POLITYKA PRYWATNOŚCI
I3ATM SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
z siedzibą MARSZ. JÓZEFA PIŁSUDSKIEGO, nr 74/320, 50-020 WROCŁAW
*KRS **0000854287** NIP **8971882745***

*(dalej jako **"Spółka"**)*

§ 1.
[Podstawa prawna]

1. Niniejsza **„Polityka Prywatności**" zwana dalej „**Dokumentem" lub "Polityką**", stanowi wdrożenie zobowiązań wynikających z rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz uchylająca dyrektywę 95/46/WE („RODO").

2. Niniejszy Dokument ma na celu wyjaśnienie i uregulowanie kwestii związanych z bezpieczeństwem informacji, w szczególności danych osobowych, gromadzonych i przetwarzanych w systemie informatycznym, jak i ewentualnie w formie papierowej lub innych procedur przetwarzania danych w Spółce i poświadcza, że osoby zarządzające Spółką wypełniają zobowiązania wynikające z przepisów RODO oraz zachowują należytą staranność w przetwarzaniu danych osobowych w ramach usług świadczonych przez Spółkę.

3. Każdy pracownik Spółki, a także osoby współpracujące ze Spółką, mające dostęp do systemu informatycznego i przetwarzające dane osobowe, a także przetwarzające dane w tradycyjnej formie papierowej, muszą zapoznać się z tym dokumentem i podpisać stosowne oświadczenie. Podpisanie oświadczenia jest dowodem, że pracownik (współpracownik) przeczytał i zaakceptował zasady dotyczące polityki bezpieczeństwa w Spółce.

4. Ze względu na zakres, rodzaj i sposób przetwarzania danych osobowych przyjęto najwyższy możliwy poziom bezpieczeństwa systemu.

5. Dokument ten powinien zostać udostępniony w ramach komunikacji prowadzonej przez Spółkę wewnętrznie, ale także udostępniony dla Klientów i osób, których dane mogą być potencjalnie przetwarzane, poprzez opublikowanie na stronie internetowej Spółki lub na urządzeniach służących do obsługi Klientów i świadczenia usług Spółki.

§2

[Definicje]

Określenia użyte w tym Dokumencie oznaczają:

1) **Administrator** - osoba prawna lub fizyczna decydująca o celach i środkach przetwarzania danych osobowych. Administratorem Danych jest Spółka, która przetwarza dane osobowe uzyskane we własnym imieniu, w tym dane uzyskane bezpośrednio lub

pośrednio od Klientów, którzy wyrazili zgody na powierzenie Spółce przetwarzania danych osobowych, w zakresie niezbędnym do realizacji usług świadczonych przez Spółkę.

2) **Dane Osobowe** - wszelkie informacje związane z osobą fizyczną, które pozwalają określić tożsamość tej osoby, jej miejsce zamieszkania, dane do kontaktu i cechy charakterystyczne, w tym dane wrażliwe.

3) **Dane wrażliwe** - wszelkie informacje związane z osobą fizyczną, ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub ideologiczne, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, orientacji seksualnej, dane dotyczące wyroków skazujących i naruszeń prawa lub powiązanych środków bezpieczeństwa, dane dotyczące indywidualnych decyzji lub decyzji administracyjnych.

4) **Inspektor Ochrony Danych (IOD)** - osoba fizyczna wyznaczona przez Administratora, sprawująca nadzór nad przetwarzaniem danych osobowych, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w Spółce, w szczególności w celu zapobiegania nieupoważnionemu dostępowi do miejsc i systemu, w których Spółka przetwarza dane osobowe. Zakres odpowiedzialności Inspektora Ochrony Danych jest określony w niniejszej Polityce oraz w przepisach rozporządzenia o ochronie danych osobowych (RODO) i innych powszechnie obowiązujących przepisów prawa.

5) **Mechanizm uwierzytelniania użytkownika** - indywidualnie ustawiane hasło i identyfikator umożliwiające dostęp do określonych zasobów informacyjnych w systemie informatycznym.

