POLITYKA BEZPIECZEŃSTWA

<<nazwa spółki>>

Wydanie 1

xx.xx.xxxx

Spis treści

1. INFORMACJE OGÓLNE 3
2. DEFINICJE 4
3. ZAKRES STOSOWANIA POLITYKI 3
4. OGÓLNE ZASADY OCHRONY DANYCH OSOBOWYCH 3
5. ZAKRES OBOWIĄZKÓW I ŚWIADOMOŚĆ PRACOWNIKÓW 6
    1. Obowiązki Administratora 6
    2. Obowiązki IOD/Koordynatora ds. ochrony danych osobowych 7
    3. Obowiązki Pracownika 7
6. SZCZEGÓŁOWE ZASADY OCHRONY DANYCH OSOBOWYCH 4
    1. Prawa osób, których dane dotyczą 4
    2. Rejestr czynności przetwarzania 9
    3. Rejestr kategorii czynności przetwarzania 9
    4. Powierzenie przetwarzania danych osobowych 9
    5. Retencja danych 10
    6. Zarządzanie incydentami bezpieczeństwa oraz naruszeniami ochrony danych osobowych 6
    7. Uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych 6
    8. Ocena Skutków dla Ochrony Danych Osobowych (OSOD) 11
    9. Audyty systemu ochrony danych osobowych i przegląd dokumentacji 7
7. ŚRODKI ORGANIZACYJNE NIEZBĘDNE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZY PRZETWARZANIU DANYCH OSOBOWYCH 12
    1. Zastosowane środki ochrony do zabezpieczenia fizycznego pomieszczeń, w których przetwarzane są dane osobowe: 12
8. ZARZĄDZANIE SYSTEMAMI INFORMATYCZNYMI 13
    1. Procedura zarządzania uprawnieniami do przetwarzania danych w systemie informatycznym 14
    2. Procedura rozpoczęcia i zakończenia pracy 15
    3. Zarządzanie nośnikami danych, w tym kopiami danych. 16
9. POSTANOWIENIA KOŃCOWE 17

(.....)

3. Zakres stosowania Polityki

Niniejszą Politykę stosuje się do wszelkich operacji przetwarzania danych osobowych w Spółce, w tym do przetwarzania danych w systemach informatycznych.

Spółka przetwarza m.in. dane osobowe:

1. klientów, kontrahentów
2. kandydatów do pracy, pracowników oraz byłych pracowników,
3. członków należących do organów Spółki,
4. osób współpracujących na zasadach stałych, jednorazowych lub doraźnych w celu wykonywania umowy,
5. osób reprezentujących lub osób kontaktowych partnerów oraz innych podmiotów, z którymi współpracuje Spółka.

4. Ogólne zasady ochrony danych osobowych

1. Podstawowe zasady ochrony danych osobowych w Spółce

Spółka przetwarza dane osobowe zgodnie z poniższymi zasadami:

1. **przetwarzanie danych osobowych rzetelnie, zgodnie z prawem i przejrzyście**: Spółka posiada podstawę prawną i cel biznesowy przetwarzania danych oraz transparentnie informuje osoby o sposobach tego przetwarzania;
2. **przetwarzanie danych osobowych jest ograniczone do pierwotnego celu**: dane nie są wykorzystywane w sposób niezgodny z pierwotnym celem ich gromadzenia;
3. **przetwarzanie danych osobowych jest ograniczone do niezbędnego minimum**: Spółka gromadzi i przechowuje jedynie dane niezbędne do realizacji celu;
4. **dane osobowe są dokładne i aktualne**: Spółka zapewnia poprawność i aktualność danych tam, gdzie ma to zastosowanie;
5. **przetwarzanie danych osobowych nie dłużej niż jest to konieczne do realizacji określonego celu biznesowego lub wymogów prawa**: wprowadzono zasady usuwania i retencji przetwarzanych danych;
6. **stosowanie adekwatnych do ryzyka środków zabezpieczeń danych osobowych** również, gdy są one przekazywane przez strony trzecie: stosowane są środki bezpieczeństwa odpowiednie dla danej kategorii danych oraz zasady doboru podwykonawców;
7. **przetwarzanie danych osobowych zgodnie z prawami przysługującymi osobom**: zapewnia się realizację praw każdej osobie, której dane są przetwarzane;
8. **rozliczalność** (wykazanie stosowania wdrożonych zasad): Spółka konsultuje zmiany zgodnie
   z zasadą ochrony danych w fazie projektowania, utrzymuje rejestr czynności przetwarzania, stosuje podejście oparte na ryzyku oraz przeprowadza ocenę skutków dla ochrony danych, gdy ma to zastosowanie.

