POLITYKA
OCHRONY DANYCH OSOBOWYCH

obowiązująca w spółce:

Q-Systems spółka z ograniczoną odpowiedzialnością

ZATWIERDZAM

_____

(data i podpis Administratora Danych)

Spis treści:

Podstawa prawna:

- **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- ogólne rozporządzenie o ochronie danych (Dz.U.UE.L.2016.119.1 z dnia 2016.05.04);**
- **USTAWA z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 z dnia 2018.05.24);**
- **USTAWA z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U.2018.917 t. j. z dnia 2018.05.16).**

§ 1
DEKLARACJA I ZASTOSOWANIE

1. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO- rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 osobowych). Niniejsza Polityka stanowi schemat wymogów, zasad i regulacji ochrony danych osobowych w spółce Q- Systems spółka z ograniczoną odpowiedzialnością, zwanej dalej Spółką.

2. Polityka została opracowana na podstawie aktualnie obowiązujących przepisów w zakresie ochrony danych osobowych.

3. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w niniejszej Polityce Ochrony Danych Osobowych obowiązują wszystkich pracowników i współpracowników Spółki.

4. Administrator Danych ma świadomość znaczenia i wagi ochrony informacji, ze szczególnym uwzględnieniem ochrony danych osobowych i wdraża środki służące realizacji tej ochrony.

5. Polityka dotyczy wyposażenia, systemów, urządzeń przetwarzających informacje w formie elektronicznej, papierowej lub jakiejkolwiek innej.

6. Polityka określa środki techniczne i organizacyjne zastosowane przez Administratora Danych dla zapewnienia ochrony danych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych zarówno w systemie informatycznym jak i w formie materialnej, albo w sytuacji podejrzenia o takim naruszeniu.

7. Zakres obowiązywania dokumentu:

7.1. Niniejsza Polityka obowiązuje wszystkich pracowników, współpracowników, a także partnerów handlowych Spółki.

7.2. Każdy z pracowników ma obowiązek zapoznania się z treścią Polityki.

7.3. Nieprzestrzeganie postanowień, zawartych w dokumentacji bezpieczeństwa informacji, może skutkować sankcjami w pełnym zakresie dopuszczonym przez stosunek pracy pomiędzy Administratorem Danych i pracownikiem oraz obowiązujące przepisy prawa.

7.4. Stosowanie zasad ochrony danych osobowych oraz regulacji wewnętrznych, odnoszących się do danych osobowych, stanowi podstawowy obowiązek pracowniczy.

§ 2
DEFINICJE

1.Definicje, użyte w niniejszym dokumencie mają następujące znaczenie:

Polityka- oznacza niniejszą Politykę Ochrony Danych Osobowych, o ile co innego nie wynika wyraźnie z treści lub z kontekstu;

RODO- oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 osobowych (Dz. Urz. UE L 119, s. 1);

Dane osobowe lub dane- oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. 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;

Dane szczególnych kategorii- oznaczają dane osobowe, wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;

Dane karne- oznaczają dane osobowe, wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa;

Dane dzieci- oznaczają dane osób poniżej 16 roku życia;

Osoba- oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z treści lub z kontekstu;

Przetwarzanie danych- rozumie się przez to jakiekolwiek operacje lub zestaw operacji, wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczenie, usuwanie lub niszczenie;

Administrator Danych- rozumie się przez to spółkę Q- Systems Spółka z ograniczoną odpowiedzialnością z siedzibą w Lesznie, zwaną dalej Spółką;

Specjalista ds. ochrony danych osobowych- (dalej Specjalista odo)- rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony przetwarzanych danych osobowych i innych informacji prawem chronionych. Nadzoruje on stosowanie środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem, lub zniszczeniem, a także przeprowadzi kontrole w zakresie określonym regulacjami wewnętrznymi Administratora Danych. Specjalista nie jest Inspektorem Ochrony Danych Osobowych. Administrator może ustanowić Specjalistę, a jeśli tego nie zrobi, to obowiązki przypisane Specjaliście wykonuje Administrator;

Administrator Systemu Informatycznego- rozumie się przez to osobę nadzorującą prawidłowe funkcjonowanie sprzętu, oprogramowania i jej konserwację, odpowiadającą za koordynowanie techniczno- organizacyjnej obsługi systemów teleinformatycznych, zwanego dalej „Informatykiem" lub „ASI". Administrator może ustanowić Administratora Systemu Informatycznego, a jeśli tego nie zrobi, to obowiązki przypisane Administratorowi Systemu Informatycznego wykonuje Administrator;

