POLITYKA OCHRONY DANYCH OSOBOWYCH

1. Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**" (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych stosowanych w ramach działalności gospodarczej prowadzonej przez Bożenę Monikę Kowalską działającą pod firmą KOWALSKA BOŻENA MONIKA, "PANTERA", ul. Garibaldiego 4 lok. 21P, 04-078 Warszawa (dalej jako **Administrator**).
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).

2. Polityka zawiera:

a) opis zasad ochrony danych stosowanych przez Administratora;

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

3. Odpowiedzialna za wdrożenie i utrzymanie niniejszej Polityki jest Bożena Monika Kowalska, która odpowiada również za nadzór i monitorowanie przestrzegania Polityki.

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 Administrator powierzył przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość).
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.

5. Ochrona danych osobowych u Administratora – zasady ogólne

5.1. Filary ochrony danych osobowych u Administratora:

(1) **Legalność** − Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

(2) **Bezpieczeństwo** − Administrator zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

(3) **Prawa Jednostki** − Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

(4) **Rozliczalność** − Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

5.2. Zasady ochrony danych

Administrator przetwarza dane osobowe z poszanowaniem następujących zasad:

(1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);

(2) rzetelnie i uczciwie (rzetelność);

(3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);

(4) w konkretnych celach i nie „na zapas" (minimalizacja);

(5) nie więcej niż potrzeba (adekwatność);

(6) z dbałością o prawidłowość danych (prawidłowość);

(7) nie dłużej niż potrzeba (czasowość);

(8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

5.3. System ochrony danych

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

1) **Inwentaryzacja danych.** Administrator dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:
   a) przypadków przetwarzania danych specjalnych i danych „kryminalnych" (**dane wrażliwe**);
   b) przypadków przetwarzania danych osób, których Administrator nie identyfikuje (**dane niezidentyfikowane**);
   c) przypadków przetwarzania danych dzieci;
   d) profilowania;
   e) współadministrowania danymi.
2) **Rejestr.** Administrator opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych u Administratora.
3) **Podstawy prawne.** Administrator 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 Administrator przetwarza dane na podstawie prawnie uzasadnionego interesu Administratora.
4) **Obsługa praw jednostki.** Administrator spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) **Obowiązki informacyjne.** Administrator przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
   b) **Możliwość wykonania żądań.** Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

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

d) **Zawiadamianie o naruszeniach.** Administrator ustala konieczność zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5) **Minimalizacja.** Administrator przestrzega następujących zasad zarządzania minimalizacją (*privacy by default*):

a) zasada zarządzania **adekwatnością** danych;

b) zasada reglamentacji i zarządzania **dostępem** do danych;

c) zasada zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;

6) **Bezpieczeństwo.** Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

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

b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie – wzór takiej oceny stanowi **Załącznik nr 13 – „Ocena skutków dla ochrony danych"**;

c) dostosowuje środki ochrony danych do ustalonego ryzyka;

d) posiada system zarządzania bezpieczeństwem informacji – który stanowi **Załącznik nr 3 – „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"**

e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami – wskazane w punkcie 12.8 poniżej.

7) **Przetwarzający.** Administrator posiada zasady doboru przetwarzających dane na rzecz Administratora, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia – **Załącznik nr 1 „Lista sprawdzająca**".

8) **Eksport danych.** Administrator weryfikuje, czy przekazuje dane 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.

9) ***Privacy by design*.** Administrator zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji u Administratora 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.

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

6. Inwentaryzacja

6.1. 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.

6.2. Dane niezidentyfikowane

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

6.3. 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.

6.4. Współadministrowanie

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

7. Rejestr Czynności Przetwarzania Danych

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.

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

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

7.4. W Rejestrze, dla każdej czynności przetwarzania danych, którą Administrator uznał 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) opis kategorii odbiorców danych (w tym przetwarzających), (VII) informację o przekazaniu poza EU/EOG; (VIII) ogólny opis technicznych i organizacyjnych środków ochrony danych.

8. Podstawy przetwarzania

8.1. Administrator wskazuje w Rejestrze podstawy prawne (wynikające z RODO) przetwarzania danych dla poszczególnych czynności przetwarzania.

8.2. 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 (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

8.3. Administrator zna podstawy prawne, na jakich dokonuje konkretnych czynności przetwarzania danych osobowych.

9. Sposób obsługi praw jednostki i obowiązków informacyjnych

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

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

9.3. Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

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

9.5. 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.

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

10. Obowiązki informacyjne

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

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

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

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

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

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

10.7. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.

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

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

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

11. Żądania osób

11.1. **Prawa osób trzecich**. 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. Odpowiednie procedury stanowią **Załączniki 7-12 do niniejszej Polityki.**

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

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

11.4. **Dostęp do danych**. Na żądanie osoby dotyczące dostępu do jej danych, 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.

11.5. **Kopie danych**. Na żądanie, Administrator wydaje osobie 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.

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

11.7. **Uzupełnienie danych**. Administrator uzupełnia i aktualizuje dane na żądanie osoby. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Administrator nie musi przetwarzać danych, które są mu zbędne). 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.

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

(1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,

(2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

(3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

(4) dane były przetwarzane niezgodnie z prawem,

(5) konieczność usunięcia wynika z obowiązku prawnego,

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

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.
Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, podejmuje on 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 Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

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

a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

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

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

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

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

11.10. Przenoszenie danych. Na żądanie osoby 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.

11.11. Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o jego uzasadniony interes lub, 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.

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

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

11.14. Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu. 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**, 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.

12. 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.

12.1. Minimalizacja zakresu

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

12.2. Minimalizacja dostępu

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).
Administrator stosuje kontrolę dostępu fizycznego.
Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.
Administrator dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

12.3. Minimalizacja czasu

Administrator wdraża mechanizmy kontroli cyklu życia danych osobowych, 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 Administratora, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Administratora.

