POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W FIRMIE NKU.RADOM.PL Bartłomiej Guść, 26-600 Radom, ul. Żeromskiego 30

WYDANIE I

Radom, lipiec 2018 ROK

Spis treści

Rozdział I

Postanowienia ogólne, definicje

§ **1**

Postanowienia ogólne

1. Polityka bezpieczeństwa danych osobowych jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez NKU.RADOM.PL Guść Bartłomiej, 26-600 Radom ul. Żeromskiego 30.
2. Podstawą do opracowania i wdrożenia dokumentu są:

1) ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku.

2) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 Z 27.4.2016 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 z 2016 r. Nr 119, s.1).

3. Przetwarzanie danych osobowych w Podmiocie jest dopuszczalne wyłącznie pod warunkiem przestrzegania ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 Z 27.4.2016 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 z 2016 r. Nr 119, s.1).
4. Polityka bezpieczeństwa danych osobowych ma zastosowanie do ochrony zbiorów danych osobowych przetwarzanych w Podmiocie, w celu ich bezpiecznego wykorzystania, oraz określa zasady korzystania z systemów informatycznych.

§ **2**

Definicje

1. Określenia i skróty użyte w Polityce bezpieczeństwa danych osobowych oznaczają:

1) OchrDanychU – ustawę z dnia 10 maja 2018 roku o ochronie danych osobowych.

2) RODO - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 Z 27.4.2016 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 z 2016 r. Nr 119, s.1).

3) Podmiot - NKU.RADOM.PL Guść Bartłomiej, 26-600 Radom, ul. Żeromskiego 30

4) Administrator Danych Osobowych – NKU.RADOM.PL Guść Bartłomiej, 26-600 Radom, ul. Żeromskiego 30, zwanego dalej „ADO".

5) Administrator Systemów Informatycznych – osobę wyznaczoną przez ADO, zwaną dalej „ASI";

6) system informatyczny – zespół środków technicznych (urządzenia komputerowe, drukujące, łączności, oprogramowanie), zespół zabezpieczeń środków technicznych, sieć informatyczna i udostępniane przez nią zasoby;

7) bezpieczeństwo systemu informatycznego – wdrożenie środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów OchrDanychU i RODO oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem danych;

8) Inspektor ochrony danych – osobę wyznaczoną przez ADO, zwaną dalej „IOD";

9) zbiór danych osobowych – dane osobowe zgromadzone w usystematyzowany sposób, pozwalający na łatwe dotarcie do konkretnej informacji;

10) profilowanie – dowolna forma zautomatyzowanego przetwarzania danych osobowych, która 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.

11) przetwarzanie danych osobowych – wykonywanie operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie, niezależnie od formy, w jakiej wykonywane są te czynności;

12) osoba upoważniona lub użytkownik systemu – osobę posiadającą upoważnienie wydane

przez ADO lub uprawnioną przez niego osobę i dopuszczoną jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwaną dalej „użytkownikiem".

13) osoby zatrudnione przy przetwarzaniu danych osobowych – wszystkie osoby, w tym użytkowników systemu informatycznego, mające dostęp do danych osobowych.

Rozdział II

Obszary przetwarzania danych osobowych

§ 3

Obszar przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych w Podmiocie obejmuje budynek, pomieszczenie w których przetwarzane są dane osobowe (miejsce, w których wykonuje się operacje na danych osobowych, tj. wpisuje, zmienia, kopiuje), oraz miejsce, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji, pomieszczenia, w których składowane są uszkodzone nośniki danych).
2. Obszar przetwarzania danych osobowych określony jest w „Wykazie obszarów, w których przetwarzane są dane osobowe", stanowiącym załącznik nr 1 do Polityki bezpieczeństwa danych osobowych. Wykaz ten prowadzony jest przez ADO i zawiera następujące informacje:

1) lokalizację budynku,
2) wskazanie piętra budynku,
3) określenie zabezpieczenia pomieszczenia.

3. Obszar przetwarzania danych oraz warunki ochrony tego obszaru określone zostały w załączniku nr 2 do Polityki bezpieczeństwa danych osobowych „Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe".

