

Polityka ochrony danych osobowych

1. Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**” (dalej: **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w firmie Sped-Service Maria Zofia Mulewska (dalej: **Sped- Service**).

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 w Sped- Service,
- b) odwołania do załączników uszczegółwiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

3. Odpowiedzialna za wdrożenie i utrzymanie niniejszej Polityki jest właścicielka firmy Maria Mulewska.

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 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 Sped- Service powierzyła przetwarzanie danych osobowych (np. usługodawca, IT, zewnętrzna księgowość, prawnik).

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 oznacza Inspektora Ochrony Danych Osobowych.

RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

5. OCHRONA DANYCH OSOBOWYCH W SPED- SERVICE – ZASADY OGÓLNE

5.1. Filary ochrony danych osobowych:

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

5.2. ZASADY OCHRONY DANYCH

Sped- Service przetwarza dane osobowe z poszanowaniem następujących zasad:

- (1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
- (2) rzetelnie i uczciwie (rzetelność);
- (3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
- (4) w konkretnych celach (minimalizacja);
- (5) nie więcej niż potrzeba (adekwatność);
- (6) z dbałością o prawidłowość danych (prawidłowość);
- (7) nie dłużej niż potrzeba (czasowość);
- (8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

5.3. System ochrony danych

System ochrony danych osobowych w Sped- Service składa się z następujących elementów:

1. Inwentaryzacja danych. Sped- Service dokonuje identyfikacji zasobów danych osobowych w firmie, 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 Sped- Service nie identyfikuje (dane niezidentyfikowane);
- c) przypadków przetwarzania danych dzieci;
- d) profilowania;
- e) współadministrowania danymi.

2. Rejestr. Sped- Service opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w firmie.

3. Obsługa praw jednostki. Sped- Service spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

- a) **obowiązki informacyjne.** Sped- Service spełnia prawem wymagane obowiązki informacyjne i zapewnia udokumentowanie realizacji tych obowiązków;
- b) **możliwość wykonania żądań.** Sped- Service weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;
- c) **obsługa żądań.** Sped Service zapewnia odpowiednie procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane;

d) **zawiadamianie o naruszeniach.** Sped- Service stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych (zarządzanie incydentami) .

4. Minimalizacja. Sped- Service posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

- a) zasady zarządzania **adekwatnością** danych;
- b) zasady zarządzania **dostępem** do danych;
- c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności.

5. Bezpieczeństwo. Sped Service zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

- a) dostosowuje środki ochrony danych do ustalonego ryzyka;
- b) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.

6. Przetwarzający. Sped- Service posiada zasady doboru przetwarzających dane na rzecz Sped- Service, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

7. Eksport danych. Sped Service weryfikuje, czy 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.

8. Privacy by design. Sped-Service zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Sped- Service 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.

6. INWENTARYZACJA

6.1. Dane szczególnych kategorii i dane karne

Sped- Service 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 Sped- Service, postępuje zgodnie z przyjętymi zasadami w tym zakresie.

6.2. Dane niezidentyfikowane

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

6.3. Współadministrowanie

Sped- Service identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie, zgodnie z przyjętymi zasadami.

7. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

7.1 Sped- Service prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

7.2. Rejestr jest jednym z podstawowych narzędzi umożliwiających Sped Service rozliczanie większości obowiązków ochrony danych.

7.3. W Rejestrze dla każdej czynności przetwarzania danych, którą Sped- Service uzna za odrębną dla potrzeb Rejestru, odnotowuje się co najmniej: (i) nazwę czynności, (ii) cel przetwarzania, (iii) opis kategorii osób, (iv) opis kategorii danych, (v) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu, jeśli podstawą jest uzasadniony interes, (vi) sposób zbierania danych, (vii) opis kategorii odbiorców danych (w tym przetwarzających), (viii) informację o przekazaniu poza EU/EOG; (ix) ogólny opis technicznych i organizacyjnych środków ochrony danych.

7.4. Wzór Rejestru stanowi Załącznik do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”.

8. PODSTAWY PRZETWARZANIA

8.1. Sped- Service dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

8.2. Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne, władza publiczna, uzasadniony cel), Sped- Service dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne.

8.3. Sped- Service 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.).

9. SPOSÓB OBSŁUGI PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH

9.1. Sped- Service dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

9.2. Sped- Service ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej firmy informacji o prawach osób, sposobie, skorzystania z nich w Sped- Service, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu w tym celu.

9.3. Sped- Service dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

9.4.. Sped- Service dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

10. OBOWIĄZKI INFORMACYJNE

10.1. Sped- Service określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

10.2. Sped- Service informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

10.3. Sped- Service informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

10.4. Sped- Service informuje osobę o planowanej zmianie celu przetwarzania danych.

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

10.6. Sped- Service informuje osobę o prawie sprzeciwu względem przetwarzania danych.

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

11. ŻĄDANIA OSÓB

11.1. Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, Sped- Service wprowadza proceduralne gwarancje ochrony praw 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), Sped- Service może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

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

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

11.4. Dostęp do danych. Na żądanie osoby dotyczące dostępu do jej danych Sped- Service 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.

11.5. Kopie danych. Na żądanie Sped- Service wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Co do zasady nie pobiera się opłaty za wydanie kopii danych. Jednakże, ADO może pobrać opłatę ustaloną w rozsądnej wysokości, wynikającą z kosztów administracyjnych za kolejne dostarczenie osobie, której dane dotyczą kolejnej kopii danych osobowych podlegających przetwarzaniu. Ponadto pobranie opłaty jest możliwe, gdy żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter.

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

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

11.8. Usunięcie danych. Na żądanie osoby Sped- Service 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,

W przypadku usunięcia danych Sped- Service informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.9. Ograniczenie przetwarzania. Sped- Service 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) Sped- Service nie potrzebuje już danych osobowych, ale są one potrzebne osobie, 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 Sped- Service zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Sped- Service 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. W przypadku ograniczenia przetwarzania danych Sped- Service informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.10. Przenoszenie danych. Na żądanie osoby Sped- Service 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 Sped- Service, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej.

11.11. Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, Sped- Service **uwzględni** sprzeciw, o ile nie zachodzą po stronie Sped- Service ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

12. MINIMALIZACJA

Sped- Service 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.

12.1. Minimalizacja zakresu

Sped- Service weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

12.2. Minimalizacja dostępu

Sped- Service stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe). Sped- Service stosuje kontrolę dostępu fizycznego. Sped- Service dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.

12.3. Minimalizacja czasu

Sped- Service 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, dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Sped- Service.

13. BEZPIECZEŃSTWO

Sped- Service zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych.

13.1. Analizy ryzyka i adekwatności środków bezpieczeństwa :

Sped- Service zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania- wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych. Sped- Service ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa. W tym ustala przydatność i stosuje takie środki jak, w szczególności:

(i) zabezpieczenie dostępu do systemów komputerowych hasłami

(ii) szyfrowanie danych osobowych,

(iii) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

(iv) 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. Zgłaszanie naruszeń

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

14. PRZETWARZAJĄCY

Sped- Service posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Sped- Service 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 Sped- Service.

15. EKSPORT DANYCH

Sped- Service rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy.

16. PROJEKTOWANIE PRYWATNOŚCI

Sped service 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 Sped- Service 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.