POLITYKA OCHRONY DANYCH OSOBOWYCH

1. **1.** Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**” (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Eropa sp zoo ul. Twarda 18 00-105 Warszawa (dalej „Operator”).

   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).

1. **2.** Polityka zawiera:

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

1. **3.** Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest osoba upoważniona do składania oświadczeń woli w imieniu Operatora

   za nadzór i monitorowanie przestrzegania Polityki odpowiadają:

   i. (i) Inspektor Ochrony Danych, jeżeli został powołany u Operatora;
   ii. (ii)komórka audytu wewnętrznego, jeżeli funkcjonuje u Operatora;

   za stosowanie niniejszej Polityki odpowiedzialni są:

   i. (iii) Operator;
   ii. (iv) komórka organizacyjna odpowiedzialna za obszar bezpieczeństwa informacji;
   iii. (v) komórki organizacyjne przetwarzające dane osobowe w dużym rozmiarze;
   iv. (vi) pozostałe komórki organizacyjne;
   v. (vii) wszyscy członkowie personelu Operatora.

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

1. 4. 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 Operator powierzył przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość, zarządca systemu).

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.

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.
Operator oznacza Eropa sp zoo ul. Twarda 18 00-105 Warszawa

1. 5. Ochrona danych osobowych u Operatora – zasady ogólne

1. 5.1. Filary ochrony danych osobowych u Operatora:

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

1. 5.2. Zasady ochrony danych

Operator przetwarza dane osobowe z poszanowaniem następujących zasad:

a. (1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
b. (2) rzetelnie i uczciwie (rzetelność);
c. (3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
d. (4) w konkretnych celach i nie „na zapas” (minimalizacja);
e. (5) nie więcej niż potrzeba (adekwatność);
f. (6) z dbałością o prawidłowość danych (prawidłowość);
g. (7) nie dłużej niż potrzeba (czasowość);
h. (8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

1. 5.3. System ochrony danych

System ochrony danych osobowych u Operatora składa się z następujących elementów:

a. **1) Inwentaryzacja danych.** Operator dokonuje identyfikacji zasobów danych osobowych u Operatora, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:

a. a) przypadków przetwarzania danych specjalnych i danych „kryminalnych” (**dane wrażliwe**);
b. b) przypadków przetwarzania danych osób, których Operator nie identyfikuje (**dane niezidentyfikowane**);
c. c) przypadków przetwarzania danych dzieci;
d. d) profilowania;
e. e) współadministrowania danymi.

a. **2) Rejestr.** Operator opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych u Operatora (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych u Operatora.

b. **3) Podstawy prawne.** Operatora zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
   a. a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
   b. b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Operator przetwarza dane na podstawie prawnie uzasadnionego interesu Operatora.

a. **4) Obsługa praw jednostki.** Operator spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a. **a) Obowiązki informacyjne.** Operator przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
   b. **b) Możliwość wykonania żądań.** Operator weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
   c. **c) Obsługa żądań.** Operator zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.
   d. **d) Zawiadamianie o naruszeniach.** Operator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

a. **5) Minimalizacja.** Operator posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:
   a. a) zasady zarządzania **adekwatnością** danych;
   b. b) zasady reglamentacji i zarządzania **dostępem** do danych;
   c. c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;

a. **6) Bezpieczeństwo.** Operator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
   a. a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich

kategorii;

b. b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
c. c) dostosowuje środki ochrony danych do ustalonego ryzyka;
d. d) posiada system zarządzania bezpieczeństwem informacji;
e. e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami.

a. **7) Przetwarzający.** Operator posiada zasady doboru przetwarzających dane na rzecz Operatora, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.
b. **8) Eksport danych.** Operator posiada zasady weryfikacji, czy Operator 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.
c. ***9) Privacy by design*.** Operator zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Spółce uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.
d. 10) Przetwarzanie transgraniczne. Operator posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

a. 6. Inwentaryzacja

1. 6.1. Dane wrażliwe

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

1. 6.2. Dane niezidentyfikowane

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

1. 6.3. Profilowanie

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

1. 6.4. Współadministrowanie

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

a. 7. Rejestr Czynności Przetwarzania Danych

1. **7.1.** 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. **7.2.** Operator prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

1. **7.3.** Rejestr jest jednym z podstawowych narzędzi umożliwiających Operatorowi rozliczanie większości obowiązków ochrony danych.

1. **7.4.** W Rejestrze, dla każdej czynności przetwarzania danych, którą Operator uznał za odrębną dla potrzeb Rejestru, Operator 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 Operatora, 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.

1. **7.5.** Wzór Rejestru stanowi **Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”.** Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Operator rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

a. 8. Podstawy przetwarzania

1. **8.1.** Operator dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

1. **8.2.** Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Operatora) Operator 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.

1. **8.3.** Operator 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.).

1. **8.4.** Kierownik komórki organizacyjnej Operatora ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Operatora, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes Operatora.

1. 9. Sposób obsługi praw jednostki i obowiązków informacyjnych

1. **9.1.** Operator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

1. **9.2.** Operator ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Operatora informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich u Operatora, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z Operatorem w tym celu, ewentualnym cenniku żądań „dodatkowych" itp.

