POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH NEW PLAYERS POLAND SP. Z O.O.

Spis treści

I WPROWADZENIE 1
II PODSTAWA PRAWNA 2
III SŁOWNICZEK 2
IV PRZETWARZANIE DANYCH OSOBOWYCH 5
Dane osobowe 5
Przetwarzanie danych osobowych 6
Zasady przetwarzania danych 9
Powierzenie przetwarzania danych 11
Udostępnianie danych 12
Rejestrowanie czynności przetwarzania 13
V UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH 14
VI OBOWIĄZKI PODMIOTOWE W OBSZARZE OCHRONY DANYCH OSOBOWYCH 15
Obowiązki Administratora Danych Osobowych 16
Obowiązki Inspektora Ochrony Danych 18
Obowiązki Upoważnionych 19
VII OCENA RYZYKA I PRZEGLĄDY 20
VIII ZAGROŻENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH ORAZ INCYDENTY 21
Instrukcja postępowania w przypadku zagrożenia bezpieczeństwa danych osobowych 21
Instrukcja postępowania w przypadku incydentów bezpieczeństwa danych osobowych 22
IX WYKAZY 25
Środki organizacyjne 25
Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych 26
Środki ochrony fizycznej danych 26

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej oraz opis działalności administratora danych osobowych, obszar przetwarzania danych osobowych i sprzęt wyorzystywany do przetwarzania danych osobowych
……...27
Środki ochrony w ramach narzędzi programowych i baz danych
……29
X POSTANOWIENIA KOŃCOWE 30

I. WPROWADZENIE

Polityka Bezpieczeństwa Danych Osobowych, zwana dalej Polityką, została sporządzona przez Spółkę New Players Poland sp. z o.o. z siedzibą w Niepołomicach (32-005) przy ul. Nagietkowej 33, zwana dalej Administratorem w związku z wymaganiami 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 – dalej Rozporządzenie UE) oraz ustawy krajowej o ochronie danych osobowych.

Niniejszy dokument stanowi zbiór spójnych, precyzyjnych reguł i procedur, według których Administrator buduje, zarządza oraz udostępnia zasoby i systemy informacyjne i informatyczne. Ustanawia przewidziane do wykonania działania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych. Polityka ustanawia zasady bezpieczeństwa przetwarzania danych osobowych, które powinny być przestrzegane i stosowane przez Administratora i przez wszystkie osoby przetwarzające dane osobowe, wraz z powołaniem na właściwe podstawy prawne. Polityka reguluje zasady organizacji pracy przy zbiorach danych osobowych przetwarzanych w systemie informatycznym oraz metodami tradycyjnymi. Opisano w niej również zagrożenia bezpieczeństwa przetwarzanych danych osobowych oraz sposoby reakcji na przypadki naruszeń bezpieczeństwa.

Niniejszy dokument pełni również funkcję informacyjną i edukacyjną, poprzez zaprezentowanie obowiązków i odpowiedzialności osób związanych z przetwarzaniem danych osobowych. Administrator stosuje adekwatne do sytuacji

środki, aby zapewnić bezpieczeństwo informacji oraz danych osobowych, które przetwarza.

Uzupełnieniem i dopełnieniem naszej Polityki jest Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (załącznik nr 1), ustanawiająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.

II. PODSTAWA PRAWNA

Zasady przetwarzania danych osobowych w szczególności regulują:

- 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 (dalej zwane RODO)
- Ustawa o ochronie danych osobowych z dnia 10.5.2018 ze zmianami
- Ustawa o świadczeniu usług drogą elektroniczną
- Kodeks pracy i przepisy o ochronie danych w zakresie zatrudnienia

III. SŁOWNICZEK

IOD – Inspektor Ochrony Danych, będący wyznaczoną przez Administratora Danych Osobowych osobą nadzorującą stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną.

ADO – Administrator Danych Osobowych, będący organem, jednostką organizacyjną, podmiotem lub osobą fizyczną, decydujący o celach i środkach przetwarzania danych osobowych.

ASI – Administrator Systemu Informatycznego, będący wyznaczoną przez Administratora Danych Osobowych osobą odpowiedzialną za prawidłowe funkcjonowanie sprzętu, oprogramowania i ich konserwację, w zakresie wskazanym przez ADO.

Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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 (IP), w tym dane pobierane dzięki plikom cookies lub jeden bądź kilka szczególnych czynników określających fizyczną,

fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dane wrażliwe (tzw. szczególna kategoria danych) - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, korzystania z usług medycznych, seksualności lub orientacji seksualnej oraz dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.

Dane wrażliwe dot. wyroków skazujących oraz czynów zabronionych: dane osobowe szczególnej kategorii, które wolno przetwarzać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone przepisami prawa.

Prezes UODO – Prezes Urzędu Ochrony Danych Osobowych, będący organem powołanym do spraw z zakresu ochrony danych osobowych**.**

Podmiot – podmiot wskazany na pierwszej tytułowej stronie Polityki, dla celów którego niniejsza Polityka zostaje opracowana i wdrożona**.**

Polityka – niniejszy dokument Polityki Bezpieczeństwa Danych Osobowych.

Przetwarzanie danych – oznacza 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.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Upoważniony – osoba posiadająca formalne upoważnienie wydane przez Administratora Danych Osobowych lub przez osobę wyznaczoną, uprawniona do przetwarzania danych osobowych.

Usuwanie danych – zniszczenie danych osobowych lub ich modyfikacja, która uniemożliwia ustalenie tożsamości osoby, której dane dotyczą.

