POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. SŁOWNICZEK I WYKAZ SKRÓTÓW

1.1. Słowniczek

Administrator Danych Osobowych (ADO)	DB Energy SA z siedzibą we Wrocławiu al. Armii Krajowej 45, 50-541 Wrocław, zwana dalej również jako Spółka, ADO lub Administrator Danych tj. osoba prawna, która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych
Inspektor Ochrony Danych Osobowych (IODO)	osoba wyznaczona przez ADO do nadzorowania oraz wdrażania zasad ochrony danych osobowych w Spółce
Administratorzy Systemów Informatycznych (ASI)	osoby odpowiedzialne za nadzór i bezpieczeństwo nad infrastrukturą IT i systemami informatycznymi Spółki
Biuro	Biuro przy al. Armii Krajowej 45, 50-541 Wrocław
Dane osobowe	wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przetwarzane przez Administratora Danych zarówno w systemach informatycznych jak i tradycyjnie (wersja papierowa). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź klika szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej
Dane osobowe szczególnych kategorii	dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby
Hasło	ciąg znaków literowych, cyfrowych lub innych, znany jedynie Użytkownikowi
Identyfikator internetowy (login)	ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną (Użytkownika) do przetwarzania danych osobowych w systemie informatycznym
Instrukcja Zarządzania	instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych obowiązująca u ADO
Integralność danych	właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany
Naruszenie ochrony danych osobowych	naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez ADO
Nośniki danych	wszelkie nośniki, na których informacje zapisane są w postaci elektronicznej, w szczególności dyski, dyskietki, dyski CD-ROM, karty magnetyczne lub pamięci przenośne. Na potrzeby niniejszej Polityki Bezpieczeństwa za nośnik danych uważa się również dokument (dokumenty) papierowy zawierający(e) dane osobowe
Polityka Bezpieczeństwa Danych Osobowych	niniejszy dokument

Przepisy szczególne	powszechnie obowiązujące akty prawne regulujące tematykę ochrony danych osobowych, w tym Rozporządzenie ogólne, ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną
Pseudonimizacja	Przetworzenie danych osobowych w taki sposób, żeby nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji
Rejestr czynności przetwarzania	Pisemny (w tym elektroniczny) rejestr czynności przetwarzania prowadzony przez ADO zawierający imię, nazwisko lub nazwę oraz dane kontaktowe administratora danych, cele przetwarzania, opis kategorii osób których dane dotyczą, kategorie odbiorców danych, planowane terminy usunięcia danych, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa
Rozporządzenie ogólne	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
Rozliczalność	właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi
System informatyczny	zespół urządzeń, sprzętu komputerowego, oprogramowania oraz baz danych przetwarzających dane osobowe
Użytkownik	osoba upoważniona przez ADO do przetwarzania danych osobowych bez względu na formę w jakiej te dane są przetwarzane (elektronicznie, tradycyjnie)
Usuwanie danych	zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą
Zakres zbierania danych osobowych	kategorie danych osobowych, które podlegają przetwarzaniu przez ADO
Zbiór danych osobowych	każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie

1.2 Stosowane skróty

UODO	Urząd Ochrony Danych Osobowych
ADO	Administrator Danych Osobowych
IODO	Inspektor Ochrony Danych Osobowych

2. DEFINICJA, CELE I ZAKRES ZASTOSOWANIA POLITYKI BEZPIECZEŃSTWA

1.Definicja Polityki Bezpieczeństwa	• Polityka Bezpieczeństwa Danych Osobowych to dokument opisujący całokształt działań zmierzających do uzyskania i utrzymania wymaganego poziomu bezpieczeństwa danych osobowych, na każdym etapie ich przetwarzania. • Polityka Bezpieczeństwa Danych Osobowych to w szczególności zbiór zasad dotyczących bezpieczeństwa danych osobowych ustalonych w oparciu o: o wymagania wynikające z przepisów prawa mających zastosowanie do działalności Spółki, o szacowanie ryzyka w związku z prowadzeniem działalności gospodarczej przez Spółkę, o wewnętrzne wymogi i uwarunkowania lokalowe Spółki.

2. Cel Polityki Bezpieczeństwa	1. Wdrożenie Polityki Bezpieczeństwa Danych Osobowych w Spółce ma na celu zabezpieczenie przetwarzanych przez ADO danych osobowych, bez względu na formę (elektroniczną bądź tradycyjną) w jakiej to przetwarzanie następuje. 2. Celem Polityki Bezpieczeństwa Danych Osobowych jest w szczególności: • zabezpieczenie zasobów systemów informatycznych, infrastruktury technicznej, sprzętu i osprzętu przed kradzieżą, zniszczeniem lub uszkodzeniem, • uniemożliwienie dostępu do informacji stanowiących dane osobowe, zawartych w systemach informatycznych zarządzanych przez ADO osobom do tego nieupoważnionym, • uniemożliwienie zniszczenia lub nieuprawnionej zmiany danych osobowych przetwarzanych w sposób tradycyjny (papierowy) oraz elektroniczny, • zabezpieczenie dokumentacji papierowej zawierającej dane osobowe przed ich kradzieżą lub kopiowaniem, • ochrona wizerunku Spółki jako podmiotu przetwarzającego dane osobowe, • zapewnienie odpowiedniego poziomu wiedzy wśród Użytkowników, • zapewnienie zgodności z prawem, rzetelności i przejrzystości, minimalizacji, prawidłowości, ograniczenia przechowywania, integralności i poufności, oraz rozliczalności danych osobowych przetwarzanych przez Spółkę, zastosowanie zasad privacy by design oraz privacy by default,, • zapewnienie gotowości podejmowania działań w sytuacji otrzymania żądania od osoby, której dane dotyczą dostępu do danych osobowych jej dotyczących, wniosku informacyjnego, usunięcia danych (prawa do bycia zapomnianym), sprostowania, ograniczenia przetwarzania, wycofania zgody na przetwarzanie danych, żądania przeniesienia danych, • zapewnienie gotowości do podejmowania działań w sytuacjach kryzysowych tj. wystąpienia incydentu (np. wycieku dany osobowych), zgłoszenia sprzeciwu przez osobę, której dane dotyczą wobec przetwarzania, wniesieniu skargi do Organu nadzorczego.
3. Zakres stosowania	1. Polityka Bezpieczeństwa Danych Osobowych dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny (papierowo), jak również w systemach informatycznych. 2. Procedury i zasady wskazane w Polityce Bezpieczeństwa Danych Osobowych stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych w Spółce, zarówno zatrudnionych jak i innych (np. świadczących czynności na podstawie umów cywilnoprawnych, stażystów, praktykantów etc.).

3. OBOWIĄZKI ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH

3.1. Zasady ogólne

3.1.1. Organizacja przetwarzania danych osobowych w Spółce opiera się na wyodrębnieniu następujących kategorii osób:

- organu zarządzającego ADO (członkowie Zarządu Spółki),
- Użytkowników (osoby upoważnione do przetwarzania danych osobowych przez Administratora, w tym Opiekunowie Zbiorów),
- Personelu pomocniczego.

3.1.2. Dostęp do danych osobowych posiadają osoby tworzące organ zarządzający ADO oraz Użytkownicy (w tym Opiekunowie Zbiorów). Personel pomocniczy nie przetwarza danych osobowych, może natomiast przebywać w obszarze przetwarzania danych na podstawie zgody wydanej przez ADO. Zgoda, o której tu mowa stanowi załącznik nr 6 do niniejszej Polityki Bezpieczeństwa.

3.1.3. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, mają obowiązek zapoznać się (i podpisać stosowne oświadczenie potwierdzające ww. czynność) z obowiązującymi zasadami ochrony danych osobowych określonymi w niniejszej Polityce Bezpieczeństwa Danych Osobowych i Instrukcji Zarządzania i podpisać oświadczenie o zachowaniu danych osobowych i sposobów ich zabezpieczenia (np. hasła dostępowe) w tajemnicy (załącznik nr 1 do Polityki Bezpieczeństwa Danych Osobowych).

