POLITYKA OCHRONY DANYCH OSOBOWYCH

1. Przedsiębiorstwo Wielobranżowe Robert Rosłon jest Administratorem danych w rozumieniu art. 4 pkt 7 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 z dnia 4 maja 2016 r.).
2. W celu zapewnienia przetwarzania danych osobowych przez Administratora danych zgodnie z obowiązującym prawem, a w szczególności zapewnienia najwyższej ochrony przetwarzanych danych osobowych, Administrator Danych Osobowych przyjmuje niniejszą Politykę.
3. Niniejsza Polityka jest zgodna z:
   a) rozporządzeniem 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 z dnia 4 maja 2016 r. — dalej: RODO);
   b) ustawą z dnia …… 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. ……..— dalej: u.o.d.o.);
   c) ustawą z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t. j. Dz. U. 2017 poz. 1219, z późn. zm. — dalej: u.ś.u.d.e.);
   d) ustawą z dnia 26 czerwca 1974 r. — Kodeks pracy (t. j. Dz. U. 2018 poz. 108, z późn. zm. — dalej: k.p.);
   e) ……..
4. Polityka stanowi część składową systemu ochrony danych osobowych obowiązującego u Administratora danych, określając w szczególności:
   a) zasady przetwarzania danych osobowych u Administratora danych;
   b) procedury stosowane u Administratora danych;
   c) wzorce dokumentów i formularzy stosowanych przez Administratora danych.
5. Niniejsza Polityka jest środkiem prawnym przewidzianym w art. 24 ust. 2 RODO.
6. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest ……, a w ramach …….:
   a) ……., któremu powierzono nadzór nad obszarem ochrony danych osobowych;
   b) osoba wyznaczona przez …….. do zapewnienia zgodności z ochrona danych osobowych;
7. Za nadzór i monitorowanie przestrzegania Polityki odpowiadają:
   a) Inspektor Ochrony Danych, jeżeli został powołany w …….;
   b) komórka audytu wewnętrznego, jeżeli funkcjonuje w ……..;

8. Za stosowanie niniejszej Polityki odpowiedzialni są:
   a) ……
   b) komórka organizacyjna odpowiedzialna za obszar bezpieczeństwa informacji;
   c) komórki organizacyjne przetwarzające dane osobowe w dużym rozmiarze;
   d) pozostałe komórki organizacyjne;
   e) wszyscy członkowie personelu ……...
9. …… powinien też zapewnić zgodność postępowania kontrahentów …….. z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez ……..

10. Na potrzeby niniejszej Polityki przyjmuje się następujące definicje użytych pojęć:

    1) **Dane** oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to 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;
    2) **Dane szczególnie chronione** 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;
    3) **Dane karne** oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa;
    4) **Dane dotyczące dzieci** oznaczają dane osób poniżej 16. roku życia;
    5) **Eksport danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej;
    6) **IOD lub Inspektor** oznacza Inspektora Ochrony Danych Osobowych;
    7) **Osoba** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu;
    8) **Polityka** oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu;
    9) **Podmiot przetwarzający** oznacza organizację lub osobę, której ……..powierzyła przetwarzanie danych osobowych;
    10) **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.
    11) **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).

11. **Fundamenty systemu ochrony danych osobowych:**

1) Administrator danych tworzy system ochrony danych osobowych w swojej organizacji, budując go na następujących fundamentach:

a) **bezpieczeństwo** — Administrator danych jest zobowiązany zapewnić bezpieczeństwo przetwarzania danych osobowych, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze;

b) **legalność** — Administrator danych, jak również wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, są zobowiązani przeprowadzać jakiekolwiek operacje związane z danymi osobowymi przy zachowaniu pełnej zgodności z obowiązującym prawem;

c) **podejście oparte na ryzyku** — Administrator danych jest zobowiązany zidentyfikować ryzyka towarzyszące przetwarzaniu danych osobowych oraz ustalić ich wpływ na operacje związane z danymi osobowymi, a w szczególności na prawa i wolności osób fizycznych;

d) **poszanowanie praw osób fizycznych** — Administrator danych, jak również wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, są zobowiązani ułatwić osobom fizycznym realizację ich praw związanych z ochroną danych osobowych;

e) **rozliczalność** — Administrator danych, jak również wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, są zobowiązani dokumentować sposób spełnienia obowiązków wynikających z przepisów z zakresu ochrony danych osobowych.

