

# **POLITYKA OCHRONY DANYCH OSOBOWYCH**

**Perlik Aluminium Sp. K.**

<b>Data przyjęcia:</b>	<b>1 lutego 2025 r.</b>
<b>Wersja</b>	<b>1</b>

Spis treści

2.	Informacje ogólne .....	4
3.	Zakres informacji objętych dokumentem oraz zakres zastosowania .....	5
4.	Interpretacja postanowień Polityki oraz zasada maksymalnego poziomu bezpieczeństwa danych .....	5
5.	Prowadzenie Polityki wraz z Rejestrem Czynności i Rejestrem Kategorii .....	5
6.	Sposób aktualizacji oraz przeglądania Polityki.....	5
7.	Metody zapoznawania się z Polityką .....	6
8.	Główne obszary, w których przetwarzane są dane .....	6
9.	Dokumentacja przetwarzania danych .....	6
9.1.	Upoważnienia do przetwarzania danych i zasady ich nadawania.....	6
9.2.	Umowy powierzenia danych do przetwarzania .....	7
9.3.	Zgody na przetwarzanie danych.....	7
9.4.	Obowiązek informacyjny ADO .....	7
9.5.	Procedura stosowania DPIA .....	8
9.6.	Polityka czystego biurka .....	8
9.7.	Polityka retencji danych.....	9
9.8.	Procedura reagowania na incydenty.....	9
9.9.	Rejestr incydentów.....	9
9.10.	Współadministrowanie.....	9
10.	Realizacja przez ADO praw osób, których dane dotyczą .....	10
11.	Rejestr Czynności.....	10
12.	Rejestr Kategorii .....	11

**1. Wyjaśnienia terminów użytych w dokumencie (na podstawie art. 4 i n. RODO)**

- 1.1. „administrator danych osobowych” (ADO)** podmiot (odpowiednio organ, jednostka organizacyjna, osoba fizyczna), który decyduje o celach i środkach przetwarzania danych osobowych;
- 1.2. Administrator Systemu Informatycznego (ASI)** - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagających specjalnych uprawnień, odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych osobowych;
- 1.3. „dane osobowe”** oznaczają 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;
- 1.4. „Data Protection Impact Assessment” (DPIA)** ocena skutków planowanych operacji przetwarzania dla ochrony danych, której dokonuje ADO jeżeli dany rodzaj przetwarzania (w szczególności z użyciem nowych technologii) ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
- 1.5. „Europejski Obszar Gospodarczy” (EOG)** Państwa Unii Europejskiej oraz Islandia, Norwegia i Liechtenstein;
- 1.6. „hasło”** ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- 1.7. „identyfikator użytkownika”** ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- 1.8. „odbiorca”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych osobowych mającymi zastosowanie stosownie do celów przetwarzania;
- 1.9. „państwo trzecie”** państwo nienależące do EOG;
- 1.10. „poufność danych”** właściwość zapewniająca, że dane osobowe nie są udostępniane nieupoważnionym podmiotom w rozumieniu art. 5 ust. 1 lit. f) RODO;
- 1.11. „powierzenie przetwarzania danych”** sytuacja zlecenia na podstawie umowy przez ADO innemu podmiotowi (Procesorowi) dokonywania w imieniu ADO określonych operacji na danych osobowych (przetwarzania ich w imieniu ADO). Procesor nie decyduje samodzielnie o celach i środkach przetwarzania;

- 1.12.** „procesor” osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane w imieniu ADO;
- 1.13.** „przetwarzanie danych” oznacza operację lub zestaw operacji wykonywanych na danych lub zestawach danych 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;
- 1.14.** „rozliczalność” odpowiedzialność administratora za przestrzeganie zasad RODO i możliwość wykazania ich przestrzegania, w szczególności: zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość danych, ograniczenie przechowywania, integralność i poufność;
- 1.15.** „szczególne kategorie danych” dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, o których mowa w art. 9 ust. 1 RODO;
- 1.16.** „system informatyczny” zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- 1.17.** „usuwanie danych” zniszczenie danych lub ich modyfikacja, uniemożliwiająca ustalenie tożsamości osoby, której dane dotyczą;
- 1.18.** „uwierzytelnianie” działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
- 1.19.** „zgoda” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

## **2. Informacje ogólne**

Dla zachowania zgodności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz.UE.L Nr 119, str. 1) (dalej: „**RODO**”), Perlik Aluminium Sp. K. (dalej: „**Spółka**”), działając jako ADO sporządziła niniejszą Politykę wraz z rejestrem czynności przetwarzania danych osobowych, a także rejestrem kategorii czynności przetwarzania.