3.2. Obowiązki Administratora Danych Osobowych

Administratorem Danych jest osoba prawna (Spółka), a cechą wyróżniającą jest to, że decyduje o celach i środkach przetwarzania danych osobowych. Z uwagi na bezosobowy charakter tej definicji należy przyjąć, że organem zarządzającym ADO jest Zarząd Spółki.

W ramach swych obowiązków ADO jest odpowiedzialny za:

3.2.1. Nadzorowanie, aby będące w jego posiadaniu dane osobowe były przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (art. 5 ust. 1 a) Rozporządzenia ogólnego);

3.2.2. Zbieranie danych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzanie dalej w sposób niezgodny z tymi celami (ograniczenie celu) – art. 5 ust. 1 b) Rozporządzenia ogólnego;

3.2.3. Adekwatne stosowne oraz ograniczone do tego, co niezbędne do celów przetwarzania (minimalizacja danych);

3.2.4. Wyodrębnienie zbiorów przetwarzanych danych osobowych, a także ich bieżące aktualizowanie.

3.2.5. Zapewnienie środków technicznych i organizacyjnych do ochrony przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną.

3.2.6. Prowadzenie dokumentacji opisującej sposób przetwarzania danych osobowych: Polityka Bezpieczeństwa Danych Osobowych i Instrukcja Zarządzania oraz dokumenty z nimi związane.

3.2.7. Przechowywanie danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą przez okres nie dłuższy niż jest to niezbędne do celów w których dane te są przetwarzane.

3.2.8. Wyznaczenie osoby pełniącej funkcję IODO w przypadku gdy wyznaczenie IODO będzie obowiązkowe mając na uwadze przepisy prawa, lub ADO podejmie decyzję o konieczności takiego wyznaczenia.

3.2.9. Prowadzenie rejestru czynności przetwarzania w przypadku gdy prowadzenie takiego rejestru będzie dla ADO obowiązkowe, mając na uwadze przepisy prawa, lub ADO podejmie decyzję o jego prowadzeniu.

3.2.10. Upoważnianie do przetwarzania danych Użytkowników (upoważnienia w imieniu ADO nadaje, na podstawie pełnomocnictwa IODO jeśli został wyznaczony).

3.2.11. Wydawanie upoważnień na przebywanie w obszarze przetwarzania danych osobowych dla Personelu pomocniczego.

3.2.12. Niezwłoczne sprostowanie danych osobowych w przypadku otrzymania takiego żądania od osoby której dane dotyczą lub ich uzupełnienie w przypadku kiedy dane są niekompletne, a także ograniczenie przetwarzania.

3.2.13. Niezwłoczne usunięcie danych osobowych na żądanie osoby, której dane dotyczą w przypadkach wskazanych w Rozporządzeniu ogólnym tj. jeśli osoba której dane dotyczą cofnęła zgodę na której opiera się ich przetwarzanie, dane nie są już niezbędne do celów w których zostały zebrane, osoba wniosła sprzeciw wobec przetwarzania.

3.2.14. Informowanie procesorów przetwarzających dane o żądaniach osoby której dane dotyczą co do usunięcia danych osobowych.

3.2.15. Udostępnianie osobom, których dane dotyczą na ich żądanie dane ich dotyczące w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego.

3.2.16. Stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji.

3.2.17. Wdrażanie odpowiednich środków technicznych i organizacyjnych tj. pseudonimizacja, zaprojektowanie w celu skutecznej realizacji zasad ochrony danych tj. minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń w celu zapewnienia ochrony zgodniej z przepisami prawa i w celu ochrony praw osób, których dane dotyczą, a także w celu przetwarzania wyłącznie tych danych osobowych, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

3.2.18. Uwzględnienie ochrony danych w fazie projektowania (privacy by design) – zapewnienie ochrony proaktywnej i prewencyjnej polegającej na zapewnieniu ochrony danych na etapie tworzenia systemu, projektu w celu zapobiegania powstawianiu naruszeń w przyszłości i eliminowaniu zidentyfikowanych zagrożeń,

3.2.19. Uwzględnienie domyślnej ochrony danych (privacy by default) we wszelkich systemach na jakich działa ADO – tj. takie konstruowanie usług, systemów, aplikacji by możliwe było skonfigurowanie ustawień prywatności zgodnie z wolą i decyzją osoby której dane dotyczą.

3.3. Inspektor Ochrony Danych Osobowych

Osoba wyznaczona przez ADO mająca za zadanie:

3.3.1. informowanie ADO oraz innych podmiotów przetwarzających dane (Użytkowników, Opiekunów Zbiorów, podmiotów przetwarzających) o spoczywających na nich obowiązkach i doradzanie im w tej sprawie,

3.3.2. monitorowanie przestrzegania przepisów prawa o ochronie danych i polityk ADO, w tym podział obowiązków, działania zwiększające świadomość, szkolenia, oraz powiązane z tym audyty,

3.3.3. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie wykonania,

3.3.4. współpracę z Organem nadzorczym,

3.3.5. pełnienie funkcji punktu kontaktowego dla Organu nadzorczego, prowadzenie konsultacji,

3.3.6. pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą zwracających się do ADO z wnioskami w trybie przewidzianym w przepisach 15-22 Rozporządzenia ogólnego.

3.4. Obowiązki Opiekunów Zbiorów:

3.4.1. Zawiadamianie ADO o zamiarze utworzenia, likwidacji, modyfikacji struktury lub zmiany lokalizacji zbioru.

3.4.2. Zawiadamianie ADO o zamiarze powierzenia przetwarzania danych zawartych w zbiorze, przy czym zawiadomienie to musi nastąpić zanim Spółka powierzy dane osobowe.

3.4.3. Zawiadamianie ADO o zamiarze rozpoczęcia pracy na danych osobowych ze zbioru zewnętrznego (zakup bazy danych).

3.4.4. Współdziałanie z ADO w zakresie przestrzegania zasad ochrony danych osobowych opisanych w Polityce Bezpieczeństwa Danych Osobowych i Instrukcji Zarządzania.

3.4.5. Wykonywanie innych obowiązków wymaganych prawem, w szczególności wskazanych w pkt. 3.2.

3.5. Obowiązki Użytkowników

3.5.1. Przestrzeganie zasad ochrony danych osobowych określonych w Polityce Bezpieczeństwa Danych Osobowych i Instrukcji Zarządzania. Każdy Użytkownik zobowiązany jest zapoznać się, przed dopuszczeniem do przetwarzania danych, z wyżej wymienionymi dokumentami oraz złożyć stosowne oświadczenie, potwierdzające znajomość ich treści (załącznik nr 1 do Polityki).

3.5.2. Uczestnictwo w szkoleniach z zakresu ochrony danych osobowych.

3.5.3. Przetwarzanie danych osobowych zgodnie z celami przetwarzania.

3.5.4. Zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą.

3.5.5. Informowanie ADO o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony danych osobowych.

3.5.6. Współpraca z ADO w zakresie wprowadzania zasad bezpiecznego przetwarzania danych osobowych oraz reagowania na wszelkie zdarzenia mogące mieć wpływ na obniżenia poziomu tego bezpieczeństwa.

3.5.7. Współpraca z ADO w zakresie wymiany informacji na tematy związane z ochroną danych osobowych.

3.5.8. Zapewnienie poufności danych osobowych, do których uzyskują dostęp.

3.5.9. W odniesieniu do sprzętu komputerowego i urządzeń teleinformatycznych, a także w związku z korzystaniem z zasobów systemów informatycznych służących do przetwarzania danych Użytkownik jest zobowiązany do:

- dbania o bezpieczną eksploatację systemu informatycznego; w przypadku wykrycia zagrożenia Użytkownik ma obowiązek poinformować o tym fakcie ADO,
- dbania o bezpieczeństwo użytkowanego komputera, w tym celu Użytkownik ma obowiązek regularnie zmieniać hasła dostępowe do systemu operacyjnego oraz aplikacji służących do przetwarzania danych osobowych (obowiązek ten ma charakter bezwzględny jeśli istnieje podejrzenie, że hasło mogło zostać poznane przez osobę nieupoważnioną); hasła nie mogą być zapisywane i pozostawiane w łatwo dostępnych miejscach,
- wykazywania ostrożności przy odbieraniu poczty elektronicznej przychodzącej od nieznanych adresatów lub o podejrzanym tytule e-maila,

3.5.10. Dbanie o to, by dokumenty były przechowywane w zamkniętych szafach lub szufladach. Dostęp do kluczy mogą mieć tylko osoby upoważnione do przetwarzania danych.

