Polityka Ochrony Danych Osobowych

SPIS TREŚCI:

PREAMBUŁA

Niniejszy dokument zawiera informacje o zabezpieczeniach, dlatego też został objęty ochroną na zasadzie tajemnicy przedsiębiorstwa w myśl art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Dokument może zostać udostępniony innym podmiotom po zawarciu stosownej umowy między innymi o zachowaniu poufności lub gdy obowiązek zachowania poufności wynika z przepisów prawa.

Polityka Ochrony Danych Osobowych została opracowana i wdrożona w celu zapewnienia Bezpieczeństwa Informacji oraz celem ochrony podstawowych praw i wolności osób fizycznych w tym prawa do ochrony danych osobowych, o których mowa w ROZPORZĄDZENIU 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).

DEFINICJE:

Ilekroć w Polityce Ochrony Danych Osobowych jest mowa o:

1. **Organizacji –** rozumie się przez to firmę: ZAKŁAD TECHNICZNO-BUDOWLANY "POLBAU" SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, z siedzibą w Opolu ul. GRUNWALDZKA 25, zarejestrowana w Krajowym Rejestrze Sądowym prowadzonym przez Sąd Rejonowy w Opolu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego, KRS NR 0000047992, NIP: 7540025059.
2. **Polityce ODO –** rozumie się przez to niniejszy dokument (Polityka Ochrony Danych Osobowych) wraz z dokumentami powiązanymi, które są dokumentami współistniejącymi i są uzupełnieniem do niniejszej Polityki. Dokumenty te stanowią element Polityki Bezpieczeństwa Informacji w Organizacji.

3. **Polityce Bezpieczeństwa Informacji –** rozumie się przez to zbiór procedur, instrukcji, wytycznych, które tworzą jako całość system bezpieczeństwa w Organizacji. Dokumentami składającymi się na Politykę Bezpieczeństwa Informacji są Polityka Ochrony Danych Osobowych i dokumenty powiązane, współistniejące z tymi dokumentami.

4. **Administratorze** - oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; w tym dokumencie tą nazwą określa się firmę: ZAKŁAD TECHNICZNO-BUDOWLANY "POLBAU" SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ. Organizacja jest administratorem danych m.in. wobec danych pracowników (obecnych i byłych), kandydatów do pracy, współpracowników (obecnych i byłych), klientów (obecnych i byłych).

5. **Podmiocie przetwarzającym-** rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora; ZAKŁAD TECHNICZNO-BUDOWLANY "POLBAU" SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ może występować w roli podmiotu przetwarzającego, gdy przetwarza dane osobowe wykonując usługi na rzecz Administratora danych w oparciu o zawarte umowy współpracy i umowy powierzenia przetwarzania danych osobowych.

6. **Danych Osobowych**– rozumie się przez to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej

7. **Szczególne kategorie danych osobowych** - rozumie się przez to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, dane dotyczące seksualności lub orientacji seksualnej osoby, której dane dotyczą;

8. **Przetwarzaniu –** rozumie się przez to 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;

9. **Zbiór danych** – rozumie się przez to każdy zestaw uporządkowanych danych o charakterze osobowym, dostępny według określonych kryteriów;

10. **Administratorze systemu informatycznego (ASI)** – należy przez to rozumieć osobę wyznaczoną do nadzorowania infrastruktury teleinformatycznej oraz wykonywania czynności wymagających specjalnych uprawnień lub osobę nadzorującą wykonywanie tych czynności przez podmiot zewnętrzny na podstawie umowy;

11. **Administratorze Danych Osobowych (ADO)** – rozumie się przez to Zarząd Spółki i osobę wyznaczoną w organizacji, odpowiedzialną za nadzór nad przestrzeganiem zasad ochrony informacji w organizacji w imieniu organizacji, w tym danych osobowych;

12. **Systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

13. **Zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

14. **Naruszenie ochrony danych osobowych** - rozumie się przez to 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;

15. **Osoba działająca z upoważnienia -** każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych wewnątrz struktury organizacyjnej administratora danych lub podmiotu przetwarzającego.

