KODEKS DOBRYCH PRAKTYK RODO

W

Łódzkim Zakładzie Usług Komunalnych

ZATWIERDZAM
Dyrektor Łódzkiego Zakładu
Usług Komunalnych

Wojciech WOLSKI

Dnia 25.03.2019 r.

INSPEKTOR OCHRONY DANYCH OSOBOWYCH
prawnik Erwin RYTER

INSTRUKCJA 1

Wytyczne dla pracownika/osoby współpracującej (zwanej dalej pracownikiem/użytkownikiem) w Łódzkim Zakładzie Usług Komunalnych (zwanej danej ŁZUK) związane z przetwarzaniem danych osobowych

Zasady i poziomy bezpieczeństwa

Wszystkie osoby zatrudnione w ŁZUK zobowiązane są do zachowania odpowiedniego poziomu bezpieczeństwa korzystania z Systemów Informatycznych(dalej „SI") i Urządzeń Informatycznych (dalej „UI"), a w szczególności do przestrzegania poniższych zasad:

1)Do wszelkich SI i UI dostęp posiadają tylko upoważnione osoby, zgodnie z zasadami panującymi w ŁZUK. Wszelkie odstępstwa powinny być zgłaszane do Administratora Danych Osobowych reprezentowanego przez każdorazowego dyrektora ŁZUK lub inną wskazaną przez niego osobę.

2) Wykorzystywanie SI i UI powinno być zawsze zgodne z zaleceniami ADO w tym tylko w celach służbowych.

3)Użytkownik zobowiązany jest do zachowania należytej staranności przy obsłudze SI i UI,

4)W celu zachowania wysokiego poziomu bezpieczeństwa korzystanie z SI i UI w celach prywatnych jest dozwolone tylko za zgodą ADO.

5) Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym

Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest do sprawdzenia urządzenia , którego używa podczas wykonywania pracy oraz swojego stanowiska pracy w szczególności pod kątem okoliczności wskazujących na możliwość naruszenia ochrony danych osobowych, w razie stwierdzenia takowego naruszenia niezwłocznie powinien o tym poinformować ADO lub bezpośredniego przełożonego.

Rozpoczęcie pracy (przebieg czynności)

Uruchomienie urządzenia informatycznego i zalogowanie się poprzez podanie swojego identyfikatora i hasła dostępu do systemu operacyjnego (lub dane dostępowe na innych poziomach logowania)

Zapewnienie warunków do dyskretnego podania danych dostępowych.

Uruchomienie aplikacji, wpisując swój identyfikator i hasło dostępu.

Rozpoczęcie pracy.

Zawieszenie pracy (przebieg czynności)

Przy opuszczeniu stanowiska pracy należy dopilnować, aby dane osobowe nie wyświetlały się na ekranie. W takiej sytuacji sugeruje się zablokowanie urządzenia końcowego poprzez zastosowanie wygaszacza ekranu z jego zabezpieczeniem hasłem.

Przy opuszczeniu stanowiska pracy na dłuższy czas, należy wylogować się z aplikacji oraz zablokować urządzenie końcowe.

Zakończenie pracy (przebieg czynności)

Należy wylogować się z aplikacji i zamknąć aplikację.

Należy zamknąć system.

Wyłączyć monitor, jeśli korzystamy z monitora z niezależnym zasilaniem

Należy zabezpieczyć stanowisko pracy, w szczególności nośniki danych, dokumenty i wydruki zawierające dane osobowe.

6) Jeśli przetwarzanie danych osobowych odbywa się z wykorzystaniem komputera lub innych urządzeń przenośnych należy pamiętać o:

a) przechowywaniu urządzenia przenośnego w warunkach zapewniających bezpieczeństwo, tj. zamykanych szafach po zakończeniu pracy, w bagażniku podczas jazdy samochodem (pod żadnym pozorem nie zostawiać na przednim siedzeniu)

b) w przypadku wystąpienia kradzieży lub zgubienia urządzenia przenośnego, pracownik jest zobowiązany natychmiast powiadomić o tym fakcie ADO, a powiadomienie powinno zawierać informacje, jakiego rodzaju dane były na tym urządzeniu przechowywane, oraz czy ewentualny dysk, komputer był szyfrowany.

c) użytkownik podczas transportu urządzenia przenośnego zobowiązany jest do jego zabezpieczenia, a w szczególności:

- zaleca się przenoszenie go w teczce/aktówce, chroniącej jej zawartość oraz niepozostawianie jej bez dozoru
- użytkownik zobowiązany jest do nie pozostawiania urządzeń przenośnych w samochodzie podczas postoju w szczególności parkowania
- podczas jazdy zabrania się przewożenia urządzeń przenośnych na siedzeniach, zaleca się przewożenie ich w bagażniku.
- pracownicy, którzy pracują na urządzeniach przenośnych w miejscach publicznych zobowiązani są chronić wyświetlane na ekranie dane przed wglądem osób nieupoważnionych. W szczególności pomocne są folie zabezpieczające na ekran, które w znacznym stopniu ograniczają wyświetlaną na

ekranie zawartość, należy pamiętać by nie odtwarzać danych na urządzeniach pod monitoringiem ani frontem do osób trzecich.