Podmiot przetwarzający- oznacza organizację lub osobę, której Spółka powierzyła przetwarzanie danych osobowych;

Użytkownik- rozumie się przez to osobę upoważnioną przez Administratora danych do przetwarzania informacji i danych osobowych;

RCPD lub Rejestr- oznacza Rejestr Czynności Przetwarzania Danych Osobowych;

Aktywa- wszystko, co ma wartość dla organizacji (wartość materialna: np. pracownicy, komputery, bazy danych itp.; wartość niematerialna: dobre imię, wizerunek itp.);

Zbiór danych- rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

System informatyczny- rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

Bezpieczeństwo danych- zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

Usuwanie danych- rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

Komórka organizacyjna- rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z podziałem organizacyjnym przeprowadzonym przez Administratora Danych;

Pomieszczenia- rozumie się przez to budynki i pomieszczenia określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawnie chronione;

Incydent- pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń, związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

§ 3
ZASADY I CELE OCHRONY DANYCH

1. System zarządzania bezpieczeństwem danych osobowych w Spółce opiera się na następujących zasadach ochrony informacji:

a. **Legalność-** Spółka dba o ochronę prywatności i przetwarza dane zgodnie z prawem, w oparciu o podstawę prawną. Podstawą prawną może być w szczególności właściwy przepis prawa, umowa, zgoda upoważnionej osoby, żywotny interes osoby, której dane dotyczą lub uzasadniony interes;
b. **Bezpieczeństwo-** Spółka zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie;
c. **Respektowanie Praw Jednostki-** Spółka umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje;
d. **Rzetelność**- Spółka przetwarza dane rzetelnie i uczciwie oraz z dbałością o prawidłowość danych;
e. **Transparentność**- oznacza przejrzystość dla osoby, której dane dotyczą;
f. **Minimalizacja**- przetwarzanie następuje w konkretnych, istniejących lub przewidywalnych i realnych celach, lecz nie "na zapas";
g. **Adekwatność**- przetwarzanie następuje w zakresie nie większym niż wynika to z uzasadnionej potrzeby;
h. **Czasowość-** przetwarzanie następuje nie dłużej niż trwa uzasadniona potrzeba;
i. **Bezpieczeństwo-** przetwarzanie następuje z zapewnieniem odpowiedniego bezpieczeństwa danych;
j. **Zasada znajomości wymagań polityki ochrony danych**- każdy pracownik powinien zostać zapoznany z regułami oraz z kompletnymi i aktualnymi procedurami ochrony danych i podpisać stosowne oświadczenie o zapoznaniu się z zasadami obowiązującej polityki;
k. **Zasada uprawnionego dostępu-** każdy pracownik stosuje się do obowiązujących zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji;
l. **Zasada przywilejów koniecznych**- każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań;
m. **Zasada świadomości zbiorowej-** wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie;
n. **Zasada obecności koniecznej**- prawo przebywania w określonych miejscach mają tylko osoby do tego upoważnione;
o. **Zasada stałej gotowości-** niedopuszczalne jest tymczasowe wyłączenie mechanizmów zabezpieczających;
p. **Zasada odpowiedniości-** używane mechanizmy muszą być adekwatne do sytuacji.

2. Zastosowane zabezpieczenia mają służyć w szczególności osiągnięciu poniższych celów i zapewnić:

a. **integralność**- rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
b. **integralność systemu**- rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej jak i przypadkowej;
c. **poufność**- rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

§ 4
ŚRODKI I NARZĘDZIA SŁUŻĄCE OCHRONIE DANYCH

System ochrony danych osobowych w Spółce składa się z następujących elementów:

1. **Inwentaryzacja danych-** Spółka dokonuje identyfikacji zasobów danych osobowych w Spółce, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych, a w tym w szczególności:

a. przypadków przetwarzania danych osobowych osób fizycznych;
b. przypadków przetwarzania danych szczególnych kategorii i danych karnych;
c. przypadków przetwarzania danych dzieci;
d. profilowania;
e. współadministrowania danymi.

2. **Rejestr-** Spółka opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych (Rejestr lub RCP).

3. **Podstawy prawne-** Spółka identyfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, jak również identyfikuje przypadki przetwarzania danych na podstawie zgody oraz identyfikuje przypadki, gdy Spółka przetwarza dane na podstawie prawnie uzasadnionego interesu Spółki.