Zawarte w niniejszej Polityce opisy zasad i procedur przetwarzania danych osobowych i ich zabezpieczenia mają na celu uporządkowanie procesów przetwarzania danych, a także realizację przez ADO zasady rozliczalności.

### **3. Zakres informacji objętych dokumentem oraz zakres zastosowania**

Na Politykę składa się zestaw obowiązujących zasad i reguł dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Spółki, w tym w szczególności dotyczących:

- a. prowadzenia dokumentacji przetwarzania danych osobowych;
- b. realizacji praw osób, których dane dotyczą;
- c. wdrażania technicznych i organizacyjnych środków bezpieczeństwa, zarówno przetwarzanych tradycyjnie, czyli w formie papierowej, jak i danych przetwarzanych w systemach informatycznych.

Elementem polityki są prowadzone przez Spółkę zgodnie z art. 30 ust. 1 i 2 RODO:

- a. jako ADO rejestr czynności przetwarzania (dalej: „**Rejestr Czynności**”),
- b. jako Procesora rejestr kategorii czynności przetwarzania (dalej: „**Rejestr Kategorii**”).

Rejestr Kategorii i Rejestr Czynności zwane są wspólnie „**Rejestrami**”, a każdy z osobna „**Rejestrem**”.

Politykę stosuje się do wszelkich czynności stanowiących w myśl RODO przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych, ich zakres, cel zebrania, sposób lub czas przetwarzania, stosowane są zasady przetwarzania danych ujęte w niniejszym dokumencie bądź w innych regulacjach wewnętrznych Spółki regulujących zasady przetwarzania danych osobowych.

### **4. Interpretacja postanowień Polityki oraz zasada maksymalnego poziomu bezpieczeństwa danych**

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony przetwarzanych danych osobowych oraz realizacji praw osób, których dane dotyczą.

Każda osoba mająca dostęp do danych osobowych na podstawie nadanego upoważnienia, została zapoznana z zasadami zachowania maksymalnego poziomu bezpieczeństwa danych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań.

### **5. Prowadzenie Polityki wraz z Rejestrem Czynności i Rejestrem Kategorii**

Polityka oraz zawarte w niej Rejestr Czynności i Rejestr Kategorii, zgodnie z art. 30 ust. 3 RODO, są prowadzone w formie elektronicznej oraz udostępniane przez Spółkę na żądanie organu nadzorczego.

### **6. Sposób aktualizacji oraz przeglądania Polityki**

Mając na uwadze zapewnienie zgodności Polityki z przepisami prawa oraz standardami ochrony danych osobowych, osoba upoważniona przez ADO dokonuje corocznie przeglądów i w razie konieczności aktualizacji Polityki. W razie konieczności do końca każdego roku przygotowuje projekt zmian w treści Polityki. Projekt zmian zawiera informacje pozwalające na wyeliminowanie niezgodności stanu opisanego w Polityce ze stanem faktycznym.

Niezależnie od powyższego Polityka, a w szczególności Rejestr Czynności i Rejestr Kategorii podlegają aktualizacji każdorazowo w przypadku likwidacji, utworzenia lub zmiany procesów przetwarzania danych, a także w przypadku zmiany przepisów prawa dotyczącego ochrony danych osobowych.

W celu zapewnienia kontroli nad procesem przetwarzania danych oraz w celu zapewnienia aktualności dokumentu Polityki, wszystkie działania dotyczące sfery ochrony danych są raportowane oraz konsultowane z osobą upoważnioną przez ADO.