3.6. Obowiązki Personelu pomocniczego:

3.6.1. Zakaz przetwarzania danych osobowych (np. kserowania dokumentów, wynoszenia ich, wpuszczania do pomieszczeń osób postronnych etc.), do których otrzymują dostęp poprzez obecność w obszarach przetwarzania danych osobowych.

3.6.2. Przebywanie w obszarze przetwarzania danych tylko na podstawie zgody udzielonej przez ADO. Zgoda, o której tu mowa stanowi załącznik nr 5 do niniejszej Polityki Bezpieczeństwa.

3.6.3. Zachowanie w tajemnicy wszelkich danych osobowych, do których Personel pomocniczy uzyskał dostęp poprzez wykonywanie swoich czynności służbowych.

4. ZASADY UDOSTĘPNIANIA DANYCH OSOBOWYCH

4.1. Biorąc pod uwagę, że udostępnianie danych jest jedną z form ich przetwarzania, jest ono dopuszczalne wtedy, gdy spełniony jest jeden z warunków, o którym mowa w art. 6 Rozporządzenia ogólnego (artykuł określa warunki, które uzasadniają udostępnianie danych „zwykłych") bądź w art. 9 Rozporządzenia ogólnego (artykuł wylicza sytuacje, które uzasadniają udostępnienie danych szczególnych kategorii tzw. danych wrażliwych np. informacji o stanie zdrowia).

4.2. Udostępnienie danych „zwykłych" jest możliwe pod warunkiem ziszczenia się jednej z poniższych przesłanek (podmiot zwracający się o udostępnienie danych będzie w stanie wykazać, że przesłanka taka zachodzi):

- osoba, której dane dotyczą, wyrazi zgodę na udostępnienie danych osobowych,

- udostępnienie danych jest konieczne do wykonania umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- udostępnienie danych jest niezbędne dla wypełnienia obowiązku prawnego ciążącego na administratorze,
- udostępnienie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej,
- udostępnienie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (konieczność wskazania ogólnej podstawy prawnej),
- udostępnienie danych jest niezbędne dla wypełnienia prawnie uzasadnionych interesów realizowanych przez administratorów danych albo stronę trzecią.

4.3. Udostępnianie danych wrażliwych jest możliwe pod warunkiem ziszczenia się jednej z poniższych przesłanek (podmiot zwracający się o udostępnienie danych będzie w stanie wykazać, że przesłanka taka zachodzi):

- osoba, której dane dotyczą, wyrazi zgodę na piśmie na udostępnienie danych w jednym lub kilku konkretnych celach,
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą,
- udostępnienie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, nie jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
- udostępnienia dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą,
- udostępnienia dokonuje się w zakresie danych dotyczących osoby, która upubliczniła je w sposób oczywisty,
- udostępnienie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy,
- udostępnienie danych jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą,

- udostępnienie danych jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia,

- udostępnienie danych jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego tj. ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową,

- udostępnienie danych jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, proporcjonalnych do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

4.4. Użytkownicy, których zadania służbowe wiążą się z udostępnianiem danych osobowych mają obowiązek prowadzić (w formie pisemnej lub elektronicznie) ewidencję danych, które są udostępniane (określającą wnioskodawcę, podstawę udostępnienia, zakres danych oraz datę ich udostępnienia). Wzór ewidencji stanowi załącznik nr 3 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

4.5. W razie wątpliwości czy dane osobowe mogą zostać udostępnione, Użytkownik zobowiązany jest zasięgnąć opinii ADO lub IODO jeśli został wyznaczony w Spółce.

5. ZASADY POWIERZANIA PRZETWARZANIA DANYCH OSOBOWYCH.

5.1. Powierzenie przetwarzania danych osobowych Procesorom następuje w drodze umowy, o której mowa w art. 28 Rozporządzenia ogólnego. Zalecany wzór umowy powierzenia przetwarzania danych stanowi załącznik nr 2 do Polityki Bezpieczeństwa Danych Osobowych.

5.2 Za przygotowanie właściwej umowy powierzenia przetwarzania danych odpowiedzialny jest ADO. Przy przygotowaniu ww. umowy ADO współpracuje z Opiekunem Zbioru, który inicjuje bądź jest bezpośrednio zaangażowany we współpracę z Procesorem.

5.3 Przekazanie zbiorów Procesorowi w celu ich przetwarzania nie powoduje zmiany właściwego administratora danych osobowych.

5.4 Procesor, któremu powierzono przetwarzanie danych obowiązany jest zapewnić wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych (art. 20 ust. 1 Rozporządzenia ogólnego) oraz wykorzystywać powierzone mu dane wyłącznie w celach i w zakresie, które zostały wskazane przez ADO w zawartej z nim umowie.

5.5 Procesor, któremu powierzono przetwarzanie danych obowiązany jest w szczególności do:

- stosowania odpowiednich środków ochrony danych osobowych, w tym do zapewnienia fizycznej ochrony pomieszczeń w których przetwarzane są dane, zapewnienia adekwatnych do zagrożeń środków organizacyjnych oraz informatycznych, zgodnie z przepisami prawa,
- niezwłocznego powiadomienia ADO o przypadkach naruszenia przetwarzania powierzonych danych osobowych oraz do dokumentowania wszelkich informacji, które mogą pomóc w ustaleniu okoliczności tego naruszenia,
- tworzenia kopii bezpieczeństwa systemów informatycznych, w których przetwarzane są powierzone dane osobowe, jeżeli jest to niezbędne do prawidłowej realizacji przedmiotu umowy,
- zapewnienia aby każdy pracownik i/lub współpracownik Procesora przetwarzający powierzone dane osobowe posiadał upoważnienie do przetwarzania tych danych osobowych oraz zobowiązał się do zachowania danych w tajemnicy,
- zniszczenia lub zwrotu przekazanych danych stosownie do zapisów umowy powierzenia przetwarzania danych,
- nie korzystania z usług innego podmiotu przetwarzającego bez uprzedniej zgody ADO wyrażonej na piśmie,
- pomocy w miarę możliwości Administratorowi danych wywiązać się z obowiązku odpowiadania na żądanie osoby której dane dotyczą w zakresie prawa dostępu do danych, prawa do ich sprostowania, usunięcia danych („prawo do bycia zapomnianym"), ograniczenia przetwarzania, przenoszenia danych, sprzeciwu, nie podleganiu profilowaniu,
- umożliwienia ADO przeprowadzania inspekcji, audytów i przyczynienia się do nich.

5.6 Lista firm, którym Spółka powierza dane osobowe do przetwarzania stanowi załącznik nr 4 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

6. REJESTROWANIE CZYNNOŚCI PRZETWARZANIA

Rejestr czynności przetwarzania prowadzi każdy Administrator danych w przypadku gdy jest do tego zobowiązany na podstawie przepisów Rozporządzenia ogólnego. W rejestrze zamieszcza się następujące informacje:

a) nazwę i dane kontaktowe Administratora danych (inspektora danych osobowych jeśli został powołany),

b) cele przetwarzania,

c) opis kategorii osób których dane dotyczą, opis kategorii danych osobowych,

d) kategorie odbiorców, którym dane zostały ujawnione,

e) przekazanie danych do państwa trzeciego, jeśli ma zastosowanie,

f) planowane terminy usunięcia poszczególnych kategorii danych, jeśli ich wskazanie jest możliwe,

g) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób których dane dotyczą.

Obowiązek prowadzenia rejestru czynności przetwarzania nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, Rozporządzenia ogólnego lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 Rozporządzenia ogólnego. Sytuacje opisane powyżej oceniane są odrębnie dla każdego przedsiębiorcy lub podmiotu przetwarzającego dane osobowe.

