POLITYKA OCHRONY DANYCH OSOBOWYCH

§ 1

1. Administrator, świadomy zagrożeń dla bezpieczeństwa przetwarzanych danych osobowych, deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania m. in. takim zagrożeniom, jak:

   a. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby Systemu informatycznego, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie;

   b. niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne);

   c. awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie procedur serwisowych w tym przyzwolenie na naprawę sprzętu zawierającego Dane osobowe poza siedzibą Administratora;

   d. naruszenie bezpieczeństwa danych przez nieautoryzowane ich Przetwarzanie;

   e. ujawnienie osobom nieupoważnionym zasad ochrony danych stosownych przez Administratora;

   f. celowe lub przypadkowe rozproszenie danych w Internecie z ominięciem zabezpieczeń Systemu informatycznego lub wykorzystaniem błędów Systemu informatycznego Administratora;

   g. ataki z Internetu;

   h. naruszenia zasad określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem zasad ochrony danych, w tym zwłaszcza:

      - niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy;
      - naruszenie bezpieczeństwa danych przez nieautoryzowane ich Przetwarzanie;
      - ujawnienie osobom nieupoważnionym zasad ochrony danych stosowanych u Administratora;
      - ujawnienie osobom nieupoważnionym danych przetwarzanych przez Administratora, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru w niedostatecznie nadzorowanych pomieszczeniach Administratora;
      - niewykonywanie kopii zapasowych zgodnie z przyjętymi u Administratora procedurami;
      - Przetwarzanie danych osobowych niezgodnie z celem określonym przez Administratora, w tym dla celów prywatnych;
      - wprowadzanie zmian do Systemu informatycznego Administratora i instalowanie jakiegokolwiek oprogramowania bez zgody ASI.

§ 2 Definicje

Ilekroć dane pojęcie zostanie napisane w Polityce dużą literą, ma ono znaczenie określone poniżej:

1) **Administrator** – rozumie się przez to Martę Wróbel prowadzącą działalność gospodarczą pod firmą FOLKSTAR Marta Wróbel ustalającą cele i sposoby przetwarzania danych osobowych;

2) **Anonimizacja** – rozumie się przez to takie przekształcenie danych osobowych, po którym niemożliwe jest przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do

określonej lub możliwej do zidentyfikowania osoby fizycznej, przy czym proces ten jest nieodwracalny;

3) **Członek personelu** – rozumie się przez to osobę zatrudnioną u Administratora na podstawie stosunku pracy, umów cywilnoprawnych (np. umowy o dzieło lub umowy zlecenia), przedsiębiorcę wykonującego działalność osobiście i jednoosobowo (w tym w ramach umów o współpracy), osobę odbywającą praktyki, stażystę, osobę skierowaną do pracy w ramach umów z agencjami pracy tymczasowej wykonującą pracę związaną z Przetwarzaniem danych osobowych u Administratora;

4) **Dane osobowe** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (**„osoba, której Dane dotyczą”**). Osobą możliwą do zidentyfikowania jest osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie Identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

5) **Szczególne kategorie Danych osobowych**– rozumie się przez to Dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby,

6) **Dane dotyczące wyroków i naruszeń prawa -** dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa;

7) **Dane osobowe zwykłe –** rozumie się przez to Dane osobowe, które nie są danymi osobowymi Szczególnych kategorii ani Danymi dotyczącymi wyroków i naruszeń prawa;

8) **Hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie Użytkownikowi;

9) **Identyfikator** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w Systemie informatycznym;

10) **Integralność i poufność danych** – rozumie się przez to właściwość zapewniającą odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem Przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych

11) **Komisja** – rozumie się przez to Komisję Europejską

12) **Odbiorca danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się Dane osobowe, w tym procesora, z wyjątkiem organów publicznych, które mogą otrzymywać Dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem polskim

13) **Ograniczenie przetwarzania**– rozumie się przez to oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

14) **Organ nadzorczy** – rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych

15) **Organizacja międzynarodowa** – rozumie się przez to organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy,

16) **Osoba upoważniona do przetwarzania danych osobowych** – rozumie się przez to członka personelu, który został upoważniony przez Administratora do przetwarzania danych osobowych u Administratora;

17) **Państwo trzecie** – rozumie się przez to każde państwo nienależące do Europejskiego Obszaru Gospodarczego (zwanego dalej: EOG),

18) **Powierzenie przetwarzania danych osobowych** – rozumie się przez to zlecenie wykonania czynności przetwarzania danych osobowych przez procesora na rzecz Administratora na podstawie stosownego postanowienia w umowie, zapewniającego warunki bezpieczeństwa danych osobowych zgodnie z przepisami Rozporządzenia lub na podstawie odrębnej pisemnej umowy powierzenia przetwarzania danych osobowych zawartej zgodnie z art. 28 ust. 3 Rozporządzenia;

19) **Procesor** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza Dane osobowe w imieniu Administratora,

20) **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;

21) **Rozliczalność** – rozumie się przez to właściwość zapewniającą możliwość wykazania przestrzegania przepisów Rozporządzenia;

22) **Rozporządzenie** – rozumie się przez to Rozporządzenie 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 oraz uchylenia dyrektywy 95/46/WE (ogólne Rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1)

23) **Przedsiębiorca –** Marta Wróbel prowadząca działalność gospodarczą pod firmą FOLKSTAR Marta Wróbel.