## **7. Metody zapoznawania się z Polityką**

Każda osoba upoważniona do przetwarzania danych przez Spółkę ma obowiązek zapoznania się z Polityką i stosowania zasad w niej opisanych. Spółka udostępnia do zapoznania się osobom upoważnionym treść dokumentu lub wyciąg z dokumentu na etapie rozpoczynania współpracy, co dana osoba potwierdza poprzez podpisanie się na otrzymanym upoważnieniu.

Polityka udostępniania jest również pracownikom w formie elektronicznej na zasobach sieciowych Spółki.

## **8. Główne obszary, w których przetwarzane są dane**

Spółka przetwarza dane głównie w pomieszczeniach zlokalizowanych w siedzibie przy ul. Teofila Morawskiego 31, 63-460 Ociąż (Nowe Skalmierzyce) oraz na zasobach sieciowych Spółki na urządzeniach informatycznych stosowanych przez pracowników Spółki.

## **9. Dokumentacja przetwarzania danych**

Dokumentacja przetwarzania danych przechowywana jest przez ADO.

### **9.1. Upoważnienia do przetwarzania danych i zasady ich nadawania**

Zgodnie z RODO, ADO musi zapewnić, aby każda osoba fizyczna działająca z ich upoważnienia, mająca dostęp do danych osobowych, przetwarzała je wyłącznie na ich polecenie.

W celu wypełniania wspomnianego obowiązku, w strukturze wewnętrznej Spółki do przetwarzania danych dopuszczone są wyłącznie osoby posiadające upoważnienie nadane przez ADO (wzór upoważnienia stanowi Załącznik nr 1 do Polityki), które zawiera w szczególności:

- zakres danych objętych upoważnieniem;
- zakres operacji przetwarzania;
- okres obowiązywania upoważnienia;
- oświadczenie o zapoznaniu się z przepisami o ochronie danych oraz dokumentacją dotyczącą przetwarzania danych obowiązującą u ADO;
- obowiązek zachowania poufności danych oraz sposobów ich gromadzenia i zabezpieczania.

Każdorazowa weryfikacja zakresu upoważnienia i odpowiednia jego modyfikacja w stosunku do osób zatrudnionych jest dokonywana w przypadku zmiany zakresu kompetencji.

Upoważnienie (w tym zmiana jego zakresu) zostaje nadane na wniosek osoby przełożonej osoby mającej zostać dopuszczoną do przetwarzania danych, co do zasady w formie pisemnej lub mailowej (w drodze wyjątku – ustnie). Zakres danych, do których uzyskuje dostęp pozostaje w związku z wykonywanymi na rzecz Spółki czynnościami.

Celem realizacji zasady rozliczalności Spółka archiwizuje upoważnienia do przetwarzania danych osobowych.

## **9.2. Umowy powierzenia danych do przetwarzania**

Podstawą przetwarzania danych w imieniu Spółki przez podmioty trzecie, oraz przetwarzania danych przez Spółkę w imieniu innych administratorów, są umowy powierzenia danych do przetwarzania.

Spółka dochowuje staranności, aby w każdym przypadku powierzenia danych podmiotowi trzeciemu, biorąc pod uwagę specyfikę konkretnych sytuacji, w tym swobodę kontraktowania stron, przy precyzowaniu warunków współpracy określonych w art. 28 RODO, zapewniała sobie możliwość jak najszerzego kontrolowania podmiotów przetwarzających (przeprowadzania audytów i inspekcji) oraz wpływu na dalsze powierzenie danych, tak aby w jak największym stopniu zagwarantować bezpieczeństwo przetwarzania danych.

Jednocześnie, w zakresie w jakim Spółka przetwarza dane jako podmiot przetwarzający zostały wdrożone odpowiednie techniczne i organizacyjne środki bezpieczeństwa.

Spółka zapewnia, aby w przypadkach przekazywania danych do państw trzecich w ramach mechanizmu powierzenia, transfer danych odbywał się wyłącznie do państw, w stosunku do których Komisja Europejska stwierdziła występowanie odpowiedniego stopnia ochrony danych zgodnie z art. 45 ust. 3 RODO, lub w przypadku braku takiej decyzji, aby zostały zapewnione odpowiednie zabezpieczenia takiego transferu, w szczególności za pomocą standardowych klauzul ochrony danych przyjętych przez Komisję Europejską.

