

Polityka przetwarzania danych osobowych

K&K Bielickie Sp. z o.o.

Spis treści

1.	METRYKA DOKUMENTU	3
2.	INFORMACJE OGÓLNE.....	3
3.	DEFINICJE	4
3.	OBOWIĄZKI ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH.....	9
4.	ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH	16
5.	DOSTĘP DO DANYCH OSOBOWYCH	16
6.	ZGODNOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH Z PRAWEM.....	17
7.	REALIZACJA PRAW PODMIOTÓW DANYCH	18
9.	UWZGLĘDNIENIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLA OCHRONA DANYCH	21
10.	WSPÓŁADMINISTRATORZY ORAZ PROCES WSPÓŁADMINISTROWANIA	21
11.	POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH.....	22
12.	PROWADZENIE REJESTRU CZYNNOŚCI PRZETWARZANIA (RCP)	23
14.	BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH	23
15.	ZARZĄDZANIE INCYDENTAMI I NARUSZENIAMI OCHRONY DANYCH OSOBOWYCH 24	
16.	PRZEPROWADZENIE OCENY SKUTKÓW DLA OCHRONY DANYCH (DPIA)	25
17.	DOKONANIE UPZEDNICH KONSULTACJI Z ORGANEM NADZORCZYM.....	25
18.	PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTWA TRZECIEGO (POZA EOG)...	26
19.	REALIZACJA ZASADY OGRANICZONEGO PRZETWARZANIA (CZASOWOŚCI).....	26
20.	PRZESTRZEGANIE ZASADY „CZYSTEGO BIURKA”	27
21.	ZASADY BEZPIECZEŃSTWA PRZETWARZANIA W PRZYPADKU PRACY ZDALNEJ	27
22.	REALIZACJA ZASADY ROZLICZALNOŚCI	29
23.	PRZEGLĄD POLITYKI, DOKONANIE SPRAWDZENIA I AUDYTY	30
24.	SZKOLENIA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH.....	31
25.	DOKUMENTACJA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH	31
26.	POSTANOWIENIA KOŃCOWE	32

1. Metryka dokumentu

Lp.	Data	Autor	Opis zmiany

2. Informacje ogólne

- 1) **[Informacje wstępne]** W celu spełnienia wymogów rozporządzenia UE 2016/679 z 27 kwietnia 2016 oraz Ustawy o ochronie danych osobowych z 10 maja 2018 roku i innych przepisów prawa w krajowym porządku prawnym, Spółka, występująca w roli Administratora, Współadministratora, Podmiotu przetwarzającego, wdrażają polityki w celu zapewnienia prawidłowego przetwarzania danych osobowych osób fizycznych w organizacji.
- 2) **[Cel Polityki]** Polityka w obszarze przetwarzania danych osobowych osób fizycznych (dalej Polityka) ma na celu zapewnienie przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa, bez względu na formę przetwarzania (elektroniczną bądź tradycyjną/papierową) danych osobowych. Celem Polityki w szczególności jest:
 - a) spełnienie wymogów wynikających z obowiązujących przepisów w zakresie ochrony danych osobowych (RODO, UODO, przepisy szczególne w krajowym porządku prawnym),
 - b) określenie odpowiedzialności za przetwarzania danych osobowych przez użytkowników danych osobowych oraz wskazane przez Administratora danych osoby powołane do pełnienia funkcji w procesie zarządzania systemem ochrony danych osobowych w organizacji,
 - c) określenie zasad postępowania w procesach związanych z przetwarzaniem danych osobowych w poszczególnych obszarach w organizacji,
 - d) określenie zasad przetwarzania danych osobowych w obszarach wpływających lub mogących wpływać na bezpieczeństwo przetwarzania danych osobowych,
 - e) minimalizacja ryzyka wystąpienia incydentu lub naruszenia ochrony danych osobowych,
 - f) minimalizacja ryzyka niezapewnienia realizacji przysługujących podmiotom danych praw i wolności,
 - g) zapewnienie realizacji praw osób, których dane dotyczą w związku z przetwarzaniem ich danych osobowych,
 - h) zapewnienie przez organizację ciągłości działania w obszarze przetwarzania danych osobowych,

- i) zapewnienie bezpieczeństwa we współpracy z klientami oraz kontrahentami we wszystkich obszarach związanych z przetwarzaniem danych osobowych,
 - j) budowania ciągłych relacji z klientami oraz kontrahentami w oparciu o zaufanie i profesjonalne podejście przestrzegania wymogów przepisów prawa w zakresie ochrony danych osobowych.
- 3) **[Zakres przedmiotowy]** Niniejsza Polityka jest dokumentem opisującym całokształt działań zmierzających do uzyskania i utrzymania poprawności przetwarzania danych osobowych z wymogami obowiązującego prawa, na każdym etapie ich przetwarzania. Polityka to w szczególności zbiór zasad dotyczących przetwarzania danych osobowych ustalonych w oparciu o wymagania wynikające z przepisów prawa.
 - 4) **[Zakres podmiotowy]** Zakres niniejszej Procedury obowiązuje wszystkich pracowników, współpracowników Administratora, niezależnie od formy prawnej współpracy, zatrudnienia lub świadczenia usług.
 - 5) **[Merytoryczny nadzór nad Polityką]** Merytoryczny nadzór nad Procedurą, obejmuje Koordynator ds. ODO ze wsparciem merytorycznym Zespołu ds. ODO w K&K Bielickie Sp. z o.o. (dalej KIA).
 - 6) **[Akceptacja i przyjęcie do stosowania]** Polityka wymaga akceptacji Administratora oraz zatwierdzenia do jej stosowania w K&K Bielickie Sp. z o.o. (dalej KIA) w sposób przyjęty.

3. Definicje

2.1. Przyjęte w Polityce definicje w zakresie przetwarzania danych osobowych:

Lp.	Definicja	Wyjaśnienie
1.	„Administrator”	Oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
2.	„Spółka”/ „Organizacja”	K&K Bielickie Sp. z o.o. (dalej KIA);
3.	„Bezpieczeństwo przetwarzania danych osobowych”	Zapewnienie odpowiedniego poziomu poufności, integralności i dostępności danych osobowych, zapewnienie ochrony danych osobowych przed nieautoryzowanym dostępem, modyfikacją, zatajeniem, kradzieżą lub zniszczeniem, oraz niedopuszczenie do wystąpienia incydentu lub naruszenia ochrony danych,

		niedopuszczenie do naruszenia praw i wolności osób, których dane dotyczą;
4.	„Dane osobowe”	Oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); 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;
5.	„Dane osobowe szczególnie chronione”	Za dane osobowe szczególnie chronione uważa się wszystkie dane osobowe, które zostały wymienione w art. 9 i 10 RODO;
6.	„Dane osobowe zwykłe”	Za dane osobowe zwykłe uważa się wszystkie dane osobowe, które nie zostały wymienione w art. 9 i 10 RODO;
7.	„Inspektor Ochrony Danych (IOD)”	Osoba wyznaczona przez Administratora lub/i podmiot przetwarzający do pełnienia funkcji IOD zgodnie z obowiązującymi przepisami prawa w obszarze ochrony danych osobowych,
8.	„Koordynator ds. ODO”	O ile ma to zastosowanie, wyznaczona przez Administratora osoba do nadzorowania, koordynowania, merytorycznego wspierania procesów związanych z ochroną danych osobowych w organizacji;
9.	„Naruszenie ochrony danych osobowych”	Oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
10.	„Obowiązki Administratora”	Administrator, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, wdraża odpowiednie środki techniczne, organizacyjne, fizyczne oraz prawne, aby przetwarzanie odbywało się zgodnie z obowiązującymi przepisami prawa;

11.	„Ocena skutków dla ochrony danych (DPIA)”	Przez DPIA rozumie się podjęcie przez Administratora czynności opisanych w art. 35, 36 RODO;
12.	„Organ nadzorczy”	Oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51. Organem nadzorczym dla Spółki jest Prezes Urzędu Ochrony Danych Osobowych;
13.	„Państwo trzecie”	Administrator, Współadministrator, Podmiot przetwarzający, któremu przekazywane są dane osobowe lub uczestniczy w procesie przetwarzania danych, mający swoją siedzibę poza EOG;
14.	„Polityki Ochrony Danych”	Przyjęte przez Administratora zasady przetwarzania danych osobowych w organizacji wraz z niezbędną dokumentacją (polityki, instrukcje postępowania, formularze, pozostała dokumentacja opracowana w związku z zarządzaniem systemem ochrony danych osobowych w organizacji);
15.	„Prawa osoby, których dane dotyczą”	Prawa osoby, której dane dotyczą wymienione w RODO, w szczególności: prawo do zachowania prywatności, do decydowania o swoich danych, prawo do ochrony danych osobowych, prawo do bycia poinformowanym, prawo do zgłoszenia sprzeciwu, prawo do żądania zaprzestania przetwarzania danych osobowych, do bycia przejrzystym i do przejrzystej komunikacji oraz trybu wykonywania praw, dostępu do danych, do sprostowania danych, do usuwania danych, do bycia zapomnianym, do ograniczenia przetwarzania, do przenoszenia danych, do kopiowania danych, do bycia reprezentowanym, do odszkodowania i odpowiedzialność, prawo do wniesienia skargi do organu nadzorczego;
16.	„Podmiot przetwarzający”	Oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
17.	„Przetwarzanie”	Oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie,

		rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
18.	„Rejestrowanie czynności przetwarzania” (RCP/RKCP)	Administrator, podmiot przetwarzający prowadzą określony w art. 30 RODO rejestry (Rejestr czynności przetwarzania (RCP), Rejestr kategorii czynności przetwarzania (RKCP). Administrator wyznacza osobę lub osoby w organizacji do prowadzenia i aktualizacji RCP oraz RKCP zgodnie z przyjętymi zasadami. RCP oraz RKCP przekazywany jest przez Administratora na każde wezwanie organu nadzorczego. W przypadku wyznaczenia IOD, za prowadzenie RCP oraz RKCP odpowiada IOD;
19.	„Rejestr incydentów i naruszeń”	Wykaz prowadzonych przez Administratora incydentów oraz naruszeń w zakresie przetwarzania danych osobowych;
20.	„Rozporządzenie (RODO)”	UE Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG);
21.	„Ryzyko przetwarzania danych osobowych”	Dokonanie przez Administratora analizy, oceny, ryzyka w zakresie bezpieczeństwa przetwarzania danych osobowych w tym prawdopodobieństwa naruszenia praw i wolności osób, których dane dotyczą. Metodologia szacowania ryzyka i określenia prawdopodobieństwa naruszenia praw i wolności osób, które dane dotyczą pozostaje do decyzji Administratora lub podmiotu przetwarzającego. Procedury dot. przeprowadzenia analizy, oceny i ryzyka związanego z przetwarzaniem danych osobowych stanowią odrębne dokumentu;
22.	„Sprawdzenie zgodności”	Oznacza dokonanie przez Administratora lub wyznaczoną osobę (wewnątrz lub na zewnątrz organizacji) do dokonania sprawdzenia zgodności przetwarzania danych z wymogami prawa (np. w formie audytu) w obszarze przetwarzania danych osobowych;

23.	„System zarządzania ochroną danych osobowych”	Ogół podjętych przez Spółkę działań mających na celu identyfikację, opracowanie, wdrożenie, bieżące zarządzanie, kontrolowanie zasad przetwarzania danych osobowych w organizacji. Za funkcjonowanie systemu zarządzania ochroną danych osobowych odpowiada Administrator oraz wyznaczone przez Administratora osoby – jeżeli ma to zastosowanie;
24.	„Upoważnienie do przetwarzania”	Administrator danych lub osoba wyznaczona przez Administratora, zapewnia, aby dostęp do danych osobowych posiadały wyłącznie osoby upoważnione do przetwarzania danych osobowych. Administrator danych nadaje pisemne (elektroniczne lub papierowe) upoważnienia do przetwarzania danych osobowych w sposób przyjęty w organizacji;
25.	„Uprzednie konsultacje”	Przez pojęcie uprzednich konsultacji rozumie się podjęcie czynności przez Administratora opisanych w art. 36 RODO;
26.	„Użytkownik danych”	Każda osoba, która została dopuszczona do przetwarzania danych osobowych w imieniu Administratora, Współadministratora lub podmiotu przetwarzającego;
27.	„Właściciel procesu”	Osoba, która w imieniu Administratora decyduje o celach i sposobach przetwarzania danych pełniąc, zgodnie ze strukturą organizacyjną, funkcję Dyrektora, Kierownika, Managera lub osoba odpowiedzialna za dany projekt, proces / procesy biznesowe w organizacji, w tym za przetwarzanie danych osobowych w związku z realizacją powierzonych przez Spółkę zadań w obszarach, za które odpowiada;
28.	„Współadministrator”	Jeżeli co najmniej dwóch Administratorów danych wspólnie ustala cele i sposoby przetwarzania, są oni Współadministratorami zgodnie z art. 26 RODO;
29.	„Zasady przetwarzania danych osobowych”	Zasady przetwarzania danych osobowych określone RODO, w szczególności: zasada celowości, ograniczonego celu, proporcjonalności, rzetelności i przejrzystości – zrozumiała komunikacja, minimalizacji danych osobowych, merytorycznej poprawności, prawidłowości, czasowości, ograniczanie przechowywania, integralności, poufności, rozliczalności, terytorialności, zasada

		uwzględnienia prywatności w fazie projektowania oraz domyśle przetwarzanie danych;
30.	„Zespół ds. ODO”	Zespół osób (w składzie Inspektor Ochrony Danych, Koordynator ds. ODO, Dział IT, Dział Prawny) w celu wdrożenia, monitorowania, aktualizacji, udzielania merytorycznego wsparcia Właścicielom procesu, Użytkownikom danych osobowych, lub dokonania sprawdzenia zgodności przetwarzania danych z wymogami prawa w zakresie ochrony danych osobowych;

3. Obowiązki związane z przetwarzaniem danych osobowych

3.1. Niniejszy dokument wprowadza zakres obowiązków związanych z przetwarzaniem danych osobowych, w szczególności dla:

- a) Administratora danych (ADO),
- b) Współadministratorów,
- c) Podmiotu przetwarzającego,
- d) Inspektora Ochrony Danych (IOD),
- e) Koordynatora ds. ODO,
- f) Właścicieli procesów,
- g) Użytkowników danych osobowych,
- h) Zespołu ds. ODO.

3.2. Obowiązki Administratora danych (ADO)

- 1) Do obowiązków Administratora danych, w obszarze zarządzania systemem ochrony danych osobowych, w szczególności należy:
 - a) zaangażowanie najwyższego kierownictwa we wszelkie kwestie związane z zapewnieniem prawidłowego przetwarzania danych osobowych w organizacji,
 - b) zapewnienie wsparcia merytorycznego w opracowaniu, wdrożeniu, bieżącym zarządzaniu i kontroli systemu zarządzania ochroną danych osobowych w organizacji,
 - c) zapewnienie przestrzegania w organizacji wewnętrznych postanowień w zakresie zasad przetwarzania danych osobowych,
 - d) systematyczne podnoszenie wiedzy Użytkowników danych osobowych,
 - e) zapewnienie, aby dostęp do danych osobowych posiadały osoby wyłącznie do tego upoważnione oraz zobowiązane do zachowania poufności oraz tajemnicy przetwarzania danych osobowych,
 - f) sprawowanie nadzoru nad prawidłowym wykonaniem przyjętych rozwiązań w obszarze przetwarzania danych osobowych,
 - g) bieżąca współpraca z Inspektorem Ochrony Danych oraz Zespołem ds. ODO.

3.3. Obowiązki Współadministratorów

- 1) W przypadku wystąpienia procesu współadministrowania, do obowiązków Współadministratorów w zakresie przetwarzania danych osobowych należy:
 - a) Identyfikacja obszarów, w których zachodzi proces współadministrowania danymi osobowymi,
 - b) dokonanie przez Współadministratorów wspólnych uzgodnień w obszarze przetwarzania danych osobowych, w szczególności do:
 - realizacji przez Współadministratorów praw podmiotu danych w zakresie przewidzianym przepisami prawa, w szczególności w odniesieniu do art. 13 i 14 RODO,
 - o ile ma to zastosowanie, wskazania punktu kontaktowego dla osób, których dane dotyczą w celu otrzymania wyczerpujących informacji na temat procesu współadministrowania,
 - c) zapewnienie przez Współadministratorów dostępności przez podmiot danych do zasadniczej treści dokonanych przez Współadministratorów uzgodnień,
 - d) zapewnienie, iż osoba, której dane dotyczą, może wykonywać przysługujące jej prawa w zakresie ochrony danych osobowych wobec każdego ze Współadministratorów
 - e) bieżąca współpraca z IOD.

3.4. Obowiązki Podmiotu przetwarzającego

- 1) W przypadku wystąpienia procesu powierzenia przetwarzania danych osobowych do Spółki (Spółka występująca w roli Podmiotu przetwarzającego), do obowiązków Podmiotu przetwarzającego w zakresie przetwarzania danych osobowych w szczególności należy:
 - a) identyfikacja powierzenia przetwarzania danych osobowych do Spółki,
 - b) przestrzeganie postanowień zawartych w umowie powierzenia przetwarzania danych osobowych lub innym instrumencie prawnym,
 - c) prowadzenie, zgodnie z zakresem merytorycznym wskazanym w art. 30 ust. 2 RODO, Rejestru kategorii czynności przetwarzania,
 - d) wykonywanie swoich zadań przewidzianych w art. 28 RODO oraz innych artykułach odnoszących się do obowiązków podmiotu przetwarzającego,
 - e) bieżąca współpraca z IOD.

3.5. Obowiązki Inspektora Ochrony Danych (IOD)

- 1) Administrator oraz podmiot przetwarzający zapewniają, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych

osobowych. Inspektor Ochrony Danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

- 2) Administrator oraz podmiot przetwarzający wspierają 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.
- 3) Administrator oraz podmiot przetwarzający zapewniają, by Inspektor Ochrony Danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań.
- 4) Inspektor Ochrony Danych nie jest odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań.
- 5) Osoby, których dane dotyczą, mogą kontaktować się z Inspektorem Ochrony Danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO
- 6) Inspektor Ochrony Danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.
- 7) Inspektor Ochrony Danych może wykonywać inne zadania i obowiązki niezwiązane z pełnieniem funkcji IOD pod warunkiem, iż takie zadania i obowiązki nie powodowały konfliktu interesów.
- 8) Inspektor Ochrony Danych ma następujące zadania:
 - a) informowanie Administratora, podmiotu przetwarzającego, Użytkowników danych osobowych, Właścicieli procesów, Koordynatora ds. ODO o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
 - b) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
 - c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO,
 - d) współpraca z organem nadzorczym,
 - e) pełnienie funkcji 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 prowadzenie konsultacji we wszelkich innych sprawach,
 - f) bieżąca współpraca z Zespołem ODO,
 - g) IOD na bieżąco prowadzi RCP oraz RKCP.
- 2) Inspektor Ochrony Danych wypełnia swoje zadania z należyтым uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

3.6. Obowiązki Koordynatora ds. ODO

Do obowiązków Koordynatora ds. ODO w zakresie przetwarzania danych osobowych w szczególności należy:

- 1) bieżące informowanie ADO oraz IOD o wszystkich sprawach związanych z przetwarzaniem danych osobowych w organizacji w celu wypełnienia przez ADO zadań i obowiązków, za które odpowiada,
- 2) o ile ma to zastosowanie bieżące informowanie Współadministratorów o wszystkich sprawach związanych z przetwarzaniem danych osobowych w organizacji w celu wypełnienia przez Współadministratorów zadań i obowiązków, za które odpowiadają,
- 3) Koordynator ds. ODO wspiera poszczególne funkcje w organizacji w celu prawidłowego wykonania przez nie spoczywających na nich obowiązków w obszarze przetwarzania danych osobowych, w szczególności:
 - a) Właścicieli procesów,
 - b) Dział IT,
 - c) Użytkowników danych osobowych,
 - d) Zespół ds. ODO,
 - e) IOD,
- 4) Koordynator ds. ODO uczestniczy w opracowaniu, wdrożeniu i bieżącym zarządzaniu wewnętrznymi politykami w zakresie ochrony danych osobowych w organizacji,
- 5) Koordynator ds. ODO nadzoruje zgodności przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa oraz wewnętrznymi regulacjami (politykami, procedurami),
- 6) Koordynator ds. ODO opracowuje, wdraża, aktualizuje, bierze czynny udział, prowadzi nadzór nad procesami, dokumentacją w zakresie ochrony danych osobowych w zależności od potrzeb organizacji, w szczególności:
 - a) w obszarze zarządzania procesem nadawania upoważnień do przetwarzania danych osobowych w imieniu ADO,
 - b) w obszarze realizacji przysługujących podmiotom danych praw w zakresie przetwarzania danych osobowych,
 - c) o ile ma to zastosowanie, w procesie współadministrowania,
 - d) o ile ma to zastosowanie, w procesie uwzględnienia prywatności w fazie projektowania oraz domyślnej ochrony danych,
 - e) o ile ma to zastosowanie, w procesie powierzenia przetwarzania danych osobowych do oraz przez Spółkę,
 - f) w procesie identyfikacji, analizy, oceny, postępowania z ryzykiem w zakresie przetwarzania danych osobowych,
 - g) o ile ma to zastosowanie, w procesach związanych z bezpieczeństwem przetwarzania danych osobowych w infrastrukturze IT (na poziomie software/hardware),
 - h) o ile ma to zastosowanie, w procesie przekazywania danych osobowych poza EOG,
 - i) w procesie zarządzania incydentami i naruszeniami w obszarze przetwarzania danych osobowych,

- j) w procesie dokonywania oceny skutków dla ochrony danych oraz uprzednich konsultacji z organem nadzorczym,
 - k) w procesie współpracy z organem nadzorczym,
 - l) oraz pozostałych procesach wynikających z przepisów prawa w zakresie ochrony danych osobowych wynikających z przepisów prawa oraz wewnętrznych polityk w zakresie ochrony danych osobowych,
- 7) Koordynator ds. ODO prowadzi i na bieżąco aktualizuje dokumentację związaną z przetwarzaniem danych osobowych, za którą odpowiada zgodnie z obowiązującymi przepisami prawa, w szczególności:
- a) prowadzi wykaz incydentów i naruszeń ochrony danych osobowych,
 - b) wspiera ADO w przygotowaniu i przeprowadzeniu szkoleń w zakresie ochrony danych osobowych,
 - c) wspiera ADO w przeprowadzeniu sprawdzeń, audytów w zakresie ochrony danych osobowych,
 - d) prowadzi nadzór nad pozostałą dokumentacją w zakresie ochrony danych osobowych, wynikającą z przepisów prawa oraz spoczywających na ADO zadań.

3.7. Obowiązki Właścicieli procesów

Do obowiązków Właścicieli procesów w obszarze przetwarzania danych osobowych należy:

- 1) bieżąca współpraca oraz informowanie IOD oraz Zespołu ds. ODO o wszystkich kwestiach związanych z przetwarzaniem ochrony danych osobowych w obszarach, za które odpowiadają, w szczególności o:
 - a) zidentyfikowaniu nowych procesów, czynności przetwarzania, celów lub zbiorów danych osobowych,
 - b) zmianie zakresu przetwarzania danych osobowych,
 - c) zmianie kategorii przetwarzanych danych osobowych,
 - d) zmianie wykonywanych operacjach przetwarzania na danych osobowych,
 - e) zmianie okresu, przez który przetwarzane są dane osobowe,
 - f) wystąpieniu ujawniania danych osobowych, w tym powierzenia przetwarzania danych osobowych,
 - g) wystąpienia transferu danych poza EOG,
- 2) bieżące monitorowanie prawidłowego przetwarzaniem danych osobowych w obszarze, za który odpowiada,
- 3) podejmowanie bieżących konsultacji z Zespołem ds. ODO w sprawach związanych z ujawnianiem danych osobowych, w szczególności poza EOG,
- 4) podejmowanie bieżącej konsultacji z Zespołem ds. ODO w sprawach związanych z powierzeniem przetwarzania danych osobowych, w szczególności poza EOG,
- 5) podejmowanie bieżącej konsultacji z Zespołem ds. ODO w sprawach związanych z procesem współadministrowania,

- 6) bieżące informowanie i konsultacje z Zespołem ds. ODO wszelkich kwestii związanych z wdrażaniem nowych rozwiązań w zakresie IT na poziomie software i hardware, w których przetwarzane są lub będą dane osobowe,
- 7) Właściciel procesu zobowiązany jest natychmiastowego zgłaszania do Zespołu ds. ODO wszelkich otrzymanych zapytań dot. realizacji praw podmiotu danych,
- 8) Właściciel procesu zobowiązany jest natychmiastowego zgłaszania do Zespołu ds. ODO mogących powstać lub zaistniałych zagrożeniach, które mogą przyczynić się do wystąpieniem incydentu lub naruszenia bezpieczeństwa przetwarzania danych osobowych,
- 9) Właściciel procesu zobowiązany jest do natychmiastowego zgłaszania do Zespołu ds. ODO incydentów lub naruszeń w zakresie ochrony danych osobowych oraz zobowiązany jest dostarczenia wszelkich niezbędnych informacji, dokumentacji, dowodów bądź wyjaśnień dot. incydentu lub wystąpienia naruszenia w obszarze przetwarzania danych osobowych,
- 10) Właściciel procesu uczestniczy w procesie identyfikacji, analizy, oceny i przygotowania planu postępowania z ryzykiem ochrony danych osobowych w obszarze, za który odpowiada,
- 11) Właściciel procesu wspiera, uczestniczy i realizuje procesy związane z ustaleniem oraz realizacją zasady czasowości (retencja danych osobowych) w procesach, za które odpowiada,
- 12) dokłada należytej staranności, aby Użytkownicy danych osobowych podlegający bezpośrednio pod Właściciela procesu, przestrzegali wewnętrznych postanowień w zakresie przetwarzania danych osobowych w organizacji i w zależności od potrzeb, informuje Zespół ds. ODO o konieczności przeprowadzenia szkolenia w zakresie ODO,
- 13) odpowiada za przestrzeganie bezpieczeństwa przetwarzania danych osobowych przez użytkowników danych osobowych, podlegającym bezpośrednio pod Właściciela procesu,
- 14) uczestniczy w pozostałych procesach w zakresie ochrony danych osobowych, wynikających z przepisów prawa lub podjętych wewnętrznych postanowień w organizacji,
- 15) współpracuje z pozostałymi Właścicielami procesu w zakresie wprowadzania zasad przetwarzania danych osobowych oraz reagowania na wszelkie zdarzenia mogące mieć wpływ na obniżenia poziomu tego bezpieczeństwa,
- 16) współpraca z pozostałymi Właścicielami procesu w zakresie wymiany informacji na tematy związane z przetwarzaniem i ochroną danych osobowych w organizacji.

3.8. Obowiązki Użytkowników danych osobowych

Do obowiązków Użytkowników danych osobowych należy przestrzeganie zasad ochrony danych osobowych określonych w Polityce oraz innych przyjętych do stosowania dokumentach ochrony danych osobowych. Do obowiązków Użytkowników danych osobowych w szczególności należy:

- 1) uczestnictwo w szkoleniach z zakresu zasad przetwarzania danych osobowych w organizacji,
- 2) przestrzeganie wewnętrznych postanowień w zakresie bezpieczeństwa przetwarzania danych osobowych określonych w przyjętych do stosowania dokumentach,
- 3) niezwłoczne informowanie Właściciela procesu o wszelkich wpływających zapytaniach w sprawie realizacji praw osób których dane dotyczą (podmiotów danych),
- 4) informowanie Właściciela procesu o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu bezpieczeństwa przetwarzania ochrony danych osobowych,
- 5) informowania Właściciela procesu o zaistniałych bądź mogących powstać zagrożeniach związanych z incydentami lub naruszeniami bezpieczeństwa przetwarzania danych,
- 6) niezwłoczne informowania Właściciela procesu o wszelkich incydentach i naruszeniach w zakresie ochrony danych osobowych oraz dostarczenia wszelkich niezbędnych informacji, dokumentacji, dowodów bądź wyjaśnień w procesie wystąpienia naruszenia w obszarze przetwarzania danych osobowych,
- 7) zapewnienia poufności oraz tajemnicy w zakresie przetwarzanych danych osobowych oraz form ich zabezpieczenia,
- 8) w odniesieniu do sprzętu komputerowego oraz wszelkich urządzeń teleinformatycznych, a także w związku z korzystaniem z zasobów systemów informatycznych służących do przetwarzania danych, Użytkownik danych osobowych w szczególności zobowiązany jest do dbania o bezpieczną eksploatację systemu informatycznego oraz otrzymanych narzędzi IT wraz z urządzeniami peryferyjnymi w tym zewnętrznych nośników danych osobowych, do którego otrzymał uprawnienia. W przypadku wykrycia zagrożenia, Użytkownik danych osobowych ma obowiązek natychmiastowego poinformowania o tym fakcie Właściciela procesu,
- 9) dbanie o to, aby wszelkie dokumenty zawierające dane osobowe, niezależnie od formy przetwarzania, chronione przed nieuprawnionym dostępem, modyfikacją, utratą, anonimizacją, nieodwracalną pseudonimizacją, zniszczeniem lub inną operacją mogącą naruszyć bezpieczeństwo przetwarzania danych osobowych oraz wpływać na realizację praw osób, których dane dotyczą lub prowadzić do negatywnych skutków podmiotu danych,
- 10) przestrzeganie zasady „czystego biurka”,
- 11) przestrzegania zasad bezpieczeństwa w przypadku pracy zdalnej,
- 12) współpraca z pozostałymi Użytkownikami danych osobowych w zakresie wprowadzania zasad bezpiecznego przetwarzania danych osobowych oraz reagowania na wszelkie zdarzenia mogące mieć wpływ na obniżenia poziomu tego bezpieczeństwa,
- 13) współpraca z pozostałymi Użytkownikami danych osobowych w zakresie wymiany informacji na tematy związane z bezpieczeństwem przetwarzania i ochroną danych osobowych,
- 14) Właściciel procesu, może wydawać Użytkownikom danych, dalsze wytyczne związane z bezpieczeństwem przetwarzania danych osobowych w obszarach, za które odpowiada,

15) Bieżąca współpraca z Zespołem ds. ODO.

3.9. Obowiązki Zespołu ds. ODO

W przypadku powołania przez Administratora Zespołu ds. ODO, do obowiązków Zespołu ds. ODO należy udzielanie Administratorowi oraz Koordynatorowi ds. ODO, Współadministratorom, Podmiotom przetwarzającym, Właścicielom procesu, Użytkownikom danych osobowych merytorycznego wsparcia we wszelkich kwestiach związanych z zarządzaniem systemem ochrony danych osobowych w organizacji.

4. Zasady dotyczące przetwarzania danych osobowych

4.1. Administrator danych zapewnia, aby dane osobowe w organizacji przetwarzane były zgodnie z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych oraz z uwzględnienia poniższych zasad:

- a) dane osobowe przetwarzane są zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą – realizacja Zasady zgodność z prawem, rzetelność i przejrzystość,
- b) dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami - Zgodnie z zasadą celowości oraz Zasadą ograniczonego celu,
- c) dane osobowe przetwarzane są adekwatnie, stosownie oraz w zakresie ograniczonym i niezbędnym do realizacji celu, w którym zostały zebrane – realizacja Zasady minimalizacji danych osobowych,
- d) dane osobowe są prawidłowe i w razie potrzeby na bieżąco uaktualniane – realizacja Zasady aktualizacji danych osobowych,
- e) dane osobowe 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 - realizacja Zasady czasowości, retencji danych lub inaczej Zasady ograniczenia przechowywania,
- f) dane osobowe przetwarzane są 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 – realizacja Zasady integralności i poufności przetwarzania danych osobowych,
- g) Administrator danych odpowiedzialny jest za przestrzeganie w/w zasad przetwarzania danych osobowych i musi być w stanie wykazać ich przestrzeganie – realizacja Zasady rozliczalności przetwarzania danych osobowych z wymogami przepisów prawa.

5. Dostęp do danych osobowych

- 5.1. Administrator danych zapewnia, aby dostęp do danych osobowych posiadały wyłącznie osoby upoważnione (w tym poprzez wydawane przez ADO polecenia),
- 5.2. Upoważnienie do przetwarzania danych osobowych podpisuje Administrator lub osoba posiadająca odrębne pełnomocnictwo od Administratora,
- 5.3. Upoważnienie do przetwarzania danych osobowych nadawane jest przed dopuszczeniem osoby do przetwarzania danych osobowych,
- 5.4. Koordynator ds. ODO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
- 5.5. Nadane upoważnienia do przetwarzania danych osobowych archiwizowane są w sposób przyjęty w organizacji.
- 5.6. Dostęp do danych osobowych przetwarzanych na poziomie teleinformatycznym, nadawany jest zgodnie z przyjętymi w organizacji zasadami, wskazanymi we właściwej dokumentacji.

6. Zgodność przetwarzania danych osobowych z prawem

- 6.1. Administrator danych zapewnia, aby dane osobowe przetwarzane były wyłącznie i zgodnie z obowiązującymi przepisami prawa i muszą być w stanie wskazać przesłanki prawne (przesłanki legalności) przetwarzania danych osobowych, w szczególności dla:
 - a) danych zwykłych – zgodnie z art. 6 RODO,
 - b) szczególnej kategorii danych osobowych (danych szczególnie chronionych) – zgodnie z art. 9 oraz 10 RODO.
- 6.2. O ile ma to zastosowanie, za wskazanie przesłanek prawnych (przesłanek legalności) przetwarzania danych osobowych w organizacji odpowiada Właściciel procesu adekwatnie do celów przetwarzania danych osobowych w procesach, za które odpowiada.
- 6.3. Przetwarzanie danych osobowych w oparciu o „zgode”
 - 1) Administrator danych zobowiązany jest do zwrócenia szczególnej na przesłankę prawną, jaką jest „zgoda” podmioty danych na przetwarzania danych osobowych,
 - 2) Administrator danych dokłada należytej staranności, aby udzielona przez osobę, której dane dotyczą zgodna na przetwarzanie danych osobowych odpowiadała zasadom wskazanym w obecnie obowiązujących przepisach prawa,
 - 3) Administrator danych, zobowiązany jest do udokumentowania oraz archiwizowania udzielonej przez podmiot danych zgody (w wersji elektronicznej lub papierowej),
 - 4) W przypadku przetwarzania danych osobowych w oparciu przesłankę legalności, jaką jest „zgoda”, Administrator danych zobowiązany jest do zastosowania i bezzwłocznego realizowania prawa osoby, której dane dotyczą w przypadku wycofania udzielonej zgody lub udokumentowania jej wyrażenie na życzenie osoby, której dane dotyczą,
 - 5) w przypadku przetwarzania danych osobowych w oparciu o „zgode”, ADO przeprowadza tzw. „Test zgody” według przyjętej w organizacji metodologii i przed

pierwszą czynnością wykonana na danych osobowych przetwarzanych w oparciu o „zgode”,

6.4. Przetwarzanie danych osobowych w oparciu o prawnie uzasadniony interes administratora

- 1) Administrator danych, zobowiązany jest do zwrócenia szczególnej uwagi na przesłankę prawną przetwarzania danych osobowych, jaką jest „prawnie uzasadniony interes realizowany administratora”,
- 2) Administrator dokłada należytej staranności, aby w/w przesłanka legalności przetwarzania danych osobowych była właściwie przeanalizowana według przyjętej w organizacji metodologii i przed pierwszą czynnością wykonaną na danych osobowych przetwarzanych w oparciu o „prawnie uzasadniony interes realizowany przez administratora”,
- 3) w przypadku przetwarzania danych osobowych w oparciu o „prawnie uzasadniony interes realizowany przez administratora”, ADO przeprowadza tzw. „Test równowagi” według przyjętej w organizacji metodologii i przed pierwszą czynnością wykonaną na danych osobowych przetwarzanych w oparciu o „prawnie uzasadniony interes realizowany przez administratora”.

7. Realizacja praw podmiotów danych

7.1. Administrator danych zobowiązany jest do zachowania należytej staranności w procesie realizacji praw osób, których dane dotyczą, określonych w RODO oraz przepisów o ochronie danych osobowych w krajowym porządku prawnym.

7.2. Administrator danych zapewnia, aby:

- a) osoba, której dane dotyczą została w sposób zrozumiały, z zachowaniem określonego w przepisach prawa terminem, przejrzysto poinformowana o trybie wykonania przysługującej jej praw w zakresie ochrony danych osobowych, na zasadach określonych w obowiązujących przepisach prawa,
- b) osoba, której dane dotyczą otrzymała wszystkie niezbędne informacje w chwili podawania swoich danych osobowych (spełnienie obowiązku informacyjnego w przypadku zbierania danych od osoby, której dane dotyczą), na zasadach określonych w obowiązujących przepisach prawa,
- c) osoba, której dane dotyczą otrzymała wszystkie niezbędne informacje w przypadku pozyskiwania danych osobowych w sposób inny, niż od osoby, której dane dotyczą (spełnienie obowiązku informacyjnego w przypadku zbierania danych niebezpośrednio od osoby, której dane dotyczą), na zasadach określonych w obowiązujących przepisach prawa,
- d) osoba, której dane dotyczą miała prawo dostępu do swoich danych osobowych oraz uzyskania wyczerpujących informacji na temat przetwarzanych przez Administratora danych, Współadministratorów danych osobowych (spełnienie obowiązku

informacyjnego na żądanie osoby, której dane dotyczą), na zasadach określonych w obowiązujących przepisach prawa,

- e) osoba, której dane dotyczą miała prawo sprostowania jej danych osobowych, na zasadach określonych w obowiązujących przepisach prawa. Administrator danych, Współadministrator informuje o sprostowaniu każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator danych, Współadministrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda,
- f) osoba, której dane dotyczą miała prawo do usunięcia jej danych osobowych (realizacja prawa do bycia zapomnianym), na zasadach określonych w obowiązujących przepisach prawa. Administrator danych, Współadministrator informuje o usunięciu danych każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator danych, Współadministrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda,
- g) osoba, której dane dotyczą miała prawo do zgłoszenia ograniczenia przetwarzania jej danych osobowych, na zasadach określonych w obowiązujących przepisach prawa. Administrator danych informuje o ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator danych, Współadministrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda,
- h) osoba, której dane dotyczą miała prawo do przenoszenia jej danych osobowych na zasadach określonych w obowiązujących przepisach prawa,
- i) osoba, której dane dotyczą miała prawo do zgłoszenia sprzeciwu wobec przetwarzania jej danych osobowych na zasadach określonych w obowiązujących przepisach prawa,

7.3. Osoba, której dane dotyczą miała prawo do uzyskania kopii jej danych osobowych na zasadach określonych w obowiązujących przepisach prawa.

7.4. W przypadku żądania przez osobę, której dane dotyczą, realizacji jej praw, przez Spółkę podejmowane są następujące działania:

- 1) w przypadku wystąpienia relacji pomiędzy podmiotem danych a ADO:
 - a) otrzymanie wniosku od osoby (ustny / pisemny) o realizację prawa,
 - b) weryfikacja tożsamości osoby oraz przekazanie klauzuli informacyjnej art. 13 RODO,
 - c) weryfikacja czy zachodzi przetwarzanie i możliwości realizacji prawa na wniosek osoby,
 - d) realizacja lub poinformowanie o częściowym lub całkowitym braku możliwości realizacji prawa osoby,
 - e) potwierdzenie realizacji prawa osoby i archiwizacja dokumentacji,
- 2) w przypadku wystąpienia relacji pomiędzy podmiotem danych a Spółką występująca w roli podmioty przetwarzającego:

- a) otrzymanie wniosku od osoby (ustny / pisemny) o realizację prawa,
 - b) weryfikacja czy zachodzi przetwarzanie i możliwości realizacji prawa na wniosek osoby,
 - c) powiadomienie i przekazanie żądania osoby, której dane dotyczą do ADO,
 - d) powiadomienie osoby, której dane dotyczą o przekazu jej żądania do ADO,
 - e) archiwizacja dokumentacji w celach dowodowych,
- 3) w przypadku wystąpienia relacji pomiędzy podmiotem danych a Spółką występująca w roli współadministratora:
- a) otrzymanie wniosku od osoby (ustny / pisemny) o realizację prawa,
 - b) weryfikacja tożsamości osoby oraz przekazanie klauzuli informacyjnej art. 13 RODO (3) Weryfikacja czy zachodzi przetwarzanie i możliwości realizacji prawa – Współadministrator,
 - c) powiadomienie i przekazanie żądania do właściwego Współadministratora – jeżeli ma to zastosowanie,
 - d) w przypadku, gdy realizacja prawa podmiotu danych spoczywa na Spółce, realizacja lub poinformowanie o częściowym lub całościowym braku możliwości realizacji prawa osoby i archiwizacja dokumentacji.

7.5. Jeżeli w wyniku wewnętrznych konsultacji, Administrator danych uzna, iż żądanie realizacji praw osoby, której dane dotyczą nie wynikają z przysługach jej praw lub ich realizacja wiązałaby się z niewykonaniem obowiązku prawnego na Administratorze danych, lub znacząco naruszałaby prawa i wolności osób postronnych lub znacząco naruszałby inne wewnętrznie obowiązujące zasady w organizacji, Administrator danych, zobowiązany jest do przedstawienia swoich wniosków oraz podjęcia decyzji w sprawie realizacji lub odmówienia realizacji prawa osoby, której dane dotyczą, przy czym w/w czynności muszą odbyć się w zgodności z obowiązującym prawem.

7.6. Realizacja praw podmiotów danych – kopiowanie danych osobowych

- 1) W przypadku konieczności realizacji praw osób, których dane dotyczą, wymagających przekazania kopii danych osobowych, Administrator danych, zapewniają, aby:
- a) realizacja prawa do otrzymania kopii swoich danych osobowych nie może naruszać praw i wolności pozostałych osób,
 - b) o ile ma to zastosowanie, forma realizacji prawa do otrzymania kopii swoich danych osobowych wymaga uprzedniego ustalenia formy ich przekazania oraz terminu ich przekazania z osobą, której dane dotyczą, z uwzględnieniem wymogów przepisów prawa,
 - c) przypadku realizacji prawa do uzyskania kopii danych osobowych, Administrator danych ustala zasady finansowe realizacji tego prawa, przy czym pierwsze wydanie kopii danych osobowych ustala się za wolne od opłat.

7.7. Realizacja praw podmiotów danych – prawo do bycia poinformowanym

1. Administrator danych zapewnia, iż:

- a) w zależności od zidentyfikowanego celu przetwarzania danych osobowych oraz od relacji pomiędzy stronami, w przypadku zbierania danych osobowych bezpośrednio

od osoby, której dane dotyczą, o wyczerpującym poinformowaniu podmiotu danych i przekazaniu wszelkich informacji określonych w art. 13 RODO,

b) w zależności od zidentyfikowanego celu przetwarzania danych osobowych oraz od relacji pomiędzy stronami, w przypadku zbierania danych osobowych niebezpośrednio od osoby, której dane dotyczą, o wyczerpującym poinformowaniu podmiotu danych i przekazaniu wszelkich informacji określonych w art. 14 RODO,

c) w zależności od zidentyfikowanego celu przetwarzania danych osobowych oraz od relacji pomiędzy stronami, w przypadku wystąpienia podmiotu danych o przekazanie wyczerpujących informacji zgodnie z art. 15 RODO, Administrator danych:

- przekazują w/w informacje w zakresie zgodnym z obowiązującymi przepisami prawa w obszarze ochrony danych osobowych,
- przekazują w/w informacje w terminie zgodnie z obowiązującymi przepisami prawa w obszarze ochrony danych osobowych.

2. Administrator danych muszą być w stanie wykazać, iż prawo do bycia poinformowanym jest przez nich realizowane i na bieżąco monitorowane.

8. Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie

8.1. W przypadku wystąpienia w organizacji zautomatyzowanego podejmowanie decyzji, w tym profilowania, Administrator danych, zobowiązany jest do zastosowania przepisów prawa określonych w art. 22 RODO oraz do udokumentowania zasad przetwarzania danych osobowych w związku z profilowaniem i zautomatyzowanym przetwarzaniem danych osobowych w sposób przyjęty u Administratora danych.

9. Uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych

9.1. O ile ma to zastosowanie, Administrator danych, przed pierwszą czynnością wykonaną na danych osobowych dla nowych usług, produktów, projektów, wdrożeń rozwiązań teleinformatycznych lub innych działań, zobligowany jest do przeprowadzenia i udokumentowania uwzględnienia prywatności w fazie projektowania.

9.2. Zakres merytoryczny realizacji Zasady uwzględnienia prywatność na etapie projektowania (wskazanie przestrzeganie wymogów przepisów prawa w zakresie ochrony danych osobowych na etapie planowania) oraz domyślna ochrona danych osobowych pozostaje do decyzji ADO, ze szczególnym uwzględnieniem postanowień art. 25 RODO.

10. Współadministratorzy oraz proces współadministrowania

10.1. W przypadku zidentyfikowania procesu współadministrowania, Administrator danych zobligowany jest do podjęcia czynności przewidzianych w art. 26 RODO oraz

zgodnie z obowiązkami Współadministratorów określonych w niniejszej Polityki w punkcie 3.3.

11. Powierzenie przetwarzania danych osobowych

11.1. W celu sprawowania kontroli nad procesem ujawniania danych osobowych oraz w celu zagwarantowania realizacji praw podmiotów danych, każda osoba uprawniona przez Spółkę, która procesuje ofertę, zlecenie lub umowę lub inny instrument prawny (z klientem lub kontrahentem), informuje o tym fakcie Koordynatora ds. ODO oraz Zespół ds. ODO w sposób przyjęty w organizacji.

11.2. Koordynator ds. ODO wraz z Zespołem ds. ODO podejmuje dalsze kroki, w zależności od identyfikacji ról w związku z planowanym zawarciem współpracy pomiędzy stronami dla poszczególnych schematów:

- 1) **w przypadku identyfikacji powierzenie przetwarzania danych osobowych przez Spółkę:**
 - a) przesłanie do podmiotu przetwarzającego ankiety weryfikującej podmiot przetwarzający,
 - b) przeprowadzenia analizy i ocen ryzyka związanego ze współpracą z podmiotem przetwarzającym,
 - c) przygotowanie i zawarcie umowy powierzenia przetwarzania danych osobowych lub zastosowanie innego instrumentu prawnego,
 - d) przeprowadzenie audytu podmiotu przetwarzającego – analiza i ocena otrzymanych informacji,
 - e) archiwizacja dokumentacji w celach dowodowych,
 - f) aktualizacja dokumentacji w zakresie ODO (np. wykaz procesorów),
- 2) **w przypadku identyfikacji powierzenia danych osobowych do Spółki (Spółka jako Procesor):**
 - a) wypełnienie ankiety weryfikującej procesora przesłanej przez ADO – jeżeli ma to zastosowanie,
 - b) zawarcie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego,
 - c) przygotowanie indywidualnego Rejestru kategorii czynności przetwarzania (RKCP – art. 30 RODO),
 - d) nadanie upoważnień do przetwarzania danych osobowych – jeżeli ma to zastosowanie,
 - e) archiwizacja dokumentacji w celach dowodowych,
- 3) **w przypadku identyfikacji dalszego powierzenie przetwarzania przez Spółkę (Spółka jako Procesor):**
 - a) w zależności od postanowień umowy powierzenia przetwarzania danych osobowych, zawartych pomiędzy Administratorem a Spółką występującą w roli

- podmiotu przetwarzającego, powiadomienie ADO o dalszym powierzeniu przetwarzania – jeżeli ma to zastosowanie,
- b) wypełnienie ankiety weryfikującej procesora przesłanej przez Spółkę – jeżeli ma to zastosowanie,
 - c) zawarcie umowy powierzenia lub innego instrumentu prawnego z dalszym podmiotem przetwarzającym,
 - d) przeprowadzenie audytu dalszego podmiotu przetwarzającego – analiza i ocena otrzymanych informacji,
 - e) archiwizacja dokumentacji w celach dowodowych.

12. Prowadzenie Rejestru czynności przetwarzania (RCP)

- 12.1. Zgodnie z art. 30 ust. 1 RODO, Administratorzy zobligowani są do prowadzenia Rejestru czynności przetwarzania (RCP) w zakresie merytorycznym przewidzianym w w/w przepisie prawa.
- 12.2. Za prowadzenie i aktualizację RCP odpowiada Koordynator ds. ODO ze wsparciem merytorycznym Zespołu ds. ODO,
- 12.3. RCP prowadzony jest w wersji elektronicznej i dostępny jest na każde żądanie organu nadzorczego.
- 12.4. W celu zapewnienia bieżącej aktualizacji RCP, Właściciele procesu zobowiązani są do niezwłocznego informowania Koordynatora ds. ODO o wszelkich zmianach w zakresie ochrony danych osobowych, wpływających na aktualizację RCP.

13. Prowadzenie Rejestru kategorii czynności przetwarzania (RKCP)

- 13.1. Zgodnie z art. 30 RODO ust. 2, Spółka występując w roli podmiotu przetwarzającego, zobowiązana jest do prowadzenia Rejestru kategorii czynności przetwarzania (RKCP) w zakresie merytorycznym przewidzianym w w/w przepisie prawa oraz zgodnie z postanowieniami umowy powierzenia przetwarzania danych osobowych,
- 13.2. Za prowadzenie i aktualizację RKCP odpowiada Koordynator ds. ODO ze wsparciem merytorycznym Zespołu ds. ODO,
- 13.3. RKCP prowadzony jest w wersji elektronicznej i dostępny jest na każde żądanie organu nadzorczego lub Administratora danych, który powierzył przetwarzanie danych osobowych do Spółki.
- 13.4. W celu zapewnienia prowadzenia i bieżącej aktualizacji RKCP, Właściciele procesu zobowiązani są do niezwłocznego informowania Koordynatora ds. ODO o zawarciu umowy lub innego instrumentu prawnego dot. powierzenia przetwarzania danych osobowych do Spółki oraz o wszelkich zmianach w zakresie ochrony danych osobowych, wpływających na aktualizację RKCP.

14. Bezpieczeństwo przetwarzania danych osobowych

- 14.1. Zgodnie z art. 32 RODO Administrator danych, z uwzględnieniem stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:
- a) pseudonimizację i szyfrowanie danych osobowych,
 - b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
 - c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
 - d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
- 14.2. Administrator danych, zobligowane są do udokumentowania zastosowania art. 32 RODO w sposób przyjęty w organizacji.
- 14.3. Metodologię do zastosowania art. 32 RODO z uwzględnieniem procedur dot. systemu zarządzania bezpieczeństwem informacji w organizacji stanowią odrębne dokumenty.

15. Zarządzanie incydentami i naruszeniami ochrony danych osobowych

- 15.1. Zgodnie z art. 33 RODO, Administrator danych zobowiązany jest do bieżącego monitorowania incydentów oraz naruszeń ochrony danych osobowych w organizacji oraz do:
- a) zapewnienia szkolenia Użytkowników danych osobowych w zakresie zgłaszania incydentów i naruszeń w obszarze ochrony danych osobowych,
 - b) opracowania metodologii do analizy i oceny incydentów oraz naruszeń w zakresie ochrony danych osobowych,
 - c) podejmowania decyzji w sprawie zgłoszenia oraz dokonania zgłoszenia naruszenia do organu nadzorczego zgodnie z art. 33 RODO,
 - d) podejmowania decyzji w sprawie oraz dokonania zawiadomienia osoby, której dane dotyczą o naruszeniu danych osobowych zgodnie z art. 34 RODO,
 - e) bieżącego prowadzenia wykazu incydentów oraz naruszeń w zakresie ochrony danych osobowych wraz z niezbędną dokumentacją w sposób przyjęty w organizacji,
 - f) podejmowania decyzji w sprawie wdrożenia środków technicznych, organizacyjnych, fizycznych oraz prawnych w celu zaradzenia wszelkim mogącym powstać negatywnym skutkom dla podmiotu danych w wyniku zidentyfikowanych incydentu

lub naruszenia ochrony danych osobowych, oraz zapewnienia, aby incydent lub naruszenie nie wystąpiło w przyszłości.

15.2. Administrator danych, zobowiązany jest do udokumentowania zastosowania art. 33 oraz 34 RODO w sposób przyjęty w organizacji.

15.3. Plan postępowania w przypadku wystąpienia incydentu lub naruszenia ochrony danych osobowych stanowi odrębny dokument.

16. Przeprowadzenie oceny skutków dla ochrony danych (DPIA)

16.1. Zgodnie z art. 35 RODO, Administrator danych przeprowadza ocenę skutków dla ochrony danych, jeżeli:

a) w wyniku przeprowadzonego szacowania ryzyka dla ochrony danych wskazane zostaną obszary (poziomy ryzyka) o wysokim prawdopodobieństwie naruszeniu praw i wolności osób, których dane dotyczą,

b) jeżeli Administrator danych dokonuje:

- systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną,

- przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO,

-systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie,

c) lub jeżeli Administrator danych przeprowadzają operacje przetwarzania obligatoryjnie podlegającym dokonania oceny skutków dla ochrony danych zgodnie z komunikatem organu nadzorczego.

16.1. Administrator danych zobowiązany jest do udokumentowania zastosowania lub braku konieczności zastosowania art. 35 RODO w sposób przyjęty w organizacji.

16.2. Metodologia do zastosowania art. 35 RODO stanowi odrębny dokument.

17. Dokonanie uprzednich konsultacji z organem nadzorczym

17.1. Zgodnie z art. 36 RODO, Administrator danych, zobowiązany jest do dokonania uprzednich konsultacji z organem nadzorczym, jeżeli w wyniku dokonania oceny skutków dla ochrony danych, nie zastosował środków technicznych lub organizacyjnych

w celu zminimalizowania wysokiego ryzyka naruszenia praw i wolności osób, których dane dotyczą.