1. **9.3.** Operator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

1. **9.4.** Operator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

1. **9.5.** W celu realizacji praw jednostki Operator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Operatora, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,

1. **9.6.** Operator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

1. 10. Obowiązki informacyjne

1. **10.1.** Operator określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

1. **10.2.** Operator informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

1. **10.3.** Operator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

1. **10.4.** Operator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.

1. **10.5.** Operator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).

1. **10.6.** Operator informuje osobę o planowanej zmianie celu przetwarzania danych.

1. **10.7.** Operator informuje osobę przed uchyleniem ograniczenia przetwarzania.

1. **10.8.** Operator informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

1. **10.9.** Operator informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

1. **10.10.** Operator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

1. 11. Żądania osób

1. **11.1. Prawa osób trzecich**. Realizując prawa osób, których dane dotyczą, Operator 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.), Operator może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

1. **11.2. Nieprzetwarzanie**. Operator informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

1. **11.3. Odmowa**. Operator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

1. **11.4. Dostęp do danych**. Na żądanie osoby dotyczące dostępu do jej danych, Operator 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 Operator nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

1. **11.5. Kopie danych**. Na żądanie Operator wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Operator 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.

1. **11.6. Sprostowanie danych**. Operator dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Operator ma prawo odmówić sprostowania danych, chyba

że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Operator informuje osobę o odbiorcach danych, na żądanie tej osoby.

1. **11.7. Uzupełnienie danych**. Operator uzupełnia i aktualizuje dane na żądanie osoby. Operator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Operator nie musi przetwarzać danych, które są Operatorowi zbędne). Operator może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Operatora procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

1. **11.8. Usunięcie danych.** Na żądanie osoby, Operator usuwa dane, gdy:

a. (1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
b. (2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
c. (3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
d. (4) dane były przetwarzane niezgodnie z prawem,
e. (5) konieczność usunięcia wynika z obowiązku prawnego,
f. (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).

Operator 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 Operatora, Operator 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 Operator informuje osobę o odbiorcach danych, na żądanie tej osoby.

1. **11.9. Ograniczenie przetwarzania.** Operator dokonuje ograniczenia przetwarzania

danych na żądanie osoby, gdy:

a. a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
b. b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
c. c) Operator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
d. d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Operatora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Operator 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. Operator informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Operator informuje osobę o odbiorcach danych, na żądanie tej osoby.

1. **11.10. Przenoszenie danych.** Na żądanie osoby Operator 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 Operatorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Operatora.

1. **11.11. Sprzeciw w szczególnej sytuacji.** Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Operatora w oparciu o uzasadniony interes Operatora lub o powierzone Operatorowi zadanie w interesie publicznym, Operator **uwzględni** sprzeciw, o ile nie zachodzą po stronie Operatora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

1. **11.12. przeciw przy badaniach naukowych, historycznych lub celach statystycznych.** Jeżeli Operator prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może **wnieść** umotywowany jej

szczególną sytuacją sprzeciw względem takiego przetwarzania. Operator uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

1. **11.13. Sprzeciw względem marketingu bezpośredniego.** Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Operatora na potrzeby marketingu bezpośredniego (w tym **ewentualnie** profilowania), Operator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

1. **11.14. Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.** Jeżeli Operator 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**, Operator zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Operatora, chyba że taka automatyczna decyzja (i) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Operatorem; lub (ii) jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej osoby.

1. 12. MINIMALIZACJA

Operator 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.

1. 12.1. Minimalizacja zakresu

Operator zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO. Operator dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok. Operator przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

1. 12.2. Minimalizacja dostępu

Operator 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).

Operator stosuje kontrolę dostępu fizycznego. Operator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających. Operator dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Operatora.

1. 12.3. Minimalizacja czasu

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

1. 13. BEZPIECZEŃSTWO

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

1. 13.1. Analizy ryzyka i adekwatności środków bezpieczeństwa

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

a. (1) Operator zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
b. (2) Operator kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
c. (3) Operator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Operator 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. (4) Operator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Operator ustala przydatność i stosuje takie środki i podejście jak:
    a. (i) pseudonimizacja,
    b. (ii) szyfrowanie danych osobowych,
    c. (iii) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
    d. (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.

1. 13.2. Oceny skutków dla ochrony danych

Operator a dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie. Operator stosuje metodykę oceny skutków przyjętą u Operatora.

1. 13.3. Środki bezpieczeństwa

Operator 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 u Operatora i są bliżej opisane w procedurach przyjętych przez Operatora dla tych obszarów.

1. 13.4. Zgłaszanie naruszeń

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

1. 14. PRZETWARZAJĄCY

Operator posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Operatora 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 Operatorze. Operator przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące **Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych”**. Operator rozlicza przetwarzających z wykorzystania pod-przetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

1. 15. EKSPORT DANYCH

Operator 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), Operator okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

1. 16. PROJEKTOWANIE PRYWATNOŚCI

Operator 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 Operatora 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.

1. 17. POSTANOWIENIA KOŃCOWE

Niniejsza polityka ochrony danych osobowych wchodzi w życie z dniem 25 maja 2018 roku, na podstawie uchwały zgromadzenia wspólników

ORGAN NADZORCZY I SKARGI

1. W związku przetwarzaniem danych osobowych każdej osobie przysługuje prawo do wniesienia skargi na działanie lub zaniechanie Administratora do organu nadzorczego, którym jest:

Prezes Urzędu Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa