POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w Polot Media Sp. z o.o. Sp. k.

Spis treści:

Wprowadzenie

W coraz większym stopniu instytucje, ich systemy i sieci informatyczne stają w obliczu zagrożeń pochodzących z rozmaitych źródeł, takich jak oszustwa dokonywane za pomocą komputerów, komunikatorów, urządzeń mobilnych oraz sieci. Maskarady, szpiegostwo, sabotaż, wandalizm, pożar lub powódź to zjawiska aktywnej lub losowej utraty informacji oraz danych. Źródła uszkodzeń takie, jak wirusy komputerowe, haking komputerowy i ataki powodujące odmowę usługi stają się coraz powszechniejsze, ambitniejsze i bardziej wyrafinowane. Odpowiednie zabezpieczenia, ochrona przetwarzanych danych, niezawodność funkcjonowania oraz systematyczna i wielowątkowa organizacja edukacji użytkowników stają się podstawowymi wymogami stawianymi współczesnym systemom informatycznym, a informacja oraz wspierające ją procesy, systemy i sieci są ważnymi aktywami działalności jednostki organizacyjnej, mającymi wpływ na markę i efekty biznesowe.

Jednym słowem poufność, dostępność i integralność informacji ma podstawowe znaczenie dla utrzymania konkurencyjności, płynności finansowej, zysku i zgodności z przepisami prawa oraz wizerunku jednostki.
Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń. Jednocześnie deklaruje zaangażowanie kierownictwa i wyznacza procesowe podejście instytucji do zarządzania bezpieczeństwem informacji. Ponadto niektóre zabezpieczenia opisane w niniejszym dokumencie są traktowane jako **zasady przewodnie** w zarządzaniu bezpieczeństwem informacji, możliwe do zastosowania i zapewniające odpowiedni punkt wyjścia dla procesu wdrażania bezpieczeństwa informacji.

Omawiane zasady opierają się na obowiązujących uregulowaniach prawnych, a należą do nich w szczególności:

- ochrona danych osobowych i prywatności osób,
- ochrona dokumentów instytucji,

- prawa własności intelektualnej,
- dokumenty polityki ochrony danych osobowych,
- odpowiedzialność związana z bezpieczeństwem informacji,
- edukacja w dziedzinie bezpieczeństwa informacji,
- wsparcie i zaangażowanie kadry kierowniczej,
- upowszechnianie wytycznych dotyczących polityki bezpieczeństwa informacji wśród wszystkich użytkowników,
- zgłaszanie przypadków naruszenia bezpieczeństwa.

Głównym celem **POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH (PBDO)** jest organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych danych osobowych, oraz systematyczne edukowanie użytkowników systemu ochrony danych osobowych.

PBDO jest jednocześnie materiałem określającym zadania w zakresie właściwej realizacji poufności i integralności danych osobowych przez nadanie uprawnień legalizujących przetwarzanie danych użytkownikom systemu ochrony informacji.

Rozdział I

Przepisy ogólne, definicje oraz objaśnienia

§1

Definicje

1. Ilekroć w dokumencie jest mowa o:

1) **rozporządzeniu, zamiennie RODO** – rozumie się przez to 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);

2) **danych osobowych** – rozumie się przez to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3) **zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
4) **przetwarzaniu danych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
5) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
6) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
7) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
8) **administratorze danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to

również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

9) **zgodzie osoby, której dane dotyczą** – oznacza to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

10) **odbiorcy danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

11) **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;

12) **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;

13) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

14) **profilowaniu** – oznacza to dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

15) **pseudonimizacji** – oznacza to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi

uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

16) **podmiocie przetwarzającym** – oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

17) **naruszeniu ochrony danych osobowych** – oznacza to 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.

18) **użytkowniku** – osobie przetwarzającej dane na polecenie administratora danych (współpracownicy tzn. pracownicy, oraz osoby zatrudnione na podstawie umów cywilno-prawnych).

19) **Szyfrowaniu (kryptografia) -** czyli proces przekształcania danych w formę nieodczytywalną, bez znajomości odpowiedniego klucza, szyfru.

§2

1. Polityka Bezpieczeństwa Danych Osobowych w uporządkowanej formie opisuje działania organizacyjne i techniczne, których celem jest zapewnienie bezpieczeństwa danych osobowych w Polot Media Sp. z o.o. Sp. k. zwanym dalej Polot Media lub zamiennie Administratorem Danych, w skrócie ADO (administrator danych osobowych), oraz w relacjach powierzania danych osobowych wykonawcom w ramach realizowanych projektów lub umów.