7. WYKAZ OBSZARÓW, W KTÓRYCH PRZETWARZANE SĄ PRZEZ SPÓŁKĘ POSZCZEGÓLNE ZBIORY DANYCH OSOBOWYCH.

7.1. Zbiory w stosunku do których Spółka jest ADO

Nazwa zbioru danych	Adres miejsca przechowywania danych ze zbioru	Wykaz pomieszczeń (nr pokoju)
1. Zbiór „Pracownicy i umowy cywilnoprawne”	• AFK Centrum Obsługi Biznesu Sp. z o.o. ul. Świeradowska 51-57 , 50-559 Wrocław	I piętro Centrum Handlowe Ferio-Gaj
	• Serwer firmy DB Energy SA, al. Armii Krajowej 45, 50-541 Wrocław	
2. Zbiór „Kandydaci do pracy”	• DB Energy SA, al. Armii Krajowej 45, 50-541 Wrocław • Serwer firmowy DB Energy SA, al. Armii Krajowej 45, 50-541 Wrocław	
3. Zbiór „Akcjonariusze i Rada Nadzorcza””	• DB Energy SA, al. Armii Krajowej 45, 50-541 Wrocław • Serwer firmowy DB Energy SA, al. Armii Krajowej 45, 50-541 Wrocław	
4. Zbiór „Dane kontaktowe”	• Serwer firmowy DB Energy SA, DB Energy SA, al. Armii Krajowej 45, 50-541 Wrocław	Należy przyjąć, że dane osobowe z tego zbioru mogą znajdować się na każdym komputerze
5. Zbiór „Ewidencja korespondencji przychodzącej/wychodzącej”	• DB Energy SA, al. Armii Krajowej 45, 50-541 Wrocław	Pocztowa książka nadawcza Spółki

Dane z opisanych wyżej zbiorów mogą być przetwarzane także w innych obszarach, ponieważ w firmie dopuszczalna jest praca zdalna przy pomocy komputerów przenośnych.

8. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO ICH PRZETWARZANIA

8.1. Zbiór „Pracownicy i umowy cywilnoprawne”

Zbiór danych osobowych o nazwie „Pracownicy i współpracownicy" przetwarzany jest w formie kartotek papierowych oraz w systemie informatycznym przy wykorzystaniu następujących aplikacji:

- Serwer firmowy Spółki DB Energy – BIURO -> KADRY-> PRACOWNICY-> DB ENERGY SA

8.2. Zbiór „Kandydaci do pracy"

Zbiór danych osobowych o nazwie „Kandydaci do pracy" przetwarzany jest w czasie trwania danej rekrutacji w formie papierowej oraz znajduje się na serwerze Spółki w folderze BIURO-> KADRY-.> KANDYDACI DO PRACY, do którego dostęp posiadają tylko osoby upoważnione. oraz na serwerze hostingowym i przetwarzany jest w systemie informatycznym przy wykorzystaniu następujących aplikacji.

- Program pocztowy/ webmail
- Microsoft Office

Po zakończeniu rekrutacji aplikacje osobowe kandydatów do pracy przetwarzane w formie papierowej są niszczone za pomocą niszczarki. W przypadku braku uzyskania zgody od kandydata na przetwarzanie danych w celach kolejnych przyszłym rekrutacji – dane osobowe kandydatów usuwane są również z systemu.

8.3. Zbiór „Akcjonariusze i Rada Nadzorcza"

Zbiór danych osobowych o nazwie „Akcjonariusze i Rada Nadzorcza" przetwarzany jest w formie papierowej oraz w systemie informatycznym przy wykorzystaniu następujących aplikacji:

- Serwer firmowy Spółki DB Energy – BIURO -> BIURO-> AKCJONARIUSZE I RADA NADZORCZA

8.4. Zbiór „Dane kontaktowe"

Zbiór danych osobowych o nazwie „Dane kontaktowe" przetwarzany jest w formie papierowej (wizytówki, foldery informacyjne) oraz w systemie informatycznym przy wykorzystaniu następujących aplikacji:

- Program pocztowy/web mail
- Microsoft Office
- System wFirma.pl

8.5. Zbiór „Ewidencja korespondencji przychodzącej/wychodzącej"

Zbiór danych osobowych o nazwie „Ewidencja korespondencji przychodzącej/wychodzącej" przetwarzany jest w formie papierowej przy użyciu pocztowej książki nadawczej.

9. OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI

9.1 Zbiór „Pracownicy i umowy cywilnoprawne"

System informatyczny	Zawartość pól informacyjnych
Katalog personalny	Imiona i nazwisko, imiona rodziców, nazwisko rodowe, data urodzenia, obywatelstwo, PESEL, NIP, miejsce zameldowania, adres zamieszkania, adres do korespondencji, informacja o stopniu niepełnosprawności, wykształcenie, zawód, przebieg dotychczasowego zatrudnienia, dodatkowe uprawnienia, zainteresowania, stan rodziny (imiona i nazwiska oraz daty urodzenia dzieci), osoba, którą należy powiadomić w razie wypadku (imię, nazwisko, adres i telefon), nr i seria dowodu osobistego, dane osoby ubezpieczonej (PESEL, NIP, nr i seria dowodu osobistego, imię i nazwisko, data urodzenia, stopień pokrewieństwa, informacja o stopniu niepełnosprawności, adres zamieszkania), nr rachunku bankowego

Podstawa prawna przetwarzania danych: art. 6 ust. 1 lit. c) Rozporządzenia ogólnego.

Opiekun Zbioru (Opiekunowie Zbioru): Paulina Czaja, Przemysław Kurylas

Okres przechowywania danych: zgodnie z rozporządzeniem Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. 1996.62.286) po ustaniu zatrudnienia obowiązek przechowywania dokumentacji pracowniczej (akt osobowych) przez 50 lat, licząc od dnia zakończenia pracy.

Podmioty, którym przekazywane są dane osobowe:

- Zakład Ubezpieczeń Społecznych,
- Urząd Skarbowy,
- Fitsport Polska Sp. z o.o. (karty Multisport),
- Lux Med Sp. z o.o. (opieka medyczna),
- Centrum Medyczne ENEL-MED S.A. (opieka medyczna)
- Nationale Nederlanden Towarzystwo Ubezpieczeń na Życie S.A.,
- Przewoźnicy w celu rezerwacji/zakupu biletów podróżnych, hotelom w celu rezerwacji zakwaterowania podczas podróży służbowych,
- AFK Centrum Obsługi Biznesu Sp. z o.o. w celach obsługi kadrowo-płacowej,
- Kontrahenci w ramach realizacji usług przez DB Energy SA i dla DB Energy SA w celu wykonywania obowiązków pracowniczych,
- Narodowe Centrum Badań i Rozwoju w ramach projektu nr POIR.01.01.01-00-1561/15,
- Europejski Fundusz Leasingowy SA – upoważnienia do wyjazdów zagranicznych w ramach leasingowanych aut służbowych,
- Towarzystwa ubezpieczeń komunikacyjnych w ramach likwidacji szkód komunikacyjnych.

Ocena skutków dla ochrony danych: działalność Spółki w zakresie przetwarzania danych z tego zbioru nie spełnia rygorów określonych w art. 35 ust. 1 i 3 Rozporządzenia ogólnego.

Opis zbioru: Dane z opisywanego zbioru obejmują informacje o byłych i aktualnych pracownikach etatowych Spółki, a także osobach, które wykonują na jej rzecz czynności na podstawie umów cywilnoprawnych (umowy zlecenia, umowy o dzieło, umowy o świadczenie usług). Czynności związane z prowadzeniem dokumentacji pracowników prowadzone są przez AFK Centrum Obsługi

Biznesu Sp. z o.o. Spółka DB Energy nie posiada wewnętrznej obsługi księgową oraz kadrowo-płacowej, w związku z tym powierza przetwarzanie tych danych podmiotom trzecim w tym zakresie.

9.2 Zbiór „Kandydaci do pracy"

System informatyczny	Zawartość pół informacyjnych
Program pocztowy /webmail	Imiona i nazwisko, data urodzenia, adres zamieszkania, adres do korespondencji, wykształcenie, zawód, przebieg dotychczasowego zatrudnienia, dodatkowe uprawnienia, zainteresowania, wizerunek, adres IP

Podstawa prawna przetwarzania danych: art. 6 ust. 1 lit. a) Rozporządzenia ogólnego.

