e) dane genetyczne,
   f) dane dotyczące zdrowia,
   g) dane dotyczące życia seksualnego,
   h) dane dotyczące wyroków skazujących lub naruszeń prawa,

   należy uznać, że w występuje duże prawdopodobieństwo takiej szkody. Niemniej jednak każde z takich zdarzeń należy rozpatrywać indywidualnie.
11. Kryteria oceny ryzyka dla osób fizycznych będącego wynikiem naruszenia:
   a) rodzaj naruszenia
   b) charakter, wrażliwość i ilość danych osobowych
   c) łatwość identyfikacji osób fizycznych
   d) waga konsekwencji dla osób fizycznych
   e) cechy szczególne danej osoby fizycznej
   f) cechy szczególne administratora danych
   g) liczba osób fizycznych, na które naruszenie wywiera wpływ.
12. Głównymi kryteriami branymi pod uwagę przy ocenie dotkliwości naruszenia danych osobowych są:
   a) Kontekst przetwarzania danych (KPD) – określa typ naruszonych danych wraz z liczbą czynników związanych z ogólnym kontekstem przetwarzania;
   b) Łatwość identyfikacji (ŁI) – określa jak łatwo można wywnioskować tożsamość osób z danych związanych z naruszeniem;
   c) Okoliczności naruszenia (ON) – określają szczególne okoliczności naruszenia, które są związane z rodzajem naruszenia, w tym głównie z utratą bezpieczeństwa naruszonych danych, jak również wszelkie złośliwe zamiary.
13. Aby zdefiniować wynik dla kontekstu przetwarzania, Administrator danych powinien wykonać następujące kroki:
   a) Określić rodzaje danych osobowych, których dotyczyło naruszenie;
   b) Sklasyfikować dane w co najmniej jednej z czterech kategorii: dane podstawowe, dane szczególnej kategorii, dane finansowe, dane behawioralne (związane z nawykami). W ten sposób otrzymujemy podstawowy wynik KPD;
   c) Punktacja – wynik podstawowy:
      - Dane podstawowe – 1 pkt.,
      - Dane behawioralne – 2 pkt.,

- Dane finansowe – 3 pkt.,
- Dane szczególnej kategorii – 4 pkt.

d) Ocenić występowanie czynników bądź zakresów danych, które zwiększają lub zmniejszają wynik podstawowy.

14. Łatwość identyfikacji ocenia jak łatwo będzie dla strony, która ma dostęp do zestawu danych, jednoznacznie dopasować je do określonej osoby. Wyróżniamy cztery poziomy ŁI: znikome (0,25 pkt.), ograniczone (0,5 pkt..), znaczące (0,75 pkt.) i maksymalne (1,0 pkt.).
15. Przy określaniu okoliczności naruszenia należy brać pod uwagę utratę poufności, integralności i dostępności danych oraz złośliwe zamiary, które uzupełniają KPD I ŁI w następujący sposób:
    a) Utrata poufności następuje, gdy strony uzyskują dostęp do informacji, do których nie są upoważnione. Stopień utraty poufności zależy od zakresu ujawnienia, tj. potencjalnej liczby i rodzaju stron, które mogą mieć bezprawny dostęp do informacji.
    b) Utrata integralności występuje, gdy oryginalna informacja jest zmieniona i zastąpiona, a zmienione informacje mogą być szkodliwe dla jednostki.
    c) Utrata dostępności następuje, gdy nie można uzyskać dostępu do oryginalnych danych. Sytuacja może być czasowa lub trwała.
    d) Złośliwy zamiar to element, który określa, czy naruszenie było spowodowane błędem czy też działaniem zamierzonym. Obejmuje to przypadki kradzieży i włamania, jak również przekazywanie danych osobowych osobom trzecim w celu osiągnięcia zysku. Złośliwe intencje to czynnik, który zwiększa prawdopodobieństwo, że dane są wykorzystane w szkodliwy sposób dla jednostki. W zależności od rodzaju okoliczności naruszenia przyznajemy wartości 0, 0,25 lub 0,5.
16. Końcowy wynik oceny dotkliwości naruszenia oblicza się wzorem (DN): DN = KPD x ŁI + ON. Wyliczony wynik:
    a) Niski: $DN < 2$
    b) Średni: $2 \leq DN < 3$
    c) Wysoki: $2 \leq DN < 3$
    d) Bardzo wysoki: $4 \leq DN$

    należy odnotować w rejestrze naruszeń.

Obowiązek zachowania poufności i ochrony danych osobowych

§20

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
    a) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach,
    b) zachowania w tajemnicy danych osobowych do których mam lub będzie miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora,
    c) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora,
    d) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
    e) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.
3. Osoby zapoznane z treścią Polityki lub przeszkolone zobowiązane są podpisać oświadczenie o poufności.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom

nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.

5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
6. Na podstawie art. 30 ust. 4 RODO w związku z art. 4 pkt 21 RODO zabrania się udostępniania rejestru czynności przetwarzania danych osobowych innym podmiotom niż organowi nadzorczemu, którym jest Prezes Urzędu Ochrony Danych Osobowych.
7. W przypadku gdy podmiot jest podmiotem przetwarzającym (np. w ramach projektu realizowanego ze środków europejskich) dozwolone jest częściowe udostępnienie rejestru kategorii czynności przetwarzania danych osobowych, ale wyłącznie w zakresie fragmentu dotyczącego kontrolowanej czynności.

Postępowanie dyscyplinarne

§21

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Administratora za naruszenie przepisów karnych zawartych RODO i ustawie.

