



## **POLITYKA OCHRONY DANYCH OSOBOWYCH**

W SPÓŁCE

**„XOPERO SOFTWARE” SPÓŁKA AKCYJNA  
Z SIEDZIBĄ W GORZOWIE WLKP.**

WERSJA DOKUMENTU: **1.0**

WESZŁA W ŻYCIE: **05.02.2018**

TERMIN NASTĘPNEJ WERYFIKACJI: **05.02.2019**

## DZIAŁ I: ZASADY

### I. CEL POLITYKI OCHRONY DANYCH OSOBOWYCH

1. Polityka Ochrony Danych Osobowych została utworzona w związku z wymaganiami zawartymi 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).
2. Określa się następujące definicje najważniejszych pojęć użytych w niniejszym dokumencie:
  - a) **Polityka** lub **PODO** – niniejsza Polityka Ochrony Danych Osobowych.
  - b) **Spółka** – rozumie się przez to XOPERO SOFTWARE S.A. z siedzibą w Gorzowie Wlkp., ul. Herberta 3, 66-400 Gorzów Wlkp., wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000684240, NIP nr 599-306-66-03, REGON nr 080285693.
  - c) **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.
  - d) **Przetwarzanie** – operacja 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.
  - e) **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

### II. PODSTAWOWE ZASADY

Spółka wdraża niniejszą Politykę, aby zapewnić, że dane osobowe przekazane do przetwarzania przez Spółkę będą:

- a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- b) zbierane w konkretnych, wyraźnych i uzasadnionych celach oraz nieprzetwarzane dalej w sposób niezgodny z tymi celami;
- c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
- d) prawidłowe i w razie potrzeby uaktualniane;
- e) 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;
- f) 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.

### III. ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych przez Spółkę w podstawowym zakresie odbywa się na podstawie zgody osoby, której dane dotyczą.
2. Zgoda może być udzielona zarówno pisemnie, jak i za pośrednictwem środków porozumiewania się na odległość.
3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Jednakże wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.
4. Przetwarzanie danych osobowych przez Spółkę odbywa się ponadto w zakresie, w jakim 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. Zgoda na przetwarzanie danych osobowych może być udzielona jedynie przez osobę, która ukończyła 18 rok życia. W imieniu osób poniżej tej granicy wieku, zgoda musi być wyrażona przez przedstawicieli ustawowych tej osoby.

### IV. POZOSTAŁE PODSTAWY PRZETWARZANIA DANYCH OSOBOWYCH

Spółka może przetwarzać dane osobowe także, gdy:

- a) 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;
- b) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

- d) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- e) 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.

### **V. DOSTĘP DO DANYCH OSOBOWYCH**

1. Osoba, której dotyczą dane osobowe, jest uprawniona do uzyskania od Spółki potwierdzenia, czy przetwarzane są przez Spółkę dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
  - a) cele przetwarzania;
  - b) kategorie odnośnych danych osobowych;
  - c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
  - d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
  - e) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
  - f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Spółka dostarczy osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Spółka może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.
3. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

### **VI. SPROSTOWANIE DANYCH OSOBOWYCH**

Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

### **VII. USUNIĘCIE DANYCH OSOBOWYCH („BYCIE ZAPOMNIANYM”)**

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego usunięcia dotyczących jej danych osobowych, a Spółka bez zbędnej zwłoki usunie dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
  - a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
  - b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
  - c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
  - d) dane osobowe były przetwarzane niezgodnie z prawem;
  - e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie polskim;
  - f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.
2. W przypadku gdy Spółka dokonała upublicznienia danych osobowych, a ma obowiązek usunąć te dane zgodnie z postanowieniem powyżej, to – biorąc pod uwagę dostępną technologię i koszt realizacji – Spółka podejmuje rozsądne działania, w tym środki techniczne, by poinformować wszystkich innych administratorów przetwarzających takie dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.
3. Spółka będzie miała prawo odmówić usunięcia w całości lub części danych osobowych, jeżeli ich przetwarzanie jest niezbędne:
  - a) do korzystania z prawa do wolności wypowiedzi i informacji;
  - b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa, któremu podlega Spółka;
  - c) do ustalenia, dochodzenia lub obrony roszczeń.

