POLITYKA
OCHRONY DANYCH OSOBOWYCH

1. Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**” (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w przedsiębiorstwie działającym pod firmą **Firma Handlowo-Usługowa Monika Mądel** z siedzibą w miejscowości Partynia (dalej jako: **Przedsiębiorstwo**).

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:

- opis zasad ochrony danych obowiązujących w Przedsiębiorstwie;

- odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);

3. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest właściciel Przedsiębiorstwa

Za nadzór i monitorowanie przestrzegania Polityki odpowiada:

- Przedsiębiorca

Za stosowanie niniejszej Polityki odpowiedzialni są:

- Przedsiębiorca

- wszyscy członkowie personelu Przedsiębiorstwa.

Spółka powinna też zapewnić zgodność postępowania kontrahentów Przedsiębiorstwa z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Przedsiębiorstwo.

4. 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 wrażliwe oznaczają dane specjalne i dane karne.
Dane specjalne 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 Spółka powierzyła przetwarzanie danych osobowych (np. usługodawca IT, przychodnie lekarskie, firma ochroniarska, ubezpieczyciele, dostawcy oprogramowania, notariusz, sąd rejestracyjny, biura projektowe, usługodawca BHP).
Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.
RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.
Przedsiębiorstwo oznacza przedsiębiorstwo Firma Handlowo-Usługowa Monika Mądel

5. Ochrona danych osobowych w Przedsiębiorstwie – zasady ogólne

Filary ochrony danych osobowych w Spółce:

Legalność − Przedsiębiorstwo dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

Bezpieczeństwo − Przedsiębiorstwo zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

Prawa Jednostki − Przedsiębiorstwo umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

Rozliczalność − Przedsiębiorstwo dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

Przedsiębiorstwo przetwarza dane osobowe z poszanowaniem następujących zasad:

- 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).

System ochrony danych osobowych w Przedsiębiorstwie składa się z następujących elementów:

a. Przedsiębiorstwo dokonuje identyfikacji zasobów danych osobowych w Przedsiębiorstwie, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:

   - przypadków przetwarzania danych specjalnych i danych „kryminalnych”

   - przypadków przetwarzania danych dzieci;

   - współadministrowania danymi.

b. Przedsiębiorstwo opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w Spółce (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Przedsiębiorstwie.

c. Przedsiębiorstwo zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

   - utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,

   - inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Przedsiębiorstwo przetwarza dane na podstawie prawnie uzasadnionego interesu Przedsiębiorstwa.

d. **Obsługa praw jednostki.** Przedsiębiorstwo spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

   - Obowiązki informacyjne. Przedsiębiorstwo przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.

   - Możliwość wykonania żądań. Przedsiębiorstwo weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

   - Obsługa żądań. Przedsiębiorstwo zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane.

   - Zawiadamianie o naruszeniach. Przedsiębiorstwo stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

e. **Minimalizacja.** Przedsiębiorstwo posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

   - zasady zarządzania **adekwatnością** danych;
   - zasady reglamentacji i zarządzania **dostępem** do danych;
   - zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;

f. Przedsiębiorstwo zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

   - przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

- dostosowuje środki ochrony danych do ustalonego ryzyka;

- posiada system zarządzania bezpieczeństwem informacji;

- stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami.

Przetwarzający. Przedsiębiorstwo posiada zasady doboru przetwarzających dane na rzecz Przedsiębiorstwa, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.
Eksport danych. Przedsiębiorstwo posiada zasady weryfikacji, czy Przedsiębiorstwo nie przekazuje danych do państw trzecich (czyli poza UE) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

Privacy by design - Zasada prywatności w fazie projektowania.

Przedsiębiorstwo zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Przedsiębiorstwie uwzględniają konieczność oceny wpływu zmiany na ochronę danych, 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. Przedsiębiorstwo posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

6. Inwentaryzacja

Dane wrażliwe - Przedsiębiorstwo identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe (dane specjalne i dane karne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, Przedsiębiorstwo postępuje zgodnie z przyjętymi zasadami w tym zakresie.

Dane niezidentyfikowane - Przedsiębiorstwo identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.

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

7. Rejestr Czynności Przetwarzania Danych

RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

Przedsiębiorstwo prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

Rejestr jest jednym z podstawowych narzędzi umożliwiających Przedsiębiorstwu rozliczanie większości obowiązków ochrony danych.

W Rejestrze, dla każdej czynności przetwarzania danych, którą Przedsiębiorstwo uznało za odrębną dla potrzeb Rejestru, Przedsiębiorstwo odnotowuje:

- opis kategorii osób;
- cel przetwarzania;
- podstawę prawną przetwarzania;
- opis kategorii danych;
- szczególne kategorie danych;
- opis kategorii odbiorców danych;
- sposób przetwarzania danych;
- sposób zbierania danych;
- okres przechowywania danych;
- opis technicznych i organizacyjnych środków ochrony danych.

8. Podstawy przetwarzania

Przedsiębiorstwo dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

Przedsiębiorstwo wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

Kierownik komórki organizacyjnej Przedsiębiorstwa ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Przedsiębiorstwa, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes Przedsiębiorstwa.

9. Sposób obsługi praw jednostki i obowiązków informacyjnych

Przedsiębiorstwo dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

Przedsiębiorstwo ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Przedsiębiorstwa informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Spółce, w tym wymaganiach dotyczących

identyfikacji, metodach kontaktu ze Przedsiębiorstwem w tym celu, ewentualnym cenniku żądań „dodatkowych” itp.

Przedsiębiorstwo dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

Przedsiębiorstwo wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

W celu realizacji praw jednostki Przedsiębiorstwo zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Przedsiębiorstwo, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,

Przedsiębiorstwo dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

10. Obowiązki informacyjne

Przedsiębiorstwo określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

Przedsiębiorstwo informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

Przedsiębiorstwo informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

Przedsiębiorstwo informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.