12. **Zasady ochrony danych osobowych:**

1) Administrator danych przetwarza dane osobowe w oparciu o następujące zasady:
2) **zasada czasowości** — dane osobowe są przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
3) **zasada integralności i poufności** — dane osobowe są przetwarzane w sposób zapewniający 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.
4) **zasada minimalizacji danych** — dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
5) **zasada ograniczenia celu** — dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
6) **zasada prawidłowości** — dane osobowe są prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
7) **zasada zgodności z prawem, rzetelności i przejrzystości** — dane osobowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

13. **System ochrony danych:**

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

1) **Bezpieczeństwo.** ……. zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
   a) dostosowuje środki ochrony danych do ustalonego ryzyka;
   b) posiada system zarządzania bezpieczeństwem informacji;
   c) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
   d) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
   e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami.
   2) **Eksport danych.** …….. posiada zasady weryfikacji, czy ……..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.
3) **Inwentaryzacja danych.** ……. dokonuje identyfikacji zasobów danych osobowych w …….., klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:
   a) przypadków przetwarzania danych specjalnych i danych „kryminalnych” (**dane szczególne**);
   b) przypadków przetwarzania danych osób, których …… nie identyfikuje (**dane niezidentyfikowane**);
   c) przypadków przetwarzania danych dzieci;
   d) profilowania;
   e) współadministrowania danymi.
4) **Minimalizacja.** ……. posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:
   a) zasady zarządzania **adekwatnością** danych;
   b) zasady reglamentacji i zarządzania **dostępem** do danych;
   c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;
5) **Obsługa praw jednostki.** …… spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) **Obowiązki informacyjne.** …….. przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
   b) **Możliwość wykonania żądań.** …….. weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

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

6) **Podstawy prawne.** …….. zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,

b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy …….. przetwarza dane na podstawie prawnie uzasadnionego interesu ……

7) **Przetwarzający.** …….. posiada zasady doboru przetwarzających dane na rzecz ……, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

8) ***Privacy by design*.** …… zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w …… 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.

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

10) **Rejestr.** …… opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w …… (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w …….

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

14. **Podmioty tworzące system ochrony danych osobowych:**

1) Współadministrator danych osobowych:

1. Administrator danych może wspólnie ustalać cele i sposoby przetwarzania danych osobowych ze współadministratorem danych osobowych — jeżeli taka konieczność wynika z przedsięwzięć realizowanych przez Administratora danych.
2. Administrator danych jest zobowiązany zawrzeć ze współadministratorem danych osobowych umowę o współadministrowanie danymi osobowymi.
3. W umowie o współadministrowanie danymi osobowymi należy określić w szczególności:

a) zakresy odpowiedzialności Administratora danych i współadministratora danych osobowych;

b) sposób realizowania obowiązków wynikających z przepisów z zakresu ochrony danych osobowych;

c) sposób spełnienia obowiązków informacyjnych z art. 13 RODO i art. 14 RODO;

d) punkt kontaktowy — jeżeli jest to wskazane;

e) relacje pomiędzy Administratorem danych i współadministratorem danych osobowych a podmiotami danych;

f) sposób przekazania podmiotom danych treści uzgodnień pomiędzy Administratorem danych a współadministratorem danych osobowych.

2) Inspektor Ochrony Danych:

1. W przypadkach wskazanych w art. 37 ust. 1 RODO lub w prawie polskim Administrator danych jest zobowiązany wyznaczyć Inspektora Ochrony Danych.
2. W przypadkach innych niż wskazane w ust. 1, Administrator danych może podjąć decyzję o dobrowolnym wyznaczeniu Inspektora Ochrony Danych.
3. Administrator danych zawiadamia Prezesa Urzędu Ochrony Danych Osobowych w terminie 14 dni o:

a) wyznaczeniu Inspektora Ochrony Danych, podając jego dane kontaktowe;
b) zmianie Inspektora Ochrony Danych, podając jego dane kontaktowe;
c) rezygnacji z wyznaczania Inspektora Ochrony Danych, jeżeli wcześniej był wyznaczony.