4. **Obsługa praw jednostki-** Spółka spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

a. **obowiązki informacyjne-** Spółka przekazuje osobom prawem wymagane informacje przy zbieraniu danych;
b. **możliwość wykonania żądań-** Spółka zapewnia możliwość efektywnego wykonywania każdego typu prawnie uzasadnionego żądania, a dotyczącego zmiany lub usunięcia danych osobowych lub też informacji o przetwarzaniu danych osobowych;
c. **zawiadamianie o naruszeniach-** Spółka ustala czy konieczne jest zawiadomienie osób dotkniętych zidentyfikowanym naruszeniem ochrony danych**.**

5. **Minimalizacja-** Spółka nadzoruje powierzanie danych osobowych dążąc do realizacji zasady minimalizacji *(privacy by default).*

6. **Bezpieczeństwo-** Spółka zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

a. przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
b. przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
c. dostosuje środki ochrony danych do ustalonego ryzyka;
d. stosuje instrukcję postępowania w sytuacji naruszenia danych osobowych pozwalającą na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych- zarządza incydentami.

7. **Przetwarzający-** Podejmując współpracę z przetwarzającym Spółka dokonuje oceny prawidłowości przetwarzania przez niego danych osobowych i dokonuje wyboru podmiotu również w oparciu o kryterium prawidłowości przetwarzania danych osobowych. Spółka zawiera właściwe umowy powierzenia danych osobowych.

8. ***Privacy by design-*** Spółka zarządza zmianami wpływającymi na prywatność/zasady i zakres przetwarzania danych osobowych. W tym celu przed uruchomieniem nowych projektów i inwestycji w Spółce ocenia się wpływ tej zmiany na ochronę danych oraz zapewnienie prywatności (a w tym zgodności celów przetwarzania,

bezpieczeństwa danych i minimalizacji), co bierze się pod uwagę już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

9. **Działania organizacyjne-** Spółka podejmuje właściwe działania organizacyjne polegające w szczególności na:

a. wdrożeniu rozwiązań organizacyjnych w biurze oraz rozwiązań informatycznych, sprzyjających realizowaniu zasad ochrony danych osobowych;
b. przeszkoleniu użytkowników w zakresie bezpieczeństwa i ochrony informacji;
c. przypisaniu użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła);
d. okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych;
e. identyfikacja zagrożeń i analiza ryzyka.

§ 5
REJESTR CZYNNOŚCI

1. Spółka prowadzi Rejestr Czynności Przetwarzania Danych (RCPD), w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. RCPD stanowi formę dokumentowania czynności przetwarzania danych.

2. Rejestr prowadzi Administrator lub Specjalista ds. Ochrony Danych Osobowych, jeśli został powołany.

3. W rejestrze czynności przetwarzania zamieszcza się w szczególności wszystkie następujące informacje:

a. nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie- Specjalistę ds. Ochrony Danych Osobowych;
b. cele przetwarzania;
c. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e. podstawę prawną przetwarzania.

4. Spółka dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania w formie elektronicznej, a wspomagająco może używać wydruków.

§ 6
POWIERZANIE DANYCH

1. W przypadku zawierania umów z firmami zewnętrznymi, zalecane jest zawarcie umowy powierzenia i określenie w niej następujących wymagań bezpieczeństwa:

a. zakres i cel czynności oraz danych mających być przedmiotem współpracy z firmą zewnętrzną;
b. zakresy odpowiedzialności w przypadku utraty lub ujawnienia danych;
c. informacji i danych osobowych, które mają być chronione;
d. zasad zwrotu lub niszczenia informacji przy zakończeniu umowy;
e. działań podejmowanych w przypadku naruszenia warunków umowy.

§ 7
PRAWA JEDNOSTKI I OBOWIĄZKI INFORMACYJNE

1. Spółka dba o czytelność i prostą formę przekazywanych informacji w komunikacji z osobami, których dane przetwarza.

2. Spółka dba o dotrzymywanie terminów realizacji obowiązków względem osób, których dane przetwarza. Żądania są realizowane w terminie miesiąca od dnia otrzymania żądania. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań.

W terminie miesiąca od otrzymania żądania Spółka informuję osobę, której dane dotyczą o takim przedłużeniu terminu z podaniem przyczyn opóźnienia.

