POLITYKA OCHRONY DANYCH OSOBOWYCH

wersja obowiązująca od dnia 12.07.2021

1. POSTANOWIENIA OGÓLNE

1.1. Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych” (dalej: ***Polityka***) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w **Femicare Magdalena Czyżo** z siedzibą w Grudziądzu (dalej: ***Administrator***).

1.2. Niniejsza Polityka stanowi politykę ochrony danych osobowych w rozumieniu 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) (dalej: ***RODO***).

1.3. Niniejsza Polityka zawiera:

1.3.1. opis zasad ochrony danych osobowych;

1.3.2. odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);

1.4. Do stosowania niniejszej Polityki zobowiązane są wszystkie osoby upoważnione przez Administratora do przetwarzania danych osobowych.

1.5. W przypadku powierzenia przetwarzania danych osobowych osobom trzecim (tj. podmiotom przetwarzającym) przez Administratora, Administrator dokłada wszelkich starań, aby zapewnić zgodność postępowania podmiotów przetwarzających z niniejszą Polityką.

2. WDROŻENIE POLITYKI I NADZÓR

2.1. Nadzór nad przestrzeganiem niniejszej Polityki sprawuje Magdalena Czyżo.

3. DEFINICJE

3.1. **Administrator** oznacza **Femicare Magdalena Czyżo.**

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

3.3. **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).

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

3.5. **Dane wrażliwe** oznaczają dane specjalne i dane karne.

3.6. **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.

3.7. **Dane karne** oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

3.8. **Dane dzieci** oznaczają dane osób fizycznych poniżej 16. roku życia.

3.9. **Osoba** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

3.10. **Podmiot przetwarzający** oznacza organizację lub osobę, której Administrator powierzył przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość).

3.11. **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.

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

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

4. OGÓLNE ZASADY OCHRONY DANYCH OSOBOWYCH

4.1. Ochrona danych osobowych u Administratora opiera się na następujących filarach:

4.1.1. **Legalność** − Administrator dba o ochronę prywatności osób, których dane dotyczą i przetwarza ich dane zgodnie z prawem.

4.1.2. **Bezpieczeństwo** − Administrator zapewnia odpowiedni poziom bezpieczeństwa danych osobowych podejmując stale działania w tym zakresie.

4.1.3. **Prawa Jednostki** − Administrator umożliwia osobom, których dane dotyczą, wykonywanie swoich praw i prawa te realizuje.

4.1.4. **Rozliczalność** – Administrator bieżąco dokumentuje wykonywanie obowiązków z zakresu ochrony danych osobowych w taki sposób, aby w każdej chwili móc wykazać zgodność przetwarzania danych osobowych z przepisami ochrony danych osobowych.

4.2. W czasie przetwarzania danych osobowych, Administrator stosuje następujące zasady ochrony danych:

4.2.1. **Legalizm** – dane osobowe są przetwarzane w oparciu o podstawę prawną i zgodnie z prawem.

4.2.2. **Rzetelność** – Administrator przetwarza dane osobowe rzetelnie i uczciwie.

4.2.3. **Transparentność** – Administrator przetwarza dane osobowe w sposób przejrzysty dla osób, których dane dotyczą.

4.2.4. **Minimalizacja** – przetwarzane przez Administratora dane osobowe są adekwatne, stosowne oraz ograniczone do celów, w których są przetwarzane.

4.2.5. **Prawidłowość** – Administrator dba o to, aby przetwarzane dane były prawidłowe.

4.2.6. **Ograniczenie przetwarzania** – Administrator przetwarza dane wyłącznie przez czas konieczny do osiągnięcia celów, w których dane są przetwarzane.

4.2.7. **Integralność i poufność** – Administrator przetwarza dane osobowe w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych.

4.3. Administrator utrzymuje system ochrony danych, który składa się z następujących elementów:

4.3.1. **Inwentaryzacji danych** – Administrator dokonuje identyfikacji zasobów danych osobowych, a w szczególności:

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

(b) przypadków przetwarzania danych dzieci;

(c) profilowania;

(d) przypadków przekazywania danych osobowych poza EOG;

(e) współadministrowania danymi.

4.3.2. **Rejestru czynności przetwarzania danych osobowych** – Administrator opracowuje, prowadzi i utrzymuje Rejestr czynności danych osobowych (dalej: ***Rejestr***).