§ 4

Wykaz zbiorów danych przetwarzanych w Podmiocie i programów zastosowanych do przetwarzania danych

1. Wykaz zbiorów danych przetwarzanych w Podmiocie określony został w załączniku nr 3 do Polityki bezpieczeństwa danych osobowych – „Wykaz zasobów danych osobowych i systemów ich przetwarzania". Wykaz ten zawiera następujące informacje:

1) nazwę zbioru danych,
2) określenie systemu przetwarzania danych osobowych,
3) lokalizację miejsca przetwarzania danych osobowych,
4) stosowane przy przetwarzaniu danych osobowych oprogramowanie,
5) precyzyjny zakres danych osobowych w systemie (pola i relacje pomiędzy nimi),
6) określenie pól informacyjnych w systemie,
7) określenie sposobu przepływu danych pomiędzy systemami,
8) wskazanie możliwość wydruku zakresu przetwarzania danych osobowych.

2. Szczegółowe informacje dotyczące stosowanego sprzętu oraz oprogramowania danego systemu informatycznego są zawarte w instrukcjach zarządzania systemem, załącznik nr 4 do Polityki bezpieczeństwa danych osobowych. Działające systemy to programy: Outlook, oraz system operacyjny Windows 10

3. Przetwarzanie danych osobowych odbywa się na stacji roboczej użytkownika.

§5

Rejestr czynności przetwarzania

1. Administrator danych prowadzi Rejestr czynności przetwarzania danych, załącznik nr 5 do Polityki bezpieczeństwa danych osobowych. Rejestr czynności przetwarzania danych zawiera:

1) nazwę administratora danych osobowych;
2) nazwę współadministratorów;
3) dane kontaktowe administratora danych;
4) dane Inspektora ochrony danych oraz dane kontaktowe do IOD, jeżeli został powołany;
5) cel przetwarzania danych;
6) kategoria przetwarzanych danych;
7) kategoria osób, których dane dotyczą;
8) kategoria odbiorców, którym dane ujawniono lub zostaną ujawnione;
9) planowane terminy usunięcia danych;
10) opis wdrożonych zabezpieczeń technicznych i organizacyjnych.

STRUKTURA ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH W PODMIOCIE

Lp.	Zbiór danych osobowych	Zawartość poszczególnych pól informacyjnych i powiązania między nimi
I.	Pracownik	Imię i nazwisko, data urodzenia, PESEL, adres zameldowania, imiona rodziców, numer telefonu, adres e-mail, seria i numer dowodu
II.	Kontrahenci	Nazwa,NIP, REGON, adres działalności, numer telefonu, adres e-mail, imię i nazwisko
III.	Osoby fizyczne	Imię i nazwisko, data urodzenia, PESEL, adres zameldowania, imiona rodziców, numer telefonu, adres e-mail,forma zatrudnienia, numer i seria dowodu, stan cywilny

§ 6

Sposób przepływu danych pomiędzy poszczególnymi systemami

1. W ramach procesów przetwarzania danych nie dochodzi do przepływu danych pomiędzy różnymi systemami informatycznymi.

§ **7**

Określenie środków technicznych i organizacyjnych niezbędnych

1. Środki techniczne i organizacyjne zapewniają poufność, integralność i rozliczajność przetwarzania danych osobowych. W systemie informatycznym obowiązują zabezpieczenia na poziomie wysokim. Szczegółowe omówienie środków zabezpieczenia technicznego i organizacyjnego znajduje się w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych" , stanowiącej załącznik nr 4 do Polityki bezpieczeństwa danych osobowych.

Rozdział III

Zarządzanie przetwarzaniem danych osobowych oraz czuwanie nad ich bezpieczeństwem

§ **8**

Zadania administratora danych osobowych

1. Zadania administratora danych osobowych w Podmiocie pełni właściciel- Pan Bartłomiej Guść
2. Do obowiązków ADO należą w szczególności:

1) obowiązek informacyjny wobec osoby, której dane dotyczą (art. 13 i 14 RODO);

2) dochowanie szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane dotyczą;

3) udzielanie, w określonych terminach, informacji o celu i zakresie przetwarzanych danych osobowych;

4) uzupełnianie, uaktualnienie, sprostowanie danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcie ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane przez administratora;

5) ograniczenie przetwarzania danych na wniosek osoby której dane dotyczą (art. 18

6) przeniesienie danych na wniosek osoby której dane dotyczą (art. 20 RODO);

7) usunięcie danych na wniosek osoby której dane dotyczą (art. 17 RODO);

8) poinformowanie o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku (art.19 RODO);