Ograniczenie przetwarzania - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzani.

Profilowanie - oznacza 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.

Pseudonimizacja - oznacza 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.

Zbiór danych - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

Odbiorca - oznacza 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;

Strona trzecia - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które - z upoważnienia administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe.

Zgoda osoby, której dane dotyczą - oznacza 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.

Naruszenie ochrony danych osobowych - oznacza 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.

Dane genetyczne - oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.

Dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

Dane dotyczące zdrowia - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia, w tym dot. nałogów.

Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem

Zgoda osoby, której dane dotyczą – oznacza 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.

Identyfikator użytkownika (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych
w systemie informatycznym.

Hasło – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

IV. PRZETWARZANIE DANYCH OSOBOWYCH

Dane osobowe

Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przy rozstrzyganiu czy określona informacja lub informacje stanowią dane osobowe, Podmiot dokonuje zindywidualizowanej oceny, przy uwzględnieniu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby.

Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy

fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Danymi osobowymi będą zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia.

Przetwarzanie danych osobowych

Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy gdy:

1. kiedy osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2. kiedy przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3. kiedy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4. kiedy przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5. kiedy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6. kiedy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Podmiot przetwarza dane wrażliwe (tzw. szczególnej kategorii danych) w zakresie zadań Administratora w ramach świadczenia usług szkoleniowych:

1. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego przewidują, że osoba, której dane dotyczą, nie może uchylić zakazu;
2. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej;

3. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
4. przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
5. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
6. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
7. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
8. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego;
9. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym

   w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
10. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, na podstawie prawa Unii Europejskiej lub prawa państwa członkowskiego, które

są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Obowiązki informacyjne o przetwarzaniu danych

W przypadku zbierania danych od osoby, której te dane dotyczą, Administrator Danych Osobowych podaje jej wszystkie następujące informacje:

1. swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
2. dane kontaktowe inspektora ochrony danych;
3. cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
4. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) Rozporządzenia RODO – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią, w szczególności: marketing bezpośredni, monitoring;
5. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
6. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony;
7. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
8. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
9. informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
10. jeżeli przetwarzanie odbywa się na podstawie zgody – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
11. informacje o prawie wniesienia skargi do organu nadzorczego;
12. informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane

dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

13. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 Rozporządzenia RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Podanych wyżej zasad nie stosuje się, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub jeżeli osoba, której dane dotyczą, posiada już te informacje.

W przypadku zbierania danych nie od osoby, której te dane dotyczą Administrator Danych Osobowych jest zobowiązany poinformować tę osobę bezpośrednio po utrwaleniu danych dodatkowo o:

1. źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
2. kategoriach odnośnych danych osobowych.

Podanych wyżej zasad nie stosuje się, jeżeli:

1. przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
2. poinformowanie wymaga niewspółmiernie dużego wysiłku – w szczególności, gdy dane przetwarzane są w celach archiwizacyjnych, statystycznych, badań naukowych,
3. przekazanie informacji okazuje się niemożliwe,
4. utrwalenie lub ujawnienie danych jest wyraźnie nakazane prawem UE lub prawa krajowego,
5. dotyczy to tajemnicy zawodowej wynikającej z prawa UE lub prawa krajowego.

Zasady przetwarzania danych

Podmiot realizuje obowiązki poprzez dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, zapewniając aby dane te były:

1. **przetwarzane zgodnie z prawem,**
   (zgodne z wszelkimi normami prawa, zarówno tymi już istniejącymi w momencie wejścia w życie Rozporządzenia RODO, jak i tymi, które dopiero później zostały wprowadzone do porządku prawnego. Zgodność z prawem

dotyczy przestrzegania zarówno przepisów prawa materialnego, jak i przepisów dotyczących postępowania);

2. **zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;**
3. **merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,** (informacje wynikające z danych przetwarzanych przez administratora są zgodne z prawdą, kompletne oraz odpowiadają aktualnemu stanowi rzeczy. Administrator Danych Osobowych przetwarza dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane);
4. **przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;**
5. Administrator Danych Osobowych **stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną**, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Dodatkowo Podmiot zapewnia bezpieczeństwo informacji poprzez:

1. **poufność informacji**
   (informacje nie są udostępniane lub wyjawiane osobom nieupoważnionym, osoby nieuprawnione nie mają dostępu do danych),
2. **integralność informacji**
   (informacje są kompletne i niezmieniane w sposób nieuprawniony),
3. **dostępność informacji**
   (informacje są dostępne dla upoważnionych pracowników)
4. **rozliczalność działań**
   (wszystkie istotne czynności wykonane przy przetwarzaniu danych zostały zarejestrowane i jest możliwe zidentyfikowanie osoby, która daną czynność wykonała),
5. **niezawodność działań**
   (wykonywane czynności prowadzi do zamierzonych skutków).
6. **minimalizacja danych** – podmiot wdraża procedury służące realizacji zasady minimalizacji przetwarzania danych osobowych pod względem:

a. adekwatności danych osobowych do celów przetwarzania, obejmujących ograniczenie ilości przetwarzanych danych osobowych oraz zakresu przetwarzania do celu przetwarzania,
b. ograniczenia dostępu do danych osobowych wyłącznie do osób upoważnionych, dla których wykorzystanie danych osobowych w określonym zakresie jest niezbędne dla prawidłowej realizacji obowiązków,
c. ograniczenia czasu przechowywania danych osobowych do okresu, dla którego przechowywanie danych osobowych jest niezbędne ze względu na realizację celu przetwarzania lub obowiązków nałożonych na Podmiot,