Opiekun Zbioru (Opiekunowie Zbioru): Paulina CzajaMonika Pacuła, Przemysław Kurylas.

Podmioty, którym przekazywane są dane osobowe: dane z tego zbioru nie są przekazywane innym podmiotom.

Okres przechowywania zbioru: dane przechowywane na potrzeby danej rekrutacji, w przypadku wyrażenia zgody przez kandydata na przetwarzane danych osobowych na poczet przyszłych rekrutacji, dane są przechowywane przez okres 6 miesięcy.

Ocena skutków dla ochrony danych: działalność Spółki w zakresie przetwarzania danych z tego zbioru nie spełnia rygorów określonych w art. 35 ust. 1 i 3 Rozporządzenia ogólnego.

Opis zbioru: Dane zbierane w celu prowadzenia procesu rekrutacji. Dane pozyskiwane są za pośrednictwem portali internetowych (np. Pracuj.pl, infopraca.pl Gazeta) oraz firm headhunterskich. Dane te przesyłane są na ogólnego maila: biuro@dbenergy.pl.

9.3 Zbiór „Akcjonariusze i Rada Nadzorcza"

System informatyczny	Zawartość pól informacyjnych
katalog personalny	Imiona i nazwisko, imiona rodziców, nazwisko rodowe, data urodzenia, obywatelstwo, PESEL, NIP, miejsce zameldowania, adres zamieszkania, adres do korespondencji osoba, którą należy powiadomić w razie wypadku (imię, nazwisko, adres i telefon), nr i seria dowodu osobistego, nr rachunku bankowego

Podstawa prawna przetwarzania danych: przetwarzanie jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa: Dz.U.2013.0.1030 t.j. Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych, art. 341. Przetwarzanie jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa:

Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych (Dz. U. Nr 94, poz. 1037 z późn. zm.). Dane osobowe przetwarzane są na podstawie art. 6 ust. 1 b) RODO, art. 6 ust. 1 c) RODO

Opiekun Zbioru (Opiekunowie Zbioru): Paulina Czaja, Monika Pacuła

Podmioty, którym przekazywane są dane osobowe: Sądy oraz właściwe organy administracji publicznej

Okres przechowywania zbioru: Przez okres pozostawania akcjonariuszem, członkiem rady nadzorczej, a po jego zakończeniu przez okres przedawnienia roszczeń jaki może podnieść ADO oraz jakie mogą być podniesione przeciwko ADO, a także przez okres niezbędny do ochrony praw i interesów ADO.

Ocena skutków dla ochrony danych: działalność Spółki w zakresie przetwarzania danych z tego zbioru nie spełnia rygorów określonych w art. 35 ust. 1 i 3 Rozporządzenia ogólnego.

Opis zbioru: Akcjonariusze i członkowie Rady Nadzorczej DB Energy SA. Dane zbierane w celu prowadzenia księgi akcyjnej. Prowadzenie ewidencji członków Rady Nadzorczej. Osoby prawne oraz osoby fizyczne

a) Zbiór „Dane kontaktowe"

System informatyczny	Zawartość pól informacyjnych
Program pocztowy/ webmail, System Wfirma.pl,Microsoft Office	Imię i nazwisko, adres e-mail, stanowisko służbowe, Numer telefonu

Ponadto w zbiorze tym przetwarzane są następujące dane (wizytówki, foldery reklamowe, osoby kontaktowe wpisane w umowach, etc.):

- Imię i nazwisko
- Miejsce pracy
- Stanowisko służbowe
- Adres e-mail
- Nr telefonu

Podstawa prawna przetwarzania danych: art. 6 ust. 1 lit. f) Rozporządzenia ogólnego.

Opiekun Zbioru (Opiekunowie Zbioru): w przypadku tego zbioru nie wyznacza się Opiekuna Zbioru.

Okres przechowywania: okres 3 lat od zakończenia współpracy z danym kontrahentem, a w przypadku osób fizycznych okres 10 lat.

Podmioty, którym przekazywane są dane osobowe: dane z tego zbioru nie są przekazywane innym podmiotom.

Ocena skutków dla ochrony danych: działalność Spółki w zakresie przetwarzania danych z tego zbioru nie spełnia rygorów określonych w art. 35 ust. 1 i 3 Rozporządzenia ogólnego.

Opis zbioru: Na opisywany zbiór składają się dane kontaktowe osób z różnych firm, zbierane poprzez wymienianie się wizytówkami, dane z umów, które zawiera Spółka, kontakty osobiste etc. Są to dane niezbędne do wykonywania codziennych obowiązków służbowych. Dane te przetwarzane są w formie tradycyjnej (np. wizytówki) oraz elektronicznej, przede wszystkim przy pomocy programu pocztowy.

b) Zbiór „Ewidencja korespondencji wychodzącej/przychodzącej"

System informatyczny	Zawartość pól informacyjnych
Pocztowa książka nadawcza	Imię i nazwisko, stanowisko służbowe, adres, miejsce pracy

W tym zbiorze zbierane są dane w następującym zakresie:

- Imię i nazwisko
- Miejsce pracy
- Stanowisko służbowe
- Adres korespondencyjny

Podstawa prawna przetwarzania danych: art. 6 ust. 1 lit. f) Rozporządzenia ogólnego.

Opiekun Zbioru (Opiekunowie Zbioru): Paulina Czaja, Monika Paculа

Okres przechowywania: okres 3 lat od zakończenia współpracy z danym kontrahentem, a w przypadku osób fizycznych okres 10 lat.

Podmioty, którym przekazywane są dane osobowe: dane z tego zbioru nie są przekazywane innym podmiotom.

Ocena skutków dla ochrony danych: działalność Spółki w zakresie przetwarzania danych z tego zbioru nie spełnia rygorów określonych w art. 35 ust. 1 i 3 Rozporządzenia ogólnego.

Opis zbioru: W zbiorze tym znajdują się dane osobowe osób, do których i od których przychodzi korespondencja. Dane te przetwarzane są w formie papierowej przez pocztową książkę nadawczą.

9. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI DANYCH OSOBOWYCH

9.1. Środki ochrony fizycznej (Biuro Spółki)	1. Żeby dostać się do budynku biura Spółki niezbędne jest rozbrojenie alarmu. Wejście do biura otwierane jest przez system kart magnetycznych/kluczy. 2. Budynki, w których znajduje się Biuro są nadzorowane przez monitoring zewnętrzny firmy ochroniarskiej. 3. Monitoring przy wejściu/wyjściu Biura. 4. Niepotrzebne dokumenty zawierające dane osobowe są niszczone przy pomocy niszczarek, oraz dodatkowo utylizowane za pośrednictwem specjalistycznych firm.

9.2. Środki ochrony fizycznej (serwerownia)	1. Spółka posiada umowę z firmą nazwa.pl na świadczenie usług hostingowych; 2. Spółka posiada wewnętrzny serwer znajdujący się w Biurze Spółki 3. Serwerownia stanowi wydzielone pomieszczenie z limitowanym dostępem dla upoważnionych osób. 4. Serwerownia wyposażona jest w system ppoż 5. Serwerownia jest klimatyzowana w celu zapewnienia odpowiedniej temperatury dla urządzeń. 6. Serwery podpięte są do UPS'ów. Administracja budynku prowadzi rejestr osób pobierających i oddających klucze do pomieszczenia. Klucz do serwerowni posiada Paulina Czaja .
9.3. Środki ochrony logicznej serwerów	1. Serwery zabezpieczone są poprzez system LINUX. 2. Filtrowany jest ruch przychodzący i wychodzący na routerach. 3. Serwery pocztowe zabezpieczone są systemem antywirusowym i antyspamowym firmy Microsoft. 4. Serwery pracują pod kontrolą na bieżąco aktualizowanych systemów takich jak QTS LINUX-. 5. Logowanie do systemów spoza Spółki odbywa się za pośrednictwem szyfrowanych połączeń VPN i SSL. 6. Pliki z serwera sieciowego podlegają regularnym backupom oraz wykonywane są kopie przyrostowe 7. Kopie zapasowe wykonywane są jeden raz w tygodniu przez informatyka, wykonywane są z serwera roboczego na zapasowy i przechowywane są na serwerach (roboczym i zapasowym). 8. W przypadku awarii system gwarantuje możliwość odtworzenia danych sprzed awarii.
9.4 Środki ochrony w ramach oprogramowania systemów oraz narzędzi i programów służących do przetwarzania danych osobowych	1. W Spółce stosowane jest Active Directory umożliwiające nadawanie różnych poziomów uprawnień w oparciu o grupy. 2. Logowanie do Active Directory wymaga uwierzytelnienia poprzez podanie loginu i hasła składającego się z minimum 8 znakowym będących kombinacją trzech z pośród czterech grup znakowych: wielkich i małych liter i cyfr. 3. W każdym systemie informatycznym wymagane jest osobne uwierzytelnienie poprzez podanie indywidualnie nadanego loginu i wpisania hasła. 4. Wszystkie komputery zostały wyposażone w programy antywirusowe. Na zewnętrz widoczny jest 1 adres IP.