9) poinformowanie na żądanie osoby, której dane dotyczą o odbiorcach jej danych (art. 19 RODO);

10) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną (art. 24 i 32 ust. 1 RODO);

11) kontrola wprowadzania do zbioru i przekazywania danych;

12) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

13) Uwzględnienie ochrony danych osobowych w fazie projektowania (art. 25 ust. 1 RODO);

14) Wdrożenie odpowiednich mechanizmów zapewniających domyślną ochronę danych (art. 25 ust. 2 RODO);

15) Rejestrowanie czynności przetwarzania danych (art. 30 ust. 1 RODO);

16) Współpraca z organem nadzorczym (art. 31 RODO);

17) Zgłaszanie naruszeń ochrony danych osobowych (at. 33 RODO);

18) Dokonanie oceny skutków dla ochrony danych (art. 35 RODO).

3. W podmiocie nie powołano IOD ani ASI.

§ **9**

Zadania właścicieli zasobów danych osobowych

1) Nie dotyczy

§ **10**

Obowiązki ASI

1) Nie dotyczy

Rozdział IV

Gromadzenie danych osobowych

§ **11**

Uzyskiwanie danych osobowych

1. Dane osobowe przetwarzane w Podmiocie mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą, lub z innych źródeł, w granicach dozwolonych przepisami prawa.

§ **12**

Wykorzystanie danych osobowych

1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.

2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

§ **13**

Obowiązek uzupełniania danych osobowych

1. W przypadku gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem OchrDanychU albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

Rozdział V

Przetwarzanie danych osobowych

§ **14**

Tworzenie zbiorów danych osobowych

1. ADO jest obowiązany podczas tworzenia nowych zbiorów danych osobowych do zapewnienia odpowiednich środków ochrony, w szczególności z uwzględnieniem zasady minimalizacji oraz pseudnimizacji.

Rozdział VI

Obowiązek informacyjny

§ **15**

Informacja zainteresowanych

1. ADO jest odpowiedzialny za poinformowanie osób, których dane osobowe przetwarzają, o:

1) adresie siedziby Podmiotu, pod którym dane są zbierane i przetwarzane;
2) danych kontaktowych ABI / IOD, jeżeli został powołany;
3) nazwie i danych kontaktowych przedstawiciela na terenie Unii, jeżeli istnieje;
4) celu zbierania danych;
5) podstawie prawnej przetwarzania danych;
6) okresie przechowywania danych;
7) dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej;
8) w przypadku istnienia obowiązku podania danych: wskazanie ewentualnych konsekwencji ich niepodania;

9) zautomatyzowanym podejmowaniu decyzji w tym profilowaniu;

10) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania;

11) prawie do usunięcia danych;

12) prawie do ograniczenia przetwarzania;

13) prawie wniesienia skargi do organu nadzorczego;

14) prawie do przenoszenia danych;

15) prawie do cofnięcia zgody.

2. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować o źródle danych i kategorii danych osobowych (art. 14 RODO), oraz informacji o prawie dostępu do treści swoich danych oraz prawie do ich sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, wniesienia sprzeciwu, cofnięcia zgody w dowolnym momencie.

3. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, informacje o których mowa w par. 15 ust. 1 i 2, ADO podaje:

1) w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca;

2) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą;

3) jeżeli planuje się ujawnić innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.

4. Wzór formularza stosowanego dla spełnienia obowiązków, o których mowa w ust. 1 i 2, stanowi załącznik nr 6 do Polityki bezpieczeństwa danych osobowych.

§ **16**

Zgoda na przetwarzanie danych osobowych

1. Materiały dotyczące innej niż ustawowa działalności Podmiotu mogą być wysyłane tylko do tych osób, które wcześniej wyraziły zgodę na piśmie na przetwarzanie ich danych osobowych w tym celu.

2. Kandydaci do pracy w Podmiocie w procesie rekrutacji są zobowiązani wyrazić pisemną zgodę na przetwarzanie ich danych osobowych.

3. Dokumenty złożone w celu określonym w ust. 2 są przechowywane w komórce organizacyjnej, która przetwarza te dane, i są włączane do akt osobowych pracownika.

Rozdział VII

Udostępnianie danych osobowych

§ 17

Osoby uprawnione do wglądu do danych osobowych

1. ADO udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Dane osobowe mogą być udostępniane w następujących przypadkach:

1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;

2) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;

3) na podstawie wniosku osoby, której dane dotyczą.

3. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi załącznik nr 7 do Polityki bezpieczeństwa danych osobowych.
4. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
5. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania.
6. Wniosek o udostępnienie przekazywany jest do ADO.
7. ADO jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku.

§ 18

Odmowa udostępnienia danych osobowych

1. Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

Rozdział VIII

Ochrona przetwarzania danych osobowych

§ 19

Obowiązek posiadania upoważnienia

1. Do przetwarzania danych mogą być dopuszczeni pracownicy Podmiotu posiadający upoważnienie nadane przez ADO. Wzór upoważnienia określa załącznik nr 8 do Polityki bezpieczeństwa danych osobowych.
2. ADO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi załącznik nr 9 do Polityki bezpieczeństwa danych osobowych.

§ 20

Przechowywanie imiennych upoważnień do przetwarzania danych osobowych

1. ADO zobowiązany jest do zbierania, ewidencjonowania i przechowywania:

1) oświadczeń osób przetwarzających dane osobowe o zachowaniu w tajemnicy danych, z którymi mają styczność, oraz środkach bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych; wzór formularza oświadczenia stanowi załącznik nr 10 do Polityki bezpieczeństwa danych osobowych;

2) oświadczeń osób zatrudnianych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy; wzór formularza oświadczenia stanowi załącznik nr 10 do Polityki bezpieczeństwa danych osobowych;

§ 21

Powierzenie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych odbywa się zgodnie art. 28 RODO na podstawie umowy zawartej na piśmie pomiędzy ADO a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.
2. ADO przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.
3. Projekt umowy powinien określać:

1) przedmiot umowy, czyli to, jakie dane i w jakim zakresie zostają powierzone podmiotowi przetwarzającemu;

2) czas trwania przetwarzania;

3) charakter przetwarzania;

4) cel przetwarzania;

5) rodzaj danych osobowych;

6) kategorie osób, których dane dotyczą;

7) obowiązki i prawa administratora.

4. Każda osoba delegowana do wykonywania zadań na rzecz Podmiotu, związanych z powierzeniem przetwarzania danych osobowych, obowiązana jest podpisać oświadczenie o zachowaniu w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.

5. Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 11 do Polityki bezpieczeństwa danych osobowych.

§ **22**

Obowiązki podmiotu przetwarzającego dane osobowe

1. Podmiot przetwarzający dane osobowe jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.
2. Podmiot, o którym mowa w ust. 1, jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.
3. Podmiot przetwarzający dane osobowe ponosi odpowiedzialność za ochronę przetwarzanych danych osobowych.
4. Podmiot o którym mowa w ust. 1, jest zobowiązany prowadzić Rejestr kategorii czynności przetwarzania (art. 30, ust. 2 RODO). Rejestr kategorii czynności przetwarzania zawiera następujące informacje:

1) imię i nazwisko lub nazwa podmiotu przetwarzającego;

2) dane kontaktowe podmiotu przetwarzającego;

3) imię i nazwisko lub nazwa każdego administratora, w imieniu którego działa podmiot przetwarzający;

4) nazwa przedstawiciela administratora lub podmiotu przetwarzającego, gdy ma to zastosowanie;

5) imię i nazwisko Inspektora ochrony danych;

6) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;

7) przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej - gdy ma to zastosowanie;

8) jeżeli jest to możliwe, ogólny opis techniczny i organizacyjny środków bezpieczeństwa, o których mowa w art. 32, ust 1 RODO.

5. Wzór rejestr kategorii czynności przetwarzania stanowi załącznik nr 12 do Polityki bezpieczeństwa danych osobowych.

Rozdział IX

Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych

§ 23

Określenie sytuacji naruszenia bezpieczeństwa danych osobowych

1. Przepisy niniejszego rozdziału stosuje się w przypadku:

1) stwierdzenia naruszenia zabezpieczenia systemu informatycznego w obszarze danych osobowych;

2) podejrzenia naruszenia bezpieczeństwa danych osobowych ze względu na stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej.

§ 24

Określenie osób zobowiązanych

1. Zasady postępowania przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.

§ 25

Określenie naruszenia zabezpieczenia systemu informatycznego

1. Naruszeniem zabezpieczenia systemu informatycznego, przetwarzającego dane osobowe jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1) nieautoryzowany dostęp do danych;
2) nieautoryzowane modyfikacje lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym podmiotom;
4) nielegalne ujawnienie danych;
5) pozyskiwanie danych z nielegalnych źródeł.