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

Administrator stosuje Politykę czystego biurka – stanowiącą **Załącznik nr 4 do niniejszej Polityki.**

12.4. Analizy ryzyka i adekwatności środków bezpieczeństwa

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

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

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

(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.

(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:

(i) pseudonimizacja,

(ii) szyfrowanie danych osobowych,

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

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

12.5. Oceny skutków dla ochrony danych

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

12.6. Środki bezpieczeństwa

Administrator 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 Administratora.

Zgłaszanie naruszeń
Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia – **Załączniki 5 i 6 do niniejszej Polityki.**

12.8 Procedura w przypadku stwierdzenia naruszenia danych osobowych

1. W przypadku stwierdzenia naruszenia bezpieczeństwa ochrony danych osobowych w pomieszczeniach wchodzących w skład obszaru przetwarzania danych osobowych, nośników danych, danych w formie papierowej, systemu informatycznego, urządzenia przetwarzającego dane osobowe, mebla, w którym przechowywane są dane, itp.; a także w przypadku podejrzenia takiego naruszenia, należy:

- niezwłocznie powiadomić telefonicznie lub osobiście Administratora (rozumiejąc pod tym pojęciem p. Bożenę Kowalską) o podejrzeniu lub fakcie naruszenia,
- powstrzymać się od wszelkich działań mogących utrudnić ustalenie okoliczności naruszenia,
- zabezpieczyć pomieszczenie do czasu przybycia Administratora,

2. Administrator, kiedy otrzyma zgłoszenie naruszenia bezpieczeństwa danych osobowych:

- ocenia zakres oraz rodzaj naruszenia ochrony danych,
- określa przyczyny oraz skutki naruszenia bezpieczeństwa danych,
- w przypadku danych przetwarzanych w systemie informatycznym: sprawdza, na którym stanowisku pracy nastąpiło naruszenie i czy użytkownik pracujący przy stanowisku, z którego nastąpiło naruszenie dostatecznie zabezpieczył stanowisko pracy przed wyłączeniem komputera,
- określa działania i środki, jakie należy podjąć w celu przywrócenia systemu zabezpieczeń do poprawnego funkcjonowania i przybliżonego czasu odtworzenia
- określa działania i środki, jakie należy podjąć w celu uniemożliwienia naruszenia ochrony danych osobowych w przyszłości,
- niezwłocznie informuje o zdarzeniu właściwy organ - Urząd Ochrony Danych Osobowych

3. W przypadku:

- zaniedbania zabezpieczenia danych osobowych,
- utrudniania i uniemożliwiania wykrycia naruszenia danych

Administrator jest uprawniony do dyscyplinowania osób odpowiedzialnych za zaistniały stan.

13. PRZETWARZAJĄCY

Administrator posiada zasady doboru i weryfikacji przetwarzających dane na rzecz 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 – stanowiące **Załącznik nr 1 do Polityki – „Wzór listy sprawdzającej”.**

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

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

14. EKSPORT DANYCH

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

15. PROJEKTOWANIE PRYWATNOŚCI

Administrator 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 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.

16. RETENCJA DANYCH

16.1. Administrator przechowuje dane osobowe przez okres nie dłuższy, niż jest to niezbędne do celów, dla realizacji których dane te są przetwarzane. Nie mogą być przetwarzane w nieskończoność „na zapas" i w każdym przypadku będzie podlegało ocenie, czy są one niezbędne w kontekście realizacji konkretnych celów.

16.2. Administrator usuwa dane osobowe, gdy:

- minął okres ich przydatności;
- okaże się, że cel który chcemy osiągnąć, nie wymaga już przetwarzania takich danych.

16.3. Okresy retencji

Istnieją przepisy szczególne regulujące obowiązek przetwarzania pewnych informacji przez z góry ustalony okres albo regulujące okresy przedawnienia roszczeń (przez który uzasadnione jest przechowywanie danych osobowych):

1) Dane pracownicze – art. 51 u ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz art. 125a ust 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych **(50 lat).**
2) Dane kontrahentów (osób prowadzących działalność gospodarczą) – art. 118 Kodeksu cywilnego **(3 lata).**
3) Dane kontrahentów (będących konsumentami) – art. 118 Kodeksu cywilnego **(10 lat).**
4) Dokumenty związane z ubezpieczeniami społecznymi – art. 24 ust. 4 ustawy z dnia 13 października 1998 r.o systemie ubezpieczeń społcznych **(5 lat).**
5) Dokumenty podatkowe – art. 70§1 ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa **(5 lat).**

W pozostałych przypadkach, dane osobowe będą przetwarzane do czasu osiągnięcia przez Administratora określonego w rejestrze czynności przetwarzania, celu.

16.4. Po upływie okresu przez jaki dane mogą być przechowywane, Administrator będzie dokonywał ich usunięcia:

a) Jeśli chodzi o dane w formie papierowej, to osoba wyznaczona przez administratora dokona protokolarnego fizycznego zniszczeia dokumentów umieszczając je w niszczarce.

b) Jeśli chodzi o dane w formie elektronicznej, to osoba wyznaczona przez Administratora, dokona usunięcia tych danych - w zależności od sytuacji – poprzez:

- protokolarną likwidacja sprzętu i nośników zawierających dane osobowe,
- bieżące usuwanie danych z systemów.

Administrator może również korzystać z usług wyspecjalizowanych firm, oferujących usługi ww. zakresie.

17. POSTANOWIENIA KOŃCOWE

Polityka wraz z Załącznikami wchodzi w życie z dniem 25 maja 2018 r.

.....