4.3.3. **Identyfikacji podstaw prawnych przetwarzania** – Administrator zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

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

(b) Administrator inwentaryzuje i opracowuje uzasadnienia przypadków, gdy dane osobowe przetwarzane są na podstawie prawnie uzasadnionego interesu Administratora.

4.3.4. **Obsługi praw jednostki –** Administrator spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia realizację praw osób, których dane dotyczą, w odpowiedzi na otrzymane w tym zakresie żądania, w tym:

(a) Administrator wykonuje obowiązki informacyjne poprez przekazywanie wymaganych informacji przy zbieraniu danych i w innych sytuacjach, a także organizuje i zapewnia udokumentowanie realizacji tychże obowiązków,

(b) Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania osób, których dane dotyczą przez siebie i podmioty przetwarzające.

(c) Administrator zapewnia odpowiednie nakłady i procedury, aby żądania osób, których dane dotyczą były realizowane w terminach i w sposób wymagany RODO oraz dokumentuje wykonanie tych obowiązków.

4.3.5. **Zawiadamiania o naruszeniach.** Administrator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

4.3.6. **Minimalizacja** – Administrator wdraża 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.

4.3.7. **Bezpieczeństwo –** Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

(d) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

(e) dostosowuje środki ochrony danych do ustalonego ryzyka;

(f) posiada system zarządzania bezpieczeństwem informacji;

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

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

4.3.9. **Eksport danych –** Administrator posiada zasady weryfikacji, czy nie dochodzi do przekazywania 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.

4.3.10. ***Privacy by design*.** Administrator zarządza zmianami mającymi wpływ na prywatność. W tym celu Administrator posiada procedury uruchamiania nowych projektów i inwestycji, które 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.

4.3.11. **Przetwarzanie transgraniczne –** Administrator weryfikuje, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

SZCZEGÓŁOWE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

5. ZASADY INWENTARYZACJI DANYCH OSOBOWYCH

5.1. Dane wrażliwe

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

5.2. Profilowanie

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

5.3. Współadministrowanie

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

6. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

6.1. 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.

6.2. Administrator prowadzi Rejestr czynności przetwarzania danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

6.3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Administratorowi rozliczanie większości obowiązków ochrony danych.

6.4. W Rejestrze, dla każdej czynności przetwarzania danych, którą Administrator uznała za odrębną dla potrzeb Rejestru, Administrator 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 Administratora, 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.

6.5. Wzór Rejestru stanowi **Załącznik nr 1 do Polityki – Wzór rejestru czynności przetwarzania danych.**

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

6.5.2. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Administratora) Administrator dookreśla podstawę w czytelny sposób, gdy jest to potrzebne, np. dla zgody osoby, której dane dotyczą - wskazując na jej zakres; uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.

6.5.3. Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (e-mail, telefon, sms, itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

6.5.4. Osoby upoważnione do przetwarzania danych osobowych mają obowiązek znać podstawy prawne, na jakich dokonują konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą przetwarzania danych osobowych jest uzasadniony interes Administratora, osoba upoważniona do przetwarzania danych osobowych ma obowiązek znać konkretny realizowany przetwarzaniem interes Administratora.

7. SPOSÓB OBSŁUGI PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH

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

7.2. Administrator ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: udostępnianie informacji lub odwołań (linków) do informacji o prawach osób, których dane dotyczą; sposobie skorzystania z nich w stosunku do Administratora, w tym wymaganiach dotyczących identyfikacji; metodach kontaktu z Administratorem w tym celu, ewentualnym cenniku żądań „dodatkowych" itp.

7.3. Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób, których dane dotyczą.

7.4. Administrator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób, których dane dotyczą, dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

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

7.6. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

8. OBOWIĄZKI INFORMACYJNE

8.1. Administrator określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

8.2. Administrator informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

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

8.4. Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie od osób trzecich.

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

8.6. Administrator informuje osobę o planowanej zmianie celu przetwarzania danych.

8.7. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.

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

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

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

9. ŻĄDANIA OSÓB, KTÓRYCH DANE DOTYCZĄ

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

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

9.3. Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

9.4. Na żądanie osoby dotyczące dostępu do jej danych osobowych, Administrator 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 nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

9.5. Na żądanie Administrator wydaje osobie, której dane dotyczą kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Administrator 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.