STOSOWANE SKRÓTY:

1) Polityka ODO – Polityka Ochrony Danych Osobowych
2) ASI – Administrator Systemu Informatycznego
3) ADO - Administratorze Danych Osobowych
4) IOD– Inspektor Ochrony Danych

ROZDZIAŁ I
CELE I DEKLARACJE ORGANIZACJI

CELE

Organizacja zobowiązuje się do wdrażania i stosowania odpowiednich środków technicznych i organizacyjnych z uwagi na ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku - uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania.

Celem polityki bezpieczeństwa informacji, jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych.

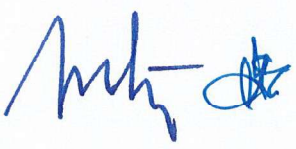
Celem Polityki bezpieczeństwa jest ochrona danych osobowych i informacji, przetwarzanych przez organizację, w szczególności ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.

ROZDZIAŁ II
OBSZARY REGULOWANE POLITYKĄ BEZPIECZEŃSTWA

Polityka ODO jako dokument podstawowy regulują następujące obszary:

1. zasady bezpieczeństwa panujące w organizacji w tym podejmowane przez organizację działania i środki w zakresie bezpieczeństwa danych w organizacji oraz zasady bezpieczeństwa systemów informatycznych
2. zasady dotyczące przetwarzania danych osobowych w organizacji
3. zasady zabezpieczania danych przetwarzanych w formie papierowej
4. zasady zabezpieczenia danych przetwarzanych w formie elektronicznej
5. zasady realizacji praw osób, których dane dotyczą
6. zasady wykrywania oraz zgłaszania naruszeń
7. zasady ciągłości działania – plan ciągłości działania

Niektóre spośród wyżej wskazanych zasad zostały bardziej szczegółowo opisane w oddzielnych Dokumentach (Dokumenty powiązane z Polityką ODO) dedykowanych dla określonych osób z organizacji wg zasady poziomu dostępu do informacji dotyczących organizacji.



ROZDZIAŁ III
POSTANOWIENIA OGÓLNE

Wypracowane w niniejszej Polityce główne zasady i wymagania mają ukierunkować działania zmierzające do budowy systemu bezpieczeństwa, a potem jego utrzymywania podczas eksploatacji systemów informatycznych, na poziomie odpowiadającym potrzebom organizacji.

Organizacja przetwarza dane osobowe głównie jako Administrator danych.

1. Zasady bezpieczeństwa panujące w organizacji w tym podejmowane przez organizację działania i środki w zakresie bezpieczeństwa danych w organizacji oraz zasady bezpieczeństwa systemów informatycznych

Organizacja podejmuje wszelkie działania, aby przetwarzanie danych w organizacji jak również poza nią odbywało się zgodnie z prawem i aby móc to wykazać. Wyboru środków dla osiągnięcia celu dokonuje się uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze.

Środki te obejmują w szczególności:

1. wdrożenie przez organizację odpowiednich polityk ochrony danych
2. wdrożenie przez organizację odpowiednich środków technicznych i organizacyjnych
3. poddawanie przez organizację stosowanych środków ochrony przeglądom i uaktualniane ich
4. przeprowadzanie w organizacji okresowych szkoleń w zakresie zasad bezpiecznego przetwarzania danych osobowych zależności od stwierdzonych potrzeb. Źródłami identyfikacji potrzeb szkoleniowych są: a) naruszenia związane z ochroną danych osobowych; b) wyniki audytów i kontroli; c) pojawienie się nowych ryzyk/zagrożeń; d) zmiany wewnętrzne i zewnętrzne mające wpływ na czynności przetwarzania danych osobowych np. szkolenia są przeprowadzane również w przypadku: zmiana zakresu przetwarzanych danych i zasad ich przetwarzania, zmiana sprzętu i oprogramowania, zmiana obszaru przetwarzania danych; zmiany przepisów o ochronie danych osobowych.
5. przeprowadzanie przez organizację analizy ryzyka

2. Zasady dotyczące przetwarzania danych osobowych w organizacji

Organizacja mając na uwadze bezpieczeństwo przedsiębiorstwa, bezpieczeństwo danych osobowych przetwarzanych w organizacji, podejmuje w szczególności następujące działania:

1. Dostęp do obszaru przetwarzania danych jest możliwy jedynie do osób upoważnionych. Przebywanie w tym obszarze innych osób jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych i wydaniu stosownego upoważnienia;
2. Przygotowuje każdą osobę do pracy z danymi osobowymi w organizacji poprzez szkolenia wstępne i okresowe
3. Stosuje politykę nadawania upoważnień do przetwarzania danych osobowych oraz zapewnia prowadzenie Ewidencji osób upoważnionych do przetwarzania danych osobowych
4. Prowadzi rejestr czynności przetwarzania
5. Dokonuje przeglądów zmian w przepisach prawnych dotyczących danych osobowych,
6. Nadzoruje przestrzeganie zasad ochrony przez osoby upoważnione i mające dostęp do danych osobowych
7. Dokonuje, nie rzadziej niż raz do roku, przeglądu nadanych uprawnień ich aktualizowania w razie potrzeby oraz ponownego zatwierdzania
8. W przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych niezwłocznie podejmuje działania naprawcze (usuwające skutki naruszenia) oraz korygujące (zapobiegające powtarzaniu się naruszenia)
9. Przeprowadza analizę potrzeb szkoleniowych w zakresie ochrony danych osobowych oraz zapewnienie realizacji tych szkoleń
10. Zapewnienia dokonywanie sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych
11. Zabezpiecza się pomieszczenia tworzące obszar przetwarzania danych, na czas nieobecności w nim osób upoważnionych, w sposób uniemożliwiający dostęp do nich osób nieupoważnionych;
12. Stosowana i pilnowana jest polityka „czystego biurka"
13. Wprowadza się ustawienia na drukarki tak, aby nie było możliwości pobrania wydruków przez osoby nieuprawnione
14. Nieaktualne, niepotrzebne lub błędne wydruki zawierające dane osobowe niszczone są niezwłocznie w niszczarkach o wysokim stopniu niszczenia;
15. Wykonywanie dla ochrony i bezpieczeństwa kopii zapasowych danych osobowych oraz programów służących do ich przetwarzania;
16. Zastosowanie ochrony antywirusowej w czasie rzeczywistym;
17. Wykorzystanie szyfrowania przy przesyłaniu danych drogą elektroniczną
18. Kontroluje, weryfikuje, aktualizuje mechanizmy ochrony danych osobowych opisane w dokumencie pt. WYKAZ ŚRODKÓW FIZYCZNYCH, TECHNICZNYCH I ORGANIZACYJNYCH OCHRONY DANYCH OSOBOWYCH I SYSTEMÓW INFORMATYCZNYCH
19. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych, w tym obowiązkowo stosuje szyfrowanie wobec przetwarzanych danych osobowych; w tym zakresie obowiązują konkretne zasady i procedury;

20. Zabezpieczenie za pomocą hasła dostępu do urządzeń przetwarzających dane osobowe lub będących elementem bezpieczeństwa;
21. Podłączenie urządzenia końcowego (komputera, drukarki) do sieci komputerowej dokonywane jest wyłącznie przez wskazanego przez Administratora pracownika wsparcia systemu informatycznego.
22. Każda nowo upoważniona osoba jest zaznajamiana z dokumentami regulującymi zasady postępowania z danymi osobowymi, które są częścią niniejszej Polityki ODO.
23. W przypadku dostępu do danych przez podmioty inne niż pracownicy, Organizacja podpisuje umowę na poufność lub umowę powierzenia przetwarzania danych;

3. Zasady zabezpieczania danych przetwarzanych w formie papierowej

Polityka Bezpieczeństwa Informacji jako całość systemu bezpieczeństwa, określa reguły przetwarzania dla wszystkich danych osobowych w Organizacji oraz zasady służące zapewnieniu ochrony dla przetwarzanych danych w postaci tradycyjnej (papierowej) oraz elektronicznej (w systemach informatycznych). Dokumenty powiązane z Polityką ODO określają konkretne zasady dla konkretnych przypadków. Przyjmuje się podstawowe zasady, a mianowicie:

1. Każdy, kto przetwarza dane osobowe obowiązany jest 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. Administrator realizuje ten cel poprzez szkolenia pracowników oraz wdrożone w organizacji Zasady postępowania z danymi osobowymi. Osoby dopuszczone do przetwarzania danych podpisują stosowne zobowiązania i oświadczenia.
2. Podczas przetwarzania danych trzeba zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.
3. Wszelkie dokumenty zwierające dane osobowe przechowywane są w szafach lub pomieszczeniach zamykanych na klucz. Dostęp do biura jest ograniczony dla osób z zewnątrz, jak również funkcjonuje system alarmowy. Obowiązuje kontrola dostępu.
4. Osoba będąca dysponentem kluczy nie może przekazywać kluczy do budynków i pomieszczeń, w których przetwarzane są dane osobom nieuprawnionym, a ponadto zobowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
5. Osoba, która utraciła posiadane klucze / karty dostępu do pomieszczeń Administratora, w których przetwarzane są dane, niezwłocznie zgłasza tą okoliczność Administratorowi. Administrator, w zakresie swoich kompetencji, podejmują wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze/kartę dostępu utracono.

6. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko, zabezpieczając dokumenty w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
7. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu stosownej umowy o powierzeniu przetwarzania danych osobowych.
8. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie.
9. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.

4. Zasady zabezpieczania danych przetwarzanych w formie elektronicznej

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze organizacja wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

W organizacji wdrożone są poniższe środki ochrony i zabezpieczeń danych:

1. Dostęp do komputera mają jedynie osoby upoważnione przez Administratora
2. Komputer ma hasła i loginy
3. Hasła do systemu informatycznego są okresowo zmieniane.
4. Dochowuje się należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy oraz czy są w odpowiedni sposób zabezpieczone.
5. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, stosuje się szyfrowanie danych np. przesyłany dokument jest zaszyfrowany, a hasło przesyłane jest innym środkiem komunikacji elektronicznej.
6. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko, zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
7. Organizacja posiada sformalizowane zasady współpracy z zewnętrznymi dostawcami zapewniające bezpieczeństwo danych i poprawność działania środowiska teleinformatycznego. Serwis sprzętu informatycznego dokonywany jest przez sprawdzonego specjalistę po uprzednim podpisaniu klauzuli poufności.
8. Organizacja wprowadza i udoskonala zasady oraz mechanizmy techniczne zapewniające, że Dane Osobowe chronione będą przed zniszczeniem bądź utratą danych poprzez:

1) Proces tworzenia kopii zapasowej danych
2) Testy odtwarzania systemu z kopii zapasowej
3) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity - System antywirusowe BitDefender i zaawansowany router z funkcjami firewalla
4) Program antywirusowy i inne narzędzia chroniące przed szkodliwym oprogramowaniem są regularnie uaktualniane.
5) Organizacja posiada sformalizowany sposób zarządzania incydentami.
6) Sprzęt i oprogramowanie powinny być eksploatowane, serwisowane i wycofywane z eksploatacji z zachowaniem właściwych procedur bezpieczeństwa.
7) Wszelkie działania związane z utrzymaniem i eksploatacją systemu informatycznego mogą być podejmowane wyłącznie przez upoważniony, wykwalifikowany personel organizacji.
8) Wszelkie oprogramowanie wykorzystywane w organizacji musi być użytkowane z poszanowaniem praw własności intelektualnej, a w szczególności zgodnie z ustawą o prawie autorskim i prawach pokrewnych.
9) Osoby korzystające z nośników informacji zobowiązane są do zachowania należytej staranności poprzez zastosowanie obowiązujących środków organizacyjno-technicznych i prawnych.
10) W przypadku wycofywania z użycia nośników informacji zawierających informacje stanowiące tajemnicę na użytkowniku spoczywa obowiązek trwałego usunięcia zapisanych informacji.

5. Pozostałe zasady zabezpieczania przetwarzanych danych

Organizacja podejmuje ciągłe działania zmierzające do budowy systemu bezpieczeństwa i zamierza wdrażać odpowiednie mechanizmy ochrony i zabezpieczeń danych. Zasady te określa dokument pt. WYKAZ ŚRODKÓW FIZYCZNYCH, TECHNICZNYCH I ORGANIZACYJNYCH OCHRONY DANYCH OSOBOWYCH I SYSTEMÓW INFORMATYCZNYCH. Dokument ten opisuje:

1. MECHANIZMY KONTROLI DOSTĘPU FIZYCZNEGO
2. MECHANIZMY KONTROLI DOSTĘPU LOGICZNEGO
3. KONTROLE NADAWANYCH UPRAWNIEŃ DO SYSTEMÓW INFORMATYCZNYCH
4. KONTROLE WYCIEKÓW INFORMACJI
5. MONITOROWANIE ZMIAN DANYCH W SYSTEMACH INFORMATYCZNYCH
6. KONTROLE PROCESU WYBORU DOSTAWCÓW
7. ZASADY ZAPEWNIENIA DOSTĘPNOŚCI DANYCH
8. SEPARACJE DANYCH

6. Zasady realizacji praw osób, których dane dotyczą

Organizacja stawia również nacisk za realizację zadań mających na celu osiągnięcie zgodności z RODO oraz urzeczywistnienie zasad dotyczących przetwarzania danych osobowych, o których mowa w art. 5 ust. 1 RODO.

Organizacja realizuje, w sytuacji, gdy zaistnieje taki obowiązek po stronie organizacji, poniższe prawa:

- Prawo do informacji (spełnienie obowiązku informacyjnego)
- Prawo dostępu do danych osobowych
- Prawo do sprostowania i uzupełnienia danych osobowych
- Prawo do bycia zapomnianym
- Prawo do żądania ograniczenia przetwarzania danych
- Prawo do przenoszenia danych
- Prawo do sprzeciwu wobec przetwarzania danych osobowych.

Prawo do informacji (spełnienie obowiązku informacyjnego)

W przypadku zbierania danych osobowych podaje się osobie, której dane dotyczą informacje, o których mowa w art. 13 i 14 RODO, chyba że osoba, której dane dotyczą dysponuje już tymi informacjami. Organizacja w tym celu opracowuje stosowne klauzule informacyjne.

Klauzule informacyjne organizacja stosuje między innymi wobec: Potencjalnych pracowników, Pracowników, Zleceniobiorców, Współpracowników (podmioty działające w strukturach organizacji), podmiotów spoza organizacji.

W przypadku wątpliwości w zakresie zbierania danych, każdy pracownik musi być uświadomiony przez organizację, że kwestie te należy konsultować z osobą odpowiedzialną za dane osobowe w organizacji.

Prawo dostępu do danych osobowych

Jeżeli osoba fizyczna zażąda informacji na temat przetwarzania dotyczących jej danych osobowych, należy udzielić jej informacji, o których mowa w art. 15 ust. 1 i 2 RODO, chyba że udzielenie takich informacji stałoby w sprzeczności z prawem Unii Europejskiej lub prawem państwa członkowskiego, w szczególności z ustawowym obowiązkiem zachowania tajemnicy.

Na żądanie osoby, której dane dotyczą, dostarcza się jej kopię danych osobowych podlegających przetwarzaniu, chyba że jej dostarczenie stałoby w sprzeczności z prawem Unii Europejskiej lub prawem państwa członkowskiego, w szczególności z ustawowym obowiązkiem zachowania tajemnicy. Sposób realizacji takiego żądania nie może wpływać niekorzystnie na prawa i wolności innych osób, a w szczególności nie może wiązać się z ujawnieniem dotyczących ich danych.

Prawo do sprostowania i uzupełnienia danych osobowych

Na żądanie osoby, której dane dotyczą, dokonuje się niezwłocznego sprostowania nieprawidłowych danych osobowych.

Na żądanie osoby, której dane dotyczą, dokonuje się niezwłocznego uzupełnienia niekompletnych danych osobowych, chyba że żądany zakres danych osobowych nie będzie adekwatny do celów, w których dane są przetwarzane.

Prawo do bycia zapomnianym

Jeżeli osoba, której dane dotyczą, żąda niezwłocznego usunięcia danych osobowych (realizacji prawa do bycia zapomnianym), należy ocenić, czy zachodzi podstawa do dalszego przetwarzania, a mianowicie:

1) Czy przetwarzanie jest niezbędne do korzystania z prawa wolności wypowiedzi i informacji?
2) Czy przetwarzanie jest niezbędne do realizacji obowiązku wynikającego z przepisu prawa Unii Europejskiej lub prawa państwa członkowskiego?
3) Czy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej organizacji?
4) Czy przetwarzanie jest niezbędne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 RODO?
5) Czy jest prawdopodobne, że usunięcie danych uniemożliwi lub poważnie utrudni przetwarzanie danych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO?
6) Czy przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń?

Po przeprowadzonej ocenie podejmuje się tym zakresie stosowne decyzje.