24) **System informatyczny Administratora**– rozumie się przez to sprzęt komputerowy, oprogramowanie, Dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, zasad przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych Klientów;

25) **Ujawnianie danych osobowych** – rozumie się przez to przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie danych osobowych;

26) **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której Dane dotyczą;

27) **Uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby fizycznej lub podmiotu;

28) **Użytkownik** – rozumie się przez to członka personelu upoważnionego na piśmie do przetwarzania danych osobowych;

29) **Zabezpieczenie Systemu informatycznego** – rozumie się przez to wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych i informatycznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;

30) **Zbieranie danych osobowych** – rozumie się przez to pozyskiwanie danych od osoby, której one dotyczą lub z innych źródeł;

31) **Zgoda osoby, której Dane dotyczą** – rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której Dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na Przetwarzanie dotyczących jej danych osobowych;

§ 3

1. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Przedsiębiorca.
2. Za nadzór i monitorowanie Polityki odpowiada Przedsiębiorca.
3. Za stosowanie niniejszej polityki jest Przedsiębiorca.

§ 4 Zasady przetwarzania danych osobowych

1. Ochrona danych osobowych w Spółce opiera się na następujących filarach:
    a. **Legalność –** Przedsiębiorca dba o ochronę prywatności i przetwarza dane zgodnie z prawem;
    b. **Bezpieczeństwo –** Przedsiębiorca zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie;
    c. **Prawa jednostki –** Przedsiębiorca umożliwia osobom, których dane przetwarza wykonywanie swoich praw i prawa te realizuje;
    d. **Rozliczalność –** Przedsiębiorca dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.
2. Przedsiębiorca przetwarza dane osobowe na następujących zasadach:
    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 dużej nie potrzeba (czasowość);
    h. Zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).
3. System ochrony danych osobowych w Spółce składa się z następujących elementów:
    a. **Inwentaryzacja danych.** Przedsiębiorca dokonuje identyfikacji zasobów danych osobowych u Przedsiębiorcy, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja).
    b. **Rejestr.** Przedsiębiorca opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w Przedsiębiorstwie (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych u Przedsiębiorcy.
    c. **Podstawy prawne.** Przedsiębiorca zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych osobowych i rejestruje je w Rejestrze w tym:
        - Utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość;
        - Inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Przedsiębiorca przetwarza dane na podstawie prawnie uzasadnionego interesu Przedsiębiorcy.
    d. **Obsługa praw jednostki.** Przedsiębiorca spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewni obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

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

e. **Minimalizacja.** Przedsiębiorca posiada zasady i metody zarządzania minimalizacją (privacy by default), w tym:
- **Zasady zarządzania adekwatnością danych;**
- **Zasady reglamentacji i zarządzania dostępem do danych;**
- **Zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.**

f. **Bezpieczeństwo.** Przedsiębiorca zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
- Przeprowadza analizę ryzyka dla czynności przetwarzania danych lub ich kategorii;
- Przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
- Dostosowuje środki ochrony danych do ustalonego ryzyka;
- Posiada system zarządzania bezpieczeństwem informacji;
- Stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.

g. **Przetwarzający.** Przedsiębiorca posiada zasady doboru przetwarzających dane na rzecz Przedsiębiorcy, wymogów co do warunków przetwarzania (umowy o przetwarzanie), zasady weryfikacji wykonywania umów o przetwarzanie.

h. **Eksport danych.** Przedsiębiorca posiada zasady weryfikacji, czy Przedsiębiorca nie przekazuje danych do państw trzecich lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

i. **Privacy by design.** Przedsiębiorca zarządza zmianami wpływającymi na prywatność. W tym celu procedur uruchomienia nowy projektów i inwestycji w Spółce uwzględniają konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

j. **Przetwarzanie transgraniczne.** Przedsiębiorca posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

§ 5 Inwentaryzacja

1. Przedsiębiorca identyfikuje przypadki, w których dochodzi do przetwarzania lub może dojść do przetwarzania danych szczególnych kategorii lub danych karnych, oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W przypadku identyfikacji przypadków przetwarzania danych szczególnych kategorii lub danych karnych Przedsiębiorca postępuje zgodnie z przyjętymi w tym zakresie zasadami.
2. Przedsiębiorca identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dane dotyczą dane niezidentyfikowane.
3. Przedsiębiorca identyfikuje przypadki, w których dochodzi do profilowania przetwarzanych danych osobowych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku identyfikacji przypadków profilowania i zautomatyzowanego podejmowania decyzji Przedsiębiorca postępuje zgodnie z przyjętymi zasadami w tym zakresie.
4. Przedsiębiorca identyfikuje przypadki współadministrowania danymi osobowymi i postępuje zgodnie z przyjętymi w tym zakresie zasadami.

