Polityka ochrony danych osobowych

1,,**Polityka ochrony danych osobowych**,, (dalej: **Polityka**) stanowi zestaw wymogów, zasad i regulacji ochrony danych osobowych u Administratora –

PARTNER SPEDYCJA SYLWIA BUGAJSKA-GRAJCZYK,

40-337 **Katowice, ul. Obrońców Westerplatte 87.**

(dalej: **Administrator**).

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s 1).

2. Polityka zawiera:

a) opis zasad ochrony danych obowiązujących u Administratora,
b) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach)

Za wdrożenie, monitorowanie i utrzymanie niniejszej Polityki odpowiedzialny jest Administrator. Administrator samodzielnie lub za pośrednictwem upoważnionej pisemnie osoby nadaje uprawnienia w systemie informatycznym oraz może wyznaczyć osobę odpowiedzialną za wdrożenie i aktualizowanie ochrony danych osobowych.

Administrator podejmuje działania, aby zapewnić zgodność postępowania kontrahentów Administratora z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Administratora.

3.SKRÓTY I DEFINICJE

Polityka oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.

RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s 1).

Dane oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.

Dane szczególnych kategorii oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Dane dzieci oznaczają dane osób poniżej 16. roku życia.

Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

Podmiot przetwarzający oznacza organizację lub osobę której Administrator powierzył przetwarzanie danych osobowych (np. Usługodawca IT, zewnętrzna księgowość).

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.

Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

IOD lub Inspektor oznacza Inspektora Ochrony Danych Osobowych

RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych

4.OCHRONA DANYCH OSOBOWYCH U ADMINISTRATORA – ZASADY OGÓLNE

Zasady przetwarzania danych osobowych u Administratora:

(1) Legalność – Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
(2) Bezpieczeństwo – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie.
(3) Prawa jednostki – Administrator umożliwia osobom, których dane przetwarza, wykonanie swoich praw i prawa te realizuje.
(4) Rozliczalność – Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

Administrator przetwarza dane osobowe opierając się na poniższych zasadach:

⇒ w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
⇒ rzetelnie i uczciwie (rzetelność);
⇒ w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
⇒ w konkretnych celach i nie „na zapas„ (minimalizacja);
⇒ nie więcej niż potrzeba (adekwatność);
⇒ z dbałością o prawidłowość danych (prawidłowość);
⇒ nie dłużej niż potrzeba (czasowość);
⇒ zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

5.SYSTEM OCHRONY DANYCH

System ochrony danych osobowych u Administratora składa się z następujących elementów:

⇒ **Inwentaryzacja danych**. Administrator dokonuje inwentaryzacji zasobów danych osobowych w Spółce, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:
a) przypadków przetwarzania danych szczególnych kategorii i danych karnych;
b) przypadków przetwarzania danych osób, których Administrator nie identyfikuje (**dane niezidentyfikowane**/UFO);
c) przypadków przetwarzania danych dzieci;
d) profilowania
e) współadministrowania danymi.

⇒ **Rejestr**. Administrator opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w Jednistce (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych u Administratora.
⇒ **Podstawy prawne.** Administrator zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Administrator przetwarza dane na podstawie prawnie uzasadnionego interesu Administratora.
⇒ **Obsługa praw jednostki.** Administrator realizuje obowiązki informacyjne wobec osób, których dane przetwarza, oraz zapewnia obsługę ich praw, odpowiadając na żądania, a także realizuje:
a) **obowiązki informacyjne.** Administrator przekazuje osobom informacje z art. 13 i 14 RODO oraz inne przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków
b) **możliwość wykonania żądań**. Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego żądania przez siebie i swoich przetwarzających;
c) **obsługa żądań.** Administrator zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane (stanowiące załącznik do niniejszej Polityki);
d) **zawiadamianie o naruszeniach**. Administrator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

⇒ **Minimalizacja.** Administrator posiada zasady i metody zarządzania minimalizacją (privacy by default), a w tym:
a) zasady zarządzania **adekwatnością** danych;
b) zasady reglamentacji i zarządzania **dostępem** do danych;
c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności.

⇒ **Bezpieczeństwo**. Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
a) przeprowadza analizy ryzyka dla czynności przetwarzania lub ich kategorii;
b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
c) dostosowuje środki ochrony danych do ustalonego ryzyka ;
d) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.