9.5 Środki organizacyjne stosowane przez firmę w celu ochrony danych osobowych	1. Każda osoba mająca dostęp do danych została zapoznana z zasadami bezpiecznego przetwarzania danych wynikającymi z niniejszej Polityki oraz Instrukcji Zarządzania. 2. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe posiadają tylko osoby upoważnione. 3. Dostęp do komputerów na których są przetwarzane dane osobowe posiadają tylko osoby upoważnione. 4. Osoby mające dostęp do danych osobowych zobowiązane są, na mocy niniejszej Polityki, do zachowania danych osobowych oraz informacji o sposobach ich zabezpieczenia w tajemnicy. 5. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych. 6. Prowadzona jest ewidencja przekazywania sprzętu. 7. Prowadzona jest dokumentacja obejmująca Politykę Bezpieczeństwa oraz Instrukcję Zarządzania. 8. Osoby przetwarzające dane osobowe zostały przeszkolone z zasad przetwarzania, prawnych regulacji dotyczących danych osobowych, oraz wszelkich konsekwencji niezgodnego z prawem przetwarzania danych.

10. WDROŻENIE ZASAD „PRIVACY BY DESIGN" ORAZ „PRIVACY BY DEFAULT"

10.1. Obowiązek uwzględnienia ochrony danych osobowych w fazie projektowania (privacy by design)– ADO wdroży odpowiednie środki organizacyjne i techniczne w momencie ustalania sposobów przetwarzania danych, oraz w trakcie samego procesu przetwarzania, poprzez w szczególności:

a) pseudonimizację

b) minimalizację danych

c) integrację niezbędnych zabezpieczeń

Prywatność ma być wbudowana w projekt, transparentność przejrzystość, poszanowanie prywatności użytkowników.

Prywatność w fazie projektowania opiera się na siedmiu następujących zasadach:

1. podejściu proaktywnym, a nie reaktywnym i zaradczym, ani naprawczym – zapobieganie powstawaniu naruszeń i eliminowanie zidentyfikowanych zagrożeń w celu zapobieżenia naruszeniu praw i wolności osób, których dane dotyczą;

2. prywatności jako ustawieniu domyślnym – zasada minimalizacji danych;

3. prywatności włączonej w projekt – prywatność jako część składowa każdego projektu, wbudowana w narzędzia, procesy i procedury;

4. pełnej funkcjonalności rozumianej jako suma dodatnia, a nie suma zerowa – bezpieczeństwo danych i poszanowanie prywatności mają być podstawą funkcjonowania

każdego procesu i na każdym jego etapie aż do usunięcia danych lub likwidacji procesu – ciągłość ochrony;

5. ochronie od początku do końca cyklu życia informacji;

6. transparentność i przejrzystość – podanie osobie której dane dotyczą pełnego zestawu informacji;

7. poszanowanie dla prywatności użytkowników – istotą jest kontrola nad danymi i swoboda w określeniu granic ingerencji w prywatność i zapewnienie osobie której dane dotyczą realizacji tych praw.

10.2. Obowiązek uwzględnienia ochrony danych osobowych w drodze domyślnej ochrony danych (privacy by default) – ADO wdraża odpowiednie środki aby domyślnie były przetwarzane tylko te dane, które są niezbędne z punktu widzenia konkretnego celu przetwarzania. Dotyczy to:

a) Ilości zbieranych danych,

b) Zakresu przetwarzania;

c) Okresu przetwarzania

d) Dostępności danych

W Spółce obowiązki te zostały spełnione poprzez przede wszystkim minimalizację pozyskiwanych przez Spółkę danych osobowych (np. zbieranie danych od pracowników jedynie w zakresie jaki pozwala Spółce wywiązać się ze spoczywających na niej obowiązków jako pracodawcy), jak również skrócenie okresu ich przetwarzania do niezbędnego minimum, uwzględniając konieczność niezakłóconego prowadzenia działalności przez Spółkę w celu osiągania zysków finansowych (np. przez okres niezbędny do obsługi roszczeń – okres przedawnienia).

11. ŚCIEŻKA POSTĘPO WANIA W PRZYPADKU OTRZYMANIA WNIOSKU INFORMACYJNEGO OD OSOBY KTÓREJ DANE DOTYCZĄ:

11.1 W przypadku otrzymania przez ADO wniosku od osoby, której dane dotyczą w trybie art. 15 Rozporządzenia ogólnego tj. wniosku o uzyskanie od ADO potwierdzenia czy dotyczące jej dane osobowe są przetwarzane przez, a jeśli tak – o uzyskanie dostępu do tych danych oraz informacji o:

a) celach przetwarzania,

b) kategoriach przetwarzanych danych osobowych,

c) czasie, przez który dane mają być przechowywane lub kryteriach przyjętych do ustalania tego okresu,

d) odbiorcach, którym dane zostały lub zostaną ujawnione (w szczególności w państwach trzecich),

e) przysługujących uprawnieniach do żądania od ADO sprostowania, usunięcia, ograniczenia przetwarzania danych, wniesienia sprzeciwu wobec przetwarzania, wniesienia skargi do UODO;

f) podejmowaniu przez ADO zautomatyzowanych decyzji (w tym profilowaniu).

11.2 Osoba której dane dotyczą ma prawo do wystąpienia z wnioskiem do ADO w każdym czasie, niezależnie od naruszenia przez ADO przepisów Rozporządzenia ogólnego. Prawo osoby do złożenia wniosku nie ulega przedawnieniu.

11.3 W przypadku gdy wskutek realizacji żądania osoby, której dane dotyczą nie ma zagrożenia naruszenia praw i wolności innych osób, których dane ADO przetwarza, ADO ma obowiązek udzielić w/w informacji, jak również dostarczyć kopii danych osobowych podlegających przetwarzaniu.

11.4 Osoba której dane dotyczą ma prawo do wystąpienia z wnioskiem do ADO w każdym czasie, niezależnie od naruszenia przez ADO przepisów Rozporządzenia ogólnego. Prawo osoby do złożenia wniosku nie ulega przedawnieniu.

11.5 W przypadku otrzymania wniosku informacyjnego od osoby, której dane dotyczą, każdy Użytkownik, do którego wpłynął taki wniosek, jest zobowiązany do poinformowania o tym fakcie ADO (lub IODO jeśli został powołany), bez zbędnej zwłoki, nie później jednak niż w ciągu 24 godzin od otrzymania wniosku

11.6 ADO (lub IODO) weryfikuje czy dane osoby, która wystąpiła z wnioskiem są przez niego przetwarzane i niezwłocznie informuje osobę o tym fakcie.

11.7 W przypadku gdy dane osoby są przetwarzane przez ADO, a osoba zażądała od ADO udzielenia jej informacji określonych w 12.1. powyżej lub kopii danych, ADO niezwłocznie przekazuje wniosek drogą mailową informatykowi.

