POLITYKA BEZPIECZEŃSTWA INFORMACJI W GS ENERGIA

Wersja:	01/2020
Data wersji:	27.12.2020 r.

Grudzień 2020

Spis treści

1. Postanowienia ogólne

Realizując obowiązki wynikające z przepisów dotyczących ochrony danych osobowych GS ENERGIA Grzegorz Sokołowski (dalej: **„GS ENERGIA”**) zmierza do spełnienia wymagań chroniących prywatność i godność każdego klienta oraz kontrahenta.

Sposób przetwarzania danych osobowych w **GS ENERGIA** oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, ujęte zostały zbiorczo w niniejszym dokumencie określającym **Politykę Bezpieczeństwa Informacji** (dalej: **PBI**). PBI wraz z jej wszystkimi załącznikami należy rozumieć jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji, zarówno wewnątrz jak i na zewnątrz organizacji. Zwraca ona uwagę na konsekwencje jakie może ponosić przedsiębiorstwo oraz określa procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Celem opracowania PBI jest określenie zasad ochrony danych osobowych przetwarzanych w **GS ENERGIA**, a co za tym idzie organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych danych osobowych. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych oraz informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności oraz rozliczalności na jak najwyższym, możliwym do uzyskania w danym czasie poziomie. Jednocześnie PBI deklaruje zaangażowanie właściciela do Zarządzania Bezpieczeństwem Informacji.

PBI zapewnia:

- **poufność** – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom;
- **integralność** – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany;
- **dostępność** – istnieje możliwość wykorzystania danych na żądanie, w założonym czasie, przez autoryzowany podmiot;
- **rozliczalność** – możliwość jednoznacznego przypisania działań poszczególnym osobom;

- **autentyczność** – zapewnienie, że tożsamość podmiotu lub zasobu jest zgodna z zadeklarowaną;
- **niezaprzeczalność** – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących jest niepodważalne;
- **niezawodność** – zamierzone zachowania i skutki są spójne.

Wszystkie podmioty zewnętrzne, którym udostępniane są dane, zobowiązane są przestrzegać zasad bezpieczeństwa informacji określonych w PBI, a także współpracować we wdrażaniu oraz doskonaleniu procedur ochrony informacji, poprzez m.in. zgłaszanie uwag i opiniowanie zastosowanych rozwiązań.

PBI została opracowana na podstawie:

- 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 (ogólne rozporządzenie o ochronie danych, dalej: RODO);
- Normy PN-EN ISO/IEC 27001 dotyczącej zarządzania bezpieczeństwem informacji;
- Normy PN-ISO/IEC 17799 dotyczącej praktycznych zasad zarządzania bezpieczeństwem informacji;
- Normy PN-EN ISO/IEC 27002 dotyczącej praktycznych zasad zabezpieczania informacji;
- Normy PN-EN ISO/IEC 27005 dotyczącej zarządzania ryzykiem w bezpieczeństwie informacji;
- Normy PN-ISO 31000 dotyczącej zarządzania ryzykiem;
- Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
- Ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO.

2. Definicje

Użyte w dokumentacji przetwarzania danych osobowych definicje i pojęcia są wspólne dla wszystkich pozostałych dokumentów, które zostały przyjęte przez Administratora w zakresie ochrony danych osobowych.

Tabela 1. Zbiór definicji i pojęć

Administrator danych osobowych	Organ, jednostka organizacyjna, podmiot lub osoba, która decyduje o celach i środkach przetwarzania danych osobowych. W dokumentacji przez administratora danych rozumie się **GS ENERGIA.**
Bezpieczeństwo danych osobowych	Zachowanie poufności, integralności i dostępności danych osobowych oraz odporności systemów i usług przetwarzania.
Dane osobowe (lub „dane")	Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby.
Dostępność	Właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu [źródło ISO/IEC 27000].
Działanie korygujące	Działanie w celu wyeliminowania przyczyny wykrytej niezgodności lub innej niepożądanej sytuacji [źródło: ISO 9000].
Działanie zapobiegawcze	Działanie w celu wyeliminowania przyczyny potencjalnej niezgodności lub innej potencjalnej sytuacji niepożądanej [źródło: ISO 9000].
Grupa zasobów	Zbiór zasobów rozpatrywanych wspólnie ze względu na podobny charakter i funkcjonalność.
Integralność	Właściwość polegająca na zapewnieniu dokładności i kompletności zasobów [źródło: ISO/IEC 27000].
Naruszenie danych osobowych	Naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do

	danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
Osoba fizyczna możliwa do zidentyfikowania	Osoba której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny lub specyficzny czynnik/czynniki określające jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
Osoba upoważniona	Osoba która otrzymała od Administratora danych upoważnienie do przetwarzania danych.
Podatność	Słabość zasobu lub zabezpieczenia, która może być wykorzystana przez zagrożenie [źródło: ISO/IEC 27000].
Poufność	Właściwość polegająca na tym, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom [źródło: ISO/IEC 27000].
Przetwarzanie danych	Jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie a zwłaszcza, które wykonuje się w systemach informatycznych.
Pseudonimizacja	Przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
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.
Skuteczność	Stopień w jakim zaplanowane działania są realizowane, a zaplanowane rezultaty osiągnięte [źródło: ISO 9000].
Upoważnienie	Oświadczenie nadawane przez Administratora, wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane we wskazanym zakresie.
Zabezpieczenie	Środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną [źródło: ISO/IEC 27000].
Zbiór danych	Każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw jest rozproszony czy podzielony funkcjonalnie.
Zasoby	Wszystko co ma wartość dla każdego kto zajmuje się przetwarzaniem informacji [źródło: ISO/IEC 29134:2017].
Zagrożenie	Potencjalna przyczyna niepożądanego incydentu, który może wywołać naruszenie praw lub wolności osób fizycznych.
Zdarzenie	Wystąpienie szczególnego zbioru okoliczności [źródło: PKN-ISO Guide 73].
Zdarzenie związane z bezpieczeństwem danych osobowych	Określony stan wskazujący na możliwość naruszenia bezpieczeństwa danych osobowych, błąd zabezpieczenia lub zajścia nieznanej dotychczas sytuacji, która może być związana z bezpieczeństwem danych osobowych.

Źródło: Opracowanie własne

3. Ogólne rozporządzenie o ochronie danych osobowych (RODO)

Celem wprowadzenia jest przystępne i syntetyczne objaśnienie zmian w dziedzinie ochrony danych osobowych w związku z wdrożeniem RODO. We wprowadzeniu zostaną zasygnalizowane następujące kwestie:

- zgody na przetwarzanie danych osobowych;
- obowiązku informacyjnego;
- praw podmiotów, których dane są przetwarzane;
- rejestru czynności przetwarzania danych;
- zgłaszania naruszeń ochrony danych osobowych;
- powierzenia przetwarzania danych;
- kodeksów i certyfikatów zgodności przetwarzania danych.

Z uwagi na to, że jedną z najczęściej stosowanych podstaw przetwarzania danych jest zgoda osoby, której dane dotyczą (czyli podmiotu danych) RODO szczególnie odnośni się do kształtu zgody i jej założeń.

Zgodnie z RODO zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli w formie oświadczenia lub wyraźnego działania potwierdzającego na przetwarzanie dotyczących jej danych osobowych, w formie ustnej, pisemnej lub elektronicznej.

Dla osób fizycznych przetwarzanie ich danych osobowych powinno być jasne, przejrzyste i rzetelne. W celu realizacji wymienionych przymiotów legalnego przetwarzania danych, podmiot powinien posiadać wiedzę w przedmiocie tego kto i po co przetwarza jego dane osobowe. Jednym z narzędzi zapewniających legalność przetwarzania jest obowiązek informacyjny, tj. zakres informacji, które administrator danych powinien przekazać podmiotowi danych w związku z przetwarzaniem jego danych osobowych.

Zgodnie z RODO administrator danych w przypadku pozyskiwania informacji od osoby, której one dotyczą jest zobowiązany do podania:

- swojej tożsamości (pełnej nazwy) i danych kontaktowych;
- danych kontaktowych Inspektora Ochrony Danych (jeżeli został powołany);

- celu i podstawy przetwarzania danych osobowych;
- prawnie uzasadnionego interesu/-ów administratora danych (jeżeli takowy istnieje);
- informacji o odbiorcach danych osobowych lub o kategoriach odbiorców;
- informacji o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
- okresu przechowywania danych;
- informacji o prawach podmiotu (dostępu do danych, przenoszenia, sprzeciwu, sprostowania, usunięcia, etc.);
- informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (zasadach podejmowania, znaczeniach i konsekwencjach).

