POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

MAKROPOL Sp. z o.o.

Przygotował:	Łukasz Szafrański - IOD	**Data:**	23.04.2018
Zatwierdził:	Maciej Bukowian - ADO	**Data:**	25.05.2018
Obowiązuje od:	25.05.2018		
Wymagania prawne:	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).		

SPIS TREŚCI:

1. Wykaz podstawowych skrótów

Skrót	Opis
ADO	Administrator Danych Osobowych
ASI	Administrator Systemów Informatycznych
IOD	Inspektor Ochrony Danych
SI	System Informatyczny
PBDO	Polityka Bezpieczeństwa Danych Osobowych
IZSI	Instrukcja Zarządzania Systemem Informatycznym
RODO	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. Wykaz podstawowych definicji

Ilekroć w niniejszej Polityce Bezpieczeństwa Danych Osobowych mowa o:

Administratorze Danych Osobowych – zwany również **ADO** 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;

Administratorze Systemu Informatycznego – rozumie się przez to pracownika Administratora Danych Osobowych lub inne osoby odpowiedzialne za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów i sieci teleinformatycznych;

Inspektorze Ochrony Danych – rozumie się przez to osobę odpowiedzialną za bieżący nadzór stosowania przepisów dot. ochrony danych osobowych;

Osobie upoważnionej – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Osobą upoważnioną może być pracownik Spółki, osoba wykonująca prace na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż;

Danych osobowych – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);

Możliwej do zidentyfikowania osobie fizycznej - rozumie się przez to osobę, 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;

Przetwarzaniu danych osobowych – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie,

przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Zbiorze danych osobowych – rozumie się przez to uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

Podmiocie przetwarzającym – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych Osobowych;

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 postepowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

Systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

Bezpieczeństwie danych osobowych – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania danych osobowych, by w każdych okolicznościach dostęp do nich był zgodny z założeniami i zapewniał ich poufność, integralność oraz dostępność;

Poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;

Integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

Dostępności danych – rozumie się przez to właściwość zapewniającą, że dane są osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez uprawnioną osobę lub podmiot;

Zgodzie osoby, której dane dotyczą – rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli przez osobę, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwalające na przetwarzanie dotyczących jej danych osobowych;

Państwie trzecim – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;

Incydencie – rozumie się przez to naruszenie bezpieczeństwa danych osobowych;

Zagrożeniu - rozumie się przez to potencjalną możliwość wystąpienia incydentu;

Naruszeniu ochrony danych osobowych - rozumie się przez to naruszenie bezpieczeństwa danych osobowych 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.

SUK – rozumie się przez ten skrót jako Służbowe Urządzenie komputerowe

3. Wprowadzenie

Polityka Bezpieczeństwa Danych Osobowych określa reguły przetwarzania danych osobowych oraz sposobów ich zabezpieczenia, jako zestaw praw, zasad i zaleceń regulujących sposób ich zarządzania, ochrony i dystrybucji w firmie **MAKROPOL sp. z o.o.**

Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń techniczno-organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.

Niniejszy dokument jest zgodny z obowiązującymi przepisami prawa, a w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

4. Cele Polityki Bezpieczeństwa Danych Osobowych

Celem Polityki Bezpieczeństwa Danych Osobowych jest określenie oraz wdrożenie zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w firmie **MAKROPOL sp. z o.o.,** a w szczególności:

1) zapewnienie spełnienia wymagań prawnych;
2) zapewnienie poufności, integralności oraz rozliczalności danych osobowych przetwarzanych w firmie;
3) podnoszenie świadomości osób przetwarzających dane osobowe;
4) zaangażowanie osób przetwarzających dane osobowe firmy w ich ochronę.

5. Zakres rozpowszechniania Polityki Bezpieczeństwa Danych Osobowych

1) Z treścią niniejszej Polityki Bezpieczeństwa Danych Osobowych powinny zapoznać się wszystkie podmioty przetwarzające dane osobowe w imieniu Administratora Danych Osobowych.

