

## **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 Firmie PENSJONAT BEATA Eugeniusz Guszpit, ul. Rybna 9, 57-320 Polanica-Zdrój.

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 Firmie;

b) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje

dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);

i) Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest

Właściciel Firmy, który odpowiada za nadzór nad obszarem ochrony danych osobowych;

ii) Właściciel Firmy zapewnia zgodność z ochroną danych osobowych, nadzór oraz monitorowanie przestrzegania Polityki

Za stosowanie niniejszej Polityki odpowiedzialny jest Właściciel Firmy

Firma zapewnia zgodność postępowania kontrahentów Firmy z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Spółkę.

3. **Skróty i definicje:**

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

**RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych

osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy

95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).

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

**Dane 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, zewnętrzna księgowość).

**Profilowanie** oznacza dowolną formę zautomatyzowanego przetwarzania danych<sup>1</sup>

osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji

lub przemieszczania się.

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

**IOD lub Inspektor** oznacza Inspektora Ochrony Danych Osobowych

**RCPD lub Rejestr** oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

**Firma** oznacza PENSJONAT BEATA MARCO WILLER, ul. Rybna 9, 57-320 Polanica-

Zdrój.

#### **4. Ochrona danych osobowych w Firmie – zasady ogólne**

##### **5.1. Filary ochrony danych osobowych w Firmie:**

**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.

##### **5.2. Zasady ochrony danych**

Spółka 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 i nie „na zapas” (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 Firmie składa się z następujących elementów:

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

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

**a)** przypadków przetwarzania danych specjalnych i danych „kryminalnych” (**dane wrażliwe**);

**b)** przypadków przetwarzania danych osób, których Spółka nie identyfikuje (**dane niezidentyfikowane**);

**c)** współadministrowania danymi.

<sup>2</sup>

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

a) przeprowadza analizy ryzyka dla czynności przetwarzania danych;

b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;

c) dostosowuje środki ochrony danych do ustalonego ryzyka;

d) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.

**6) Przetwarzający.** Firma posiada zasady doboru przetwarzających dane na rzecz Firmy,

wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

**7) Eksport danych.** Firma nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

**8) Ochrony prywatności w fazie projektowania (*Privacy by design*).** Firma zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Firmie uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów

3

przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

## **5. Inwentaryzacja**

### **A 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.

### **B Dane niezidentyfikowane**

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

### **C Współadministrowanie**

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

## **6. Rejestr Czynności Przetwarzania Danych**

A 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.

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

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

D W Rejestrze, dla każdej czynności przetwarzania danych, którą Firma uznała za odrębną

dla potrzeb Rejestru, Spółka odnotowuje 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 Firmy, 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.

E Rejestr stanowi **Załącznik nr 1 do Polityki – „Rejestr Czynności Przetwarzania Danych”**. Rejestr 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

## **7. Podstawy przetwarzania**

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

B 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

4

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.

C 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.).

D Właściciel Firmy zna podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest

uzasadniony interes Firmy, właściciel zna konkretny realizowany przetwarzaniem interes

Firmy.

## **8. Sposób obsługi praw jednostki i obowiązków informacyjnych**

**8.1.** Firma dba o czytelność i styl przekazywanych informacji i komunikacji z osobami,

których dane przetwarza.

**8.2.** Firma ułatwia osobom korzystanie z ich praw, poprzez skorzystanie z informacji o

prawach osób w Firmie, w tym wymaganiach dotyczących identyfikacji i metodach kontaktu z Firmą.

**8.3.** Firma dba o dotrzymanie prawnych terminów realizacji obowiązków względem osób.

**8.4.** Firma wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb

realizacji praw jednostki i obowiązków informacyjnych.

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

**8.6.** Firma dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

## **9. Obowiązki informacyjne**

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

**9.2.** Firma informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie

żądania tej osoby.

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

osoby.

**9.4.** Firma informuje osobę o planowanej zmianie celu przetwarzania danych.

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

lub będzie niemożliwe).

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

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

5

## **10. Żądania osób**

**10.1. 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.

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

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

**10.4. Dostęp do danych.** Na żądanie osoby dotyczące 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. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Firma nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

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

**10.6. 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.

**10.7. Uzupelnienie 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

Firmie 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.

**10.8. Usunięcie danych.** Na żądanie osoby, Firma usuwa dane, gdy:

- 1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych 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,

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.

**10.9. Ograniczenie przetwarzania.** Firma 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) Firma 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 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.

**10.10. 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 Firmie, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Firmy.

**10.11. Sprzeciw w szczególnej sytuacji.** Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Firmę w oparciu o uzasadniony interes Firmy lub o powierzone

Firmie 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

7

ustalenia, dochodzenia lub obrony roszczeń.

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

**10.13. Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.** Jeżeli Firma 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**, Firma zapewnia możliwość odwołania się do interwencji, chyba że taka automatyczna decyzja (a) jest niezbędną do zawarcia lub wykonania umowy między odwołującą się osobą a Firmą; lub (b) jest wprost dozwolona przepisami prawa; lub (c) opiera się o wyraźną zgodę odwołującej osoby.

## **11. MINIMALIZACJA**

Firma 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.

### **11.1. Minimalizacja zakresu**

Firma weryfikuje 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.

### **11.2. 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 podmiotów przetwarzających.

Firma dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje

ich nie rzadziej niż raz na rok.

### **11.3. Minimalizacja czasu**



Firma wdraża mechanizmy kontroli cyklu życia danych osobowych w Firmie, w tym weryfikacji dalszej przydatności danych względem terminów.

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..

## **12. BEZPIECZEŃSTWO**

Firma zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności

osób fizycznych wskutek przetwarzania danych osobowych przez Firmę.

### **12.1. Analizy ryzyka i adekwatności środków bezpieczeństwa**

8

Firma przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych

osobowych. W tym celu:

- 1) Firma zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
- 2) Firma kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
- 3) Firma przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Spółka analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
- 4) 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:
  - i) środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
  - ii) 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.

### **12.2. 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.

### **12.3. 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 i zapewnienia cyberbezpieczeństwa w Firmie.

#### **12.4. Zgłaszanie naruszeń**

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

#### **13. PRZETWARZAJĄCY**

Firma weryfikuje przetwarzających dane na rzecz Spółki, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych

dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Firmie.

Firma przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych

stanowiące **Załącznik nr 2 do Polityki – „umowa powierzenia przetwarzania danych”**.

Firma rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych

9

wymagań wynikających z Zasad powierzenia danych osobowych.

#### **14. EKSPORT DANYCH**

Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z

wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Firma okresowo

weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem

ochrony danych rozwiązania równoważne.

#### **15. PROJEKTOWANIE PRYWATNOŚCI**

Firma 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 Firmę 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.

10