Zgodnie z brzmieniem RODO podmioty danych zostały wyposażone w takie uprawnienia, jak:

- prawo do bycia zapomnianym – podmiot danych ma prawo zażądać od administratora niezwłocznego usunięcia jego danych osobowych, jeżeli zajdzie jedna z enumeratywnie wymienionych okoliczności z art. 17 ust. 1 pkt. a-f RODO;
- prawo do sprostowania danych – podmiot ma prawo żądać od administratora danych niezwłocznego sprostowania dotyczących jego danych osobowych, które są nieprawidłowe;
- prawo do ograniczenia przetwarzania – osoba której dane dotyczą ma prawo żądania od administratora danych ograniczenia przetwarzania jej danych osobowych, w przypadkach wymienionych w art. 18 ust. 1 pkt. a-d RODO;
- prawo do przenoszenia danych – osoba której dane dotyczą ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące oraz ma prawo przesłać dane osobowe innemu administratorowi, bez przeszkód ze strony administratora, któremu je dostarczono. Przeniesienie danych jest możliwe, jeżeli przetwarzanie

odbywa się na podstawie zgody lub wykonania umowy czy też odbywa się w sposób zautomatyzowany;

- prawo do niepodlegania, przez konkretną osobę fizyczną, decyzjom wywołującym wobec niej skutki prawne lub podobnie wpływającym na nią w inny istotny sposób, a opartym na przetwarzaniu jej danych wyłącznie w sposób zautomatyzowany (za pomocą systemów informatycznych), w tym za pomocą profilowania danych. Przepis przewiduje również wyjątki od tej zasady, m.in., gdy przetwarzanie danych opiera się na wyraźnie udzielonej zgodzie przez osobę, której one dotyczą.

Realizacja wspomnianych praw przysługujących podmiotowi danych powinna być bezpłatna. Jednak jeśli żądania osoby, której dane dotyczą wymagają od administratora dużych nakładów finansowych i czasowych, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może pobrać opłatę, adekwatną do trudności przedsięwzięcia związanego z żądaniem. Administrator powinien zapewnić podmiotom danych możliwość skorzystania ze swoich praw, również drogą elektroniczną, szczególnie kiedy przetwarzanie danych odbywa się elektronicznie.

Administrator danych bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania, powinien odnieść się do wniosku osoby, której dane dotyczą, w zakresie realizacji przysługujących jej praw. Jeżeli administrator nie spełni żądania podmiotu danych powinien podać tego przyczyny.

Celem ułatwienia administratorom wypełniania obowiązków związanych z przetwarzaniem danych osobowych z jednoczesnym ograniczeniem biurokracji w tej materii RODO wprowadza zupełnie nowe rozwiązanie, które zastępuje obowiązek rejestracji zbiorów danych – rejestr czynności przetwarzania danych osobowych. Posiadanie rejestru nie jest obowiązkowe.

RODO przewiduje obowiązek zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego. O naruszeniu administrator powinien poinformować organ niezwłocznie, nie później niż 72 godziny od wykrycia naruszenia.

Zgłoszenie musi zawierać informacje wskazane w art. 33 ust. 3 pkt. 2-d RODO, czyli m.in. charakter naruszenia, wskazywać kategorię i przybliżoną liczbę osób, których dotyczy naruszenie, możliwe konsekwencje czy dane kontaktowe IOD. Jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki powinien również zawiadomić o naruszeniu osobę, której dane dotyczą.

Z uwagi na nieprzerwanie rozwijający się segment usług outsourcingowych i coraz powszechniejsze korzystanie z tych usług przez administratorów danych, konieczne stało się bardziej precyzyjne uregulowanie współpracy pomiędzy administratorem danych osobowych, a podmiotem, na rzecz którego dochodzi do powierzenia przetwarzania danych.

RODO zawiera obligatoryjne elementy umowy powierzenia przetwarzania danych, która zgodnie z nowymi przepisami powinna zawierać: przedmiot powierzenia, czas powierzenia, charakter powierzenia, cel powierzenia, rodzaj danych osobowych podlegających powierzeniu, kategorie osób, których powierzane dane dotyczą, obowiązki i prawa administratora (prawo dokonywania kontroli warunków przetwarzania danych osobowych/obowiązek cyklicznego sprawdzania merytorycznej poprawności powierzanych danych osobowych), obowiązki procesora (m.in. zobowiązanie do zachowania poufności w zakresie przetwarzanych danych, podjęcie środków bezpieczeństwa w stosunku do przetwarzanych danych, legalne korzystanie z usług innego podmiotu przetwarzającego). „Wzór umowy powierzenia danych" stanowi załącznik nr 13 do PBI.

