Polityka Ochrony Danych

w Polana Sp. z o.o.

Niniejszy dokument, zatytułowany **Polityka Ochrony Danych w Polana Sp. z o.o.** (dalej jako: **Polityka**) stanowi mapę wymogów, zasad i organizacji w procesach przetwarzania danych osobowych w Polana Sp. z o.o.(dalej jako: **Spółka**).

1. Niniejsza Polityka jest polityką ochrony danych w rozumieniu przepisów RODO - 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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1 z dnia 2016.05.03).

2. Polityka zawiera:

a) Opis zasad ochrony danych obowiązujących w Spółce,
b) Odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów ochrony danych osobowych).

3. Odpowiedzialny za wdrożenie niniejszej polityki jest Zarząd Spółki, oraz jej pracownicy

4. Odpowiedzialni za nadzór i monitorowanie niniejszej Polityki są pracownicy wyznaczenie przez Spółkę.

5. Za stosowanie niniejszej Polityki odpowiedzialni są:

i. Spółka,
ii. wszyscy członkowie personelu Spółki,

Spółka powinna też zapewnić, w miarę możliwości, zgodność postępowania kontrahentów Spółki z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Spółkę.

6. **Skróty i definicje:**
    a. **Polityka –** oznacza niniejszą Politykę, o ile co innego nie wynika wyraźnie z kontekstu,
    b. **RODO –** oznacza 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.U.UE.L.2016.119.1 z dnia 2016.05.03),
    c. **Dane –** oznaczają dane osobowe, o ile nic innego nie wynika wyraźnie z kontekstu,
    d. **Dane wrażliwe** – oznaczają dane specjalne i karne,
    e. **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 oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby,
    f. **Dane karne –** oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa,
    g. **Dane dzieci –** oznaczają dane osób poniżej 16 roku życia,
    h. **Osoba** – oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu,
    i. **Podmiot przetwarzający** – oznacza organizację lub osobę, której Spółka powierzyła przetwarzanie danych (np. usługodawca IT, zewnętrzną księgowość),
    j. **Profilowanie –** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się,
    k. **Eksport danych –** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej,
    l. **IOD lub Inspektor –** oznacza Inspektora Ochrony Danych,
    m. **RCPD lub Rejestr –** oznacza Rejestr Czynności Przetwarzania Danych Osobowych
    n. **Spółka-** oznacza Spółkę Polana Sp. z o.o. z siedzibą pod adresem: Żelimucha 28, 78-200 Białogard.

7. Ochrona Danych w Spółce - Zasady ogólne

7.1 Filary ochrony danych w Spółce

(1) Legalność – Spółka dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

(2) Bezpieczeństwo – Spółka zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

(3) Prawa Jednostki – Spółka umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje,

(4) Rozliczalność – Spółka dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność,

7.2 Zasady ochrony danych w Spółce

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 osób, których 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);

7.3 System ochrony danych

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

1) **Inwentaryzacja danych**

   Spółka dokonuje inwentaryzacji zasobów danych osobowych w Spółce, w tym
   a) Zbiory danych,
   b) Podstawy przetwarzania,
   c) Zakres przetwarzania,
   d) Cel przetwarzania,

Wzór Inwentaryzacji przetwarzania danych osobowych w Spółce stanowi załącznik nr 1 do Polityki.

2) **Rejestr.**

Spółka opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych w Spółce. Rejestr jest narzędziem rozliczania zgodnośći z ochroną danych osobowych w Spółce.

Wzór Rejestru przetwarzania danych osobowych w Spółce stanowi załącznik nr 2 do Polityki.

3) **Podstawy prawne.**

Spółka zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych osobowych i rejestruje je w rejestrze.

4) **Obsługa praw jednostki.**

Spółka spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując zgłoszone w tym zakresie żądania, w tym:

a) **Obowiązki informacyjne –** Spółka przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;

Wzór klauzuli informacyjnych stanowią załączniki od nr 3 do nr 7.

b) **Możliwość wykonania żądań.** Spółka weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;

c) **Obsługa żądań.** Spółka zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane

d) **Zawiadamianie o naruszeniach.** Spółka stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5) **Minimalizacja*, privacy by design, privacy by default.***
Spółka przetwarza dane w czasie oraz zakresie, jaki jest niezbędny.

Spółka posiada w tym celu procedurę retencji danych, która służyć ma ustaleniu niezbędnego okresu przetwarzania danych oraz jego możliwym ograniczeniu.

Procedura retencji danych stanowi załącznik nr 8 do Polityki

Spółka, celem zapewnienia przetwarzania wyłącznie niezbędnych ilości danych, dokonuje cyklicznych, tj. corocznych, kontroli danych w tym zakresie.

6) **Bezpieczeństwo.**

Spółka zapewnia odpowiedni poziom bezpieczeństwa danych, w tym :

a) przeprowadza analizy ryzyka dla czynności przetwarzania, kategorii tych czynności lub aktywów, za których pomocą mają dane być przetwarzane;

Wzór analizy ryzyka stanowi załącznik nr 9 do Polityki

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

Wzór oceny skutków dla ochrony danych stanowi załącznik nr 10 do Polityki

c) dostosowuje środki ochrony danych do ustalonego ryzyka;

d) zarządza dostępem do danych poprzez prowadzenie ewidencji osób upoważnionych do przetwarzania danych;

Wzór upoważnienia stanowi załącznik nr 11 do Polityki.
Wzór ewidencji osób upoważnionych stanowi załącznik nr 12 do Polityki.

e) stosuje procedurę identyfikacji, oceny oraz zgłoszenia nruszeń danych osobowych do Urzędu Ochrony Danych.

7) **Przetwarzający.**

Spółka powierzając przetwarzanie danych osobowych zawiera stosowną umowę, w ramach której wprowadza wymogi przetwarzania oraz określa zasady ich weryfikacji.

Wzór umowy powierzenia przetwarzania danych stanowi załącznik nr 13 do Polityki.

8) Eksport danych.
Spółka weryfikuje, czy przekazuje dane do państw trzecich, tj. poza UE, Norwegię, Lichtenstein. W przypadku pojawienia się konieczności eksportu danych Spółka podejmuje działania, aby odbywało się to w sposób zgodny z prawem.

8. Inwentaryzacja

8.1. Dane wrażliwe

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

8.2. Dane niezidentyfikowane

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

8.3. Profilowanie

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

8.4. Współadministrowanie

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

9. Rejestr czynności przetwarzania danych

9.1. 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.

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

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

9.4. W Rejestrze, dla każdej czynności przetwarzania danych, którą Spółka uznała za odrębną dla potrzeb Rejestru, Spółka odnotowuje co najmniej: nazwę czynności, cel przetwarzania, podstawę, podmiot przetwarzający, kategorie osób, kategorie danych, szczególne kategorie danych, kategorie odbiorców, sposób przetwarzania, sposób pozyskiwania, okres przechowywania, opis środków bezpieczeństwa, dane nt. transferu do państwa trzeciego oraz dokumentację dotyczącą odpowiednich zabezpieczeń.

Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Spółka rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

10. Podstawy przetwarzania

10.1 Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Spółki) Spółka 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.

10.2 Kierownik komórki organizacyjnej Spółki ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Spółki, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes Spółki.

11 Sposób obsługi praw jednostki i obowiązków informacyjnych

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

11.2 Spółka ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Spółki informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Spółce, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu ze Spółką w tym celu, ewentualnym cenniku żądań „dodatkowych" itp.

11.3 Spółka dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

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

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

11.6 Spółka dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

Rejestr wykonania obowiązków informacyjnych stanowi załącznik nr 14 do Polityki.

Rejestr realizacji praw osób stanowi załącznik nr 15 do Polityki

12 Obowiązki informacyjne

12.1 Spółka określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

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

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

12.4 Spółka informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.

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

12.6 Spółka informuje osobę o planowanej zmianie celu przetwarzania danych.

12.7 Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania.

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

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

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

13 Żądania osób.

13.1 Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, Spółka wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W ramach procedury realizacji praw osób, których dane dotyczą Spółka prowadzi rejestr przypadków tych realizacji.

13.2 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.), Spółka może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

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

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

13.5 Dostęp do danych. Na żądanie osoby dotyczące dostępu do jej danych, Spółka 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 Spółka nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

13.6 Kopie danych. Na żądanie Spółka 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.

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

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

13.9 Usunięcie danych. Na żądanie osoby, Spółka 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,

(6) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

Spółka 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 Spółkę, Spółka 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 Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

13.10 Ograniczenie przetwarzania. Spółka 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) Spółka 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 Spółki zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Spółka 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.

Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania.

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

13.11 Przenoszenie danych. Na żądanie osoby Spółka 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 Spółce, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Spółki.

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

13.13 Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych. Jeżeli Spółka prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może **wnieść**umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Spółka uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

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

13.15 Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu. Jeżeli Spółka 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**, Spółka zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Spółki, chyba że taka automatyczna decyzja (i) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Spółką; lub

(ii) jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej osoby.

14 MINIMALIZACJA

Spółka dba o minimalizację przetwarzania danych pod kątem: (i) adekwatności danych do celów (ilości danych i zakresu przetwarzania), (ii) dostępu do danych, (iii) czasu przechowywania danych.

14.1 Minimalizacja zakresu

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

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

Spółka przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

14.2 Minimalizacja dostępu

Spółka 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).

Spółka stosuje kontrolę dostępu fizycznego.

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

Spółka dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

14.3 Minimalizacja czasu

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

15 BEZPIECZEŃSTWO

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

15.1 Analizy ryzyka i adekwatności środków bezpieczeństwa

Spółka przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

(1) Spółka zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

(2) Spółka kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

(3) Spółka 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) Spółka ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Spółka ustala przydatność i stosuje takie środki i podejście jak:

   (i) pseudonimizacja,

   (ii) szyfrowanie danych osobowych,

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

   (iv) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

15.2 Oceny skutków dla ochrony danych

Spółka dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

Spółka stosuje metodykę oceny skutków przyjętą w Spółce.

15.3 Środki bezpieczeństwa

Spółka 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 Spółce i są bliżej opisane w procedurach przyjętych przez Spółkę dla tych obszarów.

15.4Zgłaszanie naruszeń

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

15.5 Polityka czystego biurka

Celem redukcji zagrożenia dla przetwarzania danych w obszarze biurka, Spółka stosuje Politykę czystego biurka.

Polityka czystego biurka stanowi załącznik nr 16 do Polityki.

16 PRZETWARZAJĄCY

Spółka posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Spółki 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 Spółce.

Spółka przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące

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

17 EKSPORT DANYCH

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

Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Spółka okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

18 PROJEKTOWANIE PRYWATNOŚCI

Spółka 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 Spółkę 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.