17.2. Zakres merytoryczny do dokonania uprzednich konsultacji został wskazany w art. 36 RODO.

17.3. Administrator danych, zobowiązany jest do udokumentowania zastosowania lub braku konieczności zastosowania art. 36 RODO w sposób przyjęty w organizacji.

18. Przekazywanie danych osobowych do państwa trzeciego (poza EOG)

18.1. Przekazywanie danych osobowych do państwa trzeciego (poza EOG) odbywa się wyłącznie na zasadach określonych w przepisach prawa w zakresie ochrony danych osobowych (Rozdział V RODO).

18.2. W przypadku identyfikacji transferu danych poza EOG, Właściciel procesu, przed przekazaniem danych osobowych do państwa trzeciego, informuje Koordynatora ds. ODO oraz Zespołem ds. ODO w celu weryfikacji zasadności przekazania danych poza EOG oraz weryfikacji zastosowania odpowiednich zabezpieczeń wskazanych w Rozdziale V RODO dot. transferu danych poza EOG.

18.3. Przekazanie danych osobowych poza EOG wymaga przeprowadzenia analizy i oceny ryzyka związanego z transferem danych osobowych poza EOG zgodnie z przyjętą w organizacji metodologią.

18.4. Metodologia do przeprowadzenia analizy i oceny transferu danych poza EOG (do państwa trzeciego) stanowi odrębny dokument.

19. Realizacja Zasady ograniczonego przetwarzania (czasowości)

19.1. Zgodnie z Zasadę ograniczonego przetwarzania danych osobowych (zasada czasowości, retencja danych osobowych) Administrator danych przetwarzają dane osobowe w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do realizacji celów, w których dane te są przetwarzane.

19.2. W celu realizacji Zasady czasowości, retencji danych lub inaczej Zasady ograniczenia przechowywania, Administrator danych, zobligowani są do:

- a) dokonania identyfikacji procesów, czynności przetwarzania oraz celów przetwarzania w których zachodzi przetwarzanie danych osobowych,
- b) wskazania w kontekście zidentyfikowanych celów przetwarzania okresu przetwarzania danych osobowych z uwzględnieniem:
 - przepisów prawa obligujących ADO do przetwarzania danych osobowych przez okres niezbędny do realizacji określonych zadań wynikających z przepisów prawa,
 - kryteriów wyznaczania tego okresu w przypadku braku podstawy prawnej obligującej ADO do przetwarzania danych osobowych przez wyznaczony okres,
- c) Administrator danych, obliguje Właścicieli procesów do wskazania okresu przetwarzania danych osobowych w obszarach, za które odpowiadają oraz do

uprzednich konsultacji z Koordynatorem ds. ODO ze wsparciem Zespołu ds. ODO w obszarze retencji danych osobowych w przypadku:

- planowanym dokonaniem anonimizacji lub pseudonimizacji w związku ze zbliżającym się okresem usunięcia danych osobowych,
 - planowanym fizycznym, w wersji papierowej lub elektronicznej, usunięciem danych osobowych, w związku ze zbliżającym się okresem usunięcia danych osobowych,
- d) Właściciele procesu, potwierdzają dokonanie anonimizacji, psudonimizacji lub usunięcia danych osobowych w postaci protokołu dokonania w/w operacji na danych osobowych w sposób przyjęty w organizacji (np. w formie wydruku z systemu teleinformatycznego lub w formie protokołu zniszczenia dokumentacji lub nośników danych).

20. Przestrzeganie zasady „czystego biurka”

- 1) Przestrzeganie zasady „czystego biurka” obowiązuje wszystkich Użytkowników danych osobowych podczas wykonywania obowiązków w siedzibie Administratora lub w przypadku wykonywania pracy zdalnej,
- 2) Zasada „czystego biurka” polega na niepozostawianiu żadnych dokumentów lub nośników z danymi osobowymi, podczas nieobecności przy stanowisku pracy w trakcie pracy jak i po jej zakończeniu,
- 3) Każdy użytkownik danych osobowych zobowiązany jest do przechowywania na biurku tylko tych dokumentów, nośników, które są mu niezbędne do pracy w danym momencie. Należy unikać przechowywania dokumentów niepotrzebnych do realizacji bieżących zadań,
- 4) Po zakończeniu pracy z dokumentami lub nośnikami zawierającymi dane osobowe, należy je niezwłocznie odłożyć w miejsce bezpieczne, tj. np. do szuflady lub szafy lub inne dedykowane miejsce do przechowywania,
- 5) Po zakończeniu pracy lub świadczenia usług, na biurku nie powinny pozostać żadne dokumenty ani nośniki z danymi osobowymi.

21. Zasady bezpieczeństwa przetwarzania w przypadku pracy zdalnej

Użytkownik danych osobowych wykonujący pracę zdalną zobowiązany jest między innymi do:

- 1) używania bezpiecznego połączenia VPN z systemami informatycznymi,
- 2) zabezpieczanie ekranu w czasie wykonywania pracy, który powinien być niewidoczny dla osób postronnych,
- 3) blokowania komputera po zaprzestaniu pracy i oddaleniu się od sprzętu służbowego,

- 4) obowiązkowego korzystania z VPN przy połączeniach umożliwiających dostęp do danych osobowych, finansowych oraz innych ważnych niezbędnych do działania Administratora danych,
- 5) wykorzystywanie powierzonego sprzęt wyłącznie do wykonywania powierzonych obowiązków,
- 6) używania powierzonego sprzętu zgodnie z jego przeznaczeniem i instrukcją obsługi,
- 7) dbania o sprawność sprzętu i jego przydatność techniczną do używania,
- 8) niezwłocznego informowania Administratora danych o stwierdzonych zagrożeniach dla prawidłowego zabezpieczenia i funkcjonowania powierzonego sprzętu,
- 9) niezwłocznego powiadomienia Administratora danych o wystąpieniu jakichkolwiek usterek technicznych, oprogramowania, braku aktualizacji oprogramowania antywirusowego, pojawienia się komunikatu o znalezionym i nieusuniętym wirusie, problemie z logowaniem itp.,
- 10) niewykorzystywania sprzętu do przeglądania stron internetowych zawierających nielegalne treści, w tym treści propagujące nazizm, rasizm, totalitaryzm, antysemityzm i tym podobne,
- 11) chronić dostęp do sprzętu hasłem nadanym przez Administratora danych oraz nie udostępniać tego hasła osobom trzecim,
- 12) nie udostępniać sprzętu osobom trzecim,
- 13) przy opuszczaniu stanowiska pracy każdorazowo blokować komputer hasłem, ograniczając w ten sposób dostęp do niego osobom nieupoważnionym,
- 14) nie przekazywać osobom zewnętrznym danych uzyskanych lub wytworzonych w trakcie pracy lub znajdujących się w systemach komputerowych Administratora danych,
- 15) chronić sprzęt przed usunięciem danych, kradzieżą, uszkodzeniem oraz zniszczeniem,
- 16) nie instalować bez zgody Administratora danych żadnych programów, nie przechowywać i nie odtwarzać na sprzęcie danych pochodzących z wszelkiego rodzaju nośników informacji, mogących naruszać prawa autorskie osób trzecich, a także danych niewiadomego pochodzenia,
- 17) zapewnić w miejscu wykonywania pracy zdalnej stały dostęp do szerokopasmowego łącza internetowego, gwarantującego wysoką przepustowość danych przesyłanych za pośrednictwem środków komunikacji elektronicznej,
- 18) ograniczyć dostęp do danych osobowych, odchodząc od stanowiska pracy każdorazowo blokować urządzenie, na którym pracuje,
- 19) w przypadku korzystania z drukarek, skanera, upewnić się, że drukowane lub skanowane dokumenty nie pozostają zachowane w pamięci urządzenia,
- 20) podejmować środki bezpieczeństwa, aby urządzenia wykorzystywane podczas pracy zdalnej nie zostały zgubione, skradzione lub uległy uszkodzeniu lub zniszczeniu,
- 21) postępować zgodnie z obowiązującymi w organizacji zasadami dotyczącymi korzystania ze służbowej poczty elektronicznej (e-mail),
- 22) używać przede wszystkim służbowych kont email,

- 23) przed wysłaniem maila upewnić się, że wiadomość wysyłana jest do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe,
- 24) dokładnie sprawdzać nadawcę maila. Nie otwierać wiadomości od nieznanego adresata, a zwłaszcza nie otwierać załączników oraz nie klikać w link zawarty w takiej wiadomości (phishing),
- 25) dokładnie sprawdzać nadawcę maila przed przeczytaniem otrzymanej wiadomości elektronicznej,
- 26) używać tylko z zaufanego dostępu do sieci lub chmury oraz przestrzegać wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych,
- 27) zadbanie, aby przechowywane dane były w bezpieczny sposób zarchiwizowane (np. na nośnikach pamięci),
- 28) jeżeli podczas pracy zdalnej przechowywana lub generowana jest dokumentacja w wersji papierowej, zapewnienie odpowiedniego zabezpieczenia danych w miejscu wykonywania pracy zdalnej (np. przechowywanie dokumentów w zamkniętych na klucz szufladach biurka lub szafach, przestrzeganie zasady czystego biurka, zabezpieczenie dokumentów przed wglądem nieuprawnionych osób trzecich, m.in. członków rodziny),
- 29) ogranicz liczbę dokumentów wnoszonych z siedziby Administratora danych do tego, co niezbędne w stosunku do celu przetwarzania danych osobowych przez Użytkownika danych osobowych w ramach pracy zdalnej,
- 30) zapewnić, aby po zakończeniu pracy zdalnej wszelka dokumentacja została niezwłocznie przekazana lub zwrócona do Administratora danych,
- 31) natychmiastowego poinformowania Administratora danych o wszelkich zagrożeniach mogących wpływać na bezpieczeństwo przetwarzania danych osobowych podczas pracy zdalnej (np. brak możliwości wydzielenia odpowiedniej przestrzeni, tak aby ewentualne osoby postronne nie miały dostępu do dokumentów, urządzeń, w których przetwarzane są dane osobowe),
- 32) pozostania w stałym kontakcie z Inspektorami Ochrony Danych we wszelkich kwestiach związanych z przetwarzaniem danych osobowych podczas pracy zdalnej.