4. Polityka Bezpieczeństwa Informacji

PBI przedstawiona jest w formie dokumentu wraz z załącznikami, opublikowanego i dostępnego dla wszystkich wykonawców lub podwykonawców. Dokument podlega ciągłej aktualizacji i udoskonalaniu, w celu dostosowania do zmieniających się warunków działalności przedsiębiorstwa.

PBI została przygotowana w celu:

- ograniczenia możliwości nieautoryzowanego udostępnienia informacji oraz danych osobowych przetwarzanych przez kontrahentów;
- ograniczenia naruszeń przepisów prawa oraz innych regulacji;
- zapobiegania obniżeniu reputacji;
- ograniczenia strat finansowych.

PBI zakłada:

- zbieranie danych osobowych w jasno określonych celach;
- przetwarzanie danych osobowych, które jest zgodne tylko z wcześniej ustalonymi celami;
- przechowywanie danych osobowych przez określony czas, przeznaczony na realizację poszczególnych zadań;
- przedstawienie danych osobowych w sposób sformalizowany, umożliwiający łatwą identyfikację;
- przetwarzanie danych osobowych w sposób zgodny z obowiązującymi przepisami prawa.

PBI zawiera zestaw następujących załączników:

1) Upoważnienie wraz z klauzulą do przetwarzania danych;
2) Zgoda na przetwarzanie danych osobowych;
3) Umowa o pracę;
4) Klauzula informacyjna dla pracowników;
5) Zakres czynności pracownika;

6) Dane zgłoszenia do ZUS;
7) Kwestionariusz dla pracownika;
8) Kwestionariusz dla kandydata;
9) Klauzula informacyjna do umów o współpracy;
10) Procedura postępowania w przypadku naruszenia ochrony danych osobowych;
11) Regulamin ochrony danych osobowych;
12) Klauzula informacyjna – wzór;
13) Umowa powierzenia przetwarzania danych osobowych;
14) Formularz realizacji żądań podmiotu danych.

5. Odpowiedzialności i uprawnienia

Za bezpieczeństwo przetwarzanych danych osobowych odpowiedzialna jest **GS ENERGIA** (ADO). Odpowiedzialność ADO została wskazana w RODO oraz ustawie o ochronie danych osobowych wraz z aktami wykonawczymi. Podstawowe obowiązki ADO:

- zapewnienie przetwarzania zgodnego z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- zbieranie danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzanie dalej w sposób niezgodny z tymi celami;
- zapewnienie adekwatności, stosowności oraz ograniczenie przetwarzania tylko do niezbędnych celów wskazanych w PBI;
- zapewnienie prawidłowości przetwarzania danych osobowych i w razie potrzeby, ich uaktualniania;
- zapewnienie przechowywania danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą przez okres nie dłuższy niż jest to niezbędne do celów dla których dane są przetwarzane;
- zapewnienie przetwarzania danych osobowych w sposób gwarantujący odpowiedni poziom bezpieczeństwa, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
- deklaracja pełnego zaangażowania w celu zapewnienia bezpieczeństwa danych osobowych, a także prawidłowego zabezpieczenia systemu informatycznego służącego do przetwarzania;
- nadzór określający jakie dane, kiedy i przez kogo zostały do zbiorów Administratora wprowadzone, bądź z tych zbiorów usunięte oraz komu są przekazywane;

- bieżące dostosowywanie systemów informatycznych służących do przetwarzania danych i wszelkich systemów zabezpieczeń przetwarzania danych osobowych do wymogów określonych w RODO;
- zapewnienie środków technicznych i organizacyjnych niezbędnych dla zapewnienia bezpiecznego przetwarzania danych w pomieszczeniach do tego przeznaczonych;
- zapewnienie systemu i sprzętu informatycznego umożliwiającego bezpieczne przetwarzanie danych;
- dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających stosowne upoważnienie;
- zapoznania z przepisami o ochronie danych osobowych każdej osoby upoważnionej do przetwarzania danych osobowych;
- prowadzenia ewidencji osób upoważnionych;
- należytego i terminowego udzielenia informacji na wniosek osób, których dane są przetwarzane i które zwróciły się z wnioskiem o udzielenie informacji.

W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem albo są zbędne do realizacji celu dla którego zostały zebrane, Administrator jest zobowiązany bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru.

Administrator jest zobowiązany poinformować bez zbędnej zwłoki innych Administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.

ADO zobligowany jest zgodnie z RODO w razie jakichkolwiek wątpliwości do wykazania przestrzegania powyższych obowiązków.