6) **Nośniki danych IT** - urządzenia, dyski lub inne nośniki IT wykorzystywane do przetwarzania danych osobowych.

7) **Obszar przetwarzania danych osobowych** - budynki, pokoje, części pomieszczeń, w których przetwarzane są dane osobowe.

8) **Przetwarzanie danych osobowych** - wszelkie operacje wykonywane na danych osobowych, takie jak gromadzenie, zapisywanie, przechowywanie, rozwijanie, zmienianie, udostępnianie, usuwanie. Działania te są wykonywane przez Spółkę co do zasady w formie elektronicznej, poprzez system informatyczny, nie wyklucza się jednak możliwości przetwarzania w formie tradycyjnej (papierowej).

9) **RODO** - rozporządzenie Parlamentu Europejskiego i Rady UE nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz uchylające dyrektywę 95 / 46 / WE.

10) **System informatyczny** - system przetwarzania informacji z powiązanymi użytkownikami i zasobami technicznymi, finansowymi, które dostarczają i rozpowszechniają informacje.

11) **Urząd Ochrony Danych Osobowych (UODO**) - urząd powołany do monitorowania i egzekwowania stosowania w Polsce przepisów rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. (RODO) oraz przepisów ustawy z dnia 10

maja 2018 r. o ochronie danych osobowych (u.o.d.o.), organem działającym w imieniu Urzędu jest Prezes - https://uodo.gov.pl;

12) **Użytkownik** - każda osoba fizyczna, będąca pracownikiem, współpracownikiem Administratora lub powiązana z nim w jakikolwiek inny sposób, posiadająca autoryzowany dostęp do danych osobowych i upoważniona do podejmowania określonych czynności związanych z przetwarzaniem danych osobowych, w ściśle określonym zakresie praw i obowiązków, posiadająca indywidualny identyfikator i hasło umożliwiające dostęp do systemu informatycznego.

§3

[Administrator Danych Osobowych]

Administratorem Danych Osobowych jest Spółka
I3ATM SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
z siedzibą MARSZ. JÓZEFA PIŁSUDSKIEGO, nr 74/320, 50-020 WROCŁAW
, działająca zgodnie z przepisami polskiego prawa, zarejestrowana w rejestrze przedsiębiorców prowadzonym przez Sąd REJONOWY DLA WROCŁAWIA-FABRYCZNEJ WE WROCŁAWIU, VI WYDZIAŁ GOSPODARCZY KRAJOWEGO REJESTRU SĄDOWEGO pod numerem KRS 0000854287, NIP: 8971882745, REGON 386939347, reprezentowana przez Zarząd, w składzie osobowym każdorazowo określonym w rejestrze przedsiębiorców KRS.

§4

[Przypadki naruszenia ochrony danych osobowych]

1. Przypadek naruszenia ochrony danych osobowych ma miejsce m.in. gdy:
   a. stwierdzono naruszenie bezpieczeństwa systemu informatycznego, danych przesyłanych, przechowywanych lub przetwarzanych przez podmiot, którego dotyczy naruszenie,
   b. stan urządzeń, zawartość pliku z danymi osobowymi, ujawnione metody pracy, działanie programu lub jakość, telekomunikacja w sieci IT może wskazywać na złamania zasad bezpieczeństwa danych i naruszenie ochrony tych danych,
   c. skutkiem powyższych może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych.

2. Do przypadków naruszenia ochrony danych osobowych, zalicza się w szczególności:
   a. przypadkowe awarie (np. pożar, powódź);
   b. awarie sprzętu lub oprogramowania, które wskazują na celowe działanie celem nieuprawnionego pozyskania danych osobowych;
   c. nieautoryzowany dostęp lub próba uzyskania dostępu do pomieszczeń, w których przetwarzane są dane osobowe (widoczne uszkodzenia lub naruszenia bezpieczeństwa),
   d. nieautoryzowany dostęp lub próba uzyskania dostępu do danych osobowych przetwarzanych w systemie informatycznym (np. istnienie nieautoryzowanych kont dostępu, nieautoryzowana praca na koncie użytkownika w systemie informatycznym),

e. ujawnianie osobom nieupoważnionym danych osobowych, procedur i informacji związanych z bezpieczeństwem danych osobowych lub innych chronionych elementów systemu informatycznego,
f. naruszenie lub próby naruszenia integralności systemu przeznaczonego do przetwarzania danych osobowych (np. brak dostępu do sieci, aplikacje z zestawem danych, awaria komputera z powodu obecności wirusa komputerowego),
g. wykonywanie kopii danych osobowych (np. wydruków, kopii na zewnętrznych nośnikach danych) bez należytego upoważnienia lub niezgodnie z przepisami obowiązującymi w Spółce,
h. brak wykonania kopii zapasowych w sposób przyjęty w Spółce,
i. wykryte działanie wirusa komputerowego lub innej nieplanowanej modyfikacji systemu informatycznego,
j. zastąpienie, modyfikowanie lub zniszczenie plików z danymi osobowymi oraz poszczególnych danych, bez odpowiedniej autoryzacji lub w sposób, który mógłby narazić Spółkę i/lub jej Klientów na przypadkową utratę lub wyciek danych,
k. niezgodne z „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Spółce" przekazanie innemu podmiotowi sprzętu do likwidacji lub naprawy.

§5

[**Zasady mające zastosowanie do osób przetwarzających dane osobowe]**

1. Każda osoba, która przetwarza dane osobowe w systemie informatycznym w przypadku stwierdzenia, że występuje jedna lub więcej sytuacji określonych w §4, jest zobowiązana niezwłocznie powiadomić Inspektora Ochrony Danych (IOD) i Administratora Danych - nie później niż w ciągu 24 godzin, na adres e-mail: i3atm@pm.me

2. Dopóki Inspektor Ochrony Danych Osobowych (IOD) nie podejmie działań w zakresie przeciwdziałania naruszeniom ochrony danych osobowych, osoba przetwarzająca dane w imieniu Administratora Danych lub osoba, której Administrator Danych powierzył przetwarzanie danych osobowych, jest zobowiązana:
   a. ochronić miejsca lub urządzenia, w których naruszono ochronę danych osobowych, przed dostępem nieupoważnionych stron trzecich;
   b. powstrzymania się od rozpoczynania lub kontynuowania działań lub prac, które mogą zatrzeć ślady lub dowody naruszenia danych;
   c. podjąć inne niezbędne działania, aby zapobiec dalszym naruszeniom ochrony danych osobowych.

3. Administrator Danych jest zobowiązany do powiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych o wysokim ryzyku naruszenia praw i wolności osoby, której dane dotyczą, w szczególności w przypadku:
   a. utraty kontroli przez Administratora Danych nad przetwarzonymi danymi osobowymi;
   b. narażenia osoby, której dane zostały przetworzone na:
      - dyskryminację;
      - ograniczenie jego praw;

- kradzież;
- oszustwo;
- fałszowanie tożsamości;
- stratę finansową;
- uszkodzenie reputacji;
- naruszenie poufności danych osobowych chronionych tajemnicą zawodową;
- wszelkie inne znaczące szkody gospodarcze lub moralne.

§ 6

[Zasady postępowania IOD w przypadku naruszeń]

1. Inspektor Ochrony Danych natychmiast po otrzymaniu informacji o naruszeniu ochrony danych osobowych podejmuje działania w celu usunięcia naruszenia i udokumentowania go. Inspektor podejmuje również decyzję co do dalszych działań związanych ze zgłoszeniem naruszenia.

2. Jeśli wynika to z obowiązków nałożonych na IOD przez postanowienia niniejszej Polityki Prywatności, rozporządzenia RODO lub innych powszechnie obowiązujących przepisów prawa, fakt naruszenia powinien zostać zgłoszony w ciągu 72 godzin od wykrycia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych (UODO), np. w formie formularza elektronicznego - Zgłoszenie naruszenia ochrony danych osobowych.