W przypadku, gdy Spółka zawiera umowę powierzenia danych osobowych do przetwarzania, osoba odpowiedzialna za dany proces jest zobowiązana niezwłocznie powiadomić osobę odpowiedzialną za ochronę danych osobowych w Spółce o zawarciu i rozwiązaniu takiej umowy za pośrednictwem wiadomości mailowej, chyba, że wysłanie wiadomości mailowej nie było możliwe – w takim wypadku informacja przekazywana jest ustnie.

## **9.3. Zgody na przetwarzanie danych**

Spółka w zakresie w jakim nie dysponuje inną podstawą przetwarzania wskazaną w art. 6 ust. 1 lub art. 9 ust. 2 RODO, odbiera od podmiotów danych zgody na przetwarzanie ich danych.

W celu zagwarantowania ważności odbieranych oświadczeń Spółka wprowadziła system ujednoczonych zgód na przetwarzanie danych, korzystając w tym zakresie z możliwie standardowych wzorów dostosowanych do potrzeb konkretnego przypadku m.in. w części dotyczącej zakresu danych, celów przetwarzania, etc.

## **9.4. Obowiązek informacyjny ADO**

RODO wprowadza obowiązek informowania przez ADO osób, których dane dotyczą, o przetwarzaniu ich danych osobowych poprzez podanie informacji wymienionych w art. 13 i 14 RODO.

W związku z powyższym Spółka wdrożyła odpowiednie mechanizmy mające zapewnić przekazanie osobom, których dane dotyczą kompletu wymaganych przepisami informacji z zachowaniem wymaganych ram czasowych, w szczególności Spółka zagwarantowała, aby klauzula informacyjna została umieszczona:

- we wszystkich umowach (w treści - lub jako odrębny dokument, np. załącznik) na mocy których dochodzi do udostępnienia ADO danych, tj. np. w umowach o pracę (chyba, że

- dane są odbierane wcześniej w ramach formularzy – wtedy „przy” tych formularzach), umowach z kontrahentami etc.;
- w korespondencji mailowej / listownej kierowanej do podmiotów danych w związku z głównym przedmiotem działalności Spółki;
  - w związku z prowadzonymi kanałami rekrutacji (m.in. w ramach ogłoszenia o pracę, w ramach CV oraz w miejscach przyjmowania dokumentów od kandydatów do pracy).

### **9.5. Procedura stosowania DPIA**

DPIA to proces mający opisać przetwarzanie, ocenić niezbędność i proporcjonalność przetwarzania oraz pomóc w zarządzaniu ryzykiem naruszenia praw lub wolności osób fizycznych wynikającym z przetwarzania danych osobowych (oceniając ryzyko i ustalając środki mające mu zaradzić).

Spółka każdorazowo – w stosunku do poszczególnych kategorii operacji – weryfikuje, czy zachodzą podstawy dokonania DPIA – w związku z tym, że wspomniana weryfikacja jest nieodłącznym procesem wewnętrznym, Spółka wdrożyła odrębną Procedurę w zakresie postępowania na potrzeby oceny zasadności przeprowadzenia DPIA oraz ew. jej dokonania (Załącznik nr 2).

W związku z tym, że obowiązek przeprowadzenia DPIA spoczywa na podmiocie będącym ADO, Spółka w zakresie w jakim występuje jako Procesor może uczestniczyć w przeprowadzaniu DPIA przez ADO, udzielając mu m.in. niezbędnych informacji.

### **9.6. Polityka czystego biurka**

W celu określenia zasad zapobiegania dostępowi do danych osobowych przetwarzanych w miejscu pracy osób nieuprawnionych, w tym podczas wspólnego korzystania przez większą ilość osób z pomieszczeń i sprzętu współdzielonego, Spółka wdrożyła politykę czystego biurka.