Każdemu z kontrahentów podczas podpisywania umowy, nadawane jest prawo dostępu do pewnego zakresu informacji czy danych osobowych - jednak tylko do takich

informacji, danych osobowych oraz zasobów, które są niezbędne z punktu widzenia wykonywanych zadań, pełnionych ról, czy posiadanej wiedzy.

Każdy z partnerów biznesowych informowany jest również podczas udzielania dostępu do danych osobowych o sankcjach, które będą egzekwowane w przypadku nieautoryzowanego ich udostępnienia.

6. Przetwarzanie danych

Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

- osoba której dane dotyczą wyrazi zgodę, chyba, że chodzi o usunięcie dotyczących jej danych osobowych;
- jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa;
- jest to konieczne do realizacji 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;
- jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
- jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Za prawnie uzasadniony cel Administratora uznaje się w szczególności dochodzenie roszczeń z tytułu prowadzonej działalności oraz marketing bezpośredni własnych produktów lub usług, przy czym przy podejmowaniu działań marketingowych za pomocą środków komunikacji elektronicznej należy stosować przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną oraz ustawy z dnia 16 lipca 2004 r. prawo telekomunikacyjne, które przewidują dalej idącą ochronę.

Zgoda na przetwarzanie danych osobowych:

- nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;
- może obejmować przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania;
- może zostać odwołana w każdym czasie. W przypadku odwołania zgody na przetwarzanie danych osobowych Administrator zobowiązany jest usunąć wszystkie dane osobowe osoby która zgodę cofnęła, chyba, że istnieje inna

podstawa prawna upoważniająca Administratora do dalszego przetwarzania danych dla innych celów niż wskazany w cofniętej zgodzie;

- powinna być odebrana w postaci możliwej do późniejszego udowodnienia (np. pisemnie w ramach systemu informatycznego po zastosowaniu metody dwustopniowego uwiarygodniania lub jako nagranie przeprowadzonej rozmowy telefonicznej – po poinformowaniu rozmówcy o prowadzonej rejestracji).

7. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Administrator zobowiązuje się zachować w tajemnicy dane osobowe, do których posiada dostęp, sposoby zabezpieczania danych, jak również wszelkie informacje, które powziął w czasie przetwarzania danych, zarówno w sposób zamierzony jak i przypadkowy. Obowiązek zachowania danych w tajemnicy jest bezterminowy.

Podczas przetwarzania danych Administrator zachowuje szczególną ostrożność i podejmuje wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.

Podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, dochowuje się należytej staranności, w szczególności upewnia się czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy. W przypadku przesyłania za pomocą środków komunikacji elektronicznej, zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać w miarę możliwości innym środkiem komunikacji elektronicznej.

Wszelkie dokumenty zawierające dane osobowe przechowywane są w szafach lub pomieszczeniach zamykanych na klucz.

Po zakończeniu pracy z danymi stanowisko jest porządkowane, zabezpieczane są dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia. Każdy dokument zawierający dane (a nieużyteczny) niszczy się niezwłocznie. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu.

8. Procedura postępowania w przypadku naruszenia danych osobowych, kontakt z organami władzy

Celem procedury postępowania w przypadku naruszenia danych osobowych jest określenie zadań w zakresie:

- ochrony wszystkich informacji przed ich modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem, a także utratą;
- prawidłowego reagowania przy przetwarzaniu danych, w przypadku stwierdzenia naruszenia (zwłaszcza naruszenia ochrony danych osobowych) lub naruszenia zabezpieczeń systemu informatycznego;
- ograniczenia ryzyka powstania zagrożeń oraz minimalizacji skutków ich wystąpienia.

W przypadku naruszenia ochrony danych osobowych należy zgodnie z RODO zgłosić ten incydent właściwemu organowi nadzorczemu, a także w uzasadnionych przypadkach wszystkim osobom, których to naruszenie dotyczy.

Zasady postępowania w przypadku zagrożenia lub naruszenia bezpieczeństwa informacji, przykładowe incydenty oraz wzory zgłoszeń znajdują się w Załączniku nr 10 do Polityki Bezpieczeństwa Informacji – „Procedurze postępowania w przypadku naruszenia danych osobowych".

9. Postanowienia końcowe

W sprawach nieuregulowanych w PBI mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy RODO.

10. Ważność oraz zarządzanie dokumentem

Stwierdza się ważność dokumentu na dzień jego podpisania.

Właścicielem dokumentu jest Administrator danych osobowych, który jest odpowiedzialny za weryfikację oraz w razie konieczności aktualizację.

……

Właściciel