POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Spis treści

Rozdział 1 - Podstawa prawna

Niniejsza Polityka Bezpieczeństwa została sporządzona w oparciu o 78 motyw i art. 24 ust. 2 rozporządzenia 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, w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącym zasad przetwarzania i zabezpieczenia danych osobowych.

Rozdział 2 - Definicje

Ilekroć w niniejszym dokumencie zostaną użyte poniższe określenia należy je rozumieć w sposób następujący:

2.1 **Polityka Bezpieczeństwa (dalej również jako: „Polityka")** – niniejszy dokument.

2.2 **RODO** – 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,

2.3 **Administrator Danych Osobowych –** Amex Coal Sp. z o.o. z siedzibą w Sopocie (dalej jako: **ADO**).

2.4 **Dane osobowe** – 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;

2.5 **Zbiór danych osobowych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

2.6 **Przetwarzanie danych osobowych** - 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, powierzenie przetwarzania danych osobowych następuje na podstawie umowy, lub podobnego instrumentu,

2.7 **Dane wrażliwe –** dane genetyczne, biometryczne, dotyczące stanu zdrowia, ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, nałogach, życiu seksualnym, dane dotyczące skazań, orzeczeń o ukaraniu i mandatach karnych oraz inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym.

2.8 **Instrukcja –** dokument: „Instrukcja zarządzania systemami informatycznymi i urządzeniami przenośnymi służącymi do przetwarzania danych osobowych".

2.9 **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

2.10 **Osoba upoważniona –** osoba zatrudniona przez ADO z lub wykonująca zadania w ramach zawartych z ADO umów cywilnoprawnych, posiadająca pisemne upoważnienie do przetwarzania danych osobowych nadane przez ADO,

2.11 **Odbiorca danych osobowych –** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

2.12 **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu ADO.

2.13 **Usuwanie danych** – niszczenie danych osobowych lub ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

2.14 **Zabezpieczanie danych** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przed ich nieuprawnionym przetwarzaniem.

2.15 **Zgoda osoby, której dane dotyczą –** 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.

Rozdział 3 – Administrator Danych Osobowych

3.1 ADO realizuje Politykę Bezpieczeństwa w celu ochrony interesów osób, których dane osobowe dotyczą, a w szczególności zapewnia, aby dane te były przetwarzane zgodnie z prawem, w szczególności zgodnie z RODO i przepisami krajowymi, w tym zgodnie z zasadami: *privacy by design*, *privacy by default*, celowości, integralności, poufności, rozliczalności, ograniczenia celu przetwarzania danych osobowych, merytorycznej poprawności, ograniczenia przechowywania,

3.2 ADO ma obowiązek zapewnić oraz stosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

3.3 ADO sprawuje kontrolę nad przetwarzaniem danych osobowych zgodnie z RODO oraz wytycza kierunki zmierzające do zapewnienia odpowiedniej ochrony danych osobowych oraz nadzoruje przestrzeganie ustalonych zasad przetwarzania danych osobowych.

3.4 ADO określa zakres i warunki przetwarzanych danych osobowych w wydawanych zarządzeniach, regulaminach lub w indywidualnych umowach z podmiotami zewnętrznymi, którym powierzono przetwarzanie danych osobowych w imieniu ADO.

3.5 ADO:

3.5.1 podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, oraz technik zabezpieczania danych osobowych,

3.5.2 zapewnia kontrolę nad tym jakie dane osobowe, kiedy i przez kogo zostały do zbioru danych osobowych wprowadzone oraz komu są przekazywane,

3.5.3 wyznacza IDO, w przypadku gdy taki obowiązek wynika z przepisów prawa lub gdy uzna, że jest to uzasadnione; ADO może wyznaczyć IDO, określić zakres jego zadań i czynności,

3.5.4 inicjuje postępowania dyscyplinarne i karne w przypadku stwierdzonych naruszeń ochrony danych osobowych,

3.5.5 jako że przetwarzanie danych osobowych nie ma charakteru sporadycznego i potencjalnie może wiązać się z ryzykiem naruszenia praw i wolności osób, których dane są przetwarzane - prowadzi rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania, których wzory stanowią załącznik nr 15 oraz 16 do Polityki.