## DZIAŁ II: KWESTIE PODSTAWOWE

### 1. OSOBY ZAANGAŻOWANE W PROCES PRZETWARZANIA DANYCH OSOBOWYCH

#### 1.1. Administrator danych osobowych

Administratorem danych osobowych jest:

**Nazwa:** XOPERO SOFTWARE S.A. z siedzibą w Gorzowie Wlkp.  
**Forma prawna:** spółka akcyjna  
**NIP:** 599-306-66-03  
**REGON:** 080285693  
**KRS:** 0000684240  
**Adres:** ul. Herberta 3, 66-400 Gorzów Wlkp., Polska

#### 1.2. Osoby upoważnione do przetwarzania danych osobowych

Spółka prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych ze wskazaniem celów konkretnego upoważnienia oraz zbiorów danych osobowych, których dotyczy upoważnienie.

Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest w formie pisemnej oraz może być prowadzona także w formie elektronicznej. Forma pisemna stanowi załącznik nr 1 do Polityki.

Upoważnienia nadaje oraz cofa Zarząd Spółki w formie pisemnej. Wzór upoważnienia stanowi załącznik nr 2 do Polityki.

#### 1.3. Inspektor Ochrony Danych Osobowych (IOD)

IOD będzie wyznaczony, ponieważ Spółka przetwarza dane osobowe z wielu źródeł, świadcząc usługi na rzecz licznych podmiotów, tak więc profesjonalizacja kwestii dotyczących ochrony danych osobowych jest w pełni uzasadniona.

Inspektor Ochrony Danych Osobowych będzie wyznaczany przez Zarząd Spółki na co najmniej 2-letnie kadencje. IOD bezpośrednio podlega najwyższemu kierownictwu Spółki.

IOD będzie właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

IOD nie będzie otrzymywał instrukcji dotyczących wykonywania swoich zadań. Nie może być on odwołany ani karany za wypełnianie swoich zadań.

Osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem przysługujących im praw.

IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

Wzór wyznaczenia IOD stanowi załącznik nr 3 do Polityki.

### **1.4. Podmioty przetwarzające**

Spółka może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej lub elektronicznej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.

Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach podmiotu przetwarzającego dotyczących zabezpieczenia danych osobowych.

Wykaz podmiotów przetwarzających, z którymi jest prowadzona współpraca stanowi załącznik nr 4 do Polityki.

## **2. RODZAJE PRZETWARZANYCH DANYCH OSOBOWYCH**

Spółka, w różnych sytuacjach, przetwarza lub może przetwarzać następujące rodzaje danych osobowych:

- a) Imię i nazwisko,
- b) Numer identyfikacyjny (NIP, PESEL);
- c) Ograniczone dane finansowe;
- d) Dane kontaktowe: numery telefonów, e-maile, adresy korespondencyjne;
- e) Adresy IP.

Nie jest wykluczone przetwarzanie innych danych, niż tylko te, które zostały wskazane powyżej, lecz każdorazowo musi się to odbywać albo na podstawie zgody, o której mowa w Dziale I punkt III lub na jednej z pozostałych podstaw wskazanych w Dziale I punkt IV.

## **3. ZBIORY DANYCH OSOBOWYCH**

Spółka dokonuje podziału posiadanych i przetwarzanych danych osobowych na zbiory, które utworzone są w oparciu o cechę kluczową osób, których dany zbiór dotyczy, lub zawartości tego zbioru, lub sposobu pozyskiwania danych do danego zbioru.

Jednie osoby upoważnione do przetwarzania danego zbioru mogą mieć do niego dostęp.

Lista zbiorów danych osobowych stanowi załącznik nr 5 do Polityki.

## 4. NOŚNIKI DANYCH OSOBOWYCH I SYSTEMY INFORMATYCZNE

W ramach przetwarzania danych osobowych Spółka będzie wykorzystywać następujące nośniki danych:

- a) Dokumentacja papierowa;
- b) Dyski twarde;
- c) Telefony komórkowe;
- d) Pendrive;
- e) Płyty DVD/CD.