Prawo do żądania ograniczenia przetwarzania danych

Jeżeli osoba, której dane dotyczą, żąda ograniczenia przetwarzania danych osobowych, przetwarzanie tych danych zmienia się w następujący sposób:

1) Jeżeli osoba, której dane dotyczą kwestionuje prawidłowość danych osobowych, zawiesza się przetwarzanie danych osobowych do czasu weryfikacji prawidłowości tych danych, a w razie potrzeby ich sprostowania lub uzupełnienia – do czasu realizacji tych czynności.
2) Jeżeli przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania, dalsze przetwarzanie prowadzi się zgodnie z tym żądaniem.

3) Jeżeli organizacja nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń, dane osobowe przechowuje się przez okres objęty żądaniem.
4) Jeżeli osoba, której dane dotyczą wniosła sprzeciw, o którym mowa w art. 21 RODO, przetwarzanie danych osobowych zawiesza się do czasu rozpatrzenia sprzeciwu zgodnie z ust. 35 i 36.

Prawo do sprzeciwu wobec przetwarzania danych osobowych.

W razie wniesienia przez osobę, której dane dotyczą, sprzeciwu wobec przetwarzania dotyczących jej danych osobowych - oceniając zasadność sprzeciwu, należy przede wszystkim odpowiedzieć na pytanie, czy sprzeciw został wniesiony z przyczyn związanych ze szczególną sytuacją danej osoby.

Zasady postępowania opisuje art. 21 RODO.

Termin realizacji

Odpowiedzi na żądanie osoby, której dane dotyczą, udziela się bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od dnia wpływu żądania do organizacji. W odpowiedzi informuje się o działaniach podjętych w związku z żądaniem. W razie odmowy spełnienia całości lub części żądania, w odpowiedzi informuje się o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

W organizacji obowiązuje dokument pt.:

WYTYCZNE DLA PRACOWNIKÓW/ZLECENIOBIORCÓW/WSPÓŁPRACOWNIKÓW SPÓŁKI OKREŚLAJĄCE ZASADY POSTĘPOWANIA W PRZYPADKU REALIZACJI PRZEZ OSOBY ICH PRAW WG RODO.

7. Zasady wykrywania oraz zgłaszania naruszeń

Zasady wykrywania i zgłaszania naruszeń reguluje m.in. dokument pt.: POSTĘPOWANIE W PRZYPADKU WYKRYCIA NARUSZENIA OCHRONY DANYCH

8. Zasady ciągłości działania

Szczegółowe zasady w zakresie bezpieczeństwa informacji reguluje Polityka Bezpieczeństwa Informacji rozumiana jako całość systemu bezpieczeństwa, a zatem dokumenty takie jak Polityka ODO czy dokumenty z nimi powiązane. W celu zapewnienia ciągłości działania przeprowadza się konkretne działania m.in. okresowe analizy ryzyka oraz testy.

System informatyczny podlega zagrożeniom zarówno wewnętrznym jak i zewnętrznym, które Administrator danych identyfikuje i następnie podejmuje działania i środki zaradcze. Polityka bezpieczeństwa ma na celu eliminowanie lub ograniczenie do minimum ww. zagrożeń na prawidłowe działanie systemu.

Potencjalne zagrożenia, na jakie narażony jest system obrazuje tabela poniżej.

Zagrożenia wewnętrzne	Zagrożenia zewnętrzne
Czynnik ludzki	
1. Nieuczciwi pracownicy/współpracownicy /dostawcy usług (sabotaż); 2. Nieuczciwi Klienci; 3. Błędy pracowników/współpracowników powodujące nieprawidłowe działanie systemu takie jak błędy administrowania, nieprawidłowa obsługa urządzeń, uszkodzenia fizyczne urządzeń; 4. Niestosowanie się do procedur i regulaminów 5. Hakerzy z poziomu lokalnego sieci	Włamanie przez osoby trzecie Kradzież przez osoby trzecie
Awarie	Zagrożenie infekcji systemu przez wirusy komputerowe Zagrożenie przez żywioły typu powódź, pożar
1. Awaria urządzeń systemu 2. Awaria linii dostępowych do Internetu 3. Awaria systemów operacyjnych 4. Awaria oprogramowania 5. Awaria zasilania 6. Awaria systemu zabezpieczeń	
Nieprawidłowości techniczne	
1. Niewłaściwe wykorzystywanie poczty internetowej 2. Niewłaściwe wykorzystywanie systemu 3. Niewłaściwa konfiguracja systemu	
Inne nieprawidłowości	
1. Niepowołany dostęp do danych 2. Niepowołany dostęp do urządzeń systemu 3. Zagrożenie infekcji systemu przez wirusy komputerowe	