7. podmiot dokonuje okresowego przeglądu ilości przetwarzania danych, nie rzadziej niż raz w roku,
8. dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów Podmiotu, jak również z akt podręcznych i głównych. Dane takie mogą być archiwizowane i być na kopiach zapasowych systemów i informacji przetwarzanych bądź przechowywanych przez Administratora.
9. procedurę archiwizacji i korzystania z archiwum, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

Powierzenie przetwarzania danych

W przypadku konieczności przetwarzania danych przez odrębne podmioty świadczące usługi dla Administratora Danych Osobowych może on powierzyć ich przetwarzanie. Powierzenie przetwarzania odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Administrator Danych Osobowych prowadzi dokument Ewidencji podmiotów, którym Podmiot powierza dane osobowe (zał. nr 2).

Powierzenie nie polega na udostępnieniu danych. Udostępnienie jest przekazaniem danych innemu podmiotowi (odbiorcy danych), który staje się ich administratorem zaś powierzenie polega na przetwarzaniu danych przez podmiot, który nie jest administratorem tych danych.

Współadministratorzy

Administrator ustala możliwość tworzenia zasad współadministrowania danymi osobowymi poprzez wspólne ustalenie celów i sposobów przetwarzania danych. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określą odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji. W uzgodnieniach można będzie wskazać punkt kontaktowy dla osób, których dane dotyczą.

Udostępnianie danych

Udostępnianie danych osobowych, jest jedną z form ich przetwarzania. udostępnianie innemu administratorowi, by każdy z nich wykorzystywał je do realizacji własnych celów. Udostępnianie danych osobowych można określić, jako wszelkie działania umożliwiające innym niż administrator podmiotom, zapoznanie się z nimi. Pamiętamy, że:

1. nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie.
2. nie jest istotne, czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd., aby czynność była uznana za udostępnianie.
3. udostępnianie danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa.
4. udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione lub za zgodą osoby.

Administrator Danych Osobowych lub osoba przez niego upoważniona prowadzi dokument Ewidencji podmiotów, którym Podmiot udostępnia dane osobowe (zał. nr 3). Dokument zawiera informacje o udostępnieniu danych osobowych na rzecz wszystkich podmiotów, z wyłączeniem:

1. osób Upoważnionych do przetwarzania danych osobowych,
2. osób, których dane dotyczą,
3. organów państwowych lub samorządu terytorialnego, którym dane osobowe są udostępniane w związku z prowadzonym postępowaniem.

Przekazywanie danych do Państwa trzeciego lub organizacji międzynarodowej

Podmiot przekazują dane osobowe do Państwa trzeciego – Stanów Zjednoczonych Ameryki poprzez wykorzystywanie usług i narzędzi Google LLC, co nie wpływa na prawa i wolność osób trzecich.

Dane osobowe są przekazywane do odbiorców w państwach trzecich, tj. poza Europejski Obszar Gospodarczy (EOG), Unii Europejskiej lub do organizacji międzynarodowych. Informujemy, że przekazujemy dane osobowe podmiotom ze Stanów Zjednoczonych, natomiast takim, które przystąpiły do programu Privacy Shield, na podstawie decyzji wykonawczej Komisji Europejskiej z dnia 12 lipca 2016 r. Wszelkie informacje znajdują się na stronie Komisji Europejskiej dostępnej pod adresem: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacyshield_pl. Podmioty, które przystąpiły do programu Privacy Shield, gwarantują, że będą przestrzegać wysokich standardów w zakresie ochrony danych osobowych, jakie obowiązują na terenie Unii Europejskiej, dlatego korzystanie z ich usług i oferowanych technologii w procesie przetwarzania danych osobowych jest zgodne z obowiązującym prawem o ochronie danych osobowych.

Aby uniknąć sytuacji nieautoryzowanego eksportu danych, w szczególności z wykorzystaniem publicznych dostępnych usług chmurowych, Podmiot okresowo weryfikuje zachowania użytkowników, a w miarę możliwości udostępnia zgodnie z prawem – rozwiązania równoważne.

Rejestrowanie czynności przetwarzania

Administrator Danych Osobowych prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze tym zamieszcza wszystkie następujące informacje:

1. imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych, jeśli będzie powołany;
2. cele przetwarzania;
3. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
4. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
5. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w np. 49 ust. 1 akapit drugi Rozporządzenia RODO, dokumentacja odpowiednich zabezpieczeń;
6. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych; g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych

środków bezpieczeństwa, o których mowa w np. 32 ust. 1. (Rejestr czynności przetwarzania danych osobowych dla Administratora stanowi załącznik nr 4.1. do niniejszej Polityki oraz rejestr czynności przetwarzania dla Procesora stanowi załącznik nr 4.2.).

V. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych uprawnione są wyłącznie osoby Upoważnione do przetwarzania danych osobowych.
2. Każdy upoważniony ma dostęp do danych osobowych na własnych poziomach dostępu, nadawanych przez wyznaczone do tego osoby.
3. Celem niniejszej procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych osobowych i utraty ich poufności przez osoby nieupoważnione.
4. Administrator ma zabezpieczoną sieć WI-FI, do której osoba trzecia, w tym klient nie ma dostępu do sieci produkcyjnej.
5. Administrator Danych Osobowych jest uprawniony do przyznawania upoważnień w przedmiocie przetwarzania danych osobowych, w drodze pisemnego Upoważnienia do przetwarzania danych osobowych (zał. Nr 5),
6. Administrator Danych Osobowych może wyznaczyć osoby uprawnione do przyznawania upoważnień w przedmiocie przetwarzania danych osobowych, w drodze pisemnego uprawnienia.
7. Upoważnienie do przetwarzania danych osobowych następuje wyłącznie na podstawie indywidualnego upoważnienia nadanego zgodnie z przepisami ustawy o ochronie danych osobowych.
8. Nadanie upoważnienia do przetwarzania danych osobowych musi nastąpić przed rozpoczęciem przetwarzania danych przez osobę upoważnioną.
9. Administrator Danych Osobowych lub osoba przez niego upoważniona prowadzi dokument Ewidencji osób upoważnionych do przetwarzania danych osobowych (zał. Nr 6).
10. W przypadku konieczności nadania bądź zmiany uprawnień (np. z powodu zatrudnienia osoby lub zmiany stanowiska pracy), Administrator Danych Osobowych lub osoba przez niego upoważniona zobowiązany jest do sprawdzenia, czy dana osoba:
    a. odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych,

b. będzie przetwarzała dane osobowe w zakresie i celu określonym w Polityce
i instrukcji zarządzania systemem informatycznym.

11. Nadanie upoważnienia do przetwarzania danych osobowych wymaga zaznajomienia się z przepisami dotyczącymi ochrony danych osobowych, w zakresie niezbędnym do czynności wykonywanych w ramach udzielonego upoważnienia.

12. Administrator Danych Osobowych jest odpowiedzialny za organizację i przeprowadzenie szkoleń lub zaznajomienie w innej formie osób upoważnionych z przepisami dotyczącymi ochrony danych osobowych.

13. Odbycie szkolenia z zakresu ochrony danych osobowych zostaje potwierdzone przez osobę w nim uczestniczącą w formie pisemnego Potwierdzenia uczestnictwa w szkoleniu (zał. Nr 7).

VI. OBOWIĄZKI PODMIOTOWE W OBSZARZE OCHRONY DANYCH OSOBOWYCH

Polityka obowiązuje wszystkich pracowników oraz współpracowników Administratora Danych. Za przestrzeganie i utrzymanie postanowień Polityki odpowiadają:

1. Administrator,
2. Komórki organizacyjne, w których przetwarza się dane,
3. Pracownicy, Współpracownicy, Podwykonawcy – Procesorzy Danych Osobowych.

Dla skutecznej realizacji polityki, uwzględniając zakres, kontekst, cele przetwarzania oraz ryzyko naruszeń prawo lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zapewnia się:

1. wdrożenie odpowiednich środków technicznych i organizacyjnych, które zapewniają zgodność przetwarzania danych osobowych z prawem oraz niezbędne zabezpieczenie przetwarzania danych,
2. stałe monitorowanie zgodności przetwarzania danych osobowych z wymogami prawa oraz poddawanie środków, o których mowa w powyższym punkcie ciągłym przeglądom oraz uaktualnieniu,
3. kontrolę i nadzór nad przetwarzaniem danych osobowych.

Obowiązki Administratora Danych Osobowych

Nadzór nad przestrzeganiem Polityki zapewnia Administrator. Nadzór, zmierza do zapewnienia, że czynności związane z przetwarzaniem Danych są zgodne z prawem i zasadami Polityki.

Podmiot zapewnia zgodność postępowania kontrahentów, w tym Podmiotów przetwarzających z postanowieniami Polityki w zakresie ich przetwarzania danych, w tym przechowywania.

Polityka przechowywana jest i udostępniania w wersji papierowej w każdym budynku, w którym przetwarzane są dane osobowe przez Administratora i elektronicznej na komputerze Administratora Danych.

Politykę udostępnia się:

1. Obligatoryjnie wszystkim osobom upoważnionym do przetwarzania danych osobowych, celem zapewnienia osobom upoważnionym dostępu do wiedzy i informacji na temat zasad przetwarzania danych osobowych.
2. Na żądanie osób mających interes prawny można udostępniać wyciąg z Polityki w zakresie nienaruszającym bezpieczeństwa informacji danych przetwarzanych przez Administratora, z wyłączeniem zasad zabezpieczenia danych.

Poniżej przedstawiamy obowiązki Administratora Danych Osobowych ze wskazaniem podziału zadań i obowiązków związanych z organizacją ochrony danych osobowych,:

1. podejmowanie odpowiednich i niezbędnych działań mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności poprzez sporządzanie i wdrażanie właściwych warunków organizacyjnych i technicznych,

2. wprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych,

3. w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi UODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,

4. w przypadku gdy dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia

praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny ryzyka planowanych operacji przetwarzania dla ochrony danych osobowych (zgodnie z załącznikiem nr 8 niniejszej Polityki).