Rozdział 4 – Osoby Upoważnione

4.1. Do przetwarzania danych osobowych uprawniona jest jedynie osoba, która:

4.1.1. zapoznała się z przepisami prawa powszechnie obowiązującego oraz wewnątrzzakładowymi przepisami o ochronie danych osobowych,

4.1.2. odbyła zakładowe szkolenie z zakresu ochrony danych osobowych,

4.1.3. otrzymała upoważnienie do przetwarzania danych osobowych (wzór stanowi załącznik do Polityki),

4.1.4. podpisała oświadczenie, którego wzór stanowi załącznik do niniejszej Polityki),

4.1.5. zobowiązała się do zachowania poufności (na podstawie umowy lub oświadczenia).

4.2. Osoba upoważniona obowiązana jest:

4.2.1. zapoznać się z przepisami prawa i wewnętrznymi przepisami dotyczącymi ochrony danych osobowych oraz przestrzegać tych przepisów,

4.2.2. dbać o poprawność, kompletność i aktualność danych osobowych, a zachować należytą staranność przy przetwarzaniu danych osobowych w celu uniknięcia nieumyślnej ich utraty, zmiany lub zniszczenia lub ich udostępnieniu osobom nieuprawnionym,

4.2.3. wykonywać polecenia i wytyczne ADO lub przełożonego,

4.2.4. zachować dane osobowe oraz sposób ich zabezpieczania w ścisłej tajemnicy, obowiązek ten nie ustaje po ustaniu zatrudnienia osoby upoważnionej przez ADO, jak też po rozwiązaniu zawartej z nią umowy cywilnoprawnej,

4.2.5. zgłaszać naruszenia ochrony danych osobowych i stosować wewnętrzne procedury w tym zakresie (Kodeks postępowania w sprawie naruszeń stanowi załącznik do Polityki).

4.3. Upoważnienie do przetwarzania danych osobowych przestaje obowiązywać w przypadku gdy:

4.3.1. ustanie zatrudnienie lub rozwiązana zostanie umowa cywilnoprawna będąca podstawą udzielenia upoważnienia do przetwarzania danych osobowych,

4.3.2. upłynie termin na który zostało udzielone, jeżeli upoważnienie zostało udzielone na czas określony,

4.3.3. ADO lub inna osoba uprawniona odwołają upoważnienie.

4.4. Odwołanie upoważnienia do przetwarzania danych osobowych następuje w szczególności, gdy:

4.4.1. Osobie upoważnionej powierzony zostanie nowy zakres obowiązków niewymagający przetwarzania danych osobowych,

4.4.2. Osoba upoważniona rażąco naruszy bezpieczeństwo danych osobowych.

4.5. Odwołanie upoważnienia następuje w formie pisemnej. W każdym przypadku odwołanie lub wygaśnięcie upoważnienia zostaje odnotowane w rejestrze osób upoważnionych.

4.6. ADO prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych, zgodnie ze wzorem stanowiącym załącznik do Polityki Bezpieczeństwa.

4.7. Osoba upoważniona zobowiązana jest niezwłocznie powiadomić ADO lub swojego przełożonego o każdym podejrzeniu naruszenia bezpieczeństwa danych osobowych.

Rozdział 5 – Zasady przetwarzania danych osobowych

5.1. Dane osobowe muszą być:

5.1.1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”),

5.1.2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”);

5.1.3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”),

5.1.4. prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”),

5.1.5. 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 („ograniczenie przechowywania”),

5.1.6. przetwarzane 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 („integralność i poufność”).

5.2. Przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

5.2.1. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,

5.2.2. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,

5.2.3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO,

5.2.4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,

5.2.5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO,

5.2.6. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

5.3. W przypadku zbierania danych osobowych od osoby, której one dotyczą ADO jest zobowiązany podać osobie, której dane dotyczą informacje, o których mowa w art. 13 RODO. Wzór pouczenia stanowi

załącznik do Polityki Bezpieczeństwa. Niniejszy ustęp nie ma zastosowania gdy i w takim zakresie, w jakim osoba, której dane dotyczą dysponuje już tymi informacjami.