Zarządzanie ryzykiem bezpieczeństwa informacji **odbywa się poprzez**:

1. analizę ryzyka. Analiza ryzyka przeprowadzana jest raz w roku oraz przy każdej istotnej zmianie środowiska informatycznego.
2. przeprowadzane szkolenia z zakresu obsługi system, właściwego używania zasobów informatycznych, procedur, bezpieczeństwa informacji
3. przeprowadzane audyty wewnętrzne oraz zewnętrzne
4. zarządzanie incydentami

Analiza ryzyka przebiega w sposób następujący:

- następuje identyfikacji ryzyka,

- dokonuje się szacowania ryzyka,
- podejmuje się czynności mające na celu przeciwdziałania ryzyku,
- dokonuje się monitorowania i raportowania ryzyka.

Postępowanie z wynikami analizy ryzyka

- Wyniki analizy ryzyka stanowią podstawę zaprojektowania odpowiednich mechanizmów kontroli dla systemów informatycznych eksploatowanych w organizacji.
- Wdrażane mechanizmy kontroli powinny być adekwatne do oszacowanego ryzyka, zidentyfikowanych zagrożeń i ich istotności, oraz muszą zapewniać efektywność ekonomiczną

Audyt i kontrola systemów informatycznych

1. Przez audyt lub kontrolę systemów informatycznych należy rozumieć czynności mające na celu uzyskanie racjonalnego zapewnienia, że mechanizmy kontroli eksploatacji systemów informatycznych i bezpieczeństwa informacji funkcjonują zgodnie z założeniami, są adekwatne do poziomu ryzyka, wymogów prawnych i obowiązujących norm. Sprawdzeniu podlega, czy mechanizmy kontroli wewnętrznej w systemie informatycznym i związanych z nim zasobach właściwie chronią informacje, utrzymują integralność i rzetelność danych.
2. Do przeprowadzania audytu lub kontroli systemów informatycznych upoważnione są w szczególności: ASI, podmioty zewnętrzne z mocy prawa lub na podstawie umowy cywilno-prawnej, IOD w razie powołania.

ROZDZIAŁ IV
POSTANOWIENIA KOŃCOWE

Wymagania wobec osób współpracujących z Organizacją

Polityka dotyczy wszystkich osób zatrudnionych w organizacji, w rozumieniu Kodeksu pracy, a także osób, przy pomocy, których organizacja wykonuje swoje czynności, a które to osoby przyjęły na siebie zobowiązanie dotyczące jej przestrzegania.

Przegląd i aktualizacja Polityki

1. Za aktualizację i utrzymywanie spójności Polityki odpowiedzialny jest Administrator
2. Administrator korzysta ze wsparcia i pomocy IOD w przypadku jego powołania oraz z pomocy odpowiednich specjalistów /prawników.
3. Przeglądy powinny być dokonywane co najmniej raz do roku lub w trakcie roku w przypadku wystąpienia znaczących zmian, powinny obejmować:
   - Weryfikację zasad i ewentualne dostosowanie Polityki do zmieniającego się profilu ryzyka w organizacji;
   - adekwatność zapisów do zmian środowiska organizacyjnego;

- adekwatność zapisów do zmian w budowie systemu informatycznego;
- dostosowanie do zmian w obowiązującym prawie.

Wszelkie zmiany w niniejszej Polityce wymagają akceptacji Zarządu Organizacji.

Niniejszy dokument opisuje podstawowe kierunki działania Organizacji i wskazuje przyjęty schemat postępowania, który realizowany jest za pomocą konkretnych środków prawnych, organizacyjnych i technicznych. Konkretne mechanizmy działań opisuje /może opisywać dodatkowa dokumentacja regulująca dany obszar, daną materię.

******

KONIEC DOKUMENTU

Członek Zarządu
inż. Jan Mistur

Członek Zarządu
Mirosław Wiśniowski