3. Jeśli po odkryciu naruszenia ochrony danych osobowych IOD stwierdzi, że ryzyko naruszenia praw i wolności osób fizycznych (np. wystąpienie szkody materialnej lub niematerialnej) jest niewielkie, może zaniechać dalszych działań w zakresie zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych (UODO).

4. W przypadku stwierdzenia naruszenia, IOD może podejmować następujące działania, o których mowa w § 6.1 (podana lista ma charakter przykładowy):

a. identyfikacja rodzaju naruszenia, a w szczególności określenie skali naruszenia ochrony danych i możliwego sposobu dostępu do danych osób nieupoważnionych,
b. generowanie i drukowanie wszystkich możliwych dokumentów i raportów, które mogą pomóc w określeniu okoliczności zdarzenia;
c. fizyczne odłączenie urządzeń systemu IT;
d. zmiana identyfikatorów i haseł indywidualnego użytkownika;
e. blokowanie dostępu do danych do zewnętrznego odbiorcy;
f. rekonstrukcja danych osobowych z kopii zapasowych
g. nakaz wstrzymania pracy w systemie informatycznym lub jego elementach;
h. wykonywanie czynności naprawczych lub konserwacyjnych, jeśli przyczyną naruszenia był zły stan urządzeń;
i. instruowanie użytkownika lub zewnętrznego odbiorcy o zasadach pracy w systemie informatycznym, jeżeli przyczyną naruszenia jest nieprawidłowe działanie lub zaniechanie użytkownika lub odbiorcy zewnętrznego.

4. Decyzję o rodzaju i kolejności podjętych działań podejmuje wyłącznie Inspektor Ochrony Danych, niezależnie od Administratora Danych.

5. Jeśli sytuacja tego wymaga, Inspektor Ochrony Danych wyznacza zespół kryzysowy złożony z pracowników Administratora Danych wyznaczonych przez Inspektora Ochrony Danych lub zewnętrznych specjalistów w dziedzinie bezpieczeństwa systemów informatycznych.

6. Inspektor Ochrony Danych może poprosić indywidualnych Użytkowników o pomoc w podejmowanych działaniach. Obowiązkiem Użytkownika jest zapewnienie żądanej pomocy.

7. Inspektor Ochrony Danych przygotowuje raport o naruszeniu i dokumentuje incydent w rejestrze naruszeń ochrony danych osobowych, w którym rejestr zawiera w szczególności: opis naruszenia i podjęte działania, konsekwencje naruszenia, dane użytkowników lub inne osoby odpowiedzialne za naruszenie, wnioski i propozycje działań mających na celu poprawę bezpieczeństwa danych osobowych, informacje o skali naruszenia, informacje o tym, czy naruszenie zostało zgłoszone osobie, której dane dotyczą. Raport otrzymuje Administrator Danych.

8. Po otrzymaniu raportu, jeśli sytuacja tego wymaga, Administrator Danych jest zobowiązany do podjęcia odpowiednich środków w celu zwiększenia ochrony danych osobowych.

9. Administrator Danych raz w roku prowadzi szkolenia z zakresu procedur przetwarzania danych osobowych dla wszystkich pracowników i współpracowników.

§ 7

[Obowiązek zapoznania się z treścią dokumentów]

1. Każdy Użytkownik, który będzie pracować w obszarze przetwarzania danych osobowych zobowiązany jest do zapoznania się z dokumentem „Polityka Prywatności" oraz „Instrukcją zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych w Spółce".

2. Użytkownik podpisuje w tym względzie odpowiednie oświadczenie, którego szablon jest załączony do niniejszej Polityki, zatytułowanym „Oświadczenie", przechowywanym w osobistych plikach Użytkownika.

§8
[Wejście w życie Dokumentu]

Dokument wchodzi w życie z dniem 01.05.2021r.

§9
[Wykaz dokumentów stanowiących integralną część Polityki Prywatności]

1. Kluczowym dokumentem stanowiącym integralną część niniejszej "Polityki Prywatności", określającym zasady korzystania z systemu informatycznego jest „Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Spółce" wraz ze wszystkimi załącznikami i dokumentami zależnymi.