11.8 Inspektor Danych Osobowych sporządza raport (wzór raportu stanowi Załącznik nr 6 do niniejszej Polityki) zawierający kopie danych oraz/lub informacje, których podania zażądała osoba, a następnie przesyła raport ADO. Po uzyskaniu akceptacji raportu przez ADO przekazuje raport osobie, która zwróciła się z wnioskiem niezwłocznie, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku od osoby, której dane dotyczą. Raport powinien mieć taką formę jakiej zażądała osoba zwracająca się z wnioskiem

(papierowa/elektroniczna). W przypadku gdy osoba złożyła wniosek w formie elektronicznej, ADO udostępnia dane i w/w informacje również w takiej formie, chyba że osoba której dane dotyczą zażąda innej formy. ADO może przedłużyć ten termin o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań, pod warunkiem poinformowania osoby, której dane dotyczą o takim przedłużeniu terminu z podaniem przyczyn opóźnienia. Jeśli ADO nie podejmuje działań o których mowa, informuje o tym osobę której dane dotyczą o powodach niepodjęcia działań oraz możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem – wzór takiej informacji stanowi Załącznik nr 8.

11.9 Pierwsze udostępnienie danych osobie, której dane dotyczą, jak również pierwsze przekazanie ich kopii jest wolne od kosztów. W przypadku ponownego zwrócenia się tej samej osoby do ADO z podobnym wnioskiem, ADO jest uprawniony (choć nie zobligowany) do pobrania z tego tytułu stosownej opłaty, w wysokości określonej przez ADO, nie przekraczającej jednak rozsądnej wysokości opłaty wynikającej z kosztów administracyjnych ponoszonych w celu odpowiedzi na wniosek. ADO może uzależnić przekazanie kopii danych lub ich udostepnienie od wcześniejszego otrzymania od osoby, której dane dotyczą opłaty, o której mowa. ADO informuje osobę o możliwości kwestionowania w/w opłaty w drodze skargi do organu nadzorczego.

11.10 Jeżeli ADO ma uzasadnione wątpliwości co do tożsamości osoby składającej żądanie, może zażądać dodatkowych informacji niezbędnych dla potwierdzenia tożsamości tej osoby.

12. ŚCIEŻKA POSTĘPOWANIA W PRZYPADKU OTRZYMANIA WNIOSKU O SPROSTOWANIE DANYCH, USUNIĘCIE LUB OGRANICZENIE PRZETWARZANIA:

12.1 W przypadku otrzymania przez ADO wniosku od osoby, której dane dotyczą w trybie art. 16 Rozporządzenia ogólnego tj. wniosku o sprostowanie dotyczących jej danych osobowych lub ich uzupełnienia, ADO niezwłocznie przekazuje informację do Opiekuna Zbioru, który dokonuje w systemie sprostowania danych osobowych osoby w zakresie w jakim osoba, której dane dotyczą żąda sprostowania. ADO niezwłocznie, w terminie nie dłuższym jednak niż jeden miesiąc od dnia otrzymania wniosku przesyła osobie, której dane dotyczą potwierdzenie sprostowania dotyczących jej danych osobowych. ADO może przedłużyć ten termin o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań, pod warunkiem poinformowania osoby, której dane dotyczą o takim przedłużeniu terminu z podaniem przyczyn opóźnienia. Jeśli ADO nie podejmuje działań o których mowa, informuje o tym osobę której dane dotyczą o powodach niepodjęcia działań oraz możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem – wzór takiej informacji stanowi Załącznik nr 8.

12.2. W przypadku gdy osoba, której dane dotyczą zażądała uzupełnienia niekompletnych danych osobowych, ADO niezwłocznie przekazuje żądanie do Opiekuna Zbioru, który dokonuje takiego uzupełnienia. W przypadku gdy przetwarzanie danych osobowych, o które osoba której dane dotyczą dokonuje uzupełnienia wymaga zgody takiej osoby – ADO odbiera taką zgodę zgodnie z art. 6 ust. 1 a) Rozporządzenia ogólnego (w przypadku danych szczególnych kategorii – zgodnie z art. 9 ust. 1 a)) oraz zgodnie z art. 7 Rozporządzenia

ogólnego tj. zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, pod rygorem uznania oświadczenia za niewiążące.

12.3 W przypadku otrzymania przez ADO wniosku od osoby, której dane dotyczą w trybie art. 17 Rozporządzenia ogólnego tj. wniosku o usunięcie danych („prawo do bycia zapomnianym") ADO ma obowiązek niezwłocznie usunąć te dane jeśli:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b) osoba, której dane dotyczą cofnął zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
c) osoba, której dane dotyczą wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
d) dane osobowe były przetwarzane niezgodnie z prawem;
e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego

Jeśli nie zachodzi żadna w okoliczności wymienionych w ppkt. a) – d) poniżej, ADO niezwłocznie usuwa dane osobowe osoby która zwróciła się z takim wnioskiem, w terminie nie dłuższym jednak niż jeden miesiąc od dnia otrzymania wniosku. ADO może przedłużyć ten termin o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań, pod warunkiem poinformowania osoby, której dane dotyczą o takim przedłużeniu terminu z podaniem przyczyn opóźnienia. Jeśli ADO nie podejmuje działań o których mowa, informuje o tym osobę której dane dotyczą o powodach niepodjęcia działań oraz możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem – wzór takiej informacji stanowi Załącznik nr 8. W przypadku gdy ADO upublicznił dane osobowe dotyczące tej osoby, w szczególności przekazał dane podmiotom trzecim (w tym podmiotom określonym w liście firm, którym Spółka powierzyła przetwarzanie danych osobowych sporządzonej zgodnie z Załącznikiem nr 4 do niniejszej Polityki) Spółka ma obowiązek poinformować takich administratorów przetwarzających (procesorów), że osoba, której dane dotyczą złożyła wniosek o usunięcie dotyczących jej danych osobowych i zażądać od procesorów usunięcia wszelkich łączy do tych danych, kopii tych danych osobowych oraz ich replikacji. Procesorzy powinni poinformować ADO (Spółkę) o wykonaniu takiego żądania w terminie nie później niż 7 dni od dnia otrzymania od ADO żądania, o którym mowa. ADO ma obowiązek usunąć dane dotyczące osoby występującej z wnioskiem biorąc pod uwagę dostępną technologię i koszt realizacji, w szczególności usunięcia wszelkich łączy do tych danych, kopii tych danych osobowych oraz ich replikacji.

Spółka ma prawo do odmowy usunięcia danych osobowych w przypadku gdy:

a) przetwarzanie danych jest niezbędne do korzystania z prawa do wolności wypowiedzi
b) informacji;
c) wywiązania się z prawnego obowiązku przez ADO;
d) do celów archiwalnych w interesie publicznym;
e) do ustalenia, dochodzenia lub obrony roszczeń przez ADO

12.4 W każdym przypadku, ADO informuje osobę, która zwróciła się do Spółki z wnioskami określonymi w niniejszym punkcie, o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, których dokonał, chyba że okaże się to niemożliwe. Jeżeli ADO ma uzasadnione wątpliwości co do tożsamości osoby składającej żądanie, może zażądać dodatkowych informacji niezbędnych dla potwierdzenia tożsamości tej osoby.

13. POSTĘPOWANIE W PRZYPADKU OTRZYMANIA ŻĄDANIA PRZENIESIENIA DANYCH

13.1 Jeżeli przetwarzanie danych odbywa się na podstawie zgody (art. 6 ust.1 lit. a) oraz art. 9 ust. 2 lit. a)) lub na podstawie umowy (art. 6 ust. 1 lit. b)), każda osoba, której dane dotyczą ma prawo do otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące które posiada ADO, oraz ma prawo przesłać dane innemu administratorowi bez przeszkód ze strony ADO.

13.2 Jeśli wykonanie żądania osoby które dane dotyczą nie wpływa niekorzystnie na prawa i wolności innych osób, ADO zobowiązany jest spełnić takie żądanie w terminie jednego miesiąca od dnia jego otrzymania. ADO może przedłużyć ten termin o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań, pod warunkiem poinformowania osoby ,której dane dotyczą o takim przedłużeniu terminu z podaniem przyczyn opóźnienia. Jeśli ADO nie podejmuje działań o których mowa, informuje o tym osobę której dane dotyczą o powodach niepodjęcia działań oraz możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem – wzór takiej informacji stanowi Załącznik nr 8.