4. Administrator danych może zatrudnić Inspektora Ochrony Danych na podstawie umowy o pracę lub na podstawie cywilnoprawnej umowy o świadczenie usług.
5. Inspektor Ochrony Danych ma za zadanie:
   - informować Administratora danych oraz osoby przez niego zatrudnione, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy prawa;
   - doradzać w sprawie przestrzegania przepisów z zakresu ochrony danych osobowych;
   - podejmować działania zwiększające świadomość w zakresie ochrony danych osobowych;
   - przeprowadzać szkolenia osób zatrudnionych w zakresie ochrony danych osobowych;
   - prowadzić audyty;
   - monitorować przestrzeganie przepisów z zakresu ochrony danych osobowych, niniejszej Polityki oraz innych dokumentów Administratora danych;
   - monitorować podział obowiązków;
   - pełnić funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzić konsultacje we wszelkich innych sprawach;
   - udzielać na żądanie Administratora danych zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorować jej wykonanie zgodnie z art. 35 RODO;
   - współpracować z Prezesem Urzędu Ochrony Danych Osobowych;
6. Administrator danych jest zobowiązany zapewnić, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
7. Administrator danych jest zobowiązany wspierać Inspektora Ochrony Danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych

zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

8. Administrator danych:
   a) nie może wydawać Inspektorowi Ochrony Danych żadnych instrukcji;
   b) nie może karać Inspektora Ochrony Danych za wykonywanie przez niego obowiązków;
   c) nie może odwołać Inspektora Ochrony Danych za wykonywanie przez niego obowiązków.
9. Inspektor Ochrony Danych podlega bezpośrednio Administratorowi danych lub najwyższemu kierownictwu Administratorów danych.

3) Osoby upoważnione:

1. Przetwarzania danych osobowych w ramach struktury Administratora danych mogą dokonywać wyłącznie osoby upoważnione przez Administratora danych.
2. Osoba upoważniona do przetwarzania danych osobowych przed przystąpieniem do czynności ma obowiązek:
   a) zapoznać się z dokumentami z zakresu ochrony danych osobowych, w szczególności z niniejszą Polityką — w zakresie ustalonym przez Administratora danych;
   b) złożyć oświadczenie na piśmie o zapoznaniu się z dokumentami z zakresu ochrony danych osobowych oraz o odbyciu szkolenia z zakresu ochrony danych osobowych;
   c) złożyć oświadczenie na piśmie o przestrzeganiu zasad ochrony danych osobowych oraz ustalonych procedur;
   d) odbyć szkolenie z zakresu ochrony danych osobowych.
3. Administrator danych zapewnia osobom upoważnionym dostęp do dokumentów z zakresu ochrony danych, z wyjątkiem tych dokumentów, które nie powinny być dostępne dla wszystkich osób upoważnionych.
4. Administrator danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.

4) **Podmioty przetwarzające**

1. Administrator danych może powierzyć przetwarzanie danych osobowych podmiotowi przetwarzającemu w zależności od własnych potrzeb.
2. Administrator danych jest zobowiązany powierzać przetwarzanie danych osobowych tylko takim podmiotom przetwarzającym, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Zakazane jest korzystanie z usług podmiotów przetwarzających, które takich gwarancji nie dają.
3. W przypadku korzystania przez podmiot przetwarzający z usług innego podmiotu przetwarzającego, który nie daje analogicznych gwarancji, o jakich mowa w ust. 2, Administrator danych jest zobowiązany wnieść sprzeciw, a w innych przypadkach — może wnieść sprzeciw, jeżeli istnieją ku niemu podstawy.
4. Administrator danych jest zobowiązany kontrolować przestrzeganie przez podmiot przetwarzający przepisów RODO przez cały okres trwania umowy.

5. W przypadku naruszania przez podmiot przetwarzający przepisów RODO Administrator danych jest zobowiązany niezwłocznie zaprzestać współpracy z podmiotem przetwarzającym.
6. Administrator danych prowadzi ewidencję podmiotów przetwarzających, z którymi zawarł umowy o powierzenie przetwarzania danych osobowych.

5. **Odbiorcy danych osobowych:**

1. Administrator danych ujawnia dane osobowe odbiorcom danych osobowych wyłącznie po zweryfikowaniu podstawy prawnej takiego ujawnienia.
2. W przypadku braku podstawy prawnej, o której mowa w ust. 1, Administrator danych odmawia ujawnienia danych osobowych jakiemukolwiek odbiorcy danych osobowych.
3. Administrator danych prowadzi ewidencję odbiorców danych osobowych.