6. Inspektor Ochrony Danych

1) **Inspektor Ochrony Danych** monitoruje przestrzeganie zasad bezpieczeństwa oraz prowadzi kontrolę przetwarzania danych osobowych.
2) **Inspektor Ochrony Danych** wykonuje w szczególności następujące zadania:
   a) identyfikacja i aktualizacji zbiorów danych osobowych;

b) przeprowadzenie oceny skutków planowanych operacji przetwarzania dla ochrony danych
c) osobowych oraz monitorowanie jej wykonania;
d) weryfikacja klauzul zgód na przetwarzanie danych osobowych oraz klauzul obowiązków informacyjnych, a w razie potrzeby przygotowanie niezbędnych zmian lub opracowanie właściwych dokumentów i klauzul;
e) analiza stosowanych przez Zleceniodawcę techniczno - organizacyjnych środków ochrony, bezpieczeństwa fizycznego oraz informatycznego związanych z przetwarzaniem danych osobowych;
f) przeprowadzenie rejestru czynności przetwarzania danych osobowych;
g) zarządzanie upoważnieniami do przetwarzania danych osobowych;
h) zarządzanie ewidencją osób upoważnionych do przetwarzania danych osobowych;
i) prowadzenie korespondencji z organem nadzorczym;
j) opiniowanie wzorów dokumentów dotyczących ochrony danych osobowych, klauzul zgód na przetwarzanie danych osobowych oraz klauzul obowiązków informacyjnych;
k) prowadzenie szkoleń dla pracowników z zakresu ochrony danych osobowych;
l) wspieranie pracy audytorów zewnętrznych w zakresie ochrony danych osobowych;
m) udział w kontrolach organu nadzorczego oraz współpraca z organem nadzorczym;
n) udział w kontrolach prowadzonych u Zleceniodawcy przez innych administratorów danych;
o) prowadzenie audytów podmiotów, którym Zleceniodawca powierzył przetwarzanie danych osobowych;
p) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
q) opiniowanie, pod względem zgodności oraz z przepisami prawa umów, procedur i innych wytworzonych dokumentów dotyczących bezpieczeństwa i przetwarzania danych osobowych;
r) podejmowanie lub wnioskowanie o podjęcie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych oraz prowadzenie adekwatnej dokumentacji w tym zakresie;

3) **Inspektorem Ochrony Danych** w firmie **MAKROPOL sp. z o.o.**, jest:
   a. Łukasz Szafrański – współwłaściciel firmy PROXICOM s.c. jako zewnętrzna firma. Do dnia 31.03.2019 r.
   b. Maciej Bukowian – przedstawiciel firmy Makropol sp. z o,o, od dnia 01.04.2019 r.
   c. Grzegorz Biszof – przedstawiciel firmy Makropol sp. z o.o. od dnia 01.11.2020 r.

4) **Administrator Danych Osobowych** upoważnia **Inspektora Ochrony Danych** do przetwarzania danych osobowych we wszystkich zbiorach **Administratora Danych Osobowych** oraz poza nimi w zakresie niezbędnym dla należytego wykonywania funkcji **Inspektora Ochrony Danych**.

7. Osoby upoważnione do przetwarzania danych osobowych

1) Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:
   a) zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki Bezpieczeństwa Danych Osobowych i Instrukcji Zarządzania Systemami Informatycznymi;
   b) stosowanie się do zaleceń Inspektora Ochrony Danych;
   c) przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych w pisemnym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków służbowych;
   d) niezwłoczne informowanie Inspektora Ochrony Danych o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w firmie;
   e) ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
   f) korzystanie z systemów informatycznych firmy w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemów informatycznych;
   g) bezterminowe zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
   h) zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.

8. Podstawowe zasady ochrony danych osobowych

1) Wszystkie dane osobowe w firmie należy przetwarzać zgodnie z obowiązującymi przepisami prawa.
2) W stosunku do osób, których dane osobowe są przetwarzane należy spełnić obowiązek informacyjny wynikający z przepisów rozporządzenia RODO.
3) Zebrane dane osobowe należy przetwarzać dla oznaczonych i zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami.
4) Należy zadbać, aby przetwarzanie danych osobowych odbywało się zgodnie z zasadami dotyczącej merytorycznej poprawności oraz adekwatnie do celów w jakich zostały zebrane.
5) Dane osobowe w firmie można przetwarzać nie dłużej niż jest to niezbędne do osiągnięcia celu ich przetwarzania.
6) Należy zapewnić poufność, integralność oraz rozliczalność danych osobowych przetwarzanych w firmie.
7) Przetwarzane dane osobowe nie mogą być udostępniane bez zgody osób, których dane dotyczą, chyba że udostępnia się te dane osobom, których dane dotyczą, osobom upoważnionym do przetwarzania danych osobowych, podmiotom którym przekazano dane na podstawie umowy powierzenia oraz

organom państwowym lub organom samorządu terytorialnego w związku z prowadzonym postępowaniem.