3. Spółka realizuje obowiązki informacyjne, w tym w szczególności:

a. **Prawo dostępu do swoich danych osobowych (prawo do bycia informowanym)**- na żądanie osoby uprawnionej Spółka informuje, czy przetwarza jej dane osobowe, przekazuje zestaw informacji odpowiadający obowiązkowi informacyjnemu, udziela dostępu do tych danych, a także wydaje kopię tych danych;
b. **Odmowa-** w uzasadnionych przypadkach Spółka informuje osobę o odmowie rozpatrzenia żądania w terminie miesiąca, licząc od dnia złożenia wniosku;
c. **Prawo do poprawnej informacji (prawo do sprostowania)-** na żądanie osoby uprawnionej, prostuje dane osobowe, które są nieprawidłowe lub uzupełnia dane niekompletne,
d. **Prawo do przenoszenia danych-** na żądanie osoby uprawnionej wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe dotyczące osoby uprawnionej, które osoba ta dostarczyła Spółce na podstawie umowy lub zgody. Na żądanie osoby uprawnionej wysyła te dane bezpośrednio innemu podmiotowi. Drugie i kolejne żądanie będzie realizowane po dokonaniu opłaty;
e. **Prawo do usunięcia danych (prawo do bycia zapomnianym)-** jeżeli zdaniem osoby uprawnionej nie ma podstaw do tego, aby Spółka przetwarzała jej dane, na żądanie osoby uprawnionej Spółka usuwa te dane;
f. **Prawo do bycia powiadomionym**- Spółka powiadamia o naruszeniu danych osobowych np. o wycieku danych;
g. **Prawo do ograniczenia przetwarzania danych-** na żądanie osoby uprawnionej, Spółka ogranicza przetwarzanie danych osobowych wyłącznie do uzgodnionych z osobą uprawnioną działań, jeżeli zdaniem osoby uprawnionej Spółka ma nieprawidłowe dane lub przetwarza je bezpodstawnie lub gdy osoba uprawniona nie chce, aby Spółka je usunęła, bo są one jej potrzebne do ustalenia, dochodzenia lub obrony roszczeń lub na czas wniesionego przez osobę uprawnioną sprzeciwu względem przetwarzania danych;
h. **Prawo do wniesienia sprzeciwu wobec przetwarzania danych-** na żądanie osoby uprawnionej Spółka nie przetwarza danych osobowych osoby uprawnionej z uwagi na jej szczególną sytuację oraz względem marketingu bezpośredniego;
i. **Sprzeciw „marketingowy"-** na żądanie osoby uprawnionej Spółka zaprzestaje przetwarzania danych osobowych w celu prowadzenia marketingu bezpośredniego;
j. **Sprzeciw z uwagi na szczególną sytuację-** na żądanie osoby uprawnionej Spółka zaprzestaje przetwarzania danych osobowych na podstawie prawnie uzasadnionego interesu w celach innych niż marketing bezpośredni, a także, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub do sprawowania powierzonej władzy publicznej. Osoba uprawniona powinna wtedy wskazać swoją szczególną sytuację, która jej zadaniem uzasadnia zaprzestanie przez Spółkę przetwarzania objętego sprzeciwem. Spółka przestanie przetwarzać dane w tych celach, chyba że wykaże, że podstawy przetwarzania przez Spółkę danych są nadrzędne wobec praw osoby upoważnionej lub też że dane tej osoby są niezbędne do ustalenia, dochodzenia lub obrony roszczeń,
k. **Prawo do wniesienia skargi do organu nadzorczego-** informuje osobę uprawnioną, że jeśli uważa, że Spółka przetwarza jej dane niezgodnie z prawem, to może złożyć w tej sprawie skargę do Prezesa Urzędu Ochrony Danych Osobowych lub innego właściwego organu nadzorczego,
l. **Prawo do cofnięcia zgody na przetwarzanie danych osobowych-** na żądanie osoby uprawnionej Spółka uwzględnia cofnięcie zgody na przetwarzanie danych osobowych objętych tą zgodą. Cofnięcie zgody nie będzie wpływać na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody osoby uprawnionej przed jej wycofaniem.

§ 8
INFORMACJE STANOWIĄCE TAJEMNICĘ PRZEDSIĘBIORSTWA

1. Przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.

2. Informacje objęte prawem tajemnicy przedsiębiorstwa:

2.1. Sprzedaż:

a. lista klientów;
b. informacje o klientach;
c. ceny transakcyjne, poufne cenniki;
d. terminy obowiązywania lub odnawiania umów;
e. fakt prowadzenia negocjacji i ich przebieg.

2.2. Marketing:

a. informacje uzyskane podczas badania klientów;
b. plany kampanii marketingowych.

2.3. Dostawcy, podwykonawcy, pracownicy:

a. informacje o dostawcach i stosowanych cenach;
b. informacja o stosowanych zakazach konkurencji;
c. informacje o wynagrodzeniach pracowników.

2.4. Badania i rozwój:

a. plany rozwoju, kierunki rozwoju;
b. wyniki badań;
c. pozytywne know- how w zakresie badań i rozwoju;
d. negatywne know- how, czyli informacje o niepowodzeniach.