2. Dokumentem określającym zasady przetwarzania danych w formie tradycyjnej, zawartych w katalogach, segregatorach lub innych zestawach danych niezwiązanych z systemem informatycznym jest: „Instrukcja i procedury dotyczące pracy z tradycyjnymi zbiorami danych w firmie”.

WYKAZ ZAŁĄCZNIKÓW:

Załącznik nr	**NAZWA ZAŁĄCZNIKA**
1	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Spółce
2	Role i obowiązki. Struktura organizacyjna Spółki
3.	Procedura dotycząca przetwarzania danych osobowych klientów Spółki
4.	Rejestr przetwarzania danych osobowych
5.	Polityka powoływania Inspektora Ochrony Danych (IOD)
6.	Procedura zgłaszania incydentów podczas przetwarzania danych osobowych;

7.	Oświadczenie pracownika / współpracownika o zapoznaniu się z procedurami dotyczącymi przetwarzania danych osobowych w Spółce - model;
8.	Upoważnienie pracownika / współpracownika do przetwarzania danych osobowych;
9.	Rejestr Naruszeń Danych Osobowych
10.	Rejestr Osób Upoważnionych Do Przetwarzania Danych Osobowych

Załącznik nr 1

do Polityki Prywatności

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Spółce I3ATM SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

§ 1.

[Podstawa prawna]

„Instrukcja zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych, zwana dalej „Instrukcją", to wykonanie zobowiązań wynikających z rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu takich danych oraz uchylająca dyrektywę 95/46 / WE ("RODO").

§2

[Zakres zastosowania]

1. Instrukcja określa zasady zarządzania systemem informatycznym w Spółce, w szczególności: sposób rejestracji i wyrejestrowania użytkownika, sposób przypisywania haseł i zasady ich używania, procedury uruchamiania i kończenia pracy, obowiązki użytkownika, metodę i częstotliwość wykonywania kopii, zasady sprawdzania obecności wirusów komputerowych oraz przeprowadzania inspekcji i konserwacji systemu.

2. Instrukcja ta obejmuje wszystkie miejsca, z których możliwy jest dostęp do przetwarzania danych osobowych w Spółce.

§3

[Strefa bezpieczeństwa]

1. Strefa bezpieczeństwa, to fizyczne lokalizacje, biura, pomieszczenia, serwerownie uznawane za obszar bezpieczny, w którym przetwarzane są dane osobowe zgodnie z zasadami określonymi w niniejszym dokumencie, są to m.in.:

siedziba Spółki pod adresem:MARSZ. JÓZEFA PIŁSUDSKIEGO, nr 74/320
50-020 WROCŁAW

2. Wymagana jest ochrona powyższego obszaru, zgodnie z zasadami określonymi w niniejszej Instrukcji.
3. Dane nie są przetwarzane ani przesyłane w jakiejkolwiek formie poza wyznaczoną do tego celu strefą bezpieczeństwa, chyba że w umowach zawartych przez Spółkę z innymi podmiotami stwierdzono inaczej, po spełnieniu wymogów powszechnie obowiązujących przepisów, w szczególności RODO.

§4

[Sposób rejestracji i wyrejestrowania użytkownika]

1. Użytkownikiem systemu informatycznego może być tylko osoba, która ma pisemne upoważnienie do przetwarzania danych i obsługi systemu i urządzeń w nim zawartych. Pisemny formularz upoważnienia stosowany w Spółce to dokument zatytułowany „Upoważnienie do przetwarzania danych osobowych".

2. Administrator Danych przydziela identyfikator każdemu Użytkownikowi zgodnie z poziomem dostępu Użytkownika do zasobów informacyjnych określonych w autoryzacji. Nadawany identyfikator Użytkownika jest unikalny w skali systemu i jest indywidualnie przypisany tylko jednemu Użytkownikowi przez cały okres jego zatrudnienia lub współpracy ze Spółką, a po wyrejestrowaniu ten sam identyfikator nie może być ponownie przypisany do innego Użytkownika.

