

POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH W MODUS

I. POSTANOWIENIA OGÓLNE

§ 1

Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest zapewnienie przez MODUS właściwego oraz zgodnego z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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 (RODO), w zakresie ochrony danych osobowych związanych z ich przetwarzaniem w całości prawnie dozwolonych.

§ 2

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1. **RODO** - Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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
2. **Administrator Danych Osobowych (ADO)** – osoba, która samodzielnie lub wspólnie z innymi osobami ustala cele i sposoby przetwarzania danych osobowych;
3. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”), przy czym możliwa do zidentyfikowania osoba fizyczna to osoba, którą 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,
4. **Przetwarzanie danych osobowych** – 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;
5. **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest scentralizowany czy rozproszony funkcjonalnie czy geograficznie;
6. **Podmiot przetwarzający** – osoba fizyczna lub prawna jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
7. **Odbiorca** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego czy jest stroną trzecią, przy czym organy publiczne, które mogą otrzymywać dane w ramach konkretnego postępowania, nie są uznawane za odbiorców, a przetwarzanie tych danych przez organy publiczne musi być zgodne z przepisami o ochronie danych osobowych mającymi zastosowanie do celów przetwarzania;
8. **Strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
9. **Zgoda osoby** – 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. **Naruszenie ochrony danych osobowych** – 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;

11. **Przedsiębiorca** - osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;
12. **Użytkownik** – osoba korzystająca z Systemu Informatycznego;
13. **Upoważniona osoba** – osobę, która z upoważnienia administratora lub podmiotu przetwarzającego może przetwarzać dane osobowe;
14. **Administrator Systemu Informatycznego** (ASI) – osoba upoważniona do zarządzania Systemem Informatycznym przez Administratora Danych Osobowych,
15. **System Informatyczny** – system przetwarzania danych wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje;
16. **Zabezpieczenie systemu informatycznego** – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

II. DEFINICJA BEZPIECZEŃSTWA INFORMACJI

§ 3

1. Utrzymanie bezpieczeństwa przetwarzanych przez Administratora informacji rozumiane jest jako zapewnienie ich zgodności z prawem, rzetelności, przejrzystości, ograniczoności celu, minimalizacji danych, prawidłowości, ograniczeniu przechowywania, integralności i poufności oraz rozliczalności.
2. Poufność informacji – rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji;
3. Integralność informacji – rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania;
4. Dostępność informacji – rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
5. Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.
6. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
 - a. Niezaprzeczalności odbioru – rozumianej jako zdolność do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie;
 - b. Niezaprzeczalności nadania – rozumianej jako zdolność do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie;
 - c. Rozliczalności działań – rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane.

III. ZAKRES

§ 4

1. W systemie informacyjnym Administratora przetwarzane są informacje służące do wykonywania zadań niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.
2. Informacje te są przetwarzane lub składowane w postaci elektronicznej, jak i papierowej.
3. Administratorem danych osobowych osoby korzystającej ze strony www.modus.waw.pl w tym kontaktującej się za pośrednictwem poczty elektronicznej Modus Sp. z o.o. Sp. Kom. lub formularza kontaktowego (dalej: „Użytkownik”), jest Modus Sp. z o.o. Sp. Kom. z siedzibą przy ul. Zamienieckiej 80/501, 04-158 Warszawa.
4. W sprawach związanych z podanymi przez Użytkownika danymi osobowymi, Użytkownik może się kontaktować z powołanym przez Modus Sp. z o.o. Sp. Kom. Inspektorem Ochrony Danych Osobowych (ODO) pod adresem e-mail: odo@modus.waw.pl

§ 5

Politykę Bezpieczeństwa stosuje się do:

1. danych osobowych przetwarzanych w systemie informatycznym,
2. wszystkich informacji dotyczących danych personelu Administratora, w tym danych osobowych, treści zawieranych umów o pracę oraz wszelkich osób fizycznych lub przedsiębiorców współpracujących z Administratorem w oparciu o umowy cywilnoprawne,
3. wszystkich danych kandydatów do pracy lub współpracy na podstawie umów cywilnoprawnych zbieranych na etapie rekrutacji,
4. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5. rejestru osób dopuszczonych do przetwarzania danych osobowych,
6. innych dokumentów zawierających dane osobowe.

§ 6

1. Zakresy określone przez dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Administratora w szczególności do:
 - a. wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
 - b. wszystkich lokalizacji – budynków lub pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
 - c. wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie, w tym współpracujących z Administratorem, również na podstawie umów cywilnoprawnych.
2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązany jest cały personel, w tym wszyscy pracownicy w rozumieniu Kodeksu Pracy, konsultanci, stażyści oraz inne osoby współpracujące na podstawie umów cywilnoprawnych, a także inne osoby lub podmioty mające dostęp do informacji podlegających ochronie na podstawie umów o powierzenie przetwarzania danych.

§ 7

Informacje niejawne nie są objęte zakresem niniejszej Polityki Bezpieczeństwa Informacji.

IV. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA INFORMACJI

§ 8

1. Dokumenty Polityki Bezpieczeństwa Informacji ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Dokumenty Polityki Bezpieczeństwa Informacji składają się z:
 - a. Niniejszego dokumentu Polityki Bezpieczeństwa Informacji,
 - b. Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych u Administratora – Załącznik numer 1 do niniejszej Polityki Bezpieczeństwa Informacji,
 - c. Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, opisującej tryb postępowania w sytuacjach naruszenia, zabezpieczenia zasobów danych osobowych, zaobserwowanych prób naruszenia tego zabezpieczenia, a także uzasadnionego podejrzenia o przygotowywanej próbie naruszenia.

V. DOSTĘP DO INFORMACJI

§ 9

Wszystkie osoby, których rodzaj wykonywanej pracy lub współpraca z Administratorem na innej podstawie niż stosunek pracy wiąże się z dostępem do danych osobowych zawierają umowy celem realizacji niniejszej Polityki Bezpieczeństwa Informacji w zakresie ochrony danych

osobowych oraz przestrzegania obowiązujących w tym zakresie przepisów prawa, a także odpowiedzialności prawnej za ich naruszenie, a także odnoszących się do Informacji Poufnych.

§ 10

Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, mogą być udostępnione jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

§ 11

Pomieszczenia, w których przetwarzane są dane osobowe, powinny być chronione, a w szczególności na czas nieobecności w nich osób przetwarzających dane zgodnie z upoważnieniem Administratora, w sposób uniemożliwiający dostęp do nich osób trzecich.

§ 12

Dane osobowe mogą być udostępnione się na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać zakres i przeznaczenie w zgodzie z obowiązującymi w tym zakresie przepisami prawa.

VI. ZARZĄDZANIE DANymi OSOBOWYMI

§ 13

1. Za bezpieczeństwo danych osobowych Jednostki, odpowiadają:
 - a. Administrator – osoba upoważniona do reprezentacji podmiotu,
 - b. Inspektor Ochrony Danych Osobowych (IODO), w przypadku jego powołania przez Administratora,
 - c. Administrator Systemy Informatycznego, w przypadku jego ustanowienia przez Administratora lub podmioty z którymi Administrator zawarł umowy na dostawę poczty mailowej oraz obsługę informatyczną.
2. Administrator lub powołany Inspektor Danych Osobowych lub inny umocowany przedstawiciel Administratora realizując Politykę Bezpieczeństwa Informacji ma prawo wydawać instrukcje regulujące kwestie związane z ochroną danych w strukturach Administratora.
3. W umowach zawieranych przez Administratora winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych udostępnionych przez Administratora.

§ 15

Zapoznanie się z dokumentami określonymi w § 8 punkt 2 niniejszej Polityki Bezpieczeństwa Informacji, wszystkie osoby, zarówno Pracownicy Administratora, jak i osoby współpracujące na innej podstawie niż stosunek pracy z Administratorem, potwierdzając własnoręcznym podpisem w sposób przyjęty u Administratora zgodnie z oświadczeniem stanowiącym Załącznik numer 2 do niniejszej Polityki Bezpieczeństwa Informacji.

§ 16

Ochrona zasobów danych osobowych Administratora jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników Administratora lub osób współpracujących z Administratorem na innej podstawie prawnej niż stosunek pracy.

VII. ZAKRESY ODPOWIEDZIALNOŚCI

§ 17

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Administratora, jak też wszystkie osoby współpracujące z Administratorem na innej podstawie prawnej niż stosunek pracy.

§ 18

Administrator zobowiązany jest do przestrzegania wszystkich przepisów o ochronie danych, w szczególności poprzez:

1. określanie indywidualnych obowiązków i odpowiedzialności osób zajmujących się przetwarzaniem danych osobowych,
2. zapoznanie osób zajmujących się przetwarzaniem danych osobowych z przepisami obowiązującymi w tym zakresie,
3. wdrażanie i nadzorowanie przestrzegania Polityki Bezpieczeństwa Informacji,
4. wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
5. działanie zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych,
6. stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania przepisów o ochronie danych osobowych,
7. odpowiedzialność za poprawność merytoryczną danych gromadzonych w systemach informacyjnych,
8. określanie, które osoby i na jakich prawach mają dostęp do danych informacji, przy czym w realizacji powyższych zadań Administratora wspierają oraz zapewniają bezpieczeństwo danych podmiot będący dostawcą usług poczty mailowej oraz podmiot zapewniający obsługę informatyczną systemów informatycznych.

VIII. PRZETWARZANIE DANYCH OSOBOWYCH

§ 20

1. Przetwarzanie danych osobowych następuje w pomieszczeniach odpowiednio zabezpieczonych.
2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być chronione w taki sposób aby na czas nieobecności w nich osób przetwarzających dane, nie był możliwy dostęp do nich osób trzecich.

§ 21

1. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć w stopniu uniemożliwiającym ich odczytanie, w szczególności w niszczarkach.
2. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora.

§ 22

W związku z przetwarzaniem danych osobowych, Użytkownik ma ponadto prawo żądać:

1. udzielenia informacji na temat przetwarzania jego danych osobowych.
2. sprostowania danych – w przypadku, gdy dane są nieaktualne, niekompletne lub z innego powodu niepoprawne,
3. ograniczenia przetwarzania danych (np. wyłącznie do ich przechowywania) przez określony czas, w przypadku:
 - a. zakwestionowania przez Użytkownika prawidłowości danych osobowych – na okres pozwalający Administratorowi sprawdzić ich prawidłowość,
 - b. rozpatrywania sprzeciwu Użytkownika,
 - c. gdy Użytkownik uzna, że przetwarzanie danych jest niezgodne z prawem i skorzystają z prawa do ograniczenia przetwarzania, zamiast żądania usunięcia danych osobowych,
 - d. gdy dalsze przetwarzanie danych przez Administratora w ograniczonym zakresie będzie potrzebne Użytkownikowi do ustalenia lub obrony ewentualnych roszczeń;
4. usunięcia danych osobowych („prawo do bycia zapomnianym”) – w przypadku, gdy:

- a. dane osobowe nie są już niezbędne do celów, w których zostały zebrane,
- b. skutecznie zostanie cofnięta zgoda na ich przetwarzanie (o ile nie mamy prawa przetwarzać danych na innej podstawie prawnej),
- c. skutecznie zostanie złożony sprzeciw wobec przetwarzania danych Użytkownika,
- d. doszłoby do przetwarzania danych niezgodnego z prawem,
- e. jeśli konieczność usunięcia danych wynika z ciężącego na Administratorze obowiązku prawnego.

§ 23

W przypadku wątpliwości/pytań odnośnie przetwarzania danych osobowych lub chęci skorzystania z przysługujących praw – prosimy o kontakt z naszym Inspektorem Ochrony Danych Osobowych (odo@modus.waw.pl, ul. Zamieniecka 80/501 Warszawa). W przypadku wyczerpania przysługujących Użytkownikowi praw względem Administratora i uznania, że przetwarzanie jego danych osobowych przez Administratora narusza przepisy dotyczące ochrony danych osobowych, informujemy o prawie do wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa, www.uodo.gov.pl.

IX. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI PRZETWARZANYCH DANYCH

§ 24

W Jednostce rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:
 - *pomieszczenia zamykane na klucz,*
 - *szafy pancerne z zamkami,*
2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
 - *przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby bez możliwości dostępu do tych danych osób nieuprawnionych,*
3. Zabezpieczenia organizacyjne:
 - ustalenie podmiotów zajmujących się zabezpieczeniem systemów informatycznych Administratora,
4. Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:
 - wykaz personelu Administratora uprawnionych do przetwarzania danych osobowych,
 - przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie przyznane przez Administratora – Załącznik numer 3 do niniejszej Polityki Bezpieczeństwa Informacji oraz Załącznik numer 4 do niniejszej Polityki Bezpieczeństwa Informacji – Rejestr upoważnień,
 - w trakcie przetwarzania danych osobowych, upoważniona osoba jest osobiście odpowiedzialna za bezpieczeństwo powierzonych mu danych,
 - przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, upoważniona osoba winna sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,
 - w trakcie przetwarzania danych osobowych, upoważniona osoba winna dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,
 - po zakończeniu przetwarzania danych upoważniona osoba winna należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

X. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§ 25

Archiwizacja informacji zawierających dane osobowe odbywa w formie elektronicznej oraz papierowej. Nośniki danych przechowywane są w zamkniętych pomieszczeniach i są zabezpieczone przed dostępem osób nieupoważnionych.

Warszawa dnia 25 maja 2018 roku

Mirosław Cieślak

Za Administratora