§ 26

Działania pracowników

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić

o tym fakcie bezpośredniego przełożonego (ewentualnie osobę przez niego upoważnioną), a następnie postępować stosownie do podjętej przez niego decyzji.

2. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:

1) opisanie działania wskazującego na naruszenie ochrony danych osobowych;

2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;

3) wskazanie istotnych informacji mogących wskazywać na przyczynę naruszenia;

4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§ **27**

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je organowi nadzorczemu.
2. W przypadku gdy jest mało prawdopodobne by naruszenie ochrony danych osobowych skutkowało ryzykiem naruszenia praw i wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienia przyczyn opóźnienia.
3. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych zgłasza je ADO, bez zbędnej zwłoki.
4. Zgłoszenie naruszenia ochrony danych osobowych o którym mowa ust. 1 i 2 musi co najmniej:

1) opisywać charakter naruszenia ochrony danych osobowych, w tym kategorię i przybliżoną liczbę zainteresowanych podmiotów danych oraz kategorię i przybliżoną liczbę osób, których dane dotyczą;

2) imię i nazwisko oraz dane kontaktowe IOD lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;

3) opis możliwych konsekwencji naruszenia ochrony danych osobowych;

4) opis środków przedsięwziętych lub proponowane przez ADO w celu zminimalizowania skutków.

5. Wzór zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu stanowi załącznik nr 13 do Polityki bezpieczeństwa danych osobowych.
6. ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności

naruszenia, jego skutki oraz podjęte działania zaradcze. Wzór udokumentowania naruszeń ochrony danych stanowi załącznik nr 14 do Polityki bezpieczeństwa danych osobowych.

§ **28**

Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

1. W przypadku gdy naruszenie ochrony danych osobowych może nieść wysokie ryzyko naruszenia praw i wolności osób fizycznych. ADO zawiadamia osoby, których dane dotyczą o naruszeniu ochrony danych osobowych.
2. Zawiadomienie o którym mowa w ust. 1 jasnym i prostym jeżykiem opisuje charakter naruszenia oraz zawiera przynajmniej informacje o których mowa w par. 27 ust. 4 pkt. 2,3 i 4.

Rozdział X

Ocena skutków dla ochrony danych i uprzednie konsultacje

§29

Ocena skutków dla ochrony danych

1. Jeżeli dany rodzaj przetwarzania (zwłaszcza z użyciem nowych technologii) ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. ADO przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.
2. Ocena skutków przetwarzania pod kątem ochrony danych jest wymagana w przypadku:

1) systematycznej, oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu;

2) przetwarzania na duża skalę szczególnych kategorii danych osobowych;

3) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

3. Wzór oceny skutków dla ochrony danych stanowi załącznik nr 15 do polityki bezpieczeństwa danych osobowych.

§30

Uprzednie konsultacje

1. Jeżeli ocena skutków pod kątem ochrony danych, wskaże że przetwarzanie niosło by duże zagrożenie, gdyby ADO nie przedsięwziął środków w celu zminimalizowania tego zagrożenia, to przed przetworzeniem danych osobowych ADO konsultuje się z organem

nadzorczym.

2. Organ nadzorczy w terminie 8 tygodni od dnia wpłynięcia wniosku w sprawie uprzednich konsultacji, wydaje zalecenia w formie pisemnej.
3. Wzór wniosku w sprawie uprzednich konsultacji stanowi załącznik nr 16 do Polityki bezpieczeństwa danych osobowych.

Rozdział XI

Odpowiedzialność służbowa i karna

§31

Przepisy karne

1. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi określonymi w art. 107 OchrDanychU, art. 83 RODO oraz w art. 130, 266–269, 287 Kodeksu karnego.

Rozdział XII
Aktualizacja

§ 32

Aktualizacja postanowień Polityki Bezpieczeństwa

1. Na podstawie audytów kontrolnych, przeprowadzanych nie rzadziej niż raz na 12 miesięcy, ADO dokona analizy zmiany w zakresie ochrony danych osobowych.
2. W przypadku ustalenia konieczności zmian zabezpieczeń w zakresie ochrony danych osobowych, w szczególności , w zakresie procedur, ADO dokona stosownej zmiany niniejszej Polityki Bezpieczeństwa.