5. wyznaczenie Inspektora Ochrony Danych, jeśli będzie to konieczne z uwagi na przepisy o ochronie danych bądź Podmiot uzna fakultatywnie konieczność powołania IOD,
6. w przypadku powołania IOD Podmiot zapewnieni IOD środki i organizacyjną odrębność, w tym środki niezbędne do niezależnego wykonywania przez niego zadań,
7. udokumentowanie powołania Inspektora Ochrony Danych poprzez wypełnienie Oświadczenia o powołaniu Administratora Bezpieczeństwa Informacji (zgodnie z zał. Nr 9 niniejszej Polityki),
8. w przypadku powołania IOD Podmiot zawiadomieni Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu Inspektora Ochrony Danych, w terminie 14 dni od dnia wyznaczenia poprzez wypełnienie na stronie internetowej urzędu (www.biznes.gov.gov.pl) wniosku o powołaniu nowego inspektora danych osobowych, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora,
9. egzekwowanie ciągłego i stabilnego rozwoju środków bezpieczeństwa przetwarzania danych osobowych zgodnie z rozwojem techniki, potrzebami, możliwościami technicznymi i finansowymi Podmiot,
10. poddawanie przeglądom skuteczność Polityki bezpieczeństwa przetwarzania danych osobowych przynajmniej raz w roku celem dokonania oceny sposobu ochrony danych,
11. zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez: organizację i nadzorowanie przestrzegania zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej,
12. prowadzenie dokumentacji opisującej zastosowaną politykę bezpieczeństwa przetwarzania danych osobowych (niniejsza Polityka oraz wynikające z niej instrukcje i procedury),
13. wdrożenie zapoznania z przepisami dotyczącymi ochrony danych osobowych oraz zagrożeniami związanymi z przetwarzaniem danych przez pracowników, zleceniobiorców i innych osób współpracujących,

14. zapewnienie kontroli nad tym, jakie dane osobowe, przez kogo i kiedy zostały wprowadzone do zbioru,
15. nadawanie i uchylanie uprawnień do przetwarzania danych osobowych w Podmiocie,
16. prowadzenie rejestru osób Upoważnionych do przetwarzania danych, zawierającego imię i nazwisko Upoważnionego, datę nadania i ustania, zakres Upoważnienia do przetwarzania danych osobowych, identyfikator w przypadku gdy Upoważniony został zarejestrowany w systemie informatycznym, służącym do przetwarzania danych osobowych,
17. zapewnienie zapoznania osób Upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
18. analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia ochrony danych osobowych i przygotowanie zaleceń i rekomendacji dotyczących eliminacji ryzyka ich ponownego wystąpienia,
19. prowadzenie zgodnych z Instrukcjami działań w przypadku stwierdzenia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych,
20. zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia,
21. dbałość o prawidłowe przetwarzanie danych osobowych, w szczególności poprzez zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu.

Obowiązki Inspektora Ochrony Danych

W przypadku powołania IOD ustala się zakres obowiązków Inspektora Ochrony Danych, na które składają się:

1. informowanie ADO oraz jego pracowników i współpracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
2. monitorowanie przestrzegania rozporządzenia, innych przepisów Unii Europejskiej 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,

3. udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
4. współpraca z organem nadzorczym w zakresie ochrony danych osobowych,
5. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w np. 36 Rozporządzenia RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
6. pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia,
7. wspieranie ADO w prowadzeniu rejestru czynności na danych osobowych.

Obowiązki Upoważnionych

Od osób upoważnionych do dostępu do danych osobowych wymagana jest:

1. znajomość Polityki oraz przepisów powszechnie obowiązującego prawa w obszarze ochrony danych osobowych, przetwarzanych przez Podmiot.
2. znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej,
3. przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami, w granicach przyznanego upoważnienia,
4. postępowanie zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych, w szczególności stosowania procedur w zakresie ochrony danych,
5. zachowanie w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia, również po ustaniu zatrudnienia, czy innego stosunku prawnego,
6. ochrona danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
7. informowanie o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe do przełożonego, który ma obowiązek poinformować Inspektora Ochrony Danych.

VII. OCENA RYZYKA I PRZEGLĄDY

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka, stosuje się średni poziom bezpieczeństwa.

1. Przegląd stanu ochrony przetwarzanych przez Podmiot danych jest przeprowadzany przynajmniej raz w roku.
2. Przegląd stanu ochrony przetwarzanych przez Podmiot danych osobowych przeprowadzają Administrator Danych Osobowych lub wyznaczeni kontrolerzy wewnętrzni na zasadach określonych w umowach powierzenia danych osobowych.
3. Przegląd obejmuje wszystkie obszary działalności i elementy infrastruktury Podmiotu, w których wymagane jest przestrzeganie zasad przetwarzania danych osobowych, w szczególności systemy informatyczne, zabezpieczenia fizyczne oraz organizacyjne.
4. Kontrolujący przygotowuje plan przeglądu z uwzględnieniem jego zakresu oraz niezbędnych zasobów, takich jak czas i ilość osób dokonujących czynności.
5. Przegląd jest protokołowany, a wzór protokołu stanowi załącznik nr 10 (Sprawozdanie ze sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych).
6.
7. Kontrolujący opracowuje wyniki przeprowadzonego przeglądu, które następnie przekazuje w formie Raportu z przeglądu Administratorowi Danych Osobowych, ewentualnie również kierownikowi kontrolowanej jednostki.
8. Na podstawie raportu pokontrolnego Administrator Danych Osobowych inicjuje działania zapobiegawcze lub kontrolujące, zmierzające do właściwego zabezpieczenia danych osobowych w przyszłości.
9. Ocena ryzyka przetwarzania danych znajduje się w załączniku Ocena ryzyka (załącznik nr 11 do Polityki bezpieczeństwa).

