POLITYKA PRYWATNOŚCI

Spis treści

Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych” (dalej jako Polityka) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Firmie DanaMed Danuta Krawczyk z siedzibą w Cieszynie przy ul.Zamkowej 22, NIP: 5482175202.

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).

Polityka zawiera:

a) opis zasad ochrony danych obowiązujących w Firmie DanaMed Danuta Krawczyk;
b) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);

Odpowiedzialny za wdrożenie i utrzymanie niniejszej Właściciel Firmy DanaMed Danuta Krawczyk

Za nadzór i monitorowanie przestrzegania Polityki odpowiada administrator danych osobowych.

Po dokonanej analizie i braku przesłanek wynikających z art. 37 RODO administrator danych nie powołuje Inspektora Danych Osobowych. W przypadku, gdy administrator lub podmiot przetwarzający podejmuje nowe działania albo świadczy nowe usługi, które mogą mieścić się w zakresie ww. artykułu, administrator danych dokona ponownej analizy w celu ustalenia obowiązku powołania IOD.

Za stosowanie niniejszej Polityki odpowiedzialni są:

- Właściciel Firmy DanaMed Danuta Krawczyk;
- komórka organizacyjna odpowiedzialna za obszar bezpieczeństwa informacji;
- komórki organizacyjne przetwarzające dane osobowe;

1. 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. U. 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 Firma powierzyła przetwarzanie danych osobowych (np. usługodawca IT).

Administrator –osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Pseudonimizacja – rozumie się przez to 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.

Przetwarzanie danych – rozumie się przez to 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.

IOD lub Inspektor oznacza Inspektora Ochrony Danych Osobowych

RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania 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.

2. Ochrona danych osobowych w Firmie DanaMed Danuta Krawczyk – zasady ogólne

2.1. Filary ochrony danych osobowych w Firmy

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

2.2. Zasady ochrony danych

Firma 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).

Zasada zgodności z prawem stanowi nadrzędną zasadę procesu przetwarzania danych. W celu jej zachowania sprawowany jest nadzór, aby spełniony był co najmniej jeden z poniższych warunków:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- 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;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- 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.

Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi:

- wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;
- kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem;
- charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa;
- ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;
- istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania.

2.3. System ochrony danych

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

1. **Inwentaryzacja danych.** Firma dokonuje identyfikacji zasobów danych osobowych

w Firmie, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:

a) przypadków przetwarzania danych specjalnych i danych „kryminalnych", danych medycznych/zdrowotnych (**dane wrażliwe**);
b) przypadków przetwarzania danych osób, których Firma nie identyfikuje (**dane niezidentyfikowane** / UFO);
c) przypadków przetwarzania danych dzieci;

2. **Rejestr.** Firma opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w Firmie (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Firmie.

3. **Podstawy prawne.** Firma 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 Firma przetwarza dane na podstawie prawnie uzasadnionego interesu Firmy.

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

a) **Obowiązki informacyjne.** Firma przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
b) **Możliwość wykonania żądań.** Firma weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
c) **Obsługa żądań.** Firma zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.
d) **Zawiadamianie o naruszeniach.** Firma stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5. **Minimalizacja.** Firma 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;

6. **Bezpieczeństwo.** Firma zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

a) przeprowadza analizy ryzyka dla czynności przetwarzania danych 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) posiada system zarządzania bezpieczeństwem informacji;
e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami.

7. **Przetwarzający.** Firma posiada zasady doboru przetwarzających dane na rzecz Firmy, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

2.4. Inwentaryzacja

Dane wrażliwe

Firma 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, Firma postępuje zgodnie z przyjętymi zasadami w tym zakresie.

Dane niezidentyfikowane

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

Współadministrowanie

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

2.5. 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.

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

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

W Rejestrze, dla każdej czynności przetwarzania danych, którą Firma uznała za odrębną dla potrzeb Rejestru, Firma odnotowuje co najmniej:

- nazwę czynności,
- cel przetwarzania,
- opis kategorii osób,
- opis kategorii danych,
- podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Firmy, jeśli podstawą jest uzasadniony interes,
- sposób zbierania danych,
- opis kategorii odbiorców danych (w tym przetwarzających),

Wzór Rejestru stanowi Załącznik do Polityki – **„Wzór Rejestru Czynności Przetwarzania Danych”**. Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Firma rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

3. Podstawy przetwarzania

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

Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Firmy) Firma dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.