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do zapewnienia ich bezpieczeństwa oraz uniemożliwienia dostępu do nich osobom nieupoważnionym. W przypadku pracy nad dokumentami zawierającymi dane osobowe nie należy pozostawiać ich bez nadzoru, po zakończonej pracy dokumenty te powinny być bezwzględnie przechowywane w zamkniętych na klucz szafach bądź szufladach. Należy bezwzględnie przestrzegać obowiązku zamykania szafek / szuflad na klucz po zakończeniu pracy i nietrzymania kluczy w zamkach na stałe.

Po zakończeniu pracy opuszczane pomieszczenia należy pozostawić zabezpieczone – osoba wychodząca jako ostatnia powinna:

- upewnić się, że wszystkie okna w pomieszczeniu zostały zamknięte;
- zamknąć drzwi wejściowe do pomieszczenia; oraz
- zabezpieczyć w odpowiedni sposób klucze.

Żaden pracownik nie powinien przekazywać innym osobom udostępnionych mu haseł i kodów dostępu, trzymać ich na biurku lub utrwać w łatwo dostępnych miejscach (np. login i hasło naklejone na klawiaturę / ścianę).

Monitor komputera powinien być ustawiony w taki sposób, aby osoby nieuprawnione nie miały możliwości wglądu w monitor. W przypadku braku ustawienia włączającego się automatycznie



po zdefiniowanym okresie wygaszacza ekranu, każdy pracownik powinien przed oddaleniem się od stanowiska pracy, zablokować komputer lub w przypadku dłuższej nieobecności wylogować się z systemu.

### **9.7. Polityka retencji danych**

Spółka wdrożyła politykę retencji danych, która szczegółowo opisuje okresy przechowywania określonych dokumentów w Spółce, z uwzględnieniem odpowiednich przepisów, oraz obowiązek usunięcia danych po okresie przechowywania (Załącznik nr 3).

### **9.8. Procedura reagowania na incydenty**

W związku ze zobowiązaniem jakie zgodnie z RODO spoczywa na Spółce dotyczącym:

- zgłaszania naruszenia ochrony danych osobowych organowi nadzorcemu; oraz
- zawiadamiania osoby, której dane dotyczą o naruszeniu ochrony danych osobowych;

w Spółce została wdrożona procedura reagowania na incydenty związane z naruszeniem ochrony danych osobowych, w tym postępowania w celu realizacji wspomnianych powinności (Załącznik nr 4).

Każdy kto stwierdził wystąpienie incydentu lub podejrzewa, że mógł on wystąpić zobowiązany jest niezwłocznie poinformować o tym osobę odpowiedzialną za ochronę danych osobowych w Spółce. Osoba ta kontaktuje się z Administratorem, wspólnie z którym podejmuje środki zaradcze, mające na celu usunięcie lub – jeśli nie jest to możliwe - ograniczenie skutków incydentu oraz wypełnia rejestr incydentów.

### **9.9. Rejestr incydentów**

Spółka prowadzi rejestr incydentów (Załącznik nr 5) . W rejestrze opisane są w szczególności:

- zidentyfikowane naruszenia bezpieczeństwa danych prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez Administratora;
- charakter incydentów;
- okoliczności naruszenia ochrony danych osobowych;
- skutki incydentu;
- osoba, która zidentyfikowała incydent;
- podjęte środki zaradcze;
- termin i sposób spełnienia obowiązków Administratora dotyczących poinformowania o incydencie:
  - osoby, której dane dotyczą;
  - organu nadzorczego;
  - administratora danych osobowych (w przypadku, gdy Spółka przetwarza dane dotknięte incydemem jako Procesor).

### **9.10. Współadministrowanie**

Jeśli Spółka w stosunku do niektórych operacji na danych osobowych może ustalać cele i sposoby przetwarzania wspólnie z innymi podmiotami, w celu prawidłowego wywiązywania się

z obowiązków określonych w art. 26 RODO Spółka każdorazowo przed rozpoczęciem takich operacji na zasadzie wspólnej administracji danymi zawiera umowę w tym zakresie.