Polityka kluczy

§22

1. Polityka kluczy obejmuje pomieszczenia Administratora.
2. Klucze do pomieszczeń posiadają jedynie osoby upoważnione przez Administratora i mogą je zabierać po zakończeniu pracy. Trzeba jednak dochować wszelkiej staranności, tak by nie zostały one skradzione lub zgubione.
3. Klucze zapasowe przechowywane są w określonym miejscu. Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą Administratora. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić.
4. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane oraz schowane w miejscu zabezpieczonym.
5. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność.
6. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
7. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
8. Po zakończeniu pracy, pracownicy są zobowiązani do zabezpieczenia pomieszczeń a w szczególności (wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych, wyłączenia oświetlenia, zabezpieczenia i zamknięcia okien i drzwi.
9. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 kodeksu pracy oraz z art. 363 § 1. kodeksu cywilnego.

Udostępnianie i powierzanie danych osobowych

§23

1. Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.
2. Administrator odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.
3. Powierzenie danych może nastąpić wyłącznie w drodze pisemnej umowy, w której podmiot przyjmujący dane zobowiązuje się do przestrzegania obowiązujących przepisów RODO. Umowa powinna zawierać informacje o podstawia prawnej powierzenia danych, celu i sposobie ich przetwarzania.
4. Powyższe regulacje nie dotyczą dziennikarzy zatrudnionych u administratora.

Obowiązek informacyjny i wyrażenie zgody

§24

1. Każdy pracownik, który zbiera dane osobowe w imieniu administratora, jest zobowiązany do przekazania zainteresowanemu obowiązku informacyjnego.
2. Dedykowany obowiązek informacyjny powinien być zamieszczony w każdym miejscu, gdzie są zbierane dane osobowe (np. na stronie internetowej, w postępowaniu przetargowym, w formularzach zgłoszeniowych).
3. Zaleca się, by obowiązek informacyjny oraz zgoda na przetwarzanie danych osobowych była, o ile to możliwe, zawsze podpisana przez osobę, której dane dotyczą.
4. Jeżeli dane osobowe zostały pozyskane w inny sposób niż od osoby, której dane dotyczą, obowiązek informacyjny należy przedstawić tej osobie:
- w rozsądnym terminie po uzyskaniu danych osobowych – najpóźniej w ciągu miesiąca,
- jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji, z tą osobą, nie później niż w ciągu miesiąca,
- jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu, nie później niż w ciągu miesiąca.
5. Użyte w art. 81 ust. 2 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych „zgromadzenie" jest pojęciem ocennym, które należy interpretować w oparciu o dany stan faktyczny. Rozpowszechnianie wizerunku danej osoby nie wymaga wyrażenia przez nią zgody, jeśli stanowi on jedynie element akcydentalny lub akcesoryjny przedstawionej całości, tzn. w razie usunięcia wizerunku nie zmieniłby się przedmiot i charakter przedstawienia.

Procedura usuwania i prostowania danych

§25

1. Pracownicy Administratora usuwając dane osobowe muszą skorzystać:
a) w przypadku danych przetwarzanych w formie papierowej (np. dokumenty, ale też wszelkie notatki, kalendarze itp.) wykorzystując niszczarkę,
b) w przypadku danych zapisanych na nośnikach danych, należy postąpić zgodnie z §14 ust. 4.
2. Jeżeli do Administratora wpłynie wniosek o usunięcie danych, to po sprawdzeniu czy dane osobowe nie są niezbędne:
a) do korzystania z prawa do wolności wypowiedzi i informacji;
b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania

realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
e) do ustalenia, dochodzenia lub obrony roszczeń
usuwa je zgodnie z zapisami ust. 1.
3. Jeżeli zachodzi jedna z przesłanek, opisanych w ust. 2, Administrator odmawia usunięcia danych.
4. Przez wniosek o usunięcie danych rozumie się również otrzymaną wiadomość e-mail, która nie zawiera treści.
5. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
6. W przypadku opisanym w ust. 4 Administrator wprowadza niezbędne zmiany w danych, w posiadaniu, których jest.
7. Administrator zwraca uwagę na różnice w okresach retencji danych osobowych w stosunku do danych przetwarzanych za pomocą różnych środków (elektronicznych, papierowych) i usuwa je po upływie określonego okresu, zgodnie z przepisami prawa lub umowami powierzenia przetwarzania danych.
8. Administrator oraz osoba wyznaczona (np. osoba zajmująca się archiwizacją) ponoszą odpowiedzialność za przestrzeganie okresów retencji (archiwizacji) dokumentacji zawierającej dane osobowe i usuwanie jej w terminie zgodnym z obowiązującymi przepisami prawa lub w przypadku braku takich uregulowań, z ustalonymi okresami niezbędnymi do realizacji celów, dla których dane są przetwarzane.

Identyfikacja obszarów wymagających szczególnych zabezpieczeń

§26

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka, stosuje się wysoki poziom bezpieczeństwa. Poziom ryzyka wyniósł 23,61, co stanowi niskie ryzyko. IOD przeprowadza okresową (nie rzadziej niż raz na sześć miesięcy) analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawiają Administratorowi propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

Załączniki

Załącznik nr 1 – Rejestr osób upoważnionych do przetwarzania danych osobowych.
Załącznik nr 2 – oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami
Załącznik nr 3 – Raportu z naruszenia bezpieczeństwa danych osobowych.
Załącznik nr 4 - Rejestr naruszeń ochrony danych osobowych.
Załącznik nr 5 - Wzór upoważnienia do przetwarzania danych osobowych.
Załącznik nr 6 - Rejestr zawartych umów powierzenia przetwarzania danych osobowych.
Załącznik nr 7 - Katalog przykładowych naruszeń.