Systemy informatyczne i programy komputerowe, które są wykorzystywane, lub będą wykorzystywane:

- a) Internetowe skrzynki pocztowe;
- b) Aplikacje web.
- c) Pakiety biurowe.

## 5. POMIESZCZENIA, W KTÓRYCH SĄ PRZETWARZANE DANE OSOBOWE

W zakresie zabezpieczenia organizacyjnego i technicznego niniejsza Polityka dotyczy siedziby Spółki i wszelkich nieruchomości znajdujących się pod bezpośrednią kontrolą Spółki.

Budynek, w którym znajdują się pomieszczenia, w których przetwarzane są dane osobowe, znajduje się pod całodobową ochroną zleconą profesjonalnemu podmiotowi zewnętrznemu (firma ochroniarska). Drzwi wejściowe do budynku zamknięte są w godzinach od 21:00 do 06:00 i uzyskanie klucza wejściowego może nastąpić wyłącznie za pośrednictwem ochrony.

Budynek, jego najbliższe otoczenie oraz wewnętrzne części wspólne (klatki schodowe, korytarze) objęte są monitoringiem audio-wizualnym. Zapis z monitoringu przechowywany jest przez 30 dni od jego wykonania.

W ramach pomieszczeń zajmowanych przez Spółkę wydziela się sektory tematyczne, oddzielone ścianami i drzwiami, z możliwością zakluczenia. Sektory są następujące:

- a) Dział biurowo-administracyjny.
- b) Dział techniczny.
- c) Dział developmentu.
- d) Dział sprzedaży.

Spółka wdrożyła szczegółową politykę zarządzania kluczami wewnętrznymi, która ma na celu ograniczenie dostępności określonych sektorów jedynie do upoważnionych osób.



## DZIAŁ III: PRACOWNICY

Niniejszy dział poświęcony jest szczególnym zasadom przetwarzania danych osobowych pracowników. W zakresie nieuregulowanym postanowienia Działów I i II Polityki mają odpowiednie zastosowanie.

### 1. Rodzaje danych osobowych pracowników

Spółka, przetwarza lub może przetwarzać następujące rodzaje danych osobowych pracowników:

- a) Imię i nazwisko;
- b) dane teleadresowe;
- c) numer identyfikacyjny;
- d) numer konta bankowego;
- e) dane dotyczące rodziny;
- f) podstawowe dane dotyczące zdrowia;
- g) historia zatrudnienia
- h) wykształcenie,
- i) zainteresowania.

### 2. Rodzaje pod-zbiorów zawierających dane osobowe pracowników

Spółka dokonuje podziału zbioru danych pracowników na pod-zbiory, które utworzone są w oparciu o wyróżniającą cechę kluczową z uwagi na zawartości tego pod-zbioru, lub sposobu pozyskiwania danych do danego pod-zbioru.

Jednie osoby upoważnione do przetwarzania danego pod-zbioru mogą mieć do niego dostęp.

Utworzone zostały następujące pod-zbiory w Spółce:

- a) Akta osobowe,
- b) Listy płac,
- c) Listy obecności,
- d) Rejestr czasu pracy,
- e) Rejestr kar dyscyplinarnych.

### 3. Systemy informatyczne i programy komputerowe, które są lub będą wykorzystywane

Dodatkowe systemy informatyczne i programy komputerowe, które są wykorzystywane, lub będą wykorzystywane przy przetwarzaniu danych osobowych pracowników:

- a) Płatnik;

### 4. Pomieszczenia, w których są przetwarzane dane osobowe pracowników

Dane osobowe pracowników będą mogły być przetwarzane w ramach sektora Biurowo-administracyjnego.

Dopuszcza się przekazanie do przetwarzania danych osobowych pracowników podmiotu trzeciego – zewnętrznej firmy księgowej lub kadrowej.