- jeśli w ŁZUK monitory umiejscowione są w miejscach, które narażone są na wgląd w wyświetlaną zawartość niepowołanych osób, należy pamiętać aby po odejściu od stanowiska pracy włączyć wygaszacz zabezpieczony hasłem tak aby uniemożliwić osobie niepowołanej wgląd do wyświetlonej zawartości

- urządzenia przenośne służące do wykonywania multimedialnych prezentacji poza obszarem przedsiębiorstwa nie powinny zwierać na dyskach danych osobowych.

- w przypadku stwierdzenia pojawienia się wirusa, Pracownik powinien niezwłocznie powiadomić o tym ADO lub inną osobę przez niego wskazaną

7) Pracownik zobowiązany jest do korzystania w infrastrukturze SI i UI tylko z pendrive i innych nośników pamięci, które są własnością i są sklasyfikowane przez ADO oraz widnieją w rejestrze nośników ŁZUK. Zabrania się podłączania do komputera i innych urządzeń wyposażanych w port USB innych nośników, niż te wskazane w zdaniu poprzedzającym. Jeśli skorzystanie z takiego nośnika jest niezbędne, powinno być dokonane po otrzymaniu akceptacji ADO i w wydzielonym od wewnętrznej sieci środowisku po uprzednim przeskanowaniu tego nośnika przez program antywirusowy.

W przypadku, zagubienia urządzenia lub stwierdzenia podejrzenia, iż mogło dojść do wycieku danych w postaci wejścia w posiadanie informacji o danych osobowych przez osoby niepożądane, pracownik jest zobowiązany niezwłocznie powiadomić o tym ADO zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.

Nośniki, zawierające dane osobowe należy przechowywać w miejscach uniemożliwiających dostęp do nich osobom nieupoważnionym.

8) Korzystanie z sieci Internet na UI dozwolone jest wyłącznie w celach służbowych. zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym, lub innym zakazanym przez prawo ze względu na wysokie ryzyko zainfekowania UI

Ustawienia przeglądarki powinny mieć wyłączone w opcjach autouzupełnianie formularzy i zapamiętywanie haseł o czym ADO poinformował wszystkie osoby przetwarzające w jego organizacji dane osobowe

Zgrywanie na UI oraz uruchamianie jakichkolwiek nielegalnych oprogramowań lub pochodzących z nielegalnych źródeł oraz plików pobranych z niewiadomego źródła jest zabronione. Takie operacje powinny być wykonywane za każdorazową zgodą ASI/ADO i tylko w uzasadnionych przypadkach.

Pracownik ponosi odpowiedzialność za szkody spowodowane przez zainstalowanie ściągniętego z Internetu oprogramowania.

9) Korzystanie z poczty elektronicznej (e-mail)

Za poprawność wprowadzenia adresu e-mail odbiorcy odpowiada pracownik. Zaleca się szczególną ostrożność przy jego wprowadzaniu pamiętając o niebezpieczeństwie powstania incydentu/sytuacji zagrożenia dla danych osobowych (w takich wypadkach zastosowanie mają panujące u ADO procedury postępowania na wypadek powstania incydentu)

Nie należy otwierać plików załączonych do nadesłanej przez nieznanego nadawcę korespondencji e-mail, bezwzględnie należy weryfikować nadawcę wiadomości.

10) Ponadto bezwzględnie zabrania się:

Instalowania prywatnych oraz tych nie pochodzącym z zalecenia ADO programów na UI będących własnością ŁZUK.

Ingerencji w programy oraz UI o czym pracownicy zostali poinformowani

Wynoszenia nośników danych należących do ŁZUK poza jej siedzibę chyba, że są do tego przeznaczone i jest na to zgoda ADO.

Zgrywania na nośniki należące do ŁZUK danych prywatnych oraz podłączania nośników prywatnych do UI w organizacji ADO

Pozostawiania UI w samochodzie podczas postoju w miejscach publicznych.

Pozostawiania urządzenia w miejscach dostępnych dla osób nieupoważnionych.

Wyłączania lub zmiany ustawień oprogramowania antywirusowego.