VIII. ZAGROŻENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH ORAZ INCYDENTY

Na bezpieczeństwo procesu przetwarzania danych osobowych składają się rozliczalność, poufność i integralność przetwarzanych danych. Rozliczalność oznacza możliwość przypisania działań osoby jednoznacznie i wyłącznie tej osobie. Poufność wyraża się zapewnieniem, że przetwarzane dane osobowe nie są udostępniane nieupoważnionym podmiotom. Integralność oznacza zapewnienie niemożliwości zmiany lub nieautoryzowanego zniszczenia danych osobowych.

W przypadku stwierdzenia naruszenia ochrony danych osobowych lub ich zagrożenia, każdy pracownik jest zobowiązany poinformować o tym fakcie Administratora Danych Osobowych, właściwą osobę przez niego upoważnioną lub przełożonego. Osoba upoważniona lub przełożony pracownika czy współpracownika jest zobowiązany powiadomić Administratora Danych Osobowych, w szczególności swojego przełożonego i IOD.

Instrukcja postępowania w przypadku zagrożenia i naruszenia bezpieczeństwa danych osobowych

Zagrożeniem bezpieczeństwa informacji jest sytuacja, w której występuje zagrożenie zaistnienia incydentu. Przykładowy katalog zagrożeń:

1. Naruszenie bezpieczeństwa systemów informatycznych, w których przetwarza się dane osobowe,
2. Udostępnianie danych osobowych osobom nieupoważnionym,
3. Przetwarzanie danych niezgodnie z założonym zakresem i celem ich przetwarzania,
4. Nieuprawnione lub przypadkowe uszkodzenie, utrata, zniszczenie lub zmianę danych osobowych,
5. nieprzestrzeganie Polityki przez osoby przetwarzające dane, np. niezamykanie pomieszczeń, szaf, biurek, brak stosowania zasad ochrony haseł, czystego biurka,
6. niewłaściwe zabezpieczenie fizyczne dokumentów, urządzeń lub pomieszczeń,
7. niewłaściwe zabezpieczenie oprogramowania lub sprzętu IT przed wyciekiem, kradzieżą lub utratą danych osobowych,
8. kradzież, zagubienie, utrata posiadania nośników elektronicznych (np. telefony, laptopy, tablety, dyski przenośne, pendrive) czy dokumentów (np. akta, kalendarze, notesy, wizytowniki, notatki),
9. przesłanie, przekazanie osobie nieuprawnionej informacji zawierających dane osobowe.

Postępowanie Administratora Danych Osobowych lub osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia zagrożenia i/lub naruszenia danych osobowych:

1. dokonanie oceny czy zaistniałe naruszenie mogło powodować ryzyko naruszania praw lub wolności osób fizycznych oraz szacuje skalę ryzyka,
2. jeśli ryzyko naruszenia praw i wolności osoby jest wysokie Podmiot zawiadamia o tym Prezesa UODO i osobę, której dane dotyczą,
3. ustalenie zakresu i przyczyn zagrożenia oraz jego ewentualnych skutków,
4. w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych,
5. w razie konieczności zainicjowanie działań dyscyplinarnych,
6. zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
7. udokumentowanie prowadzonego postępowania w Raporcie naruszeń bezpieczeństwa danych osobowych (zał. nr 12) oraz w ewidencji naruszeń i incydentów (zał. Nr 13).

Instrukcja postępowania w przypadku incydentów bezpieczeństwa danych osobowych

Incydentem jest sytuacja naruszenia bezpieczeństwa informacji ze względu na dostępność, integralność i poufność. Incydenty powinny być wykrywane, rejestrowane i monitorowane w celu zapobieżenia ich ponownemu wystąpieniu. Przykładowy katalog incydentów:

1. losowe zdarzenie wewnętrzne, np. awaria komputera, serwera, twardego dysku, błąd użytkownika, informatyka, zgubienie danych,
2. losowe zdarzenie zewnętrzne, np. klęski żywiołowe, zalanie, awaria zasilania, pożar,
3. incydent umyślny, np. wyciek informacji, ujawnienie danych nieupoważnionym osobom, świadome zniszczenie danych, działanie wirusów komputerowych, włamanie do pomieszczeń lub systemu informatycznego (wewnętrzne i zewnętrzne).

Postępowanie Administratora Danych Osobowych lub właściwej osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia incydentu:

1. ustalenie czasu zdarzenia będącego incydentem, z możliwie dokładną datą, godziną), celem spełnienia obowiązku informacyjnego do Prezesa UODO (72 godziny od powstania incydentu),
2. ustalenie zakresu incydentu,

3. określenie przyczyn, skutków oraz szacowanych zaistniałych szkód,
4. zabezpieczenie dowodów,
5. ustalenie osób odpowiedzialnych za naruszenie,
6. usunięcie skutków incydentu,
7. ograniczenie szkód wywołanych incydentem,
8. zainicjowanie działań dyscyplinarnych,
9. zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
10. udokumentowanie prowadzonego postępowania w Raport naruszeń bezpieczeństwa danych osobowych (zał. Nr 12).
11. W przypadku naruszenia ochrony danych osobowych, na administratorze danych osobowych ciąży obowiązek zgłoszenia tego faktu do organu nadzorczego zgodnie z postanowieniami np. 33 RODO oraz zawiadomienia osoby, której dane dotyczą, zgodnie z postanowieniami np. 34 RODO, w następujący sposób:

11.1. Zgłoszenie organowi nadzoru:

11.1.1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasz3a je organowi nadzorczemu właściwemu zgodnie z np. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

11.1.2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi Danych.