### **5. Czynności przetwarzania danych osobowych pracowników**

Wykaz podejmowanych czynności przetwarzania wraz z ich opisem:

- a) Rekrutacja – pobranie kwestionariusza CV, listu motywacyjnego, zgody na przetwarzanie danych osobowych.
- b) Zatrudnienie – podpisanie umowy, wstępne badania lekarskie, szkolenie BHP, kwestionariusz osoby zatrudnionej.
- c) Świadczenie pracy – weryfikacja obecności, rejestracja czasu pracy, wypłata wynagrodzeń, opłacanie należności publiczno-prawnych, nadzór nad obowiązkami pracowniczymi, korzystanie z urlopów.
- d) Zakończenie pracy – wydanie świadectwa pracy, wypłata należnych świadczeń.

### **6. Opis procesu rekrutacyjnego**

Rekrutacja odbywa się poprzez umieszczenie ogłoszenia w wybranym serwisie internetowym.

Na podstawie przesłanych dokumentów dokonuje się wstępnej selekcji kandydatów.

Wybrane osoby są zapraszane na rozmowy kwalifikacyjne do siedziby Spółki.

Rozmowa prowadzona jest przez Zarząd oraz kierownika działu do którego jest nabór.

Zdarza się, że po kilku rozmowach kwalifikacyjnych kandydaci są zapraszani na jeszcze jedną dodatkową rozmowę.

### **7. Opis czynności związanych z zakończeniem stosunku pracy**

Po ustaniu stosunku pracy niezwłocznie wydawane jest świadectwo pracy.

Akta osobowe zostają zarchiwizowane w siedzibie Spółki. Konto e-mailowe zostaje dezaktywowane, karta dostępu jest przeprogramowywana, wykasowane zostają dane z rejestratora czasu pracy.

### **8. Dokumenty żądane od pracowników w trakcie zatrudnienia**

Rodzaje dokumentów wymaganych od pracowników w trakcie zatrudnienia:

- a) Świadectwa pracy,
- b) Dyplomy,

- c) Certyfikaty
- d) Oświadczenia o członkach rodziny podlegających zgłoszeniu do ubezpieczeń
- e) Zaświadczenie lekarskie o braku przeciwwskazań do wykonywanej pracy
- f) Oświadczenie o niepełnosprawności, przynależności do oddziału NFZ, o podleganiu pod Urząd Skarbowy, o chęci skorzystania z prawa do opieki na dziecko, o zapoznaniu się przepisami BHP, regulacjami wewnętrznymi.

Dokumenty są kompletowane w dziale administracji Spółki. Po skompletowaniu zostają dostarczone do działu kadr zewnętrznej firmy kadrowej W dziale kadr zakładane i prowadzone są akta osobowe w formie papierowej. Akta osobowe przechowywane są w szafie pancernej.

### **9. Prowadzenie rejestru wyjść poza zakład pracy i zbiorczych list obecności**

Rejestr wyjść poza zakład pracy jest prowadzony w formie papierowej, znajduje się w dziale administracji.

Obecność jest potwierdzana poprzez kartę magnetyczną lub brelok magnetyczny. Prowadzone są również osobowe listy obecności w formie papierowej.

### **10. Paski wynagrodzeń**

Paski wynagrodzeń są spięte w sposób uniemożliwiający odczyt bez ich zniszczenia. Rozdawane indywidualnie przez osobę upoważnioną.

## **DZIAŁ IV: REALIZACJA OBOWIĄZKÓW ADMINISTRATORA DANYCH OSOBOWYCH**

### **1. Formy realizacji obowiązków informacyjnych**

Formy przekazywania informacji osobom fizycznym:

- a) Na stronie internetowej;
- b) Pisemnie,
- c) E-mail,
- d) Telefon.

### **2. Sposoby realizacji obowiązków informacyjnych**

Sposoby przekazywania informacji przewidzianych w RODO:

- a) specjalny dział na stronie internetowej,
- b) dedykowany dokument – karta informacyjna, udostępniona na stronie internetowej oraz jednocześnie z pobraniem danych osobowych i wyrażeniu zgody na ich przetwarzanie.
- c) W przypadkach indywidualnych – osobiste, mailowe i telefoniczne przez Inspektora Ochrony Danych Osobowych.

### **3. Sposoby uzyskiwania zgody na przetwarzanie danych osobowych**

Formy i sposoby uzyskiwania zgody:

- a) Formularz elektroniczny.
- b) Telefon.
- c) Formularz papierowy.