§ 6 Rejestr czynności przetwarzania danych osobowych (RCPD)

1. RCPD stanowi formę dokumentowania czynności przetwarzania danych osobowych, pełni rolę mapy przetwarzania danych i jet jednym z kluczowych elementów realizujących fundamentalną zasadę rozliczalności.
2. Przedsiębiorca prowadzi Rejestr czynności przetwarzania danych osobowych w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystywane są dane osobowe.
3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Spółce rozliczanie większości obowiązków ochrony danych osobowych.
4. W RCPD dla każdej czynności przetwarzania danych, którą Przedsiębiorca uznał za odrębną dla potrzeb RCPD, Przedsiębiorca odnotowuje co najmniej:
   a) nazwę czynności;
   b) cel przetwarzania;
   c) opis kategorii osób;
   d) opis kategorii danych;
   e) podstawę prawną przetwarzania;
   f) sposób zbierania danych;
   g) opis kategorii odbiorców danych;
   h) informację o przekazaniu danych poza EU/EOG;
   i) ogólny opis technicznych i organizacyjnych środków ochrony danych.

§ 7 Podstawy przetwarzania

1. Przedsiębiorca dokumentuje w RCPD podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
2. Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zdanie publiczne/władza publiczna, uzasadniony cel Przedsiębiorcy), Przedsiębiorca dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne. Np. dla zgody – wskazując jej zakres, gdy podstawą jest prawo – wskazuje konkretny przepis i inne dokumenty, np. umowę, porozumienie, żywotne interesy – wskazując kategorie zdarzeń. W

których się zmaterializują, uzasadniony cel – wskazując konkretny cel np. marketing własny, dochodzenie roszczeń.

3. Przedsiębiorca 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 itd.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczanie itp.).
4. Kierownik komórki organizacyjnej Przedsiębiorcy ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Przedsiębiorcy, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes Przedsiębiorcy.

§ 8 Sposób obsługi praw jednostki i obowiązków informacyjnych

1. Przedsiębiorca dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
2. Przedsiębiorca dba o dotrzymanie prawnych terminów realizacji obowiązków względem osób.
3. Przedsiębiorca wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
4. W celu realizacji praw jednostki Przedsiębiorca zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Przedsiębiorcę, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.
5. Przedsiębiorca dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

§ 9 Obowiązki informacyjne

1. Przedsiębiorca określa zgodnie z prawem i efektywnie sposoby wykonywania obowiązków informacyjnych.
2. Przedsiębiorca informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
3. Przedsiębiorca informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
4. Przedsiębiorca informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
5. Przedsiębiorca określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe (np. tablica o objęciu obszaru monitoringiem wizyjnym).
6. Przedsiębiorca informuje o planowanej zmianie celu przetwarzania danych.
7. Przedsiębiorca informuje osobę przed uchyleniem ograniczenia przetwarzania.
8. Przedsiębiorca informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
9. Przedsiębiorca informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszy kontakcie z tą osobą.
10. Przedsiębiorca bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie naruszenie praw lub wolności tej osoby.

§ 10 Żądania osób

1. **Prawa osób trzecich.** Realizując prawa osób, których dane dotyczą, Przedsiębiorca wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej informacji o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób, Przedsiębiorca może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
2. **Nieprzetwarzanie.** Przedsiębiorca informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
3. **Odmowa.** Przedsiębiorca 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 Przedsiębiorca informuje, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być realizowany poprzez wydanie kopii danych z tym zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Przedsiębiorca nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
5. **Kopie danych.** Na żądanie Przedsiębiorca wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Przedsiębiorca wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłatę za kolejne kopie.
6. **Sprostowanie danych.** Przedsiębiorca dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Przedsiębiorca ma prawo odmówić sprostowania danych chyba, że osoba w rozsądny sposób wykaże nieprawidłowość tych danych. W przypadku sprostowania danych Przedsiębiorca informuje odbiorców danych na żądanie tej osoby.
7. **Uzupełnienie danych.** Przedsiębiorca uzupełnia i aktualizuje dane na żądanie osoby. Przedsiębiorca ma prawo odmowy uzupełnienia danych jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania. Przedsiębiorca może polegać na oświadczeniu osoby co do nieuzupełnianych danych chyba, że będzie to niewystarczające w świetle przyjętych przez Przedsiębiorcę procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
8. **Usunięcie danych.** Na żądanie osoby Przedsiębiorca usuwa dane, gdy:
   a) dane nie są niezbędne dla celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach;
   b) zgodna na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania;
   c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;
   d) konieczność usunięcia wynika z obowiązku prawnego;
   e) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
9. Przedsiębiorca 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.

