Polityka ochrony danych osobowych

Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych” (dalej: Polityka) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych dla:

Stowarzyszenie „Ochotnicza Straż Pożarna w Markach” (dalej: Stowarzyszenie), ul. Duża 1B, 05-270 Marki, KRS 0000456448, NIP 1251620605, REGON 14660451000000.

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).

1. Polityka zawiera opis zasad ochrony danych osobowych obowiązujących u „Administratora”.

2. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest:
    1) Zarząd Stowarzyszenia, któremu powierzono nadzór nad obszarem ochrony danych osobowych,
    2) osoba wyznaczona przez zarząd do zapewnienia zgodności z ochroną danych osobowych;

za nadzór i monitorowanie przestrzegania Polityki odpowiadają:

1) Zarząd Stowarzyszenia, któremu powierzono nadzór i monitorowanie przestrzegania Polityki ewentualnie osoba wyznaczona przez zarząd do nadzoru i monitorowania przestrzegania Polityki,
2) Komisja Rewizyjna, której powierzono nadzór i monitorowanie przestrzegania Polityki;

za stosowanie niniejszej Polityki odpowiedzialni są:

1) Zarząd Stowarzyszenia,
2) Członkowie Stowarzyszenia upoważnieni do przetwarzania danych osobowych.

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

3. SKRÓTY I DEFINICJE
    1) Polityka - oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
    2) 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).

3) Dane - oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.
4) Dane szczególnej kategorii – oznaczają 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.
5) Dane karne – oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.
6) Osoba - oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
7) Podmiot przetwarzający - oznacza organizację lub osobę, której Administrator powierzył przetwarzanie danych osobowych.
8) Profilowanie – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystywaniu 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.
9) Eksport danych – oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej;
10) IOD lub Inspektor - oznacza Inspektora Ochrony Danych Osobowych.
11) RCPD lub Rejestr - oznacza Rejestr Czynności Przetwarzania Danych Osobowych.
12) Administrator oznacza - Administratora danych osobowych – tj. Stowarzyszenie „Ochotnicza Straż Pożarna w Markach”.

4. OCHRONA DANYCH OSOBOWYCH U ADMINISTRATORA - ZASADY OGÓLNE
   1) Filary ochrony danych osobowych:
      a) Legalność - Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
      b) Bezpieczeństwo - Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie.
      c) Prawa jednostki - Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
      d) Rozliczalność - Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.
   2) Administrator przetwarza dane osobowe z poszanowaniem następujących zasad:
      a) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
      b) rzetelnie i uczciwie (rzetelność);
      c) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
      d) w konkretnych celach i nie „na zapas" (minimalizacja);
      e) nie więcej niż potrzeba (adekwatność);
      f) z dbałością o prawidłowość danych (prawidłowość);
      g) nie dłużej niż potrzeba (czasowość);
      h) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

3) System ochrony danych osobowych u Administratora składa się z następujących elementów:
   a) Inwentaryzacja danych. Administrator dokonuje identyfikacji zasobów danych osobowych w działalności Stowarzyszenia, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja)
   b) Rejestr. Administrator opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w działalności Stowarzyszenia (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych.
   c) Podstawy prawne. Administrator zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
      i. utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
      ii. inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Administrator przetwarza dane na podstawie prawnie uzasadnionego interesu.
4) Obsługa praw jednostki. Administrator spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) obowiązki informacyjne. Administrator przekazuje osobom prawem wymagane informacje 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 typu 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 RODO i dokumentowane;
   d) zawiadamianie o naruszeniach. Administrator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.
5) Minimalizacja. Administrator dokonuje systematycznej minimalizacji posiadanych danych osobowych, poprzez kierowania się zasadą adekwatnością danych osobowych weryfikację ich dalszej przydatności.
6) Bezpieczeństwo. Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
   a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
   b) dostosowuje środki ochrony danych do ustalonego ryzyka;
   c) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych - zarządza incydentami.
7) Przetwarzający. Administrator przekazuje dane osobowe do podmiotów, które dają należytą gwarancję bezpieczeństwa przekazanych danych osobowych, a które to przetwarzają dane osobowe w imieniu Administratora.