2. **Polityka Bezpieczeństwa Danych Osobowych** ustala zakresy obowiązków osób i innych organizacji w procesie obiegu i ochrony informacji. Określenie zakresu przetwarzanych danych osobowych w indywidualnych umowach z podmiotami zewnętrznymi, którym zlecono przetwarzanie danych osobowych zawarte określa procedura współpracy z podmiotami zewnętrznymi.

§3

1. Dostęp do przetwarzania danych osobowych posiadają wyłącznie osoby posiadające upoważnienie wydane przez Administratora Danych, przy czym przetwarzanie danych osobowych wykonywane jest na polecenie administratora danych. Upoważnienie stanowi podstawową przesłankę legalności przetwarzania określonych danych, w zakresie rozliczalności i zarządzania dostępem użytkowników (pracowników, współpracowników).
2. Osoby użytkowników (współpracownicy) zaangażowani w procesie przetwarzania danych osobowych są zobowiązane do przechowywania danych osobowych, nie dłużej niż jest to niezbędne dla osiągnięcia **celu** ich przetwarzania, zgodnie z procedurami wewnętrznymi i przepisami prawa.
3. Użytkownicy zaangażowani w procesie przetwarzania danych osobowych w systemach informatycznych zobowiązani są do postępowania zgodnie z procedurami wprowadzonymi do stosowania w POLOT MEDIA.

§4

1. Użytkownicy przetwarzający dane osobowe zobowiązani są do informowania Administratora Danych o ewentualnych incydentach / naruszeniach bezpieczeństwa systemu ochrony danych osobowych.
2. Tryb postępowania określa procedura dotycząca postępowania w sytuacjach naruszenia ochrony danych osobowych

Rozdział II

Obszary przetwarzania danych osobowych

§ 5

Obszar przetwarzania danych osobowych

1. Obszar przetwarzania danych należy rozumieć jako obszar, w którym wykonywana jest choćby jedna z czynności będąca przetwarzaniem danych osobowych tj.:
   operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

2. Obszar przetwarzania, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze przetwarzania jest dopuszczalne za zgodą ADO lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
3. Obszarem przetwarzania jest siedziba POLOT MEDIA ul. Solskiego 55 52-401 Wrocław, budynek A i B oraz Gułów 49 57-120 Gułów gm. Wiązów (w okresie kiedy realizowane są tam produkcje POLOT MEDIA)
4. Jako obszar przetwarzania rozumie się również pomieszczenia przetwarzania danych przez procesora, któremu Administrator powierzył dane osobowe do przetwarzania – za prawidłowe zabezpieczenie i procedury odpowiada procesor zgodnie z podpisaną umową powierzenia danych.

§ 6

Rejestr czynności przetwarzania

Rejestrowanie wszelkich czynności przetwarzania danych osobowych prowadzi się w rejestrze czynności przetwarzania, którego zakres jest zgodny z zakresem wynikającym z art. 30 RODO. Rejestr czynności prowadzi IOD (na postawie informacji przekazanych przez ADO).

§ 7

Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aktualnie obowiązującymi przepisami prawa polskiego regulującymi zagadnienia ochrony danych osobowych. Administrator Danych zobowiązany jest do zastosowania, adekwatnych do stwierdzonego poziomu ryzyka dla poszczególnych systemów środków technicznych i organizacyjnych dla zapewnienia poufności, integralności, dostępności i rozliczalności przetwarzanych danych. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

Przetwarzanie danych osobowych odbywa się wyłącznie na polecenie ADO.

W zakresie środków organizacyjnych Administrator Danych wdraża:

1. Politykę Bezpieczeństwa Ochrony Danych Osobowych ,
2. Procedury Wewnętrzne regulujące proces ochrony danych osobowych w POLOT MEDIA.
3. Zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami prawa w zakresie ochrony danych osobowych, jak również z wewnętrznymi procedurami w części przeznaczonej dla użytkowników, w szczególności z niniejszą Polityką oraz z Regulaminem Użytkownika .

4. Osoby upoważnione zostają zobowiązane do zachowania tych danych w tajemnicy, również po zakończeniu pracy lub współpracy.