5. System ochrony danych osobowych

Ustanowiony w Spółce system ochrony danych osobowych jest zgodny z wymaganiami prawa właściwego i składa się z następujących elementów:

1. **upoważnienia do przetwarzania danych** – udzielanie upoważnienia do przetwarzania danych osobowych zachodzi wobec każdego pracownika i współpracownika, który w związku z wykonywaniem obowiązków służbowych przetwarza dane osobowe;
2. **inwentaryzacja danych i procesów** – identyfikacja wszystkich zasobów danych osobowych, ich kategorii oraz procesów prowadzonych w Spółce, w których dochodzi lub może dochodzić do przetwarzania danych osobowych i utrzymywanie ich w formie rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania;
3. **obsługa praw osób** – wypełnianie wszystkich obowiązków ciążących na Administratorze, w tym spełnienie obowiązku informacyjnego względem osób, których dane dotyczą, obsługa żądań w terminach i zgodnie z wymaganiami RODO i innych aktów wykonawczych oraz zawiadamianie o naruszeniach ochrony danych osobowych;
4. **zarządzanie minimalizacją danych** – wdrożenie zasad adekwatności danych, reglamentacji i zarządzania dostępem do tych danych oraz zarządzanie okresem przechowywania i weryfikacji dalszej przydatności;
5. **bezpieczeństwo** – zapewnienie odpowiedniego poziomu bezpieczeństwa danych poprzez wdrożenie adekwatnych środków technicznych i organizacyjnych odpowiadającym ryzyku.

(.....)

6. Szczegółowe zasady ochrony danych osobowych

1. Prawa osób, których dane dotyczą

a) W Spółce zgodnie z obowiązującymi regulacjami realizowane są prawa osób, których dane są przetwarzane, w tym prawo do:

- dostępu do danych,
- sprostowania danych,
- usunięcia danych,
- ograniczenia przetwarzania,
- przenoszenia danych,
- wniesienia sprzeciwu wobec przetwarzania,
- niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu.

b) Spółka dba o czytelność i formę przekazywanych informacji oraz o dotrzymywanie prawnych terminów realizacji obowiązków względem osób, których dane dotyczą, w tym określiła zasady komunikacji z nimi.

c) Spółka wprowadziła adekwatne metody identyfikacji podmiotów danych na potrzeby realizacji ich praw.

d) Spółka dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

e) **Szczegółowe zasady związane z realizacją praw osób:**

- przysługujących prawach Administrator informuje osoby, których dane dotyczą w klauzulach informacyjnych.
- Klauzule informacyjne zawierają katalog praw osób wraz ze wskazaniem kanałów komunikacji i danych teleadresowych, którymi należy zgłaszać żądania.
- Osobą odpowiedzialną za koordynację procesu realizacji praw osób jest IOD/Koordynator, a w szczególności do jego obowiązków należy:
  - przyjmowanie i weryfikacja wniosku,
  - kontakt z osobą, której dane dotyczą,
  - współpraca z pracownikami i współpracownikami odpowiedzialnymi za dany obszar przetwarzania danych.
- Wnioski dotyczące realizacji praw osób mogą m.in. być składane:
  - drogą elektroniczną,
  - telefonicznie.
- Wszyscy pracownicy, w przypadku odebrania wniosku dotyczącego realizacji praw zobowiązani są do niezwłocznego przekazania żądania do IOD/Koordynatora drogą elektroniczną.
- IOD/Koordynator w momencie otrzymania wniosku we współpracy z osobami odpowiedzialnymi za dany obszar przetwarzania danych weryfikuje jego zasadność oraz decyduje o możliwości i sposobie realizacji żądania.
- IOD/Koordynator zapewnia, aby bez zbędnej zwłoki – a w każdym razie w terminie nieprzekraczającym miesiąca od otrzymania żądania udziela osobie, której dane dotyczą informacji o:
  - działaniach podjętych w związku z wystosowanym wnioskiem,
  - konieczności wydłużenia terminu realizacji żądania wraz z podaniem przyczyn opóźnienia,
  - niepodejmowaniu działań w związku z żądaniem wraz z uzasadnieniem takiej decyzji.
- Jeżeli IOD/Koordynator lub inna osoba, które została upoważniona do realizacji praw osób ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.
- Szczegółowy tryb postępowania opisano w **Procedurze realizacji praw osób**.