9.6. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której dane dotyczą. Administrator ma prawo odmówić sprostowania danych, chyba że osoba, której dane dotyczą w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator informuje osobę, której dane dotyczą o odbiorcach danych, na żądanie tej osoby.

9.7. Administrator uzupełnia i aktualizuje dane na żądanie osoby. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administratora procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

9.8. Na żądanie osoby, Administrator usuwa dane osobowe, gdy:

9.8.1. dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,

9.8.2. zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

9.8.3. osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

9.8.4. dane były przetwarzane niezgodnie z prawem,

9.8.5. konieczność usunięcia wynika z obowiązku prawnego.

9.9. Administrator 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.

9.10. Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, Administrator podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.

9.11. W przypadku usunięcia danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

9.12. Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

9.12.1. osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

9.12.2. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

9.12.3. Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

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

9.13. W trakcie ograniczenia przetwarzania Administrator 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.

9.14. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.

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

9.16. Na żądanie osoby, której dane dotyczą Administrator 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 Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Administratora.

9.17. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o uzasadniony interes lub o powierzone zadanie w interesie

publicznym, Administrator **uwzględni** sprzeciw, o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

9.18. Jeżeli Administrator 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, której dane dotyczą, Administrator zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Administratora, chyba że taka automatyczna decyzja (i) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Administratorem ; lub (ii) jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej osoby.

10. MINIMALIZACJA

Administrator 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.

10.1. Minimalizacja zakresu

10.1.1. Administrator zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

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

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

10.2. Minimalizacja dostępu

10.2.1. Administrator 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).

10.2.2. Administrator stosuje kontrolę dostępu fizycznego.

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

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

10.2.5. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Administratora.

10.3. **Minimalizacja czasu**

10.3.1. Administrator wdraża mechanizmy kontroli cyklu życia danych osobowych, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

10.3.2. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów Administratora. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Administratora. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

11. BEZPIECZEŃSTWO

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

11.1. **Analizy ryzyka i adekwatności środków bezpieczeństwa**

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

11.1.1. Administrator zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

11.1.2. Administrator kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

11.1.3. Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich

kategorii. Administrator 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.

11.1.4. Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Administrator ustala przydatność i stosuje takie środki i podejście jak:

(a) pseudonimizacja,

(b) szyfrowanie danych osobowych,

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

(d) 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.

11.2. **Środki bezpieczeństwa**

11.2.1. Administrator stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.

11.2.2. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa u Administratora i są bliżej opisane w procedurach przyjętych przez Administratora dla tych obszarów.

11.3. **Zgłaszanie naruszeń**

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

12. PRZETWARZAJĄCY

12.1. Administrator posiada zasady doboru i weryfikacji podmiotów przetwarzających dane osobowe na zlecenie Administratora 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 Administratorze.

12.2. Administrator przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące **Załącznik nr 2 do Polityki – Wzór umowy powierzenia przetwarzania danych**.

12.3. Administrator rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z umowy powierzenia przetwarzania danych osobowych.

13. EKSPORT DANYCH

13.1. Administrator rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy.

14. PROJEKTOWANIE PRYWATNOŚCI

14.1. Administrator zarządza zmianą mającą wpływ na prywatność osób, których dane dotyczą w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.

14.2. W tym celu zasady prowadzenia projektów i inwestycji przez Administratora 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.

15. POSTANOWIENIA KOŃCOWE

15.1. Niniejsza Polityka wchodzi w życie z dniem 12.07.2021 r.

15.2. Postanowienia Polityki powtarzające powszechnie obowiązujące przepisy prawa pracy mają charakter informacyjny. W przypadku zmiany powszechnie obowiązujących przepisów prawa pracy, zastosowanie znajdują przepisy znowelizowane.

15.3. Integralną część Polityki stanowią Załączniki:

15.3.1. **Załącznik nr 1 do Umowy** – Wzór rejestru czynności przetwarzania danych

15.3.2. **Załącznik nr 2 do Umowy** – Wzór umowy powierzenia przetwarzania danych.

Administrator

Podpis: _____

Imię i nazwisko: Magdalena Czyżo