11) Merytoryczna poprawność danych

Każdy z pracowników powinien pamiętać o zasadzie **merytorycznej poprawności danych osobowych** tj. należy pamiętać aby dane osobowe były poprawne i w razie potrzeby uaktualniane. W związku z tym pracownik powinien zadbać o merytoryczną poprawność danych tak aby ewentualne pismo trafiło do rąk osoby uprawnionej wraz z treścią zgodną i aktualną z obowiązującym stanem faktycznym. W razie zaniedbań dotyczących powyższej zasady ADO może wyciągnąć konsekwencje służbowe wobec pracownika dopuszczającego się takiego niedopełnienia.

12) Zasada Ograniczenia Celu

Dane mają być przetwarzane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

Cele te powinny być określone nie później niż w momencie ich zbierania.

Zasada ta forsuje jeszcze jeden argument tj. brak wskazania celu powoduje niemożność przetwarzania danych osobowych.

Cel ma być konkretny i wyraźny, aby można było określić jakie operacje przetwarzania danych są nim objęte.

13) Prawo dostępu do danych

Osoba, której dane dotyczą ma prawo do uzyskania od ADO potwierdzenia , czy przetwarzane są jej

dane osobowe a jeśli tak to jest uprawniona do uzyskania dostępu do nich oraz do informacji takich jak:
a) cele przetwarzanie
b) kategorie danych
c) informacje o odbiorcach lub kategoriach odbiorców, którym dane zostaną udostępnione
d) planowany okres przechowywania / kryteria ustalania tego okresu
e)informacji o przysługujących prawach np. pr. do sprzeciwu/ ograniczenia przetwarzania etc.
f) informacje o prawie wniesienia skargi do organu nadzorczego
g) jeżeli dane nie pochodzą od osoby , której dotyczą to wszelki informacje o ich źródle
h) informacje o profilowaniu
Administrator za pierwszym razem dostarcza danej osobie kopię danych za kolejne dostarczenie może doliczyć "rozsądną" cenę (forma elektroniczna lub tradycyjna)
14) Prawo do sprzeciwu
Osobie , której dane są przetwarzane przysługuje prawo do sprzeciwu co oznacza zakaz dalszego przetwarzania danych przez ADO chyba, że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia dochodzenia lub obrony roszczeń.
15) Prawo do sprostowania danych
Osoba, której dane dotyczą ma prawo żądania **sprostowania** dotyczących jej osoby danych , które są **nieprawidłowe**.
Osoba ta ma prawo żądania uzupełnienia **niekompletnych** danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Należy pamiętać iż w razie zgłoszenia swoich praw tj. chęci skorzystania przez osobę fizyczną z przysługujących jej praw zawsze należy o tym poinformować osobę pod, której kierownictwem jest użytkownik oraz Administratora Danych Osobowych

16) Incydent
Przez incydent rozumiemy: pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
Można wyróżnić trzy zasadnicze grupy incydentów w ochronie danych osobowych:
umyślne incydenty (np. kradzież danych i sprzętu, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie danych, włamanie do systemu informatycznego lub pomieszczeń),
zdarzenia losowe wewnętrzne (np. awaria komputera/serwera/dysku twardego/oprogramowania,

pomyłki informatyków, utrata danych),

zdarzenia losowe zewnętrzne (np. pożar, zalanie wodą, utrata zasilania, utrata łączności).

Ponadto na wypadek zaistnienia jednej z niżej wymienionych sytuacji (wskazane przez UODO) pracownik zobowiązany jest niezwłocznie o niej poinformować ADO/IOD, bądź swojego bezpośredniego przełożonego pod rygorem poniesienia odpowiedzialności z tytułu zaniechania powiadomienia

a) Zgubienie lub kradzież nośnika/urządzenia

b) Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

c)Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

d) Nieuprawnione uzyskanie dostępu do informacji

e) Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

f) Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych

g) Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

h) Nieprawidłowa anonimizacja danych osobowych w dokumencie

i) Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

j) Niezamierzona publikacja

k) Dane osobowe wysłane do niewłaściwego odbiorcy

l) Ujawnienie danych niewłaściwej osoby

ł) Ustne ujawnienie danych osobowych

INSTRUKCJA 2

PROCEDURA postępowania w sytuacji wystąpienia incydentu w Łódzkim Zakładzie Usług Komunalnych (zwane dalej ŁZUK)

I. **Postanowienia ogólne**

§ 1

1. Niniejsza procedura określa tryb postępowania w przypadku stwierdzenia wystąpienia incydentu lub powzięcia podejrzenia o możliwości jego wystąpienia.