f) **Zgoda na przetwarzanie danych osobowych**

- We wszystkich przypadkach, w których jedyną podstawą do przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a RODO), Spółka odbiera ją w sposób sformalizowany i możliwy do udowodnienia tj. w wersji papierowej, elektronicznej lub nagranej.
- W uzasadnionych sytuacjach zgoda interpretowana jest jako wyraźne działanie potwierdzające osoby, której dane dotyczą.
- W każdym przypadku dowody wyrażenia zgody przechowywane są w systemie informatycznym lub w innym w miejscu do tego wyznaczonym.
- Niniejsze podejście pozwala wykazać Spółce, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych oraz zapewnia spełnienie obowiązku rozliczalność, o którym mowa w art. 5 ust. 2 RODO.

(.....)

6. **Zarządzanie incydentami bezpieczeństwa oraz naruszeniami ochrony danych osobowych**

a) Za incydent bezpieczeństwa uznaje się w Spółce w m.in.:
- kradzież, zagubienie lub pozostawienie w niezabezpieczonej lokalizacji nośnika zawierającego dane osobowe (np. dokumentu w wersji papierowej, pen-drive, laptopa),
- utracenie danych osobowych spowodowane działaniem umyślnym lub zdarzeniami losowymi np. awarią, nieprawidłowym działaniem lub błędną obsługą systemu informatycznego (np. pożar, zalanie, awarie systemu, zniszczenie wersji papierowej dokumentu),
- błędne wprowadzenie lub zmodyfikowanie danych osobowych,
- przekazanie danych osobowych osobom nieuprawnionym (np. wysłanie błędnie zaadresowanego listu lub wiadomości elektronicznej, przekazanie dokumentacji nieuprawnionej osobie, ustne ujawnienie danych osobowych osobom nieuprawnionym),
- nieuprawnione uzyskanie dostępu do danych wynikające np. z błędnie przydzielonych praw dostępu w systemie informatycznym, nieodpowiednio ustawionego monitora,
- działanie szkodliwego oprogramowania ingerującego w poufność, integralność lub dostępność danych osobowych,
- wszelkie inne incydenty, które mogą powodować naruszenia praw lub wolności podmiotów danych.

b) Incydent bezpieczeństwa może być uznany za naruszenia ochrony danych osobowych.

c) Szczegóły dotyczące postępowania w przypadku wystąpienia incydentu opisano w **Procedurze zarządzania incydentami**.

7. Uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych

a) Administrator zgodnie z art. 25 RODO wprowadził zasady, które nakazują uwzględnianie ochrony danych osobowych i prywatności na każdym etapie tworzenia oraz funkcjonowania procesów i systemów wykorzystywanych do przetwarzania danych osobowych, w tym również na etapie projektowania.

b) Przed rozpoczęciem nowego procesu biznesowego, w ramach którego będą przetwarzane dane osobowe lub może dochodzić do ich przetwarzania, każdy Pracownik odpowiedzialny za wdrożenie procesu jest zobowiązany zwrócić się do IOD/Koordynatora o ocenę czy proces/system spełnia wymagania przepisów prawa, w tym jest zgodny z zasadą domyślnej ochrony danych.

c) IOD/Koordynator włączany jest we wszystkie prace rozwojowe w pierwszych etap ich planowania i realizacji.

d) Administrator zapewnia takie ustawienie wykorzystywanych systemów służących przetwarzaniu danych, które ograniczają możliwość udostępniania danych tylko do tej niezbędnej do realizacji celów.

(.....)

9. Audyty systemu ochrony danych osobowych i przegląd dokumentacji

a) Polityka powinna być poddawana przeglądowi przynajmniej raz na rok i zawsze, gdy zajdą istotne zmiany dotyczące przetwarzania danych osobowych.
b) Do kontroli stanu ochrony danych osobowych w Spółce upoważnieni są Administrator i IOD/Koordynator.
c) IOD/Koordynator analizuje, czy Polityka i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do zmian organizacyjnych Administratora, zmian w budowie systemu informatycznego oraz zmian w obowiązującym prawie.
d) IOD/Koordynator po uzgodnieniu z Administratorem może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych.
e) Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z Administratorem. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym przez IOD/Koordynatora i przedstawiane w formie pisemnej do wiadomości Administratora.
f) Administrator biorąc pod uwagę wnioski z audytu, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.
g) Za wyniki przeprowadzonych audytów odpowiedzialność ponosi Administrator.