10. Jeżeli dane podlegające usunięciu zostały upublicznione przez Przedsiębiorcę, Przedsiębiorca podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane o potrzebie usunięcia danych i dostępu do nich.
11. W przypadku usunięcia danych Przedsiębiorca informuje o odbiorcach danych na żądanie tej osoby.
12. **Ograniczenie przetwarzania.** Przedsiębiorca dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
    a) osoba kwestionuje prawidłowość danych – przez 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) Przedsiębiorca 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 ze szczególną sytuacją – do czasu stwierdzenia, czy po stronie Przedsiębiorcy zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
13. W trakcie ograniczenia przetwarzania danych Przedsiębiorca przechowuje dane natomiast nie przetwarza ich 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 na ważne względy interesu publicznego.
14. Przedsiębiorca informuje osobę przed uchyleniem ograniczenia przetwarzania.
15. W przypadku ograniczenia przetwarzania danych Przedsiębiorca informuje osobę o odbiorcach danych, na żądanie tej osoby.
16. **Przenoszenie danych.** Na żądanie osoby Przedsiębiorca 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 Spółce, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w system informatycznych Przedsiębiorcy.
17. **Sprzeciw w szczególnej sytuacji.** Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych osobowych, a dane przetwarzane są przez Przedsiębiorcę w oparciu uzasadniony interes Przedsiębiorcy lub o powierzone Przedsiębiorcy zadanie w interesie publicznym, Przedsiębiorca uwzględni sprzeciw, o ile nie zachodzą po stronie Przedsiębiorcy ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia i obrony roszczeń.
18. **Sprzeciw względem marketingu bezpośredniego.** Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Przedsiębiorcę na potrzeby marketingu bezpośredniego, Przedsiębiorca uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
19. **Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.** Jeżeli Przedsiębiorca 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, Przedsiębiorca zapewnia możliwość odwołania się do interwencji i decyzji człowiek po stronie Przedsiębiorcy, chyba że taka automatyczna decyzja:
    a) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą, a Przedsiębiorcą;
    b) jest wprost dozwolona przepisami prawa;
    c) opiera się na wyraźnej zgodzie odwołującej się osoby.

§ 11 Minimalizacja

1. Przedsiębiorca dba o minimalizację przetwarzania danych pod kątem:
   a) adekwatności danych do celów;
   b) dostępu do danych;
   c) czasu przechowywania danych.
2. Przedsiębiorca zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.
3. Przedsiębiorca dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu przetwarzania nie rzadziej niż raz na rok.
4. Przedsiębiorca przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).
5. Przedsiębiorca 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 dane rezydują dane osobowe).
6. Przedsiębiorca stosuje kontrolę dostępu fizycznego.
7. Przedsiębiorca dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.
8. Przedsiębiorca dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
9. Przedsiębiorca wdraża mechanizmy kontroli cyklu życia danych osobowych u Przedsiębiorcy, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w RCPD.
10. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów produkcyjnych Przedsiębiorcy, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Przedsiębiorcę. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

§ 12 Bezpieczeństwo

1. Przedsiębiorca zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Przedsiębiorcę.
2. Przedsiębiorca przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
   a) Przedsiębiorca zapewnia odpowiedni san wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych podmiotów;
   b) Przedsiębiorca kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;

c) Przedsiębiorca przeprowadza analizę ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Przedsiębiorca 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) Przedsiębiorca ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Przedsiębiorca 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.

3. Przedsiębiorca dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności jest wysokie.
4. Przedsiębiorca stosuje metodykę oceny skutków przyjętą u Przedsiębiorcy.
5. Przedsiębiorca stosuje środki bezpieczeństwa ustalone w ramach analizy ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.
6. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Spółce i są bliżej opisane w procedurach przyjętych przez Przedsiębiorcę dla tych obszarów.
7. Przedsiębiorca stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

§ 13 Przetwarzający

1. Przedsiębiorca posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Przedsiębiorcy 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 Przedsiębiorcy.
2. Przedsiębiorca rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

§ 14 Eksport danych

1. Przedsiębiorca rejestruje w RCPD przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy.
2. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Przedsiębiorca okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodnie z prawem ochrony danych rozwiązania równoważne.

§ 15 Projektowanie prywatności

1. Przedsiębiorca zarządza zamianą mającą wpływa na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.
2. W tym celu zasady prowadzenia projektów i inwestycji przez Przedsiębiorcę odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowania bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.