11.1.3. Zgłoszenie, o którym mowa w pkt 1, musi co najmniej:

a. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d. opisywać środki zastosowane lub proponowane przez administratora
w celu zaradzenia naruszeniu ochrony danych osobowych, w tym
w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

11.1.4. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki

11.1.5. Administrator Danych Osobowych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych:

11.2.1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. 4.5.2016 L 119/52 Dziennik Urzędowy Unii Europejskiej PL.

11.2.2. Zawiadomienie, o którym mowa w pkt 1 jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w powyższym punkcie 11.1. ppkt 3 lit. b), c) i d).

11.2.3. Zawiadomienie, o którym mowa w pkt 1, nie jest wymagane, w następujących przypadkach:

a. administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b. administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w pkt 1;

c. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany

zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

11.2.4. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w pkt 3.

Postępowanie Upoważnionego w przypadku stwierdzenia wystąpienia zagrożenia do czasu przybycia Administratora Danych Osobowych lub upoważnionej przez niego osoby:

1. powstrzymanie się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
2. zabezpieczenie elementów systemu informatycznego lub/i kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych,
3. podjęcie, stosownie do zaistniałej sytuacji, wszelkich niezbędnych działań celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

IX WYKAZY

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane dane osobowe, stanowi załącznik A do Polityki bezpieczeństwa. Załącznik ten będzie aktualizowany na bieżąco w przypadku zaistniałych zmian, konieczności sprostowania, usunięcia.
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, stanowi załącznik B do Polityki bezpieczeństwa. Załącznik ten będzie aktualizowany na bieżąco w przypadku zaistniałych zmian, konieczności sprostowania, usunięcia.
3. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności
   i rozliczalności przetwarzanych danych.

Środki organizacyjne

1. Została opracowana i wdrożona polityka bezpieczeństwa;
2. Została opracowana i wdrożona instrukcja zarządzania systemem informatycznym;
3. Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające ważne upoważnienia nadane przez administratora danych;
4. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;
5. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione i przeszkolone z przepisami dotyczącymi ochrony danych osobowych;
6. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;
7. Osoby zatrudnione lub współpracujące przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
8. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;
9. Dostęp do kont użytkownik jest zabezpieczony przed wielokrotnie błędnym wpisaniem hasła dostępu.
10. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
11. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
12. Stosuje się pisemne lub elektronicznie potwierdzone umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe;
13. Prowadzi się politykę czystego biurka i ekranu.
14. Raz w roku Podmiot przeprowadza audyt w zakresie zgodności przetwarzania danych osobowych, z którego przygotowywane jest sprawozdanie ze sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych stanowiący załącznik nr 10 Sprawozdanie ze sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych).

Środki ochrony fizycznej danych.

1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o odporności na włamanie.
2. Wszystkie pomieszczenia, w których przetwarzane są dane osobowe są zamykane na klucz, bez dostępu do nich osób nieupoważnionych.
3. Obiekty, w którym przetwarzane są dane osobowe wyposażone są w system alarmowy przeciwwłamaniowy.
4. Dostęp do części pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer wizyjnych, zgodnie z wykazem budynków.
5. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych/ współpracujących tam osób możliwy jest wyłącznie przez osoby do tego upoważnione i zobowiązane do zachowania tajemnicy.
6. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej szafie.
7. Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej szafie.
8. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą wolnostojącej gaśnicy.
9. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów lub w wyniku spalenia.

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej oraz opis działalności administratora danych osobowych, obszar przetwarzania danych osobowych i sprzęt wykorzystywany do przetwarzania danych osobowych.

1. Administrator danych osobowych prowadzi działalność gospodarczą, w ramach której dochodzi do przetwarzania danych osobowych pracowników, współpracowników, danych kontrahentów, z którymi nawiązywana jest współpraca.
2. Dane osobowe przetwarzane są zarówno w formie elektronicznej, jak i papierowej.
3. Siedziba Główna Administratora znajduje się pod następującym adresem: ul. Nagietkowa 33 (32-005) Niepołomice.

4. Dane osobowe w formie elektronicznej mogą być przetwarzane z dowolnego miejsca i w dowolnym czasie, ponieważ przetwarzanie odbywa się z wykorzystaniem komputerów oraz innych urządzeń przenośnych, które są zabezpieczone hasłem i szyfrowane.
5. Przesyłanie korespondencji e-mail jest szyfrowany (certyfikat SSL).
6. Dane osobowe w formie papierowej przetwarzane są w obrębie miejsc prowadzenia działalności gospodarczej przez administratora danych osobowych.
7. Ponieważ Administrator Danych Osobowych powierza przetwarzanie danych osobowych podmiotom trzecim, do przetwarzania danych osobowych dochodzi również w innych lokalizacjach, ale w tym zakresie czynności przetwarzania dokonuje podmiot trzeci (procesor) lub ewentualnie podmioty do tego przez niego upoważnione. Administrator danych osobowych zobowiązuje ww. wskazane podmioty do stosowania odpowiednich środków ochrony i bezpieczeństwa danych osobowych wymaganych przez przepisy prawa.
8. Odpowiednie środki ochrony danych osobowych zostały wdrożone w lokalizacji, o której mowa w ust. 1 powyżej oraz na urządzeniach wykorzystywanych do przetwarzania danych osobowych. Jeżeli chodzi o podmioty, którym administrator powierzył przetwarzanie danych osobowych, oświadczyły one, że wdrożyły odpowiednie środki ochrony i bezpieczeństwa danych osobowych wymagane przez przepisy prawa i zobowiązały się je utrzymywać przez okres powierzenia przetwarzania danych.
9. Przetwarzanie danych osobowych w lokalizacji, o której mowa w ust. 1 powyżej odbywa się w ten sposób, że z tej lokalizacji następuje logowanie do systemów informatycznych służących do przetwarzania danych osobowych. W tej lokalizacji przetwarzane są również dane w formie papierowej.
10. Z uwagi na to, że do przetwarzania danych osobowych wykorzystywane są urządzenia przenośne, nie jest możliwe jednoznaczne określenie obszaru przetwarzania danych osobowych, ponieważ dane mogą być przetwarzane przy użyciu urządzeń przenośnych z dowolnego miejsca poprzez zalogowanie się do systemów informatycznych dostępnych w modelu on-line (poczta). Użytkownicy stosują odpowiednie środki ochrony, bezpieczeństwa i ostrożności w związku z przetwarzaniem danych z wykorzystaniem urządzeń przenośnych.
11. Zbiór danych osobowych przetwarzany jest przy użyciu komputerów stacjonarnych i przenośnych, tabletów, smartfonów, telefonów. Przetwarzanie