Firma 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.)

4. Sposób obsługi praw jednostki i obowiązków informacyjnych

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

Firma ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Firmy informacji lub odwołań (linków) do informacji o prawach osób, sposobie korzystania z nich w Firmie, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z Firmą w tym celu.

Firma dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

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

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

Firma dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

5. Obowiązki informacyjne

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

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

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

Firma informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie nie bezpośrednio od niej.

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

Firma informuje osobę o planowanej zmianie celu przetwarzania danych.

Firma informuje osobę przed uchyleniem ograniczenia przetwarzania.

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

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

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

6. Żądania osób

Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, Firma 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.), Firma może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

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

Odmowa. Firma 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 dotyczącej dostępu do jej danych, Firma 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.

Kopie danych. Na żądanie Firma wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

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

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

Prawo do „bycia zapomnianym". Na żądanie osoby, Firma 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,

.

Firma 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 Firmę, Firma 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 Firma informuje osobę o odbiorcach danych, na żądanie tej osoby.

Ograniczenie przetwarzania. Firma 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,
- Firma 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 Firmy zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Firma 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.

Firma informuje osobę przed uchyleniem ograniczenia przetwarzania.

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

Przenoszenie danych. Na żądanie osoby Firma 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 Firmy, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Firmy.

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

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

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

7. Minimalizacja

Firma dba o minimalizację przetwarzania danych pod kątem:

- adekwatności danych do celów (ilości danych i zakresu przetwarzania),
- dostępu do danych,
- czasu przechowywania danych.

7.1. Minimalizacja zakresu

Firma zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

Firma dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

7.2. Minimalizacja dostępu

Firma 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).

Firma stosuje kontrolę dostępu fizycznego.

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

Firma 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 Firmy, opisane w instrukcji zarządzania systemami informatycznymi.

7.3. Minimalizacja czasu

Firma wdraża mechanizmy kontroli cyklu życia danych osobowych w Firmy, 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 Firmy, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Firmę. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

8. Bezpieczeństwo

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

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych odbywało się zgodnie z prawem. Administrator musi być w stanie wykazać wypełnienie tego obowiązku.

Do środków tych należą:

- Wdrożenie przez administratora niniejszej polityki ochrony danych;
- Wdrożenie instrukcji zarządzania systemem informatycznym.

Środki te są poddawane są przeglądom i uaktualniane.

8.1. Analizy ryzyka i adekwatności środków bezpieczeństwa

Firma przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych.

W tym celu:

- Firma zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
- Firma kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
- Firma przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Firma 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.

- Firma ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Firma ustala przydatność i stosuje takie środki i podejście jak:
    - ✓ szyfrowanie danych osobowych,
    - ✓ inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
    - ✓ przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,
    - ✓ podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,
    - ✓ okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
    - ✓ 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, opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,
    - ✓ wdrożenie procedur określających postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich odpowiedzialność za bezpieczeństwo tych danych,
    - ✓ śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

8.2. Oceny skutków dla ochrony danych

Firma dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych

osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

8.3. Środki bezpieczeństwa

Firma 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 w Firmy.

Zarząd Firmy, pracownicy oraz Wolontariusze przed dopuszczeniem do dostępu do danych osobowych – podlegają przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.

Do podstawowych zabezpieczeń przed naruszeniem ochrony danych osobowych stosowanych w Jednostce należą:

1) ochrona obiektu,
2) wydzielanie pomieszczeń,
3) wyposażenie pomieszczeń w specjalne szafy,
4) zabezpieczenie wejść do pomieszczeń odpowiednimi zamkami.