15. **Rejestr Czynności Przetwarzania Danych**

1) RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

2) …….. prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

3) …… jest jednym z podstawowych narzędzi umożliwiających …….. rozliczanie większości obowiązków ochrony danych.

4) W Rejestrze, dla każdej czynności przetwarzania danych, którą …… uznała za odrębną dla potrzeb Rejestru, …… odnotowuje co najmniej:

- nazwę czynności,
- cel przetwarzania,
- opis kategorii osób,
- opis kategorii danych,
- podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu ……, jeśli podstawą jest uzasadniony interes,
- sposób zbierania danych,
- opis kategorii odbiorców danych (w tym przetwarzających),
- informację o przekazaniu poza EU/EOG;
- ogólny opis technicznych i organizacyjnych środków ochrony danych.

5) Wzór Rejestru stanowi załącznik do Polityki**.**

16. **Zarządzanie ryzykiem:**

1. Administrator danych wdraża i utrzymuje procedurę zarządzania ryzykiem.
2. Administrator danych jest zobowiązany uwzględniać ryzyko w planowanych i prowadzonych procesach przetwarzania danych osobowych.
3. Procedura zarządzania ryzykiem stanowi Załącznik do Polityki.

17. **Ocena skutków dla ochrony danych osobowych**

1. W przypadkach wskazanych w art. 35 ust. 1 RODO, art. 35 ust. 3 RODO oraz w odniesieniu do operacji przetwarzania znajdujących się w wykazie publikowanym przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 35 ust. 4 RODO Administrator Danych Osobowych jest zobowiązany przeprowadzić ocenę skutków dla ochrony danych osobowych.
2. Ocena skutków dla ochrony danych osobowych nie jest wymagana w odniesieniu do operacji przetwarzania znajdujących się w wykazie publikowanym przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 35 ust. 5 RODO.
3. Procedura przeprowadzania oceny skutków dla ochrony danych osobowych stanowi Załącznik do Polityki.

18. **Uprzednie konsultacje z Prezesem Urzędu Ochrony Danych Osobowych:**

1. Jeżeli z oceny skutków dla ochrony danych osobowych wynika, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator danych nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator danych jest zobowiązany skonsultować się z Prezesem Urzędu Ochrony Danych Osobowych.
2. Procedura przeprowadzania uprzednich konsultacji z Prezesem Urzędu Ochrony Danych Osobowych stanowi Załącznik do Polityki.

19. **Privacy by design i privacy by default:**

1. Administrator danych jest zobowiązany uwzględniać ochronę danych osobowych w fazie projektowania nowych systemów, programów, aplikacji, usług, a także w fazie projektowania nowych procesów i sposobów przetwarzania danych osobowych (privacy by design).
2. Administrator danych jest zobowiązany zapewnić domyślną ochronę danych osobowych, tj. domyślnie mogą być przetwarzane tylko te dane osobowe, które są niezbędne do osiągnięcia konkretnego celu przetwarzania (privacy by default). Rezygnacja z prywatności lub jej ograniczenie mogą nastąpić tylko na wyraźne żądanie podmiotu danych.
3. Procedura privacy by design i privacy by default stanowi Załącznik do Polityki.

20. **Minimalizacja:**

1. Administrator danych jest zobowiązany przestrzegać zasady minimalizacji.
2. W celu zapewnienia realizacji zasady minimalizacji Administrator danych w szczególności:

a) weryfikuje ilość przetwarzanych danych osobowych — Administrator danych nie może przetwarzać większej ilości danych osobowych niż to wynika z założonego celu;

b) weryfikuje zakres przetwarzanych danych osobowych — Administrator danych nie może podejmować większej liczby czynności przetwarzania niż to wynika z założonego celu;

c) ogranicza dostęp do danych osobowych poprzez stosowanie środków prawnych (umowy z klauzulami poufności, system upoważnień), środków fizycznych (kontrola dostępu osób do budynków, pomieszczeń i systemów) oraz środków logicznych (kontrola uprawnień w systemach informatycznych i dostępu do systemów informatycznych);

d) ogranicza czas przetwarzania danych osobowych — Administrator danych nie może przetwarzać danych osobowych dłużej niż to wynika z założonego celu.