2. Niniejsza procedura jest wewnętrznym dokumentem zawierającym wytyczne postępowania dla ŁZUK i jest przeznaczona dla pracowników oraz osób współpracujących, które mają do czynienia z przetwarzaniem danych osobowych.

3. Wdrożenie i stosowanie postanowień niniejszej procedury służyć ma wykrywaniu i właściwemu reagowaniu na incydenty w ŁZUK.

§ 2

Zastosowane w niniejszej procedurze, poszczególne definicje oznaczają:

1. ADO - administrator danych osobowych, tj. Łódzki Zakład Usług Komunalnych reprezentowany przez Dyrektora.

2. ASI - administrator systemów informacji

3. IOD – inspektor ochrony danych osobowych

3. Użytkownik - osoba upoważniona przez administratora do przetwarzania danych osobowych

4. System - system informatyczny tj. zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

5. Zabezpieczenie systemu informatycznego – wdrożenie przez administratora stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz w celu zapewnienia ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez osobę nieuprawnioną.

6. Przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie, a zwłaszcza tych, które są wykonywane w systemach informatycznych.

7. Incydent - to wszelkie naruszenie danych osobowych, które zgodnie z art. 4 pkt. 12 RODO 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.

8. UODO – Urząd Ochrony Danych Osobowych, organ do którego zgłasza się incydenty.

§ 3

1.Naruszenie ochrony danych osobowych, może być spowodowane następującymi sytuacjami:

a) niewłaściwym oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, wirusy komputerowe, skutki powodzi, pożaru, itp.;

b) niekontrolowanym działaniem osób trzecich, powodującym zakłócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych osobowych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu;

c) umyślnym lub nieumyślnym działaniem, a nawet zaniechaniem działania użytkowników przetwarzających dane osobowe.

2. Do typowych incydentów bezpieczeństwa danych osobowych należą:

a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);

b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych);

c) 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).

3. W przypadku stwierdzenia wystąpienia zagrożenia, ADO w porozumieniu z IOD prowadzi postępowanie wyjaśniające, w toku którego:

a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;

b) inicjuje ewentualne działania dyscyplinarne;

c) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;

d) dokumentuje prowadzone postępowania.

4. Za naruszenie ochrony danych osobowych uważa się w szczególności następujące sytuacje:

a) brak możliwości fizycznego dostępu do danych np. zagubiony klucz lub karta do pomieszczenia, bądź do mebli biurowych, w których przechowywane są dokumenty, zniszczona szafa z dokumentami, brak nośników informacji, zalane pomieszczenie, brak sprzętu komputerowego itp.;

b) brak dostępu do zawartości zbioru danych – zbiór istnieje, lecz nie można go otworzyć, ani uzyskać do niego dostępu;

c) zmienioną zawartość zbioru, niepoprawną treść, postać, data, różnicę w danych itp.;

d) próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia, w którym jest przetwarzany np. zmiana ułożenia kolejności dokumentów, otwarte drzwi lub meble biurowe, nietypowe ustawienie sprzętu lub pojawienie się nowych dokumentów;

e) różnicę funkcjonowania systemu, a w szczególności wyświetlania komunikatów i informacji o błędach oraz nieprawidłowościach w wykonywaniu operacji;

f) zniszczenie lub próby zniszczenia, w sposób nieautoryzowany danych ze zbioru lub danych systemowych;

g) zmianę lub utratę danych zapisanych na kopiach awaryjnych lub zapisach archiwalnych;

h) nieskuteczne niszczenie nośników informacji zawierających dane osobowe (dyskietki, nośniki optyczne, wydruki papierowe), umożliwiające ponowny ich odczyt przez osoby nieuprawnione;

i) próba nielegalnego logowania się do systemu lub włamania do systemu;

j) zmienione oprogramowanie systemu, stwierdzone przez użytkownika po przerwie w przetwarzaniu danych.

5. Niniejszą procedurę stosuje się także w przypadku stwierdzenia, że stan pomieszczeń i szaf, bądź mebli biurowych, w których przechowuje się dokumentację lub zawartości tej dokumentacji wzbudzają podejrzenie, lub że dostęp do nich mogły mieć osoby trzecie i nieuprawnione.

II. Zabezpieczenie przed naruszeniem obszaru przetwarzania danych osobowych

§ 4

1.Dane osobowe przetwarza się w pomieszczeniach lub częściach pomieszczeń ŁZUK, zgodnie z wytycznymi zawartymi w zasadach ochrony danych.

2. Przebywanie osób nieuprawnionych wewnątrz obszaru, w którym są przetwarzane dane jest możliwe tylko w obecności użytkownika i za zgodą administratora danych osobowych.

3. Budynki lub pomieszczenia, w których przetwarzane są dane, powinny być zamykane na czas nieobecności użytkowników, w sposób uniemożliwiający do nich dostęp osób trzecich i nieuprawnionych.

§ 5

Zabezpieczenie systemu informatycznego, w zakresie nieuwzględnionym w niniejszej Instrukcji, reguluje „instrukcja określająca sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych w ŁZUK.

III. Kontrola przestrzegania zasad zabezpieczenia systemu ochrony danych osobowych

§ 6

1.Codzienną kontrolę w zakresie ochrony danych osobowych sprawuje każdy użytkownik.

2. Nadzór nad przestrzeganiem zasad ochrony danych osobowych w komórce organizacyjnej sprawuje ADO w porozumieniu z IOD.

3. ASI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych, przetwarzanych w systemach informatycznych i określonych niniejszą procedurą oraz dokonuje stałych kontroli i oceny funkcjonowania mechanizmów technicznych zabezpieczeń systemów, w których przetwarzane są dane osobowe.

IV. Postępowanie w przypadku naruszenia zabezpieczenia systemu ochrony danych osobowych i wystąpienia incydentu

§ 7

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony, o których mowa w § 3 niniejszej procedury, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie ADO/IOD oraz ASI lub osobę upoważnioną przez administratora danych osobowych.

§ 8

1.W razie podejrzenia wystąpienia lub stwierdzenia, że doszło do wystąpienia incydentu i naruszenia bezpieczeństwa danych osobowych każdy użytkownik do momentu powiadomienia i przybycia ADO/IOD lub osoby przez niego upoważnionej jest zobowiązany w trybie niezwłocznym do:

a) zabezpieczenia dostępu do pomieszczenia lub urządzenia;

b) powstrzymania się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony;

c) zatrzymania pracy na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiania innych urządzeń, które mogą mieć związek z naruszeniem ochrony;

d) podjęcia, stosownie do zaistniałej sytuacji działań, które zapobiegną ewentualnej utracie danych osobowych.

§ 9

1.ASI oraz ADO/IOD po otrzymaniu informacji o naruszeniu lub próbie naruszenia zabezpieczenia systemu przetwarzającego dane osobowe, podejmuje działania zmierzające do usunięcia powstałego zagrożenia.

2. Po przybyciu na miejsce, o którym mowa w ust. 1 § 8, ADO/IOD realizuje czynności w kolejności:

a) ocenia sytuację, uwzględniając stan pomieszczenia, w którym przetwarzane są dane, stan urządzenia i zbioru oraz identyfikuje zakres negatywnych następstw naruszenia ochrony danych osobowych;

b) wysłuchuje relacji użytkownika lub osoby, która dokonała powiadomienia;

c) podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony;

d) w zależności od zakresu naruszenia ochrony podejmuje decyzje o dalszym postępowaniu, wydając użytkownikowi stosowne polecenia i wskazówki do obsługi urządzeń;

e) biorąc pod uwagę skalę oraz skutki naruszenia ochrony, ADO/IOD decyduje o powołaniu doraźnego zespołu mającego ograniczyć rozmiar i skutki powstałego incydentu.

§ 10

1.W przypadku naruszenia ochrony danych osobowych (wystąpienia incydentu), ADO bez zbędnej zwłoki – w miarę możliwości, **nie później niż w terminie 72 godzin po stwierdzeniu naruszenia** – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (art. 33 ust. 1 RODO).

2. **Naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych** skutkować powinno – po uprzednim przeanalizowaniu tego przypadku przez ADO - zgłoszeniem incydentu do organu nadzorczego, jednak nie każdy przypadek wykrycia uchybienia przepisów regulujących ochronę danych osobowych, będzie wiązał się z obowiązkiem notyfikacji. Przykładowo naruszeniem ochrony danych osobowych **nie będzie** błędne (niepełne) wypełnienie obowiązku informacyjnego, bądź wadliwie skonstruowanie zgody jako podstawy prawnej przetwarzania danych osobowych.

3. Obowiązek notyfikacji, jest związany z takim zdarzeniem którego efektem jest **naruszenie bezpieczeństwa przetwarzanych danych**, z tym zastrzeżeniem, że naruszenie powinno prowadzić do wystąpienia określonego w art. 4 pkt 12 RODO skutku (np. utracenia danych), przy czym nie ma znaczenia, czy naruszenie związane było z działaniem przypadkowym, czy niezgodnym z prawem.

4. Zgodnie z motywem 85 RODO brak odpowiedniej i szybkiej reakcji na naruszenie ochrony danych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych takich **jak utrata kontroli nad własnymi danymi, ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa** itp.

5. Przekroczenie terminu wskazanego w pkt. 1 § 10 obliguje administratora do wyjaśnienia w UODO przyczyn opóźnienia zgłoszenia incydentu.

6. Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

7.Zgłoszenia naruszenia dokonuje się elektronicznie za pomocą odpowiedniego formularza dostępnego na stronie UODO.

V. Postanowienia końcowe

§ 11

1.Każdy użytkownik przetwarzający dane osobowe w zbiorach ŁZUK zobowiązany jest zapoznać się z niniejszą procedurą i stosować się do jej wytycznych.

2. Niestosowanie się przez użytkownika do postanowień niniejszej procedury może doprowadzić do pociągnięcia go do odpowiedzialności dyscyplinarnej, prawnej, jak również odszkodowawczej, bądź karnej, w trybie i na zasadach przewidzianych przepisami prawa.

3. W sprawach nie uregulowanych niniejszą procedurą zastosowanie znajdują przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018, poz. 1000) oraz RODO - 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 /Dz. Urz. UE.L nr 119, str. 1.)

INFORMACJE DLA PRACOWNIKÓW

ŁÓDZKIEGO ZAKŁADU USŁUG KOMUNALNYCH

1. Łódzki Zakład Usług Komunalnych informuje Panią/Pana, że:

- administratorem Pani/Pana danych osobowych jest Dyrektor Łódzkiego Zakładu Usług Komunalnych, zwany dalej Pracodawcą;
- Pani/Pana dane przetwarzane są na podstawie art. 6 ust. 1 lit. b i c Ogólnego rozporządzenia o ochronie danych osobowych z 27 kwietnia 2016 r., dalej RODO, w celu realizacji umowy o pracę oraz wypełnienia obowiązków wynikających z obowiązujących przepisów związanych z rolą pracodawcy;
- Pracodawca nie udostępnia ani nie przekazuje Pani/Pana danych osobowych do państwa trzeciego/organizacji międzynarodowej;
- przysługuje Panu/Pani prawo dostępu do swoich danych, ich poprawiania, sprostowania, usunięcia (w zakresie wskazanym przez RODO), ograniczenia przetwarzania, przeniesienia oraz wniesienia skargi do organu nadzorczego;
- Pani/Pana dane osobowe nie będą podlegać zautomatyzowanemu przetwarzaniu, w tym profilowaniu; chyba że zajdą uzasadnione podstawy prawne,
- podanie danych jest dobrowolne, przy czym niepodanie danych uniemożliwi realizację wskazanego celu,
- przechowywanie dokumentacji pracowniczej odbywa się na zasadach określonych kodeksem pracy i w związku z tym okres przetwarzania danych będzie uzależniony od czasookresu, w którym doszło do zatrudnienia, co przedstawia się następująco:

<u>Pracownicy i zleceniobiorcy zatrudnieni od 1 stycznia 2019 r.</u>

Okres przechowywania dokumentów pracowniczych wynosi 10 lat.

<u>Pracownicy, którzy nawiązali stosunek pracy po 31 grudnia 1998 r. i jednocześnie przed 1 stycznia 2019 r.</u>

Okres przechowywania dokumentów pracowniczych wynosi 50 lat od dnia rozwiązania lub wygaśnięcia stosunku pracy. Skrócenie tego okresu do 10 lat będzie natomiast możliwe po złożeniu przez pracodawcę jednorazowego oświadczenia do ZUS o zamiarze przekazywania raportów informacyjnych z informacjami niezbędnymi do wyliczenia ranty i emerytury wszystkich zatrudnionych w tym okresie pracowników i zleceniobiorców oraz jeśli pracodawca faktycznie złoży te raporty. Złożenie wskazanego oświadczenia ma charakter dobrowolny i może zostać odwołane do czasu złożenia pierwszego raportu informacyjnego. Po rozpoczęciu procesu przesyłania raportów taka decyzja nie będzie mogła zostać zmieniona (dotyczy to wszystkich zatrudnionych pracowników).

Pracownicy zatrudnieni przed 1 stycznia 1999 r.

Okres przechowywania dokumentów pracowniczych wynosi 50 lat od dnia rozwiązania lub wygaśnięcia stosunku pracy. Wynika to z faktu, że za takiego pracownika, pracodawca nie może złożyć raportu informacyjnego.