3. Administrator wyrejestrowuje Użytkownika(blokuje nadany identyfikator) w przypadku:

a. rozwiązania stosunku pracy lub jego wygaśnięcia, rozwiązania umowy o współpracy lub jej wygaśnięcia;
b. otrzymania przez Administratora informacji o utracie przez Użytkownika uprawnień do dostępu do zasobów informacyjnych w systemie informatycznym.

§ 5
[Przydział i używanie haseł]

1. Administrator przydziela pierwsze hasło Użytkownikowi, jednocześnie nadając identyfikator.

2. Po wprowadzeniu pierwszego hasła przez Administratora, Użytkownik jest zobowiązany do zarejestrowania się w systemie i zmiany hasła.

3. Usunięcie pierwszego hasła jest obowiązkowe dla każdego Użytkownika, który ma identyfikator w systemie.

4. Obowiązują następujące zasady używania haseł:

a. hasło jest tajne, tj. Użytkownik nie może ujawnić go osobom nieupoważnionym, a jeśli hasło zostanie ujawnione, należy je natychmiast zmienić, a IOD powinien zostać niezwłocznie poinformowany o fakcie ujawnienia,
b. podczas wprowadzania hasła nie jest ono wyświetlane na ekranie;
c. hasło zmienia się co najmniej raz w miesiącu,
d. hasło nie może być zapisane w żadnej formie umożliwiającej jego pozyskanie przez osoby nieupoważnione,
e. hasło składa się z co najmniej 8 znaków, w tym wielkich i małych liter, cyfr i znaków specjalnych w kolejności losowej, tj. w kolejności nie bezpośrednio z używanej klawiatury,
f. w przypadku wyrejestrowania Użytkownika, Administrator natychmiast unieważnia hasło i odbiera możliwość dalszego dostępu do danych.

5. Właściwe wykonywanie obowiązków związanych z używaniem haseł przez użytkowników jest nadzorowane przez Administratora Danych. Nadzór ten polega w szczególności na obserwowaniu (monitorowaniu) funkcjonowania mechanizmu uwierzytelniania i przywracaniu prawidłowego stanu w przypadku nieprawidłowości. Zalecenia dotyczące procedur stosowanych przy przetwarzaniu danych osobowych są wydawane przez Inspektora Ochrony Danych, do których Administrator Danych jest obowiązany zastosować się i wdrożyć.

§ 6

[Rejestr użytkowników]

1. Administrator w porozumieniu z IOD, prowadzi ewidencję Użytkowników w zakresie:
   a. osób upoważnionych do przetwarzania danych osobowych w Spółce;
   b. podmiotów, którym Spółka, jako Administrator, powierzyła przetwarzanie danych osobowych w ramach umowy o powierzenie przetwarzania danych osobowych.

2. Rejestr Użytkowników jest sporządzany na piśmie i zawiera następujące informacje: imię i nazwisko, datę autoryzacji, datę wygaśnięcia autoryzacji i możliwe uwagi.

3. Aktualna lista Użytkowników w dniu wejścia w życie Instrukcji zarządzania systemem informatycznym znajduje się w dokumencie „Rejestr osób upoważnionych do przetwarzania danych osobowych".

4. Zapis powinien zawierać informacje zarówno o Użytkownikach aktywnych, jak i wyrejestrowanych.

5. Administrator może powierzyć prowadzenie Rejestru Użytkowników Inspektorowi Ochrony Danych lub innej wyznaczonej osobie. Taka osoba jest zobowiązana do prowadzenia ewidencji zgodnie z niniejszą Instrukcją.

§7
[Rozpoczęcie i zakończenie pracy]

1. Przed rozpoczęciem pracy w systemie informatycznym Użytkownik ma obowiązek sprawdzić urządzenie komputerowe i stację roboczą, zwracając uwagę na fakt, czy zaistniały okoliczności wskazujące na naruszenie ochrony danych osobowych. W przypadku podejrzenia, że mogło dojść do naruszenia ochrony danych osobowych Użytkownik podejmuje działania określone w dokumencie „Procedura zgłaszania incydentów podczas przetwarzania danych osobowych".