8) Eksport danych. Administrator weryfikuje, czy przekazuje dane do państw trzecich (czyli poza UE, Norwegię, Liechtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodne z prawem warunki takiego przekazywania, jeśli ma ono miejsce

5. INWENTARYZACJA
   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.
   2) Dane niezidentyfikowane. Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane, i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
   3) Profilowanie. Administrator identyfikuje 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.
   4) Współadministrowanie. Administrator identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

6. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH
   1) 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.
   2) Administrator prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
   3) Rejestr jest jednym z podstawowych narzędzi umożliwiających Administratorowi rozliczanie większości obowiązków ochrony danych.
   4) W Rejestrze dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru, Administrator odnotowuje co najmniej:
      a) nazwę czynności,
      b) cel przetwarzania,
      c) opis kategorii osób,
      d) opis kategorii danych,
      e) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Administratora, jeśli podstawą jest uzasadniony interes,
      f) sposób zbierania danych,

g) opis kategorii odbiorców danych (w tym przetwarzających),
h) informację o przekazaniu poza EU/EOG;
i) ogólny opis technicznych i organizacyjnych środków ochrony danych.

7. PODSTAWY PRZETWARZANIA
   1) Administrator dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
   2) Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, uzasadniony cel), Administrator dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne. Np. dla zgody - wskazując jej zakres, gdy podstawą jest prawo - wskazując konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy - wskazując kategorie zdarzeń, w których się zmaterializują, uzasadniony cel - wskazując konkretny cel.
   3) 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.)

8. SPOSÓB OBSŁUGI PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH
   1) Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
   2) Administrator podejmuje działania mające na celu ułatwienie osobom korzystanie z ich praw.
   3) Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
   4) Administrator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
   5) Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

9. OBOWIĄZKI INFORMACYJNE
   1) Administrator określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
   2) Administrator informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby
   3) Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
   4) Administrator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe (w tym poprzez tabliczkę o objęciu obszaru monitoringiem wizyjnym).
   5) Administrator informuje osobę o planowanej zmianie celu przetwarzania danych.
   6) Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.

7) Administrator informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
8) Administrator informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
9) Administrator 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

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 (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste), Administrator może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
2) Nieprzetwarzanie. Administrator informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
3) Odmowa. Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
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 (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 jej wydania po uiszczeniu odpowiedniej opłaty.
5) Kopie danych. Na żądanie Administrator wydaje osobie kopię 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.
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.
7) Uzupełnienie danych. Administrator uzupełnia i aktualizuje dane na żądanie osoby. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (Administrator nie musi przetwarzać danych, które są mu zbędne). Administrator może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle

przyjętych przez Administratora procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

8) Usunięcie danych. Na żądanie osoby Administrator usuwa dane, gdy:
   a) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
   b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
   c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
   d) dane były przetwarzane niezgodnie z prawem,
   e) konieczność usunięcia wynika z obowiązku prawnego,

Administrator 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 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) 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, 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 Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Administrator 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. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.

10) Przenoszenie danych. Na żądanie osoby, Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe,

dane dotyczące tej osoby, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej.

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, 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.

11. MINIMALIZACJA

1) Administrator dba o minimalizację przetwarzania danych pod kątem:
   a) adekwatności danych do celów (ilości danych i zakresu przetwarzania),
   b) dostępu do danych,
   c) czasu przechowywania danych.
2) Minimalizacja zakresu. Administrator zweryfikowała 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.
3) Minimalizacja dostępu. Administrator 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).
4) Administrator stosuje kontrolę dostępu fizycznego. Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.
5) Minimalizacja czasu. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów Administratora. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych.

12. BEZPIECZEŃSTWO

1) Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych.
2) Analizy ryzyka i adekwatności środków bezpieczeństwa. Administrator przeprowadza analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
   a) Administrator zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji,
   b) Administrator kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
   c) Administrator przeprowadza 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.

d) Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. Administrator stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa.

3) Sposoby przechowywania danych wraz ze sposobem zabezpieczenia:
   a) W formie papierowej: zamykane na klucz szafy umiejscowione w odrębnych, zamykanych pomieszczeniach, do których dostęp mają jedynie osoby upoważnione;
   b) W formie elektronicznej:
      i. Dane przechowywane są na komputerach i serwerach zabezpieczonych: programem antywirusowym, firewallem, hasłem,
      ii. Dane przechowywane na poczcie elektronicznej, do której dostęp zabezpieczony jest hasłem, dostęp posiadają jedynie osoby upoważnione;
      iii. Dane na płytach CD i pendrive – dane zabezpieczone hasłem, dostęp posiadają jedynie osoby upoważnione;
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.

13. PRZETWARZAJĄCY

Podmioty przetwarzające dane osobowe w imieniu Administratora dają wystarczającą gwarancję wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Administratorze.

14. EKSPORT DANYCH

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