⇒ **Przetwarzający.** Administrator z należytą starannością przy uwzględnieniu zapisów RODO dobiera podmiot przetwarzający Administratora i ustala wymogi co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

⇒ **Eksport danych.** Administrator posiada zasady weryfikacji, czy Administrator nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Liechtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce. Administrator nie przetwarza danych do państw trzecich.

⇒ **Privacy by design.** Administrator zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji u Administratora uwzględniają konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji)już w fazie **projektowania zmiany, inwestycji czy na początku nowego projektu.**

⇒ **Przetwarzanie transgraniczne.** Administrator posiada zasady weryfikacji kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO

6.INWENTARYZACJA

6.1. Dane szczególnych kategorii i dane karne

Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególnych kategorii lub dane karne, oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W przypadku zidentyfikowania przypadków przetwarzania danych szczególnych kategorii lub danych karnych Administrator postępuje zgodnie z przyjętymi zasadami w tym zakresie. Administrator identyfikuje:

- przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane, i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
- przypadki, w których dokonuje profilowania przetwarzanych danych, i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji Administrator postępuje zgodnie z przyjętymi zasadami w tym zakresie. Administrator nie dokonuje profilowania.

- przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

7.SPOSÓB OBSŁUGI PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH

7.1. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
7.2.Administrator ułatwia osobom korzystanie z ich praw poprzez: stosowanie rzetelnej informacji o ich prawach, zapewnienie prostego kontaktu z administratorem.
7.3.Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
7.4. Administrator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
7.5.W celu realizacji praw jednostki Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Administratora, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
7.6. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

8.OBOWIAZKI INFORMACYJNE

8**.1.**Administrator określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
8.2. Administrator informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
8.3.Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby zgodnie z art. 13 RODO.
8.4. Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej zgodnie z art. 14 RODO.
8.5. Administrator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe.
8.6. Administrator informuje osobę o planowanej zmianie celu przetwarzania danych.
8.7. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.
8.8. Administrator informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
8.9. Administrator informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
8.10. Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw wolności tej osoby. Administrator posiada w tym zakresie odpowiednią procedurę.

9.ŻĄDANIA OSÓB

9.1.Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, Administrator wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich.

W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób Administrator może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

9.2.Nieprzetwarzanie. Administrator informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

9.3.Odmowa. Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania i o prawach osoby z tym związanych.

9.4.Dostęp do danych. Na żądanie osoby dotyczące dostępu do jej danych Administrator informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO oraz udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Administrator nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

9.5.Kopie danych. Na żądanie Administrator wydaje osobie kopie danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Administrator wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.

9.6.Sprostowanie danych. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Administrator ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

9.7.Uzupełnienie danych. Administrator uzupełnia i aktualizuje dane na żądanie osoby. Administrator ma prawo omówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administratora procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy aby uznać oświadczenie za niewiarygodne.

9.8.Usunięcie danych. Na żądanie osoby Administrator usuwa dane, gdy:

(1) dane nie są niezbędne do celów w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,

(2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

(3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

(4) dane były przetwarzane niezgodnie z prawem,

(5) konieczność usunięcia wynika z obowiązku prawnego,

(6) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

Administrator określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizacje tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację czy nie zachodzą wyjątki, o których mowa w art. 17 ust. 3 RODO.

Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, Administrator podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich.

W przypadku usunięcia danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

9.9.Ograniczenie przetwarzania. Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
c) Administrator nie potrzebuje już danych osobowych, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń'
d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.

W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

9.10.Przenoszenie danych. Na żądanie osoby Administrator wydaje w ustrukturyzowanym formacie nadającym się do odczytu maszynowego, względnie w formie elektronicznej uzgodnionej z Administratorem bazy danych osobowych do których informacje są przenoszone lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Spółce, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych Administratora.
9.11.Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o uzasadniony interes Administratora lub o powierzone Administratorowi zadanie w interesie publicznym, Administrator **uwzględni** sprzeciw, o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
9.12.Sprzeciw względem marketingu bezpośredniego. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administratora na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

10. MINIMALIZACJA

Administrator dba o minimalizację przetwarzania danych pod kątem: (i) adekwatności danych do celów (ilości danych i zakresu przetwarzania), (ii) dostępu do danych, (iii) czasu przechowywania danych.

10.1.Minimalizacja zakresu

Administrator zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO. Administrator dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok. Administrator przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (privacy by design).

10.2.Minimalizacja dostępu

Administrator stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenie uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe). Administrator stosuje kontrolę dostępu fizycznego.

Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.

Administrator dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Administratora.