2. Użytkownik rozpoczyna pracę w systemie informatycznym następującymi czynnościami:
a. włączanie komputera,
b. uwierzytelnianie („logowanie") w systemie przy użyciu swojego identyfikatora i hasła;

3. Niedopuszczalne jest używanie hasła i identyfikatora innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.

4. Użytkownik niezwłocznie powiadamia Administratora Danych w przypadku 3 nieudanych prób zalogowania się do systemu.

5. Zakończenie pracy Użytkownika w systemie następuje po „wylogowaniu" z systemu. Po zakończeniu pracy Użytkownik zabezpiecza swoje stanowisko pracy, w

szczególności nośniki danych, dokumenty i wydruki zawierające dane osobowe, przed nieautoryzowanym dostępem.

6. W przypadku dłuższego okresu opuszczania miejsca pracy Użytkownik jest zobowiązany do „wylogowania się" z systemu.

7. W przypadku nieprawidłowości w mechanizmie uwierzytelniania („logowania") w systemie Użytkownik niezwłocznie powiadamia o tym Inspektora Ochrony Danych i Administratora.

§ 8
[Obowiązki Użytkownika]

1. W związku z pracą w systemie informatycznym Użytkownik jest zobowiązany do:
a. nie używania innych nośników informacji niż zaakceptowane przez Administratora Danych i IOD;
b. sprawdzenia przez oprogramowanie obecności wirusów na nośnikach danych IT otrzymanych od innych podmiotów,
c. nie instalowania żadnego oprogramowania bez zgody Administratora,
d. zamykania na czas nieobecności Użytkownika pomieszczeń, komputerów i urządzeń, w których przetwarzane są dane osobowe,
e. niszczenia wszelkich niepotrzebnych wydruków,
f. systematyczne zmienianie hasła,
g. realizowanie aktualnych zleceń Administratora i IOD w zakresie pracy i korzystania z systemu informatycznego.

2. Użytkownicy korzystający z komputera przenośnego powinni zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza strefą bezpieczeństwa i powinni zabezpieczyć dostęp do komputera za pomocą hasła i nie zezwalać osobom nieupoważnionym na dostęp do danych osobowych.

§9
[Metoda i częstotliwość wykonywania kopii]

1. Pełna kopia zestawu danych jest tworzona codziennie. Użytkownik jest zobowiązany do zapisania wszystkich dokumentów, w których dane osobowe są przechowywane lub w inny sposób przetwarzane w systemie bezpośrednio wskazanym przez Administratora, oprócz dysku komputera Użytkownika.

2. Kopie są przechowywane w odpowiednich systemach zapewniających bezpieczeństwo informacji i przetwarzanie danych osobowych, gdzie pliki danych osobowych są przechowywane na bieżąco.

3. Kopie są okresowo sprawdzane pod kątem ich przydatności, poprawności działania i możliwości odzyskiwania danych. Kopie awaryjne, które zostały uszkodzone lub stały się nieaktualne, podlegają natychmiastowej likwidacji. Decyzję o anulowaniu kopii podejmuje Administrator.

4. Nadzór nad prawidłowym wykonaniem i przechowywaniem kopii sprawuje Administrator i IOD.

5. Administrator lub Użytkownicy, w ramach udzielonego upoważnienia do przetwarzania danych osobowych i na wyraźne żądanie Administratora, są zobowiązani do usunięcia danych osobowych po zakończeniu okresu przetwarzania danych osobowych. Oznacza to, że Administrator jest zobowiązany do usunięcia danych osobowych po spełnieniu celu przetwarzania danych osobowych, chyba że ich dalsze przechowywanie wynika z przepisów powszechnie obowiązujących przepisów prawa.

§10
[Sprawdzanie obecności wirusów komputerowych]

1. Bieżące sprawdzanie infekcji wirusami komputerowymi odbywa się za pomocą oprogramowania, które automatycznie monitoruje występowanie wirusów. To sprawdzanie dotyczy wszystkich nośników danych IT używanych w systemie przetwarzania danych, jak również do celów instalacji. Administrator jest odpowiedzialny za prawidłowe funkcjonowanie oprogramowania.