5.4. W przypadku pozyskiwania danych, o których mowa w ust. 5.3. wyżej za pośrednictwem środków komunikacji elektronicznej, przekazanie klauzuli informacyjnej może nastąpić poprzez przesłanie jej jako załącznik do wiadomości e – mail lub przesłanie linku do strony internetowej, na której została zamieszczona klauzula informacyjna.

5.5. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, ADO jest zobowiązany podać osobie, której dane dotyczą informacje, o których mowa w art. 14 RODO. Wzór pouczenia stanowi załącznik do Polityki Bezpieczeństwa. Ust. 5.4. powyżej stosuje się odpowiednio. Informacje, o których mowa w niniejszym ustępie ADO podaje:

5.5.1. w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych lub

5.5.2. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą lub

5.5.3. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

5.6. Ust. 5.4. nie ma zastosowania gdy i w zakresie, w jakim:

5.6.1. osoba, której dane dotyczą, dysponuje już tymi informacjami,

5.6.2. udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. W takich przypadkach ADO podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie,

5.6.3. pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem krajowym,

5.6.4. dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

5.6.5. Dane osobowe będą usuwane po upływie okresu ich przydatności lub po upływie okresu określonego przepisami prawa.

Rozdział 6 – Zarządzanie ryzykiem i ocena skutków w zakresie przetwarzania danych osobowych

6.1. Na dzień opublikowania pierwszej wersji niniejszej Polityki ADO przeprowadził analizę ryzyk dla wszystkich procesów związanych z przetwarzaniem danych osobowych przeprowadzanych przez ADO, nie stwierdzając istnienia procesów, które mogłyby wiązać się z wysokim ryzykiem naruszenia praw i wolności osób fizycznych, których dane przetwarzane są przez ADO.

6.2. Dla każdego nowego procesu wdrażanego przez ADO przeprowadzana jest weryfikacja, czy proces ten wiąże się lub potencjalnie może wiązać się z przetwarzaniem danych osobowych („privacy by design”).

6.3. Dla procesów, które wiążą lub mogą wiązać się z przetwarzaniem danych osobowych każdorazowo przeprowadza się analizę ryzyka.

6.4. Dla każdego procesu związanego z przetwarzaniem danych osobowych, w ramach którego analiza ryzyka wykazała wysokie ryzyko naruszenia praw i wolności osób fizycznych, ADO przeprowadza analizę

skutków dla ochrony danych (DPIA), zgodnie z wytycznymi opisanymi w art. 35 RODO. Analiza przeprowadzana jest przez ADO lub zatrudniony przez niego podmiot zewnętrzny lub inną osobę wyznaczoną przez ADO.

6.5. Jeżeli w wyniku przeprowadzenia analizy DPIA okaże się, iż poziom ryzyka związany z potencjalnym naruszeniem praw i wolności osób, których dane są przetwarzane jest wysoki lub bardzo wysoki, Spółka przeprowadza konsultacje z Prezesem Urzędu Ochrony Danych Osobowych zgodnie z art. 36 RODO przed rozpoczęciem przetwarzania.

Rozdział 7 – Powierzenie przetwarzania danych

7.1. Powierzenie danych osobowych dopuszczalne jest w sytuacjach uzasadnionych potrzebami ADO.

7.2. Przed pierwszym powierzeniem przetwarzania danych osobowych, ADO weryfikuje, czy podmiot, któremu dane zostaną powierzone, gwarantuje realizacje obowiązków wynikających z przepisów prawa oraz posiada warunki i środki zapewniające bezpieczeństwo powierzanych zbiorów danych.

7.3. Potwierdzeniem informacji, o których mowa w pkt 7.2 powyżej może być: audyt, potwierdzający zgodność procesów przetwarzania z RODO, certyfikacja udzielona przez akredytowany podmiot, udział w kodeksach dobrych praktyk lub oświadczenie osoby uprawnionej do reprezentacji podmiotu, któremu zostaną powierzone dane osobowe.

7.4. Podstawę powierzenia danych powinna stanowić umowa powierzenia zgodna z art. 28 RODO lub zastosowanie odpowiednich klauzul w umowie o współpracy z podmiotem, który będzie przetwarzał dane w imieniu i na polecenie ADO (przykład umowy stanowi załącznik do Polityki).

Rozdział 8 – Techniczne i organizacyjne środki ochrony danych

8.1. Szczegółowe zasady stosowania środków technicznych mających zastosowanie do systemów informatycznych i urządzeń przenośnych został szczegółowo określony w Instrukcji Zarządzania Systemami Informatycznymi i Urządzeniami Przenośnymi stanowiącej załącznik do Polityki Bezpieczeństwa.

8.2. Wszelkie nośniki danych osobowych podlegają ochronie w takim samym stopniu jak dane osobowe, które się na nich znajdują.

8.3. Nośniki zawierające dane osobowe powinny być oznaczone w sposób umożliwiający ich identyfikację w celu zapobiegania ich przypadkowego udostępnienia do ponownego użycia lub nieumyślnemu ujawnieniu danych osobowych, a także dla szczególnej ich ochrony.

8.4. Zakazuje się osobom upoważnionym robienia kopii całych zbiorów lub takich ich części, które nie są konieczne do wykonywania przez nich obowiązków służbowych.

8.5. Usuwanie danych przechowywanych na jakichkolwiek nośnikach następuje w momencie ustania celu, dla którego były na nich gromadzone lub po upływie czasu przez jaki miały się na nich znajdować, zgodnie z następującymi zasadami:

8.5.1. dane osobowe usuwa się z nośników w sposób uniemożliwiający ich odtworzenie,

8.5.2. niszczenie nośników polega na pozbawieniu ich cech pozwalających na identyfikacje (odczytanie) danych osobowych na nich się znajdujących lub poprzez fizyczne zniszczenie (np. połamanie płyty CD),

8.5.3. nośniki papierowe należy zniszczyć w przypadku zakończenia korzystania z nich poprzez pocięcie w niszczarce pod warunkiem, że nie podlegają archiwizacji.

8.6. Dostęp do zbiorów danych przechowywanych w formie papierowej zabezpieczony jest poprzez zastosowanie zamka oraz ograniczony jest do osób upoważnionych. W przypadku, gdy możliwości finansowe nie pozwalają na zabezpieczenie w ww. sposób wszystkich zbiorów – zabezpiecza się w zamykanych szafkach zbiry o kluczowym znaczeniu dla ADO.

8.7. Jeżeli szafy, w których przechowuje się dane osobowe są zamykane na klucz to:

a) klucze do tych szaf posiadają tylko Osoby upoważnione,

b) szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane.

8.8. W pomieszczeniach w których przetwarzane są dane osobowe mogą przebywać wyłącznie upoważnione osoby, a dostęp do ww. pomieszczeń możliwy jest wyłącznie w godzinach pracy. W sytuacji, gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia administratora danych.

8.9. W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.

8.10. Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny do wykonania czynności, a następnie muszą być chowane do szaf. W przypadku, o którym mowa w ust. 10.8. - na czas przebywania osób nieupoważnionych Osoba upoważniona jest zobowiązana zabezpieczyć dane na swoim biurku w taki sposób, aby uniemożliwić zapoznanie się z ich treścią przez osoby nieupoważnione, w tym w szczególności Osoba upoważniona nie może odejść o biurka i pozostawić dokumentów zawierających dane osobowe bez dozoru.

8.11. Dostęp do komputerów, na których są przetwarzane dane, mają tylko osoby Upoważnione.

8.12. Monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane i nikt nie powinien ich przestawiać w inny sposób.

8.13. W razie potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane.

8.14. Zakazane jest korzystanie z komputerów przenośnych w środkach transportu lub miejscach publicznych, jeżeli nie ma możliwości zapobieżenia zapoznania się z danymi wyświetlanymi na monitorze przez osoby nieupoważnione.

8.15. Osoba upoważniona nie może udostępniać osobom nieupoważnionym powierzonego mu komputera.

8.16. W razie potrzeby przeniesienia danych osobowych pomiędzy komputerami należy zrobić to z zachowaniem szczególnej ostrożności. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe. Jeśli nie ma możliwości skasowania danych z nośnika (np. płyta CD-ROM), należy go zniszczyć fizycznie. W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.

8.17. Dane osobowe można przesyłać drogą elektroniczną wyłącznie do uprzedniej weryfikacji adresu e – mail i po ustaleniu, że należy on do adresata.

8.18. Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną. Dane osobowe powinny być zabezpieczane hasłem (lub zaszyfrować), które następnie należy przesłać za pomocą wiadomości sms do odbiorcy wiadomości e – mail.

8.19. Sieć komputerowa powinna jest zabezpieczona przed dostępem z zewnątrz. Osoba upoważniona nie może samodzielnie zmieniać ustawień sieci lub oprogramowania, jak również samodzielnie instalować oprogramowania.

8.20. Osoba upoważniona jest zobowiązana do regularnego skanowania swojego komputera za pomocą zainstalowanego programu antywirusowego – nie rzadziej niż raz w tygodniu.

8.21. Na komputerze służbowym Osoba upoważniona może wchodzić wyłącznie na strony internetowe niezbędne do wykonywania pracy lub świadczenia usługi objętej umową, dotyczy to również pobierania plików. W szczególności nie jest dopuszczalne korzystanie z portali plotkarskich i pobieranie muzyki lub filmów. Działania takie zwiększają bowiem ryzyko zawirusowania komputera, co stanowi zagrożenie dla bezpieczeństwa danych osobowych.

8.22. Zabronione jest otwieranie wiadomości e – mail pochodzących od nadawcy nieznanego lub niemożliwego do zidentyfikowania. W szczególności zabronione jest otwieranie linków lub pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

8.23. Komputery służbowe są zabezpieczone hasłem. Każda osoba upoważniona posiada swoją nazwę użytkownika i hasło. Osoba upoważniona, w miarę możliwości jest zobowiązana zapamiętać hasło i unikać jego zapisywania. Jednakże w przypadku zapisywania hasła – należy przechowywać je w taki sposób, aby uniemożliwić zapoznanie się z nim przez osoby trzecie. W szczególności niedopuszczalne jest zapisywanie hasła i przechowywanie go na biurku lub w formie karteczki przyklejonej do komputera.

8.24. Hasło nie może zawierać mniej niż 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne. System wymusza zmianę hasła co 30 dni.

8.25. Osoba upoważniona jest zobowiązana do zachowania swojego hasła w tajemnicy, także po jego zmianie lub upływie jego ważności.

8.26. Hasło, które zostało ujawnione lub istnieje podejrzenie jego ujawnienia musi być niezwłocznie zmienione.

8.27. W przypadku braku aktywności Osoby upoważnionej przez 1 minutę ekran komputera wyłączy się i wymagane będzie ponowne wprowadzenie hasła.

8.28. Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie

8.29. W przypadku korzystania z zasobów IT oferowanych przez zewnętrznego dostawcę, ADO korzysta wyłącznie z usług dostawców, którzy gwarantują odpowiedni poziom zabezpieczenia oferowanych usług lub produktów IT – potwierdzony certyfikacją lub oświadczeniem podmiotu udostępniającego produkt lub usługę IT.

8.30. W przypadku przechowywania zbiorów danych lub danych w tzw. „środowisku chmurowym” (na serwerach nie stanowiących części infrastruktury ADO), ADO korzysta jedynie z usług rekomendowanych i powszechnie uznanych dostawców takich usług stosujących.

8.31. We własnym środowisku informatycznym ADO stosuje zabezpieczenia adekwatne do skali działania oraz możliwości technicznych i aktualnego stanu wiedzy – stale aktualizowane oprogramowanie antywirusowe, firewall, zabezpieczenia przed nieupoważnionym dostępem (w postaci haseł).

8.32. Nieruchomości i pomieszczenia, w których przechowywane są nośniki informacji zawierających dane osobowe zabezpieczane są przed dostępem osób fizycznych – poprzez zastosowanie zabezpieczeń dostępu.

8.33. W stosunku do kluczowych zbiorów danych ADO stosuje dodatkowe zabezpieczenia w postaci zabezpieczania hasłem dostępu do plików, o ile format pliku na to pozwala (np. pliki programu ms Office) lub kodowanie dysków lub katalogów zawierających zbiory danych.

Rozdział 9 – Postępowanie w przypadku naruszenia ochrony danych osobowych

Definicja i rodzaje naruszeń ochrony danych osobowych oraz schemat postępowania w przypadku podejrzenia lub stwierdzenia takiego naruszenia zostały określone w Kodeksie Postępowania w Przypadku Naruszenia Ochrony Danych Osobowych, stanowiącym załącznik nr 6 do Polityki Bezpieczeństwa.

Rozdział 10 - Realizacja dyspozycji osób uprawnionych

10.1. Osoby uprawnione mogą złożyć następujące dyspozycje w zakresie przetwarzania ich danych osobowych:

- 10.1.1. żądanie udzielenia informacji w zakresie przetwarzania danych osobowych i wydania kopii przetwarzanych danych (prawo dostępu do danych),
- 10.1.2. żądanie sprostowania danych osobowych,
- 10.1.3. żądanie przeniesienia danych osobowych,
- 10.1.4. żądanie ograniczenia zakresu przetwarzania, np. poprzez wyłączenie niektórych celów przetwarzania,
- 10.1.5. żądanie zaprzestania profilowania danych osobowych,
- 10.1.6. żądanie zaprzestania podejmowania zautomatyzowanych decyzji opartych na profilowaniu,
- 10.1.7. żądanie usunięcia danych lub zaprzestania przetwarzania danych osobowych (realizacja „prawa do bycia zapomnianym").

10.2. W przypadku złożenia zapytania o potwierdzenie przetwarzania danych osobowych (np. imienia, nazwiska, numeru telefonu, adresu e-mail) przez jakąkolwiek osobę fizyczną, ADO lub osoba upoważniona przez ADO udzielają informacji, czy dane są przetwarzane, a w przypadku odpowiedzi pozytywnej, odpowiedź jest uzupełniona o następujące informacje wskazane w formularzu stanowiącym załącznik do Polityki Bezpieczeństwa.

10.3. W razie wątpliwości, osoba udzielająca odpowiedzi na żądanie osoby, której dane dotyczą ma prawo uzależnić udzielenie informacji od przekazania informacji, które w sposób jednoznaczny potwierdzą, że pytający jest rzeczywiście osobą, której dane są przetwarzane (np. poprzez przesłanie kopii umowy lub weryfikację dodatkowych informacji).

10.4. W przypadku, gdy zapytania od tej samej osoby lub osób reprezentujących tą samą grupę powtarzają się w sposób uporczywy, ADO ma możliwość udzielenia kolejnej informacji od złożenia opłaty, odpowiadającej kosztom udzielenia informacji – a w szczególności kosztom pracy osoby, delegowanej do udzielenia informacji.

10.5. W przypadku żądania przeniesienia danych osobowych, ADO realizuje tą dyspozycję, o ile posiada środki techniczne i przeniesienie danych jest możliwe, zaś wskazany odbiorca danych potwierdzi gotowość do przyjęcia danych oraz wskaże sposób migracji (platformę informatyczną do przekazania danych). Postanowienia ust. 10.3 oraz 10.4 powyżej stosuje się odpowiednio.

10.6. W przypadku otrzymania żądania zaprzestania przetwarzania danych osobowych, ADO wykreśla dane osobowe ze wszystkich zbiorów danych, pozostawiając jedynie informacje niezbędne do ochrony przed roszczeniami – tj. dane o sposobie i dacie pozyskania danych osobowych, zakresie przetwarzania, podstawie przetwarzania i dacie otrzymania oraz realizacji dyspozycji usunięcia danych. Dane takie przechowywane są przez okres do 11 lat po dacie otrzymania dyspozycji usunięcia danych w celach ewentualnej ochrony interesów prawnych ADO, chyba że przed tą datą doszło do przerwania lub zawieszenia okresu przedawnienia roszczeń, w taki przypadku ww. dane zostaną usunięte rok po przedawnieniu roszczenia.

10.7. W ramach realizacji prawa do bycia zapomnianym, ADO informuje wszystkich przetwarzających, odbiorców oraz strony trzecie o konieczności usunięcia danych osobowych ze zbiorów, które te dane zawierają.

10.8. O wszelkich zmianach w zakresie danych osobowych (w tym o wykreśleniu, skorygowaniu, ograniczeniu celu przetwarzania, zaprzestaniu profilowania) osoba, której zmiana ta dotyczy informowana jest na piśmie lub mailowo. W przypadku realizacji „prawa do bycia zapomnianym" ADO informuje również o przekazaniu dyspozycji o wykreśleniu danych do podmiotów, którym dane te zostały przekazane lub powierzone.

10.9. ADO bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie niniejszego rozdziału. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania ADO informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

10.10. Jeżeli ADO nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

10.11. Przy ocenie zasadności żądań osób, których dane dotyczą stosuje się przepisy ochrony danych osobowych. Poniżej przedstawiono tabelę z uwzględnieniem niektórych rodzajów żądań oraz ich dopuszczalnością na dzień wprowadzenia niniejszej Polityki. Szczegółowe wytyczne, co do dopuszczalności realizacji żądań osób, których dane dotyczą stanowią załącznik do Polityki.

Art. 6 RODO – zgodność przetwarzania z prawem	Prawa osoby, której dane dotyczą		
1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:	**Prawo do usunięcia** (art. 17 RODO)	**Prawo do przenoszenia danych** (art. 20 RODO)	**Prawo do sprzeciwu** (art. 21 RODO)
a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów	+	+	X
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy	+	+	X
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze; d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej	X	X	X
d) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi	+	X	X
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi	X	X	+
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem	+	X	+

10.12. Osoba, której dane dotyczą, ma prawo żądania od ADO ograniczenia przetwarzania jej danych osobowych w następujących przypadkach:

10.13. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający ADO sprawdzić prawidłowość tych danych,

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

10.15. ADO nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

10.16. osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania jej danych osobowych – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie ADO są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

10.17. Jeżeli na mocy ust. 10.12 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

10.18. Przed uchyleniem ograniczenia przetwarzania ADO informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.

10.19. ADO może prowadzić rejestr żądań. Wzór rejestru stanowi załącznik do Polityki.

Rozdział 11 – Przetwarzanie danych osobowych

11.1. ADO lub inna osoba wyznaczona przez ADO do nadzoru nad przestrzeganiem zasad dotyczących przetwarzania danych osobowych sprawują nadzór nad przestrzeganiem przepisów prawa, Polityki Bezpieczeństwa oraz innych wewnątrzzakładowych aktów prawa, w tym przechowuje dokumenty i informacje potwierdzające realizację obowiązków z niej wynikających.

11.2. Przynajmniej raz w roku:

1. dokonywany jest przegląd procesów pod kątem ich aktualności oraz zgodności wewnątrzzakładowymi i pozazakładowymi źródłami prawa,
2. dokonywana jest weryfikacja zbiorów danych pod kątem danych, których czas przetwarzania upłynął, które straciły podstawę przetwarzania lub nie są już potrzebne dla realizacji celów przetwarzania oraz usuwa takie dane ze zbiorów. Realizacja tego obowiązku potwierdzona zostaje poprzez sporządzenie protokołu,
3. dokonywany jest przegląd zgodności dokumentacji dotyczącej przetwarzania – w tym niniejszej Polityki z przepisami prawa, a w szczególności z RODO oraz innymi przepisami dotyczącymi ochrony danych osobowych.

11.3. ADO lub osoba wyznaczona przez ADO uczestniczy w czynnościach związanych z projektowaniem lub zmianą procesów, dokonując oceny wpływu procesów na przetwarzanie danych osobowych oraz prawa i wolności osób fizycznych, których dane będą przetwarzane.

11.4. ADO lub osoba wyznaczona przez ADO może w każdej chwili dokonywać wyrywkowych kontroli zgodności działań podejmowanych w imieniu ADO oraz dokumentów z przepisami prawa powszechnie i wewnętrznie obowiązującego.

11.5. ADO za zgodą ADO może przeprowadzić w każdym czasie audyt zgodności procesów oraz działań ADO z RODO i innymi przepisami dotyczącymi ochrony danych osobowych.

Rozdział 12 – Przekazywanie danych osobowych do Państw Trzecich

12.1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

12.2. Gdy Komisja Europejska nie wydała decyzji, o której mowa w ust. 12.1. przekazanie może nastąpić wyłącznie, gdy zapewnią odpowiednie zabezpieczenia i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej:

i. *bez zezwolenia organu nadzorczego:* odpowiednie zabezpieczenia można zapewnić za pomocą:

- prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi,
- wiążących reguł korporacyjnych lub zatwierdzonego kodeksu postępowania, zatwierdzonego mechanizmu certyfikacji,
- standardowych klauzul ochrony danych przyjętych przez Komisję w drodze decyzji,

ii. *po uzyskaniu zezwolenia organu nadzorczego,* odpowiednie zabezpieczenia można zapewnić za pomocą:

- klauzul umownych między administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej,
- postanowień uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą,

iii. *wyjątki w szczególnych sytuacjach*: w razie braku decyzji stwierdzającej odpowiedni stopień ochrony lub braku odpowiednich zabezpieczeń, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że

- osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę,
- przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a Administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą,
- przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną,
- przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,
- przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń,
- przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
- przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes,

- gdy nie ma zastosowania żaden z ww. wyjątków, przekazanie do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie, gdy (łącznie):

- ✓ przekazanie nie jest powtarzalne,
- ✓ dotyczy tylko ograniczonej liczby osób, których dane dotyczą,
- ✓ jest niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, wobec których charakteru nadrzędnego nie mają interesy ani prawa i wolności osoby, której dane dotyczą,
- ✓ Administrator ocenił wszystkie okoliczności przekazania danych i na podstawie tej oceny zapewnił odpowiednie zabezpieczenia w zakresie ochrony danych osobowych. Administrator lub podmiot przetwarzający dokumentują ocenę oraz odpowiednie zabezpieczenia
- ✓ Administrator informuje organ nadzorczy o przekazaniu,
- ✓ Poza standardowymi klauzulami informacyjnymi Administrator podaje osobie, której dane dotyczą, także informacje o przekazaniu i o ważnych prawnie uzasadnionych interesach realizowanych przez niego.

Rozdział 13 – Współpraca z Urzędem Ochrony Danych Osobowych

13.1. Za współpracę z Urzędem Ochrony Danych Osobowych (UODO) odpowiada ADO lub wyznaczony przez ADO pracownik.

13.2. Na początku kontroli osoba dedykowana do współpracy z UODO zobowiązana jest do weryfikacji dokumentów potwierdzających fakt reprezentowania UODO (legitymacja służbowa, upoważnienie do kontroli) oraz określić zakres i termin kontroli. W razie wątpliwości osoba odpowiedzialna weryfikuje uzyskane informacje poprzez kontakt z UODO.

13.3. Na żądanie UODO lub przedstawiciela UODO, udostępnia się wszelkie dokumenty oraz informacje związane z przetwarzaniem danych osobowych.

13.4. Pracownicy oraz współpracownicy ADO zobowiązani są do podjęcia wszelkich działań w celu kompleksowego wyjaśnienia wszelkich okoliczności objętych kontrolą oraz udzielenie kontrolerowi UODO wsparcia w realizacji zadań objętych zakresem kontroli.

13.5. W przypadku działań kontrolnych lub konieczności realizacji uprawnień osób uprawnionych u kontrahenta ADO, będącego podmiotem przetwarzającym, współadministratorem lub w związku z udostępnieniem przez ADO temu kontrahentowi danych osobowych, ADO udziela takiemu podmiotowi wszelkiego niezbędnego wsparcia.

Rozdział 14 - Postanowienia końcowe

14.1. Polityka Bezpieczeństwa wchodzi w życie z dniem _____ r.

14.2. Do przestrzegania Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy ADO oraz osoby, wykonujące dla ADO zadania na podstawie umów cywilnoprawnych.

14.3. Polityka Bezpieczeństwa jest poufnym dokumentem wewnętrznym przeznaczonym dla pracowników oraz innych osób upoważnionych przez ADO.

14.4. W przypadku niezgodności Polityki Bezpieczeństwa z przepisami prawa powszechnie obowiązującymi zastosowanie mają właściwe przepisy prawa.