10.3.Minimalizacja czasu

Administrator wdraża mechanizmy kontroli cyklu życia danych osobowych, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów Administratora, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane przez Administratora. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

11.REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

Administrator prowadzi Rejestr Czynności Przetwarzania Danych Osobowych, elementy rejestru zgodne są z zasadami określonymi w RODO. Administrator prowadzi Rejestr Kategorii Czynności Przetwarzania, gdy jest procesorem na podstawie umowy powierzenia przetwarzania danych osobowych.

12.PODSTAWY PRZETWARZANIA

12.1. Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne / władza publiczna, uzasadniony cel Administratora), Administrator dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne.
12.2. Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (e-mail, telefon, SMS itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
12.3. Kierownik komórki organizacyjnej Administratora ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Administratora, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes Administratora

13.BEZPIECZEŃSTWO

Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Administratora.

13.1.Analizy ryzyka i adekwatności środków bezpieczeństwa

Administrator przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

(1) Administrator zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
(2) Administrator kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
(3) Administrator przeprowadził analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Administrator analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
(4) Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Administrator ustala przydatność i stosuje takie środki i podejście, jak pseudonimizacja, szyfrowanie danych osobowych, inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, a także środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

13.2.Oceny skutków dla ochrony danych

Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

Administrator stosuje metodykę oceny skutków przyjętą u niego.

13.3.Środki bezpieczeństwa

Administrator stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.

13.4.Zgłaszanie naruszeń

Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia. W tym zakresie Administrator wdrożył procedur, stanowiącą załącznik nr 3 do niniejszej Polityki Bezpieczeństwa.

14.PRZETWARZAJĄCY

Administrator przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące **załącznik do niniejszej Polityki.**

Administrator wdrożył środki techniczne umożliwiające mu możliwość rozliczania przetwarzających z wykorzystania podprzetwarzających, jak też innych wymagań wynikających z Zasad powierzenia danych osobowych.

15.EKSPORT DANYCH

Administrator rejestruje w Rejestrze przypadki eksportu danych, czyli przekazania danych poza Europejski Obszar Gospodarczy EOG w 2017 r. - Unia Europejska, Islandia, Liechtenstein o Norwegia).

Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Administrator okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

16.PROJEKTOWANIE PRYWATNOŚCI

Administrator zarządza zmianą mająca wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania. Dlatego zasady prowadzenia przedsięwzięć przez Administratora odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowania bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

17.POSTANOWIENIA KOŃCOWE

17.1. Administrator wprowadza niniejszą Politykę z dniem 15.09.2018.
17.2. Administrator dokonuje przeglądu dokumentów dot. ochrony danych raz w roku i sporządza raport z przeglądu.
17.3.W razie zmiany przepisów prawa, Administrator na bieżąco aktualizuje dokumenty i dostosowuje je do aktualnych przepisów.
17.4. Administrator szkoli personel z zakresu ochrony danych osobowych.

Załączniki:

Załącznik nr 1 – wzór oświadczenia dla pracowników dot. znajomości zasad ochrony danych
Załącznik nr 2 - wykaz zbiorów danych osobowych
Załącznik nr 3 - Instrukcja postępowania w przypadku zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych
Załącznik nr 4 - Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
Załącznik nr 5 - Klauzula informacyjna o przetwarzaniu danych stosowana w korespondencji emailowej
Załącznik nr 6 – wzory klauzul informacyjnych
Załącznik nr 7 – polityka cookies
Załącznik nr 8 – polityka czystego biurka
Załącznik nr 9 - rejestr osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 10 - Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych
Załącznik nr 11 - Upoważnienie do przetwarzania danych osobowych
Załącznik nr 12 – wzór rejestru incydentów
Załącznik nr 13 – wzór rejestru odbiorców danych osobowych
Załącznik nr 14 – wzór - Umowa powierzenia przetwarzania danych osobowych
Załącznik nr 15 - Klauzula zgody na przetwarzanie danych osobowych zwykłych
Załącznik nr 16 – Rejestr czynności przetwarzania danych osobowych
Załącznik nr 17 – Rejestr kategorii przetwarzania danych osobowych

Legenda :
Wersja podstawowa – 1.0.0. – wersja przyjęta przez Administratora
1 – liczba kolejnego dokumentu (np. Polityki Ochrony Danych Osobowych)
0 – zmiana/wersja (kolejna) w tekście dokumentu
0 – kod osoby uprawnionej do dokonywania zmian