Stosuje się systemy informatyczne zapewniające możliwość prześledzenia ciągu następujących po sobie operacji - tzw. "ślad rewizyjny”. Stosowane są różnorodne formy zabezpieczeń, takie jak:

a. testy penetracyjne - polegające na kontrolowanych próbach włamywania się do sieci,

b. plany i procedury postępowania w sytuacjach awaryjnych,

c. mechanizmy kontroli dostępu do systemów,

d. oprogramowanie antywirusowe,

e. szyfrowanie w celu uzyskania poufności,

f. podpisy cyfrowe,

g. sieciowe zapory ogniowe (firewall),

h. narzędzia monitoringu i analizy sieci,

i. zasilanie rezerwowe,

j. kopie zapasowe.

Stosowana technologia informacji w systemach komputerowych zapewnia, że nie ma możliwości wystąpienia poniższych sytuacji w zakresie dotyczącym przetwarzania danych osobowych:

- dostępu do wspólnej bazy danych wielu użytkowników,
- wprowadzania nieautoryzowanych zmian danych w plikach,
- dokonywania nieautoryzowanych zmian w systemach lub programach,
- wprowadzania zbędnych zmian w systemach lub programach,
- dokonywania nieodpowiednich ręcznych interwencji,
- potencjalną utratę danych lub brak możliwości wymaganego dostępu do danych.

Miejsce przechowywania informacji w Jednostce jest należycie zabezpieczone poprzez:

a) kontrolowany i rejestrowany dostęp do centrum komputerowego,
b) ograniczenie dostępu fizycznego do urządzeń IT tylko do upoważnionego personelu,
c) fizyczne zabezpieczenia pomieszczeń, w których następuje przetwarzanie lub przechowywanie informacji takie jak: systemy alarmowe,
d) centrum komputerowe jest zlokalizowane z dala od miejsc narażonych na zalanie lub powódź.
e) w razie awarii, utraty lub zniszczenia sprzętu operacyjnego (programów lub danych) zapewniony będzie ciągły dostęp do systemów.

Zarząd Firmy zapewnia, że zachowany jest rozdział funkcji pomiędzy użytkownikami a tymi, którzy tworzą lub modyfikują programy użytkowe oraz odpowiadają za przetwarzanie i dystrybucję danych osobowych.

W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, zapewniono:

1) drzwi wejściowe są zabezpieczone tak, aby otwarcie z zewnątrz mogło nastąpić wyłącznie przez uprawnione osoby,

2) wydawanie kluczy do pomieszczeń podlega rejestracji, z jednoczesnym poświadczeniem przez osobę odbierającą, faktu otrzymania kluczy o oznaczonym numerze,

3) pomieszczenia, w których znajdują się serwery są wyposażone w sprawne systemy klimatyzacji, ochrony przeciwpożarowej i przeciwwłamaniowej.

Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko użytkownicy oraz Informatyk. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe innych osób jest możliwy wyłącznie w obecności, co najmniej jednego użytkownika lub za zgodą Administratora Danych. W trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych jest zabronione.

Klucze do pomieszczeń wydawane są wyłącznie osobom do tego uprawnionym. Klucze zapasowe do pomieszczeń, przechowywane są w specjalnej szafie i mogą być wydawane w sytuacjach awaryjnych. Klucze zapasowe do szaf, w których przechowywane są kartoteki powinny być umieszczone w specjalnej szafie i mogą być wydawane w sytuacjach awaryjnych. Każdorazowe zdanie i pobranie kluczy zapasowych podlega wpisowi do rejestru, w rejestrze odnotowuje się datę, godzinę i nazwisko osoby zdającej lub pobierającej klucze oraz potwierdza jej podpisem.

W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana zatem poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe.

8.4. Zgłaszanie naruszeń

Przed przystąpieniem do pracy użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych (gromadzonych w systemach informatycznych, jak i w kartotekach), użytkownik:

1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,

2) zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez

uniemożliwienie dostępu do nich osób nieupoważnionych,

3) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

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

9. Przetwarzający

Firma posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Firmy 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 Firmy.

Firma przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące Załącznik do Polityki – **„Wzór umowy powierzenia przetwarzania danych”.**

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

10. Projektowanie prywatności

Firma zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.

11. Postanowienia końcowe

Polityka jest dokumentem wewnętrznym, zawiera dane, których ujawnienie mogłoby spowodować utratę danych chronionych w związku z czym nie może być udostępniania osobom nieupoważnionym w żadnej formie.

W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy 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 ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.

Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.