Treść zawieranej umowy spełnienia warunku dotyczące uzgodnień, o których stanowi art. 26 RODO, w szczególności w przejrzysty sposób określa odpowiednie zakresy odpowiedzialności Spółki i pozostałych współadministratorów dotyczącej wypełniania obowiązków wynikających z RODO, w tym:

- w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw; oraz
- obowiązków w odniesieniu do spełniania obowiązku podawania informacji, o których mowa w art. 13 i 14 RODO.

Spółka dochowuje staranności, aby zawierane umowy każdorazowo należycie odzwierciedlały odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą.

## **10. Realizacja przez ADO praw osób, których dane dotyczą**

Na gruncie RODO osobie, której dane dotyczą przysługuje szereg praw związanych z możliwością żądania od ADO określonych operacji na danych (np. wyeksportowanie / wykonanie kopii / sprostowanie / usunięcie). Systemy stosowane przez Spółkę przewidują odpowiednie rozwiązania techniczne, które pozwolą na realizację tych praw.

Jednocześnie Spółka przestrzega praktyk opisanych w Załączniku nr 6 dotyczących realizacji żądań osób, których dane dotyczą w zakresie:

- a. prawa dostępu do danych i informacji o nich;
- b. prawa do bycia zapomnianym;
- c. prawa do sprostowania danych;
- d. prawa do ograniczenia przetwarzania;
- e. prawa do przenoszenia danych;
- f. prawa do sprzeciwu wobec przetwarzania danych.

W przypadku realizacji przez podmiot danych jego praw w stosunku do danych przetwarzanych przez Spółkę jako procesora, Spółka pomaga administratorowi wywiązać się z obowiązku odpowiadania na żądania podmiotów danych.

Spółka może spełniać żądania osób, których dane dotyczą w imieniu administratora, wyłącznie jeżeli administrator nadał Spółce odpowiednie upoważnienie i sytuacje taką przewidują ustalenia umowne między administratorem a Spółką.

Żądania osób, których dane dotyczą należy wówczas realizować zgodnie z postanowieniami powyższych praktyk lub – jeśli zasady zostały ustalone wprost między stronami – zgodnie z zawartą umową.

## **11. Rejestr Czynności**

Artykuł 30 ust. 1 RODO nakłada na Spółkę jako ADO obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych. Dotyczy on czynności przetwarzania, za które ADO odpowiada.

W Rejestrze Czynności zamieszczone są następujące informacje wymagane przepisami prawa:

- a. nazwa oraz dane kontaktowe ADO oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela ADO oraz IOD;

- b. cele przetwarzania;
- c. opis kategorii osób, których dane dotyczą, oraz kategorii danych;
- d. kategorie odbiorców, którym dane zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
- e. gdy ma to zastosowanie, informacje o przekazaniu danych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 RODO, dokumentacja odpowiednich zabezpieczeń;
- f. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

co stanowi Załącznik nr 7 do Polityki;

- m. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO;

co stanowi Załącznik nr 8 do Polityki.

## **12. Rejestr Kategorii**

Artykuł 30 ust. 2 RODO nakłada na Spółkę jako Procesora obowiązek prowadzenia rejestru kategorii czynności przetwarzania danych osobowych. W Rejestrze Kategorii zamieszczone są następujące informacje:

- a. dane identyfikujące Spółkę jako Procesora (nazwa oraz dane kontaktowe), a także dane przedstawiciela ADO lub Procesora oraz IOD – jeżeli zostali wyznaczeni;
- b. informacje o przekazaniu danych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa lub organizacji, a w przypadku przekazania, o których mowa w art. 49 ust. 1 RODO, dokumentację odpowiednich zabezpieczeń, gdy dochodzi do takiego przekazania danych do państwa trzeciego lub organizacji międzynarodowej;

co stanowi Załącznik nr 9 do Polityki;

- c. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO;

co stanowi Załącznik nr 8 do Polityki.

## **13. Załączniki:**

1. Upoważnienie do przetwarzania danych osobowych
2. Procedura DPIA;
3. Polityka retencji danych;
4. Procedura reagowania na incydenty;
5. Rejestr incydentów;
6. Realizacja praw osób, których dane dotyczą;
7. Rejestr czynności przetwarzania;
8. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa;
9. Rejestr kategorii czynności przetwarzania;