W zakresie środków technicznych wdraża się:

1. Kontrolę dostępu do obszarów fizycznych przetwarzania danych osobowych.:
2. Dla pomieszczeń, w których przetwarzane są dane osobowe wdrożono system przeciwpożarowy,
3. Wprowadzono politykę czystego biurka i czystego ekranu. Monitory komputerów, w których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający osobom trzecim podgląd wyświetlanych danych, konfiguracja wyświetlania obrazu na tych monitorach zawiera włączenie wygaszacza ekranu lub wyłączenie monitora, w przypadku braku aktywności użytkownika. Dokumenty zawierające dane osobowe, nośniki z danymi osobowymi zabezpieczone są przed dostępem osób nieupoważnionych,
4. Szczegółowe zasady bezpiecznego użytkowania systemu informatycznego. dokumentów w formie papierowej, oraz zgłaszania naruszeń przez użytkowników zawarte są w Regulaminie Użytkownika, gdzie określono zasady korzystania z legalnego oprogramowania, komputerów służbowych, sieci komputerowej służbowej poczty elektronicznej, telefonów, nośników danych oraz instrukcji postępowania z dokumentami papierowymi, a także procedurę postępowania w sytuacjach naruszenia ochrony danych osobowych.

5. ***ROZDZIAŁ III***

Zarządzanie przetwarzaniem danych osobowych oraz czuwanie nad ich bezpieczeństwem

§ 8

Zadania administratora danych osobowych

1. Administratorem danych osobowych jest POLOT MEDIA Sp. z o.o. Sp. k.. Zadania administratora danych osobowych realizuje Zarząd Spółki (zgodnie z zapisami KRS), a w ramach Zarządu: członek Zarządu, któremu powierzono nadzór nad obszarem ochrony danych osobowych.
2. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, ADO wdraża środki techniczne i organizacyjne, opisane w niniejszej Polityce;
3. Wyznacza Inspektora Ochrony Danych (IOD);
4. Realizuje obowiązek informacyjny wobec osoby, której dane dotyczą (art. 13 i 14 RODO);
5. Udziela, w określonych terminach, informacji o celu i zakresie przetwarzanych danych osobowych.;
6. Zapewnia realizację uprawnień podmiotów danych wynikających z RODO, każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w rozporządzeniu administrator danych rozpatruje indywidualnie;
7. Niezwłocznie realizuje następujące prawa osób, których dane dotyczą (jeżeli przysługują ze względu na podstawę prawną ich zbierania):
    a) prawo dostępu do danych,
    b) prawo do sprostowania danych,
    c) prawo do usunięcia danych,
    d) prawo do przenoszenia danych,
    e) prawo do sprzeciwu wobec przetwarzania danych,

f) prawo do niepodlegania decyzjom opartym wyłącznie na profilowaniu;

9. W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku;

10. Administrator danych odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia;

11. Administrator danych wyznacza zarządzającego oprogramowaniem, który przeprowadza okresową inwentaryzację oprogramowania oraz ustanawia zasady i procedury ciągłego utrzymania oprogramowania, a także pełni rolę admiratora systemu informatycznego(ASI)- w Polot Media umowa z firmą zewnętrzną.

§ 9

Zadania Inspektora ochrony danych (IOD)

1. Do zakresu obowiązków IOD należy w szczególności:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach

f) Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

§ 10

Prawa IOD

1. Inspektor ochrony danych ma prawo żądać od wszystkich osób zatrudnionych wymienionych w pkt. 1 wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

§ 11

Obowiązki administratora systemu informatycznego (ASI)

1. ASI odpowiada za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych POLOT MEDIA.

2. Do obowiązków ASI w zakresie ochrony danych osobowych należy w szczególności:

1) zapewnienie sprawnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych;
2) nadzór nad naprawami, konserwacją i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
3) nadzór nad przeglądami, konserwacją, uaktualnianiem systemów służących do przetwarzania danych osobowych;
4) podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w POLOT MEDIA w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych;
5) nadzór nad przesyłaniem danych osobowych drogą teletransmisji;

6) nadzór nad przestrzeganiem zasad bezpieczeństwa w przypadku udostępniania danych osobowych innym podmiotom drogą teletransmisji danych;
7) przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
8) podejmowanie działań w przypadku naruszeń w systemie zabezpieczeń;
9) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
10) podejmowanie działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego.
11) zapewnienie bezpieczeństwa przechowywanym danym, w szczególności wykorzystując alternatywne sposoby zabezpieczenia danych osobowych w celu bezpiecznego ich przetwarzania w systemach teleinformatycznych takie jak szyfrowanie, pseudonimizacja.
12) Informowanie ADO o wszelkich problemach i potrzebach związanych z bezpiecznym funkcjonowaniem systemu teleinformatycznego w jednostce.

Rozdział IV

Gromadzenie danych osobowych

§ 12

Uzyskiwanie danych osobowych

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

§ 13

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.