2.5. Informacje finansowe:

a. wewnętrzne dokumenty finansowe;
b. budżety, prognozy, raporty;
c. nieujawniane rachunki zysków i strat;
d. obowiązkowe sprawozdania finansowe przed ujawnieniem.

2.6. Wewnętrzne informacje o firmie:

a. sposób organizacji pracy;
b. biznes plany;
c. oprogramowanie stosowane przez firmę;
d. dokumentacja techniczna i dokumenty pochodzenia zewnętrznego.

3. Wszyscy pracownicy, współpracownicy, partnerzy Administratora Danych są zobowiązani do zachowania w tajemnicy wszelkich informacji stanowiących tajemnicę przedsiębiorstwa.

4. Za umyślne bądź nieumyślne ujawnienie informacji objętych prawem tajemnicy przedsiębiorstwa grozi odpowiedzialność dyscyplinarna, odszkodowawcza, karna, nałożona zgodnie z obowiązującymi przepisami prawa w tym zakresie.

§ 9
OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH

1. Podział zagrożeń:

a. zagrożenia losowe zewnętrzne (np. sytuacje związane z warunkami atmosferycznymi, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu pozostaje zakłócona, nie dochodzi do naruszenia poufności danych;
b. zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, Administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych;

c. zagrożenia zamierzone, świadome i celowe – najpoważniejsze naruszenia, naruszenie poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są informacje to głównie:

a. oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp;
b. niewłaściwe parametry środowiska, jak np. nadmierna wilgoć lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy;
c. awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
d. jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenie systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
e. nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych;
f. stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
g. nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie;
h. ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń;
i. praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;
j. ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.;
k. podmieniono lub zniszczono nośnik z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane;
l. naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych, itp.).

Za naruszenie ochrony danych lub zagrożenie naruszenia uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

§ 10
CZYNNOŚCI ZABEZPIECZAJĄCE PRZED NARUSZENIEM OCHRONY DANYCH

1. Każdy użytkownik podlega przeszkoleniu z przepisów w zakresie ochrony informacji oraz wynikających z nich zadań i obowiązków.

2. W przypadku udostępniania informacji w celach innych niż włączenie do zbioru, Administrator Danych udostępnia posiadane informacje osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

3. Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące środki organizacyjne:

a. dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający upoważnienie nadane przez Administratora Danych;

b. każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu wszelkich nośników z danymi;
c. należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych;
d. pomieszczenia, w których są przetwarzane dane osobowe muszą być zamykane na klucz;
e. dostęp do kluczy posiadają tylko upoważnieni pracownicy;
f. dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W przypadku gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia Administratora Danych lub Specjalisty ds. Ochrony Danych Osobowych, jeśli został powołany;
g. dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy;
h. w przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczenia tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności;
i. szafy, w których przechowywane są dane powinny być zamykane na klucz;
j. klucze do tych szaf posiadają tylko upoważnieni pracownicy;
k. szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane;
l. dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf;
m. pracownicy zobowiązani są stosować zasadę czystego biurka- wszystkie dokumenty i materiały powinny być po zakończeniu pracy chowane w przeznaczonych do tego szafkach, szufladach itp. W przypadku braku dostatecznej ilości dostępnego miejsca dokumenty i materiały powinny być pozostawiane na biurku uporządkowane.

4. Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące środki techniczne:

a. dostęp do komputerów, na których są przetwarzane dane mają tylko upoważnieni pracownicy;
b. monitory komputerów, na których przetwarzane są dane są tak ustawione aby osoby nieupoważnione nie miały wglądu w dane;
c. po zakończeniu pracy komputery przenośne (np. typu notebook) zawierające dane osobowe powinny być zabezpieczone;
d. w wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe, lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, na przykład poprzez szyfrowanie lub wprowadzanie haseł.
e. nie należy udostępniać osobom nieupoważnionym tych komputerów;
f. w przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności;
g. nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie) aby nie zostały na nich dane osobowe;
h. w wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie;
i. w przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków;
j. niezabezpieczonych danych osobowych nie należy przesyłać droga elektroniczną;
k. sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz;
l. błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w innych mechaniczny sposób uniemożliwiających powtórne ich odtworzenie.

5. Postępowanie w przypadku naruszenia ochrony danych osobowych określa odrębna Instrukcja.

§ 11
POSTANOWIENIA KOŃCOWE

Niniejsza Polityka Ochrony Danych Osobowych obowiązuje wszystkich pracowników i współpracowników Spółki.
Niniejsza Polityka Ochrony Danych Osobowych wchodzi w życie z dniem 23 maja 2018 roku.