POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

19 kwietnia 2019

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 – 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.

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 TDIKM Anna Jabłońska – Schmidt.

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 TDIKM Anna Jabłońska – Schmidt, 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

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) zapewnienia przestrzeganie przepisów o ochronie danych osobowych,

b) opiniowanie, pod względem zgodności z PBDO oraz z przepisami prawa umów, procedur i innych wytworzonych dokumentów dotyczących bezpieczeństwa i przetwarzania danych osobowych;

c) podejmowanie lub wnioskowanie o podjęcie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych oraz prowadzenie adekwatnej dokumentacji w tym zakresie;

3) **Inspektor Ochrony Danych** może wykonywać swoje obowiązki poprzez wyznaczonych zastępców.

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**, a także do wydawania w imieniu **Administratora Danych Osobowych** upoważnień do przetwarzania danych osobowych.

7. Osoby upoważnione do przetwarzania danych osobowych

1) Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:
   - zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki Bezpieczeństwa Danych Osobowych i Instrukcji Zarządzania Systemami Informatycznymi;
   - stosowanie się do zaleceń Inspektora Ochrony Danych;
   - przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych w pisemnym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków służbowych;
   - niezwłoczne informowanie Inspektora Ochrony Danych o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w firmie;
   - ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
   - korzystanie z systemów informatycznych firmy w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemów informatycznych;
   - bezterminowe zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
   - 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 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 (wzór upoważnienia stanowi załącznik Z2-PBDO) wydane przez Administratora Danych Osobowych oraz złożyły stosowne oświadczenie dot. właściwej realizacji przepisów RODO (wzór oświadczenia stanowi załącznik Z3-PBDO).
2) Administrator Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.

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 wniosek do niniejszej PBDO.
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.

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 EOG 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. 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.

14. Zarządzanie incydentami bezpieczeństwa danych osobowych

1) Zdarzeniami naruszającymi ochronę danych osobowych bądź stwarzającymi podejrzenie naruszenia zabezpieczeń tych danych mogą być następujące przypadki:
   - sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana itp.,
   - niewłaściwe parametry środowiska, takie jak np. nadmierna wilgotność, zbyt wysoka temperatura, oddziaływanie pola elektromagnetycznego,
   - awaria sprzętu lub oprogramowania, które wyraźnie wskazują na celowe działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu,
   - komunikaty alarmujące o próbie naruszenia zabezpieczeń systemu, który zapewnia ochronę danych bądź komunikat o podobnym znaczeniu,
   - odstępstwa od prawidłowego stanu danych wskazujące na niewłaściwe działania systemu

i niepożądaną jego modyfikację,

- naruszenie lub próba naruszenia integralności systemu bazy danych w tym systemie,
- modyfikacja lub próba modyfikacji danych oraz zmiana w strukturze danych dokonana bez odpowiedniego upoważnienia (autoryzacji),
- stwierdzenie niedopuszczalnej manipulacji danymi osobowymi w systemie,
- ujawnienie danych osobowych lub objętych tajemnicą procedur ochrony danych osobowych osobom nieupoważnionym, bądź innych elementów zabezpieczeń,
- funkcjonowanie sieci komputerowej lub praca systemu wykazuje nieprzypadkowe odstępstwo od prawidłowego rytmu pracy wskazujące na zaniechanie lub przełamanie ochrony danych osobowych -lub np. praca w sieci lub przy komputerze osoby do tego nieupoważnionej, sygnał o nieautoryzowanym logowaniu itp.,
- ujawnienie nieautoryzowanych kont dostępu do danych objętych ochroną,
- zniszczenie lub podmiana nośnika z danymi osobowymi bądź skasowanie lub skopiowanie danych osobowych w sposób niedozwolony lub przez osobę nieupoważnioną,
- rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji np. niewylogowanie się z systemu przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, niewykonanie w określonym terminie kopii bezpieczeństwa, praca na danych osobowych w celach prywatnych itp.,
- stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach, płytach CD /DVD w formie niezabezpieczonej itp.

2) Postępowanie w przypadku naruszenia danych osobowych.

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych każda osoba zatrudniona przy przewarzaniu tych danych jest obowiązana niezwłocznie powiadomić o tym fakcie Inspektora Ochrony Danych Osobowych i Administratora Danych Osobowych.
2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Inspektora Ochrony Danych Osobowych, Administratora Danych Osobowych lub upoważnionej osoby, należy:
   - niezwłocznie podjąć czynności niezbędnego powstrzymania niepożądanych skutków zaistniałego zdarzenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn i sprawców,
   - rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   - zaniechać - o ile to możliwe dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudniać udokumentowania i analizę,
   - podjąć inne stosowne działania przewidziane w instrukcjach technicznych

i technologicznych, dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej właściwe dla objawów sytuacji towarzyszącej naruszeniu,

- udokumentować wstępnie zaistniałe zdarzenie,
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Dyrektora lub upoważnionej osoby.

3. Po przybyciu na miejsce Inspektor Ochrony Danych Osobowych, Administrator Danych Osobowych lub osoba upoważniona:
   - zapoznaje się z zaistniałą sytuacją, identyfikuje rodzaj zaistniałego zdarzenia, dokonuje wyboru metody dalszego postępowania celem powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych osobowych,
   - może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również innych osób mogących posiadać informacje związane z zaistniałym zdarzeniem.
   - podejmuje decyzje o konieczności zgłoszenia incydentu do organu nadzorczego.

15. Przepisy karne i porządkowe

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).

16. 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).