2. W kwestii Pani/Pana obowiązków zawodowych, z którymi związane jest przetwarzanie danych osobowych pozyskanych przez Pracodawcę, Dyrektor Łódzkiego Zakładu Usług Komunalnych, zobowiązuje Panią/Pana do:

- zapoznania się z obowiązującą dokumentacją ochrony danych osobowych oraz stosowania się do niej, a w razie wątpliwości do konsultowania się z inspektorem ochrony danych osobowych,
- stosowania wszelkich instrukcji oraz zasad dotyczących przetwarzania danych osobowych, w tym nieudostępniania jakichkolwiek danych osobowych osobom trzecim bez zgody pracodawcy, nie wynoszenia żadnych nośników, dokumentów, czy informacji zawierających dane osobowe bez zgody pracodawcy
- niezwłocznego informowania i zgłaszania pracodawcy oraz inspektorowi ochrony danych osobowych wszelkich incydentów związanych z naruszeniem zasad dotyczących ochrony danych osobowych.

3. Jest Pani/Pan zobowiązana/-y do przestrzegania następujących codziennych zasad związanych z obsługą i przetwarzaniem danych osobowych petentów:

- niedozwolone jest kopiowanie dowodu osobistego lub innego dokumentu tożsamości bez konkretnej podstawy prawnej
- należy przestrzegać zasad związanych z dyskretnym przetwarzaniem danych osobowych w obecności innych petentów – obsługiwany klient ma prawo do poufnego przetwarzania jego danych
- udzielanie osobom postronnym/nieupoważnionym jakichkolwiek informacji na temat osoby fizycznej (np. innego klienta, innego pracownika ŁZUK, nawet z grona osób najbliższych osobie pytającej o dane), będzie uznane za naruszenie podstawowych obowiązków pracowniczych i skutkować może nawet dyscyplinarnym zwolnieniem pracownika oraz pociągnięciem go do odpowiedzialności odszkodowawczej
- przy realizacji wniosków i spraw petentów, pytania powinny zmierzać jedynie do uzyskania informacji w niezbędnym zakresie
- rozmowa telefoniczna sama w sobie jest przetwarzaniem danych osobowych klienta, więc należy zwracać uwagę na zakres oraz cel udzielanych w czasie rozmowy informacji (nie należy udzielać informacji na temat konkretnych danych osobowych z uwagi na znacznie ograniczoną możliwość weryfikacji rozmówcy i możliwość nagrywania rozmów przez osoby dzwoniące)
- klientom należy udzielać informacji w przejrzystym i dostosowanym do konkretnej sytuacji języku bez nadmiernego formalizmu

- nie należy na tyle głośno powtarzać danych klienta i informacji na jego temat, aby osoby postronne mogły je słyszeć, przy czym nie należy jednocześnie zaburzać normalnego trybu i toku pracy, np. w sytuacji niezrozumiałego podania danych przez klienta można poprosić o zanotowanie danych na kartce (np. obcobrzmiące imię czy nazwisko, niewyraźnie podany numer telefonu itp.).
- swoje obowiązki należy wykonywać w granicach upoważnienia do przetwarzania danych osobowych, a w sytuacjach wątpliwych należy na bieżąco konsultować się z pracodawcą lub inspektorem ochrony danych osobowych
- należy działać z tzw. należytą starannością i świadomością podczas podejmowania określonych czynności i decyzji
- należy weryfikować stan stanowiska pracy przed jej rozpoczęciem i po jej zakończeniu oraz zwracać uwagę na wszelkie budzące wątpliwość sytuacje,
- w przypadku kradzieży, zniszczenia lub zagubienia danych, jak również w sytuacji wystąpienia innych incydentów należy niezwłocznie powiadomić pracodawcę i inspektora ochrony danych osobowych
- wszelkie interwencje w sprawach należy załatwiać wyłącznie w pokojach za zamkniętymi drzwiami i bez udziału osób trzecich
- nie należy wyjaśniać jakichkolwiek spraw na korytarzach, poza pokojami, a zwłaszcza w obecności osób trzecich
- zaleca się aby drzwi do pokojów były zamykane w trakcie wykonywania pracy i prowadzenia rozmów aby nie stwarzać sytuacji, w których przypadkowe lub nieuprawnione osoby znajdujące się na korytarzach, będą słyszeć treść rozmów pracowników ŁZUK

4. Potrzeba przestrzegania „Kodeksu dobrych praktyk RODO w Łódzkim Zakładzie Usług Komunalnych" wynika z następujących okoliczności:

- RODO wymaga aby konkretna podstawa przetwarzania danych wynikała z konkretnego przepisu prawnego
- Pracownicy ŁZUK muszą wiedzieć, że w tym zakresie nie ma dowolności
- Pracownikom ŁZUK nie wolno pozyskiwać danych wedle własnego uznania
- Pracownicy ŁZUK zawsze muszą wskazać podstawę prawną dla każdej procedury związanej z przetwarzaniem danych
- W sytuacji wystąpienia nieprawidłowości i ukarania podmiotu publicznego za niezgodne z RODO przetwarzanie danych, każda nałożona kara może być dodatkowo traktowana jako naruszenie obowiązków służbowych pracownika i dyscypliny budżetowej, co może rodzić indywidualną odpowiedzialność dyscyplinarną, karną lub cywilną.