Wycofanie zgody na przetwarzanie danych osobowych może nastąpić w dowolnej formie z powyższych.

### **4. Procedura weryfikacji tożsamości zgłaszającego**

Opis sposobów weryfikacji tożsamości zgłaszającego:

- a) W przypadku kontaktu osobistego – prośba o okazanie dokumentu tożsamości, bez prawa jego zatrzymania czy też wykonania kopii.
- b) W przypadku kontaktu na odległość – pytania o rzeczy charakterystyczne i indywidualne dla konta (np. nazwa loginu, nazwa usługi, nazwa projektu, adres e-mail)

### **5. Procedura rozpoznania zgłoszeń związanych z realizacją praw**

Opis sposobu realizacji procedury związanej z realizacją praw osób, których dane osobowe są przetwarzane:

- a) Wystosowanie zgłoszenia do IOD.

- b) Przyjęcie zgłoszenia.
- c) Weryfikacja tożsamości osoby zgłaszającej
- d) Rozpatrzenie zgłoszenia – do 30 dni.
- e) Możliwość przedłużenia terminu rozpatrzenia zgłoszenia do 90 dni
- f) Podjęcie decyzji
- g) Realizacja decyzji

## **DZIAŁ V: REJESTRY I EWIDENCJE**

### **1. Rejestr czynności przetwarzania danych osobowych**

Spółka tworzy i utrzymuje na bieżąco rejestr czynności przetwarzania danych osobowych, który stanowi załącznik nr 6 do Polityki.

### **2. Rejestr naruszeń ochrony danych osobowych**

Spółka tworzy i utrzymuje na bieżąco rejestr naruszeń danych osobowych, który stanowi załącznik nr 7 do Polityki.

### **3. Ewidencja osób upoważnionych do przetwarzania danych osobowych i ich uprawnień**

Spółka tworzy i utrzymuje na bieżąco ewidencję osób upoważnionych do przetwarzania danych osobowych, która stanowi załącznik nr 1 do Polityki.

## DZIAŁ VI: ŚRODKI BEZPIECZEŃSTWA

### 1. Środki zabezpieczeń danych osobowych poza systemami informatycznymi

odpowiednie zamki w drzwiach
magnetyczne karty dostępu
system kontroli dostępu do pomieszczeń
fizyczne ograniczenie dostępu do serwerów i infrastruktury sieciowej
ochrona fizyczna
monitoring wizyjny
systemy alarmowe
całodobowy monitoring sygnału alarmu
ograniczenie dostępu do szyfrów rozbrajających alarm
nadzór nad kluczami do pomieszczeń
nadzór nad kluczami do szafy pancernej
szafa pancerna
polityka czystego biurka
odpowiednie ustawienie monitora
właściwy obieg dokumentów

**2. Środki zabezpieczeń danych osobowych w systemach informatycznych**

odpowiednia polityka haseł
odrębny identyfikator dla każdego użytkownika w systemie informatycznym
używanie oprogramowania umożliwiającego tworzenie kont użytkowników
blokada przydzielania tego samego identyfikatora innej osobie
dostęp do systemu możliwy po wprowadzeniu danych uwierzytelniających
dostęp do urządzeń po podaniu loginu i hasła
ograniczenie dostępu użytkownika do określonych zasobów
automatyczne wylogowanie z systemu po określonym czasie braku aktywności
testowanie jakości aplikacji (przegląd kodu, testy typu czarne skrzynka, testy siłowe)
programy i skanery antywirusowe
Firewall
Proxy
DNS
ochrona przed phishingiem
ochrona przed atakami Cross Site Scripting
ochrona przed Cross Site Request Forgery
ochrona przed atakami SQL Injection
wykorzystanie VNC, RConsole, TeamViewer (przy ich należytych zabezpieczeniu)
regularne aktualizowanie oprogramowania
wykonywanie kopii zapasowych danych
wykonywanie kopii zapasowych programów
wykonywanie kopii zapasowych serwerów
standaryzacja sprzętu
standaryzacja oprogramowania
kontrola instalowanego oprogramowania
Pseudonimizacja