8) Przetwarzanie danych osobowych w firmie może odbywać się zarówno w systemach informatycznych, jak i w formie tradycyjnej: kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.
9) W zakresie danych osobowych przetwarzanych w innych systemach niż informatyczne, obowiązują nadal dotychczasowe przepisy o tajemnicy służbowej, obiegu i zabezpieczaniu dokumentów służbowych.
10) Wszystkim osobom, których dane są przetwarzane przysługuje prawo do ochrony danych ich dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualniania, usunięcia jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.

9. Upoważnienie do przetwarzania danych osobowych

1) Do przetwarzania danych osobowych i obsługi zbiorów informatycznych zawierających te dane mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych Osobowych oraz złożyły stosowne oświadczenie dot. właściwej realizacji przepisów rozporządzenia RODO
2) Administrator Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych przy pomocy pełniącego funkcje Inspektora Ochrony Danych

10. Powierzenie przetwarzania danych osobowych

1) Administrator Danych Osobowych może zlecić innemu podmiotowi przetwarzanie danych osobowych w celu realizacji określonego zadania.
2) W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

11. Udostępnianie danych osobowych

1) Dane osobowe udostępnia się na wniosku udostępnienia lub w ramach podpisanych umów z Klientami.
2) Wniosek o udostepnienie danych, który wpłynął do firmy rozpatruje właściciel zbioru.
3) Wniosek o udostepnienie danych osobowych, którego sposób rozpatrzenia budzi uzasadnione wątpliwości, może zostać przesłany, wraz z informacjami niezbędnymi dla jego rozpatrzenia, do Inspektora Ochrony Danych w celu zajęcia stanowiska w sprawie. Do wniosku dołącza się projekt odpowiedzi wraz z uzasadnieniem.
4) Informacje, zawierające dane osobowe są udostępniane uprawnionym podmiotom:
   a) w formie wydruku listem poleconym lub za potwierdzeniem osobistego odbioru,
   b) w drodze teletransmisji danych (w sposób gwarantujący poufność przesyłanych danych),
   c) na elektronicznych nośnikach informacji, za potwierdzeniem odbioru,

   d) w inny sposób określony przepisami prawa lub umową.
5) Udostępniane dane osobowe podlegają kontroli przez Właściciela zbioru, z którego one pochodzą.
6) Ewidencja przypadków udostepnienia danych prowadzona jest przez Właścicieli zbiorów w wersji elektronicznej lub papierowej.

12. Przekazywanie danych osobowych poza Polskę

1) Administrator Danych Osobowych może przekazywać dane osobowe do:
   - państw Europejskiego Obszaru Gospodarczego;
   - pozostałych państw (państwa trzecie).
2) Przekazywanie danych osobowych w ramach Europejskiego Obszaru Gospodarczego traktuje się tak, jakby były przetwarzane na terenie Polski.
3) W przypadku przekazywania danych osobowych do państwa trzeciego, przekazywanie następuje zgodnie z Rozdziałem V art. 44 – 49 RODO.

13. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Inspektor Ochrony Danych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz budynków, pomieszczeń lub części pomieszczeń tworzący obszar, w którym przetwarzane są dane osobowe w formie papierowej.

14. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Inspektor Ochrony Danych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz wszystkich zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

15. Rejestr czynności prowadzonych przez Administratora

Utworzono przez Administratora – rejestr czynności przetwarzania .

16. Opis sposobu przepływu danych pomiędzy poszczególnymi systemami

Inspektor Ochrony Danych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis sposobu przepływu danych pomiędzy poszczególnymi systemami.

17. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Inspektor Ochrony Danych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej określone środki techniczne i organizacyjne niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. Aktualny opis stosowanych środków technicznych i organizacyjnych wykazane są w obszarach przetwarzania danych osobowych.

18. Zarządzanie incydentami bezpieczeństwa danych osobowych

Szczegółowy sposób zarządzania incydentami dot. ochrony danych osobowych reguluje przyjęta przez firmę „Polityka zarządzania incydentami bezpieczeństwa danych osobowych". Prowadzona przez Inspektora Ochrony Danych.