INSPEKTOR OCHRONY DANYCH (IOD) – NAJWAŻNIEJSZEJ KOMPETENCJE ORAZ PODSTAWY PRAWNE FUNKCJONOWANIA W ORGANIZACJI PUBLICZNEJ

1. Obowiązek powołania IOD w ŁZUK wynika z przepisów RODO, zgodnie z którymi ADO powołuje IOD gdy reprezentowana przez niego organizacja przetwarza dane jako organ lub podmiot publiczny.
2. IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności i zadań określonych w art. 39 RODO.
3. Zgodnie z RODO, IOD ma być pośrednikiem między zainteresowanymi stronami (np. organem ochrony danych osobowych, osobami, których dane dotyczą). Ma pełnić rolę specjalisty, którego funkcję można porównać do niezależności jaką się odznacza radca prawny/prawnik w organizacji.
4. IOD dzieli swoją lojalność między organem nadzorczym i swoim pracodawcą/organem, który go powołał.
5. Zgodnie z RODO, IOD ma odgrywać przede wszystkim rolę konsultacyjno – uświadamiająco – doradczo – kontrolną.
6. ADO jest obowiązany zapewnić aby IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych na podstawie art. 38 ust. 1 RODO.
7. Rekomenduje się, aby rola IOD sprowadzała się do partnera/organu doradczego ADO, a nie osoby, której wydawane są polecenia. Organizacja powinna zapewnić uczestnictwo IOD przy podejmowaniu decyzji dotyczących przetwarzania danych osobowych.
8. Rekomenduje się dokumentowanie przypadków i powodów postępowania niezgodnego z zaleceniami IOD. W przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi należy natychmiast skontaktować się z IOD.
9. RODO przyznaje IOD wyjątkowo dużą niezależność w związku z czym ADO powinien zapewnić, aby IOD nie otrzymywał instrukcji dotyczących wykonywanych zadań (podstawa prawna art. 38 ust. 3 RODO) oraz powinien zapewnić niezależność IOD przy realizacji zadań.
10. IOD jest zobowiązany do unikania konfliktów interesów w związku z wykonywaniami zdaniami i w tym zakresie składa ADO stosowane oświadczenie.
11. Główne zadania IOD polegają na: realizowaniu obowiązków informacyjnych, monitorowaniu przestrzegania przepisów prawa poprzez zbieranie niezbędnych informacji, analizowania i sprawdzania zgodności przetwarzania z prawem, informowania, doradzania i rekomendowania określonych działań ADO, współpracowania z organem nadzorczym, w tym pełnienia funkcji punktu kontaktowego dla organu nadzorczego w sprawach związanych z przetwarzaniem danych.

IOD informuje, że z dniem 01.02.2019 r. wprowadzono projekt Rozporządzenia Prezesa Rady Ministrów

w sprawie trybu i sposobu realizacji zadań przez inspektora ochrony danych, z którego wynikają m. in. zalecenia takie jak:

- Zapoznawanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych, w szczególności podczas szkoleń, których przedmiotem jest dokonywanie analizy teoretycznych i praktycznych zagadnień z zakresu ochrony danych osobowych
- Podnoszenie świadomości osób uczestniczących w przetwarzaniu danych poprzez bieżące informowanie o zmianach przepisów dotyczących ochrony danych osobowych – w związku z tym może pojawiać się potrzeba wdrożenia najnowszych wytycznych, dokonywania zmian w polityce ochrony danych osobowych, zaleceniu wdrożenia nowych, lub zmianie istniejących dokumentów
- Informowanie ADO oraz osób zajmujących się przetwarzaniem danych o obowiązkach wynikających z przepisów ustawy i innych przepisów o ochronie danych osobowych
- Realizacja powyższych zadań może być dokonywana ustnie, pisemnie, w postaci papierowej lub elektronicznej
- IOD sporządza dla ADO pisemne sprawozdania z wykonywanych zadań w postaci papierowej lub elektronicznej, które zawiera w szczególności: wskazanie najważniejszych działań podjętych w okresie, jakiego dotyczy sprawozdanie, opis zaistniałych problemów w zakresie przetwarzania danych.

Wszelkie zapytania na temat zasad, ochrony i przetwarzania danych osobowych należy kierować do inspektora ochrony danych osobowych Łódzkiego Zakładu Usług Komunalnych

prawnik Erwin Ryter

tel. 600 499 192, 602 151 170

e-mail: inspektor.ryter@op.pl