Przedsiębiorstwo określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).

Przedsiębiorstwo informuje osobę o planowanej zmianie celu przetwarzania danych.

Przedsiębiorstwo informuje osobę przed uchyleniem ograniczenia przetwarzania.

Przedsiębiorstwo informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

Przedsiębiorstwo informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

Przedsiębiorstwo bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

10. Żądania osób

Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, Przedsiębiorstwo 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 (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową,

dobra osobiste itp.), Przedsiębiorstwo może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

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

Odmowa. Przedsiębiorstwo informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

Dostęp do danych. Na żądanie osoby dotyczące dostępu do jej danych, Przedsiębiorstwo informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Przedsiębiorstwo nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

Kopie danych. Na żądanie Przedsiębiorstwo wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Przedsiębiorstwo wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.

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

Uzupełnienie danych. Przedsiębiorstwo uzupełnia i aktualizuje dane na żądanie osoby. Przedsiębiorstwo ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Przedsiębiorstwo nie musi przetwarzać danych, które są Spółce zbędne). Przedsiębiorstwo może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Przedsiębiorstwo procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

Usunięcie danych. Na żądanie osoby, Przedsiębiorstwo usuwa dane, gdy:

- dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
- zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
- osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
- dane były przetwarzane niezgodnie z prawem,
- konieczność usunięcia wynika z obowiązku prawnego,

Przedsiębiorstwo określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację 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 Przedsiębiorstwo,

Przedsiębiorstwo 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 Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

12. Ograniczenie przetwarzania.

Przedsiębiorstwo dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

- osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

- Spółka nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

- osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Przedsiębiorstwa zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Przedsiębiorstwo przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), 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.

Przedsiębiorstwo informuje osobę przed uchyleniem ograniczenia przetwarzania.

W przypadku ograniczenia przetwarzania danych Przedsiębiorstwo informuje osobę o odbiorcach danych, na żądanie tej osoby:

Przenoszenie danych. Na żądanie osoby Przedsiębiorstwo wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego 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 Przedsiębiorstwa.

Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Przedsiębiorstwo w oparciu o uzasadniony interes Przedsiębiorstwa lub o powierzone Przedsiębiorstwu zadanie w interesie publicznym, Przedsiębiorstwo uwzględni sprzeciw, o ile nie zachodzą po stronie Przedsiębiorstwa ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych. Jeżeli Przedsiębiorstwo prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Przedsiębiorstwo uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Sprzeciw względem marketingu bezpośredniego. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Przedsiębiorstwo na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Przedsiębiorstwo uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu. Jeżeli Przedsiębiorstwo przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Przedsiębiorstwo zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Przedsiębiorstwa, chyba że taka automatyczna decyzja :

- jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Przedsiębiorstwem;
- jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej osoby.

13. MINIMALIZACJA

Przedsiębiorstwo 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.

Minimalizacja zakresu

Przedsiębiorstwo zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO. Spółka dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

Przedsiębiorstwo przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (privacy by design).

Minimalizacja dostępu

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

Przedsiębiorstwo stosuje kontrolę dostępu fizycznego.

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

Przedsiębiorstwo 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 Przedsiębiorstwa.

Minimalizacja czasu

Przedsiębiorstwo wdraża mechanizmy kontroli cyklu życia danych osobowych w Przedsiębiorstwie, 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 produkcyjnych Przedsiębiorstwa, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Przedsiębiorstwo. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania

kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

14. BEZPIECZEŃSTWO

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

Analizy ryzyka i adekwatności środków bezpieczeństwa

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

Przedsiębiorstwo zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

Przedsiębiorstwo kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

Przedsiębiorstwo przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Przedsiębiorstwo 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.

Przedsiębiorstwo ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Przedsiębiorstwo 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,
- 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.

Oceny skutków dla ochrony danych

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

Przedsiębiorstwo stosuje metodykę oceny skutków przyjętą w Przedsiębiorstwie.

Środki bezpieczeństwa

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

Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Przedsiębiorstwie i są bliżej opisane w procedurach przyjętych przez Przedsiębiorstwo dla tych obszarów.

Zgłaszanie naruszeń

Przedsiębiorstwo stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

15. PRZETWARZAJĄCY

Przedsiębiorstwo posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Przedsiębiorstwa opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Przedsiębiorstwie.

Przedsiębiorstwo przyjęło minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych".

Przedsiębiorstwo rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

16. EKSPORT DANYCH

Przedsiębiorstwo rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2017 r. = Unia Europejska, Islandia, Lichtenstein i Norwegia). Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Spółka okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

17. PROJEKTOWANIE PRYWATNOŚCI

Przedsiębiorstwo zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania. W tym celu zasady prowadzenia projektów i inwestycji przez Przedsiębiorstwo odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

Tarnów, dnia 18 maja 2018 roku

WYKAZ ZAŁĄCZNIKÓW
DO POLITYKI OCHRONY DANYCH OSOBOWYCH:

Załącznik nr 1 – Wykaz miejsc przetwarzania danych osobowych

A. Tarnów Biuro - ul. Mostowa 14

Załącznik nr 2 – Wykaz zbiorów i systemów zastosowanych do ich przetwarzania

Załącznik nr 3 – Rejestr Czynności Przetwarzania Danych

Załącznik nr 4 – Instrukcja odpowiedniego zabezpieczenia, przetwarzania , przechowywania i likwidacji danych osobowych

Załącznik nr 5 – Wykaz nadanych upoważnień

A. Tarnów Biuro - ul. Mostowa 14

Załącznik nr 6 – Wykaz umów powierzenia

A. Tarnów Biuro - ul. Mostowa 14