13.3 ADO zobowiązany jest zapewnić wszelkie środki techniczne w celu wykonania takiego żądania.

14. POSTĘPOWANIE W PRZYPADKU WNIESIENIA SPRZECIWU PRZEZ OSOBĘ, KTÓREJ DANE DOTYCZĄ

14.1 Osoba, której dane dotyczą ma prawo wniesienia sprzeciwu do ADO wobec przetwarzania dotyczących jej danych osobowych na podstawie art. 6 ust. 1 lit. e) lub f) przy czym Spółka przetwarza dane osobowe na podstawie art. 6 ust. 1 lit. f) w zakresie następujących zbiorów danych osobowych: Zbiór „Baza CRM", Zbiór „Dane kontaktowe", Zbiór „Ewidencja korespondencji przychodzącej/wychodzącej". W przypadku otrzymania sprzeciwu od osoby, której dane dotyczą, ADO nie wolno już przetwarzać tych danych osobowych, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

14.2 Spółka nie stosuje marketingu bezpośredniego.

14.3 W przypadku otrzymania wniosku informacyjnego od osoby, której dane dotyczą, każdy Użytkownik, do którego wpłynął taki wniosek, jest zobowiązany do poinformowania o tym fakcie ADO (lub IODO jeśli został powołany), bez zbędnej zwłoki, nie później jednak niż w ciągu 24 godzin od otrzymania wniosku.

14.4 ADO powinien przy okazji pierwszej komunikacji z osobą, której dane dotyczą wyraźnie poinformować ją o prawie wniesienia sprzeciwu w sposób wyraźnie odróżniający tą informację od wszelkich innych informacji. Wzór takiej informacji stanowi Załącznik nr 9.

15. POSTĘPOWANIE W PRZYPADKU STWIERDZENIA INCYDENTU

15.1. W przypadku stwierdzenia naruszenia ochrony danych osobowych (incydentu), osoba stwierdzająca naruszenie jest zobowiązana do natychmiastowego zgłoszenia tego naruszenia ADO (lub IODO jeśli został powołany).

15.2. Zgłoszenie, o którym mowa musi opisywać charakter naruszenia, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie, jak również opisywać możliwe konsekwencje naruszenia ochrony danych osobowych.

15.3. Po otrzymaniu zgłoszenia, ADO dokonuje oszacowania konsekwencji jakie mogą nastąpić wskutek naruszenia, jak również stosuje wszelkie środki jakie mogą zaradzić naruszeniu i zminimalizować jego ewentualne negatywne skutki.

15.4. ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu. Raport o sytuacji naruszenia bezpieczeństwa danych osobowych stanowi Załącznik nr 7.

15.5. Obowiązek zgłaszania naruszeń, o których mowa ciąży na każdym Użytkowniku.

15.6. Każdy Użytkownik zapoznał się ze stosowaną w Spółce procedurą postępowania w przypadku wystąpienia naruszenia – system reakcji na incydenty – wzór oświadczenia stanowi Załącznik nr 1.

15.7. ADO podejmuje decyzję o zgłoszeniu danego naruszenia do właściwego organu nadzorczego w trybie Artykułu 33 Rozporządzenia ogólnego tj. ADO dokonuje zgłoszenia organowi nadzorczemu bez zbędnej zwłoki, w terminie 72 godzin po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

15.8. ADO podejmuje decyzję o zawiadomieniu osoby, której dane dotyczą o naruszeniu, takie zawiadomienie jest obowiązkowe jeżeli naruszenie danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osoby fizycznej. W zawiadomieniu ADO podaje osobie, której dane dotyczą informacje i środki, o których mowa w pkt. 15.2 powyżej.

16. PRZEGLĄDY POLITYKI BEZPIECZEŃSTWA I AUDYTY

16.1. Aktualizacja

16.1.1. Aktualizacji niniejszej Polityki Bezpieczeństwa Danych Osobowych dokonuje ADO.

16.1.2. Opiekunowie Zbiorów mają obowiązek współpracować z ADO, zwłaszcza w odniesieniu do aktualności informacji dotyczących systemów informatycznych, zakresów danych, Procesorów, etc. Informacje mające wpływ na aktualność Polityki Bezpieczeństwa Danych Osobowych powinny być przekazywane do ADO (drogą mailową) najdalej w ciągu 7 dni od okoliczności uzasadniających dokonanie zmiany, z zastrzeżeniem, że umowy powierzenia powinny być przedstawiane do zaopiniowania/stworzenia przed rozpoczęciem współpracy z potencjalnym Procesorem.

16.1.3. Niniejsza Polityka Bezpieczeństwa Danych Osobowych powinna być poddawana przeglądowi przynajmniej raz w roku. W razie istotnych zmian dotyczących przetwarzania danych osobowych ADO może zarządzić przegląd Polityki Bezpieczeństwa stosownie do występujących sytuacji i zdarzeń.

16.1.4. ADO analizuje, czy Polityka Bezpieczeństwa Danych Osobowych i Instrukcja Zarządzania oraz inne dokumenty, powiązane z nimi są adekwatne do:
zmian w budowie systemu informatycznego,
zmian organizacyjnych Administratora Danych,
zmian w obowiązującym prawie,
innych zmian, które mogą mieć wpływ na bezpieczeństwo danych.

16.2. Audyty

16.2.1. Raz do roku ADO przeprowadza audyt wewnętrzny, mający na celu ustalenie stopnia zgodności działalności Spółki z Rozporządzeniem ogólnym, Ustawą, Rozporządzenie i Przepisami szczególnymi.

16.2.2. Oprócz audytu, o którym mowa, ADO może zarządzić audyt ad hoc, a w przypadku zaistnienia incydentu mającego wpływ na bezpieczeństwo danych osobowych – zarządza obowiązkowo taki audyt.

17. POSTANOWIENIA KOŃCOWE

a. Z treścią niniejszej Polityki Bezpieczeństwa Danych Osobowych i jej załącznikami powinni zapoznać się wszyscy Użytkownicy (w tym Opiekunowie Zbiorów), których obowiązki służbowe wiążą się z koniecznością dostępu do danych osobowych i ich przetwarzaniem.

b. Naruszenie postanowień niniejszej Polityki Bezpieczeństwa Danych Osobowych przez osoby zatrudnione w Spółce (bez względu na formę umowy) może skutkować koniecznością rozwiązania stosownej umowy (w przypadku pracowników etatowych naruszenie jej postanowień może zostać uznane za ciężkie naruszenie obowiązków pracowniczych w rozumieniu przepisów kodeksu pracy).

c. Niniejszą Politykę Bezpieczeństwa Danych Osobowych i jej załączniki można przedstawiać partnerom lub innym podmiotom współpracującym ze Spółką na podstawie pisemnej zgody udzielonej przez ADO.

d. Niniejsza Polityka Bezpieczeństwa Danych Osobowych wchodzi w życie z dniem jej podpisania przez ADO.

18. WYKAZ ZAŁĄCZNIKÓW

- Załącznik nr 1 – oświadczenie o zapoznaniu się z systemem ochrony danych osobowych oraz o zachowaniu danych osobowych i sposobów ich zabezpieczenia w tajemnicy, jak również systemem reakcji na incydenty
- Załącznik nr 2 - wzór umowy powierzenia przetwarzania danych osobowych
- Załącznik nr 3 – ewidencja udostępnionych danych osobowych
- Załącznik nr 4 – lista firm, którym Spółka powierza przetwarzanie danych osobowych
- Załącznik nr 5 – wzór zgody na przebywanie w obszarze przetwarzania danych osobowych
- Załącznik nr 6 – wzór raportu odnośnie spełnienia obowiązku informacyjnego

- Załącznik nr 7 - wzór raportu o sytuacji naruszenia bezpieczeństwa danych osobowych
- Załącznik nr 8 – wzór informacji o niemożności spełnienia żądania osoby, której dane dotyczą
- Załącznik nr 9 – wzór informacji o prawie wniesienia sprzeciwu