21. **Podstawy przetwarzania**

1) Administrator danych dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

2) Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Administratora danych) Administrator danych dookreśla podstawę w czytelny sposób, gdy jest to potrzebne.

3) Administrator danych 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.).

4) Kierownik komórki organizacyjnej Administratora danych 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.

22. **Sposób obsługi praw jednostki i obowiązków informacyjnych:**

- Administrator danych dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

  a) Administrator danych dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

  b) Administrator danych wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

  c) W celu realizacji praw jednostki Administrator danych zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Administratora danych, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,

  d) Administrator danych dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

- **Obowiązki informacyjne:**

a) Administrator danych określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych;

b) Administrator danych informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

c) Administrator danych informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

d) Administrator danych informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej;

e) Administrator danych określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe;

f) Administrator danych informuje osobę o planowanej zmianie celu przetwarzania danych;

g) Administrator danych informuje osobę przed uchyleniem ograniczenia przetwarzania;

h) Administrator danych informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe);

i) Administrator danych informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą;

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

- **Żądania osób:**

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

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

c) **Odmowa**. Administrator danych informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

d) **Dostęp do danych**. Na żądanie osoby dotyczące dostępu do jej danych, Administrator danych 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 Administrator danych nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

e) **Kopie danych**. Na żądanie Administrator danych wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Administrator danych 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.

f) **Sprostowanie danych**. Administrator danych 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 Administrator danych informuje osobę o odbiorcach danych, na żądanie tej osoby.

g) **Uzupełnienie danych**. Administrator danych uzupełnia i aktualizuje dane na żądanie osoby. Administrator danych ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator danych może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administrator danych procedur.

h) **Usunięcie danych.** Na żądanie osoby, Administrator danych usuwa dane, gdy:

   - osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
   - dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
   - zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
   - dane były przetwarzane niezgodnie z prawem,
   - konieczność usunięcia wynika z obowiązku prawnego,
   - 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).

i) **Ograniczenie przetwarzania.** Administrator danych dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

   - osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
   - przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
   - Administrator danych nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

– osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administrator danych zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

j) **Przenoszenie danych.** Na żądanie osoby Administrator danych 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 Administrator danych, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Administrator danych.

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

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

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

n) **Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.** Jeżeli Administrator danych 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 Administrator danych, chyba że taka automatyczna decyzja (i) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Administratorem danych; lub (ii) jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej osoby.

23. **Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych:**

1. Administrator danych jest zobowiązany kontrolować, czy przekazuje jakiekolwiek dane osobowe do państw trzecich lub organizacji międzynarodowych, w szczególności w przypadku korzystania z usług innych podmiotów.

2. Administrator danych jest zobowiązany zidentyfikować i zweryfikować podstawę prawną przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych.
3. Administrator danych jest zobowiązany monitorować zmiany legislacyjne.
4. Przypadki przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych są odnotowywane w rejestrze czynności przetwarzania danych osobowych.

24. **Szkolenia:**

a) Administrator danych jest zobowiązany podejmować działania na rzecz zwiększenia świadomości z zakresu ochrony danych osobowych wśród osób przez siebie zatrudnionych oraz podnoszenia ich wiedzy i kwalifikacji w tym zakresie.

b) Administrator danych zapewnia osobom przez siebie zatrudnionym szkolenia z zakresu ochrony danych osobowych, których częstotliwość oraz stopień zaawansowania zależy od pozycji zatrudnionego w systemie ochrony danych osobowych.

25. **Postanowienia końcowe**

1. W zakresie nieuregulowanym niniejszą Polityką znajdują zastosowanie powszechnie obowiązujące przepisy prawa, w szczególności dotyczące ochrony danych osobowych.
2. W przypadku zmiany stanu prawnego, która będzie skutkować niezgodnością niniejszej Polityki z prawem, postanowienie takie traci moc. Administrator danych podejmuje niezwłoczne działania na rzecz dostosowania niniejszej Polityki do nowego stanu prawnego.
3. Niniejsza Polityka może być zmieniona lub uchylona w takim samym trybie, w jakim została przyjęta.
4. Niniejsza Polityka obowiązuje od dnia …….

26. **Wykaz załączników:**