danych przy wykorzystaniu wskazanych powyżej urządzeń polega na tym, że następuje z nich logowanie do systemów, w ramach których przetwarzane są dane osobowe. Dane mogą być również przechowywane na dyskach komputerów.

11. Komputery służące do przetwarzania danych osobowych są połączone z lokalną siecią komputerową.
12. Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła.
13. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem hasła.
14. Administrator stosuje zasady rozliczalności aktywności użytkowników poprzez program do zarządzania siecią Administratora.
15. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
16. Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
17. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji (szyfrowanie maili).
18. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
19. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
20. Zastosowano separację sieci.
21. Użyto system Firewall do ochrony dostępu do sieci komputerowej.
22. Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

Środki ochrony w ramach narzędzi programowych i baz danych

1. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
2. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
3. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
4. Zastosowano kryptograficzne środki ochrony danych osobowych.

5. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
6. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

X. POSTANOWIENIA KOŃCOWE

1. Polityka bezpieczeństwa jest dokumentem obowiązującym Podmiot w zakresie wdrażania, przestrzegania i weryfikacji zasad ochrony danych osobowych.
2. Polityka bezpieczeństwa jest dokumentem obowiązującym wszystkie osoby dopuszczone do przetwarzania danych osobowych w ramach działalności Podmiotu
3. Każda osoba dopuszczona do przetwarzania danych osobowych w ramach działalności Podmiotu ma obowiązek zapoznania się z niniejszą Polityką bezpieczeństwa, co potwierdzi oświadczeniem w formie papierowej lub/i elektronicznej (załącznik nr 14).
4. Naruszenie zasad wynikających z Polityki bezpieczeństwa może stanowić podstawę wszczęcia postępowania dyscyplinarnego przeciwko sprawcy naruszenia.
5. Wszczęcie lub przeprowadzenie postępowania dyscyplinarnego przeciwko osobie naruszającej zasady wynikające z Polityki bezpieczeństwa nie wyklucza możliwości wszczęcia postępowania karnego oraz dochodzenia roszczeń z powództwa cywilnego.
6. Polityka bezpieczeństwa wraz z załącznikami wchodzi w życie z dniem jej podpisania przez Administratora Danych Osobowych.
7. W przedmiocie spraw nieuregulowanych Polityką bezpieczeństwa, zastosowanie znajdują przepisy ustawy o ochronie danych osobowych.
8. Załączniki do niniejszej Polityki stanowią jej część pod warunkiem uzupełnienia. Lista załączników:

8.1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (zał. nr 1),

A. Ewidencja napraw, przeglądów i konserwacji systemu informatycznego,
B. Powołanie Administratora Systemu Informatycznego,
8.2. Ewidencja osób upoważnionych do przetwarzania danych osobowych (zał. nr 6),
8.3. Upoważnienie do przetwarzania danych osobowych (zał. nr 5),

8.4. Ewidencja podmiotów, którym Podmiot powierza dane osobowe (zał. nr 2),
8.5. Ewidencja podmiotów, którym Podmiot udostępnia dane osobowe (zał. Nr 3)
8.6. Potwierdzenie uczestnictwa w szkoleniu (zał. nr 7),
8.7. Wzór oceny skutków dla ochrony danych (zał. nr 8),
8.8. Wzór przeprowadzenia oceny ryzyka (zał. 11),
8.9. Raport z naruszeń i incydentów (zał. Nr 12),
8.10. Rejestr naruszeń bezpieczeństwa (zał. nr 13),
8.11. Oświadczenie upoważnionego o zapoznaniu się z Polityką Bezpieczeństwa oraz Instrukcją zarządzania informatycznego (zał. 14),
8.12. Rejestr czynności przetwarzania danych osobowych dla Administratora (zał. 4.1),
8.13. Rejestr czynności przetwarzania danych osobowych dla Procesora (zał. 4.2),
8.14. Oświadczenie o powołaniu Inspektora Ochrony Danych (zał. nr 9),
8.15. Sprawozdanie ze sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (załącznik 10).
8.16. Wykaz budynków, pomieszczeń - załącznik A.
8.17. Wykaz zbiorów danych i programów – Załącznik B.

Podpis Administratora Danych Osobowych	Data