22. Realizacja Zasady rozliczalności

- 22.1. Zgodnie z Zasadą rozliczalności, Administrator danych, zobowiązany jest do udokumentowania, iż przetwarzanie danych osobowych dokonywane jest zgodnie z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych.
- 22.2. Udokumentowanie, iż przetwarzanie danych osobowych dokonywane jest zgodnie z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych może zostać sporządzone w wersji papierowej lub elektronicznej i jest dostępne dla organu nadzorczego na każde żądanie.
- 22.3. Zakresem merytoryczny w/w dokumentu wynika z zakresu merytorycznego (poszczególnych artykułów) określonego w RODO oraz przepisach prawa *lex specialis* w krajowym porządku prawnym.

22.4. Podsumowanie dla realizacji Zasady rozliczalności stanowi odrębny dokument.

23. Przegląd Polityki, dokonanie sprawdzenia i audyty

23.1. Aktualizacja dokumentacji

- a) niniejsza Polityka poddawana jest przeglądowi oraz aktualizacji,
- b) w przypadku wystąpienia istotnych zmian dotyczących przetwarzania danych osobowych w organizacji, Administratora danych lub osoby do tego wyznaczone dokonują aktualizacji dokumentacji systemu zarządzania ochroną danych osobowych bez konieczności ponownej akceptacji Polityki.

23.2. Sprawdzenie zgodności przetwarzania danych osobowych z przepisami prawa

- a) Administrator danych, decyduje o terminie przeprowadzenia sprawdzenia zgodności w obszarze przetwarzania danych osobowych w organizacji zgodnie z obowiązującymi przepisami prawa,
- b) weryfikacja zgodności przetwarzania danych z przepisami prawa dokonywana jest w sposób ciągły.

23.3. Audyty w zakresie ochrony danych osobowych

- 1) Przeprowadzenie audytu systemu zarządzania ochroną danych osobowych w organizacji stanowi narzędzie do udokumentowania realizacji Zasady rozliczalności na gruncie RODO.
- 2) Administrator danych, przeprowadza audyt (wewnętrzny lub zewnętrzny) systemu zarządzania ochroną danych osobowych lub poszczególnych jego elementów:
 - a) na żądanie,
 - b) w przypadku wystąpienia okoliczności, mogących świadczyć o nieprzestrzeganiu zasad przetwarzania danych osobowych w organizacji,
 - c) w przypadku wystąpienia incydentów lub naruszeń ochrony danych osobowych,
 - d) w innych przypadkach, w zależności od potrzeb organizacji.

23.4. Audyt podmiotu przetwarzającego (Spółka jako ADO)

- 1) W przypadku identyfikacji powierzenia przetwarzania danych osobowych przez Spółkę, Administrator danych przeprowadza audyt podmiotu przetwarzającego w trakcie trwania powierzenia przetwarzania.
- 2) O terminie, czasie trwania, zakresie merytorycznym oraz formie audytu podmiotu przetwarzającego decyduje Administrator danych.
- 3) Dokumentacja wspierająca przeprowadzenie audytu podmiotu przetwarzającego stanowi odrębne dokumenty.

23.5. Audyt podmiotu przetwarzającego (Spółka jako Procesor)

- 1) W przypadku identyfikacji powierzenia przetwarzania danych osobowych do Spółki, Spółka udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia przez Spółkę obowiązków wynikających z powierzenia przetwarzania danych osobowych do Spółki oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.
- 2) Przeprowadzenie audytu przez Administratora danych w związku z powierzeniem przetwarzania danych osobowych do Spółki, nie może naruszać bezpieczeństwa, poufności oraz tajemnicy w stosunku do wszelkich informacji w tym danych osobowych nieobjętych audytem.

24. Szkolenia w zakresie ochrony danych osobowych

- 24.1. Administrator danych na bieżąco zapewnia wewnętrzne lub/i zewnętrzne szkolenia w zakresie ochrony danych osobowych w organizacji.
- 24.2. Rodzaje prowadzonych szkoleń w zakresie ochrony danych osobowych:
 - 1) szkolenia wstępne – dla nowych pracowników, współpracowników, przeprowadzane przed dopuszczeniem osób do przetwarzania danych osobowych,
 - 2) szkolenia okresowe – mające na celu bieżące podnoszenie wiedzy w obszarze przetwarzania danych osobowych,
 - 3) szkolenia dedykowane dla poszczególnych procesów organizacyjnych i w zależności od potrzeb organizacji w tym na prośbę Właścicieli procesów,
 - 4) szkolenia w wyniku wystąpienia incydentu lub naruszenia ochrony danych osobowych,
 - 5) pozostałe – w zależności od potrzeb organizacji,
- 24.3. Dokumentacja szkoleniowa archiwizowana jest w sposób przyjęty w organizacji.

25. Dokumentacja w zakresie ochrony danych osobowych

- 25.1. Ustala się, iż Administrator danych, może opracować oraz przyjmować do stosowania dokumentację w zakresie ochrony danych osobowych odpowiadającą identyfikowanym procesom w organizacji, przy czym postanowienia w/w dokumentów nie mogą mieć postanowień sprzecznych z przyjętymi ogólnymi zasadami przetwarzania danych osobowych w Spółce.
- 25.2. Biorąc pod uwagę w/w postanowienie, Administrator danych, prowadzi wykaz dokumentów (procedur, instrukcji postępowania oraz pozostałych dokumentów) w oparciu o których realizowane są zasady przetwarzania danych osobowych w organizacji.
- 25.3. Dokumentacja systemu zarządzania danych osobowych nadzorowana jest przez Koordynatora ds. ODO ze wsparciem merytorycznym Zespołu ds. ODO.
- 25.4. Dokumentacja systemu zarządzania danych osobowych dostępna jest wyłącznie dla osób upoważnionych, objęta jest poufnością oraz tajemnicą i nie może być w żaden sposób dystrybuowana w szczególności poza organizację.

- 25.5. W celu realizacji przepisów prawa oraz realizacji postanowień Polityki, Administrator danych, opracowuje, aktualizuje oraz przyjmuje do stosowania dokumentację (polityki, procedury, instrukcje postępowania, załączniki, inne dokumenty) w systemie zarządzania ochroną danych osobowych, przy czym:
- a) nie mogą one naruszać ogólnych postanowień zasad przetwarzania danych osobowych określonych w obowiązujących przepisach prawa,
 - b) nie mogą one naruszać ogólnych postanowień bezpieczeństwa przetwarzania danych osobowych określonych w Polityce.
- 25.6. Zgodnie z w/w postanowieniami, Administrator danych, opracowuje, wdraża i na bieżąco zarządza dokumentacją niezbędną do prawidłowego wywiązania się ze spoczywających na Administratorze obowiązków wynikających z przepisów prawa w obszarze ochrony danych osobowych zgodnie z określoną w RODO Zasadą rozliczalności.
- 25.7. Poszczególne wzory dokumentacji w obszarze ochrony danych osobowych na bieżąco dostępne są w dedykowanych folderach, nadzorowanych przez Koordynatora ds. ODO ze wsparciem merytorycznym Zespołu ds. ODO.

26. Postanowienia końcowe

- 26.1. **[Data obowiązywania dokumentu]** Niniejszy dokument wchodzi w życie z dniem 14.01.2026 i obowiązuje do odwołania lub wprowadzenia zmian.
- 26.2. **[Zmiany w Procedurze]** Zmiany w niniejszym dokumencie odnotowywane są poprzez wersjonowanie dokumentu. Dokumenty są wersjonowane i przechowywane w wersji papierowej lub/i elektronicznej.
- 26.1. **[Poufność]** Niniejsza Polityka wraz z dokumentami powiązаныmi objęta jest poufnością oraz tajemnicą, stanowi wewnętrzny dokument obowiązujący w K&K Bielickie Sp. z o.o. i nie może być w żaden sposób rozpowszechniana ani udostępniana, w szczególności poza organizację. Dostęp do polityk w zakresie ochrony danych osobowych posiadają wyłącznie osoby upoważnione.