§ 14

Obowiązek uzupełniania danych osobowych

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

Rozdział V

Procedura analizy ryzyka i oceny skutków dla ochrony danych

§ 15

Procedura analizy ryzyka i plan postępowania z ryzykiem

1. Analiza ryzyka jest przeprowadzana nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.
2. Na podstawie wyników przeprowadzonej analizy ryzyka, administrator danych wdraża sposoby postępowania z ryzykiem.
3. Każdorazowo administrator danych wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze.
4. Administrator danych nie może zlekceważyć ryzyka, którego wartość określa się jako ryzyko wysokie zgodnie z Procedurą analizy ryzyka .

§ 16

Procedura domyślnej ochrony danych

1. Administrator danych w przypadku zamiaru rozpoczęcia przetwarzania danych osobowych w nowym procesie przeprowadza analizę ryzyka oraz ocenę skutków dla ochrony danych w stosunku do tego procesu.

2. W każdym przypadku tworzenia nowego produktu lub usług administrator danych uwzględnia prawa osób, których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania.

3. Administrator danych wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

§ 17

Podstawa prawna przetwarzania danych osobowych

Przetwarzanie danych osobowych w POLOT MEDIA może odbywać się tylko i wyłącznie na podstawie prawnych przesłanek określonych w RODO, w szczególności: w art. 6 dla danych osobowych zwykłych, w art. 9 dla danych osobowych szczególnej kategorii, a art. 10 dla danych dotyczących wyroków skazujących i naruszeń prawa.

Rozdział VI

Udostępnianie danych osobowych

§ 18

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.
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 niezwłocznie, w terminie nie dłuższym jednak niż 1 miesiąc od daty jego otrzymania.

§ 19

Odmowa udostępnienia danych osobowych

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 VII

Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych

§ 21

Określenie sytuacji naruszenia bezpieczeństwa danych osobowych

1. W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2. Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia. W przypadku uzasadnionym informacje przekazywane są sukcesywnie. W przypadku opóźnienia w powiadomieniu organu nadzorczego w zawiadomieniu podaję się przyczynę opóźnienia.
3. Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, za wyjątkiem sytuacji w której zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.
4. Administrator prowadzi rejestr naruszeń.

§ 22

Określenie osób zobowiązanych

1. Zasady postępowania w przypadku naruszenia bezpieczeństwa danych osobowych są

określone w ramach procedur wewnętrznych i obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, użytkownik postępuje zgodnie z wewnętrzną instrukcją postepowania w przypadku podejrzenia naruszenia bezpieczeństwa danych osobowych.

2. Szczegółowy sposób postępowania w przypadku podejrzenia naruszenia bezpieczeństwa danych osobowych zawarte są w procedurze postępowania w sytuacjach naruszenia ochrony danych osobowych.
3. Szczegółowy sposób postępowania w przypadku naruszenia bezpieczeństwa danych osobowych zawarte są w procedurze zgłaszania incydentów do organu nadzorczego i informowania podmiotów danych

§ 23

Określenie naruszenia zabezpieczenia systemu informatycznego

Naruszeniem bezpieczeństwa systemu informatycznego, w którym przetwarza się 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.

Rozdział VIII

Odpowiedzialność, postanowienia końcowe

§ 26

Odpowiedzialność

1. Pracownik, lub osoba zatrudniona na podstawie umowy cywilno-prawnej lub współpracy w przypadku gdy:

1) przetwarza w zbiorze danych dane osobowe:
   a) do których przetwarzania nie jest upoważniony,
   b) których przetwarzanie jest zabronione,
   c) niezgodne z celem stworzenia zbioru danych;
2) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;
3) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach;
4) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw

– podlega sankcjom określonym w Kodeksie pracy lub odpowiednio w Kodeksie cywilnym, niezależnie od kar przewidzianych w aktualnie obowiązujących przepisach regulujących tematykę ochrony danych osobowych.

.

§ 27

Przepisy końcowe

1. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy RODO, a także przepisy polskie regulujące zagadnienia ochrony danych osobowych obowiązujące w okresie stosowania niniejszej Polityki, w szczególności przepisy ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. z 2018r. poz. 1000) a także wszelkie nowelizacje, jakie wejdą w życie po dniu zatwierdzenia Polityki do stosowania.

2. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce, w wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach, osoby upoważnione mają obowiązek stosowania zapisów, których stosowanie zapewni wyższy poziom ochrony danych osobowych.
3. Niniejsza Polityka jest dokumentem wewnętrznym, dlatego istnieje obowiązek zachowania w poufności treści w niej zawartych.