19. Wykaz zabezpieczeń

Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych, patrz Instrukcja zarządzania systemami informatycznymi.

W instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne

20. Regulamin Ochrony Danych Osobowych

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Osoba odpowiedzialną za stworzenie Regulaminu Ochrony Danych Osobowych jest Inspektor Ochrony Danych.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania poprzez Oświadczenie poufności

21. Analiza ryzyka

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Administrator jest odpowiedzialny za określenie listy zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania

Zagrożenia powinny być identyfikowane w odniesieniu zidentyfikowanych aktywów dla przeprowadzanych zbiorów – Lista potencjalnych aktywów

Wykaz przykładowych zagrożeń znajduje się w Lista potencjalnych zagrożeń

Wyliczenie ryzyka dla zagrożeń

Administrator określa Prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania.

Proponowaną skalę prawdopodobieństwa prezentuje Tabela A

Administrator określa Skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne

Proponowaną Skalę skutków prezentuje Tabela B

Administrator wylicza Ryzyka (R) dla zagrożeń i ich skutków w/g formuły: R = P * S

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
małe (do 100 PLN, incydent prasowy lokalny)	1
średnie (100-1000 PLN, incydent prasowy ogólnopolski)	2
duże (od 1000 PLN, naruszenie prawa)	3

Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem

Skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	WARTOŚĆ [R = P*S]
ryzyko pomijalne i akceptowalne (akceptujemy)	1-3
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	4-7
ryzyko jest nieakceptowalne (musimy obniżyć)	8-9

Analizę ryzyka przeprowadza się w przygotowanym do tego arkuszu. W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator przetwarzający dane osobowe zobowiązany jest do spełnienia wobec nich obowiązków, w tym celu opracowano klauzule informacyjne.

Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia może być on w formie mailowej skierowanej do osoby która będzie odpowiedzialna za obniżenie ryzyka.

Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych.

22. Procedura audytu

Celem audytów wewnętrznych jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Audyty prowadzone są w sposób obiektywny i bezstronny. Przestrzegana jest zasada, że audytorzy nie audytują własnej pracy.

1) Administrator jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych z roczną częstotliwością lub częściej
2) Administrator opracowuje programy audytów biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. Określa on kryteria audytu, jego cel, zakres i ewentualnie metody.
3) Administrator wyznacza audytora do przeprowadzenia audytu
4) Audytor jest zobowiązany do przygotowania się do przeprowadzenia audytu, zapoznając się z opisem audytowanego obszaru, stosowanych procedur i wyników poprzednich audytów
5) Audytor realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO
6) W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, audytor identyfikuje tzw. uchybienia lub spostrzeżenia
7) Wynik audytu zostaje udokumentowany przez audytora i przekazany Administratorowi
8) Administrator dokonuje przeglądu i analizy wyniku audytu oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych uchybień

23. Plan ciągłości działania:

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Administrator opracował zasady przywracania:

1. Zasady postępowania przy odtworzeniu systemu informatycznego

    a) W przypadku stwierdzenia krytycznej awarii sprzętu komputerowego wdrożono procedurę odzysku danych z dysku zewnętrznego, na którym tworzona jest kopia bezpieczeństwa Po uruchomieniu serwera osoba upoważniona podłącza go do sieci

    b) Przewidywany czas operacji uruchomienia– 72 godziny

    c) Procedurę odtworzenia należy wykonać w obecności ASI lub osoby upoważnionej do przywrócenia kopii bezpieczeństwa.

3. PLAN AWARYJNY NA WYPADEK BRAKU ZASILANIA W SIECI KOMPUTEROWEJ

    Wykorzystywane są laptopy z baterią, UPS, oraz agregat prądotwórczy

2 PLAN AWARYJNY NA WYPADEK UTRATY DOSTĘPU DO SIECI INTERNET

    W przypadku niedostępności Internetu , Administrator ma podpisaną biznesową umowę z dostawcą usługi, który zapewnia naprawę usterki do 24 godzin od momentu zgłoszenia.

24. Przepisy karne i porządkowe reguluje:

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).

25. Postanowienia końcowe

W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa Danych Osobowych mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).