2. Po każdej naprawie i konserwacji komputera należy sprawdzić, czy nie ma wirusów i ponownie zainstalować program antywirusowy.

3. Zewnętrzne nośniki informacji IT są sprawdzane przez program antywirusowy przed ich użyciem. Dane uzyskane poprzez teletransmisję należy umieścić - przed otwarciem - w katalogu przejścia, który podlega weryfikacji.

4. W przypadku wykrycia lub podejrzenia wystąpienia wirusa Administrator wykonuje pełną kontrolę nad urządzeniami i nośnikami informacji za pomocą programu antywirusowego. Jeśli usunięcie wirusa nie jest możliwe, Administrator powinien zlecić usługę w tym zakresie zewnętrznemu specjaliście.

5. Nadzór nad prawidłowym funkcjonowaniem oprogramowania antywirusowego sprawuje Administrator. Przeprowadza również okresowe kontrole systemu informacyjnego pod kątem wirusów.

§11
[Sposób i czas przechowywania nośników informacji, w tym kopii IT i wydruków]

1. Wszelkie dane osobowe są przechowywane tylko w urządzeniach, nośnikach danych, dopuszczonych przez Administratora, wyłącznie w przystosowanych do tego pomieszczeniach, lokalach, należących do strefy bezpieczeństwa. Do tych danych i nośników dostęp mają tylko Użytkownicy upoważnieni do przetwarzania odpowiednich plików danych osobowych. W przypadku wydruków lub dokumentów w formie papierowej, są one przechowywane w pomieszczeniach, do których dostęp posiadają wyłącznie upoważnieni Użytkownicy. Wszelkie dokumenty, wydruki, nośniki są zabezpieczone, zamknięte w odpowiednich szafkach lub wyznaczonych do tego pomieszczeniach i chronione przed dostępem osób nieupoważnionych.

2. Użytkownik uprawniony do przetwarzania danych osobowych, przygotowania wydruku zawierającego dane osobowe lub korzystania z tego wydruku (np. pracownik biurowy) jest zobowiązany do bieżącego sprawdzania przydatności wydruku w wykonanej pracy, a w przypadku jego nieprzydatności - natychmiastowego zniszczenia wydruku.

3. Likwidacja wydruków odbywa się wyłącznie przy użyciu urządzeń (niszczarek) przeznaczonych do tego celu, znajdujących się w bezpiecznej strefie.

4. Użytkownik przygotowujący wydruk zawierający dane osobowe zobowiązany jest do niezwłocznego pobrania wydruku z drukarki, kserokopiarki lub innego urządzenia powielającego, w celu ochrony danych osobowych przed nieuprawnionym dostępem.

5. Nośniki magnetyczne i optyczne z danymi osobowymi są oznaczone i przechowywane w zamkniętych szafach lub sejfach w specjalnych pomieszczeniach, dostępnych tylko dla upoważnionych użytkowników z kodem do ich otwierania.

6. Fizyczna likwidacja zniszczonych lub zbędnych magnetycznych i optycznych nośników IT z danymi osobowymi odbywa się w sposób uniemożliwiający odczyt danych osobowych.

7. Użytkownicy przetwarzający dane osobowe są zobowiązani do zachowania szczególnej ostrożności w ochronie danych osobowych, które w szczególności obejmują:

a. fizyczne zabezpieczenie dokumentów w stopniu adekwatnym do rzeczywistych zagrożeń,
b. przechowywanie dokumentów nie dłużej niż jest to konieczne do wykonania zadań,
c. korzystanie z dokumentów wyłącznie w celach związanych z pracą i zadaniami wykonywanymi w Spółce.

§12
[Zasady kontroli i konserwacji systemu]

1. Kontrole, konserwacja i naprawy urządzeń komputerowych i innych nośników danych IT są wykonywane przez Administratora, Użytkowników upoważnionych przez Administratora lub autoryzowane podmioty zewnętrzne, działające na zlecenie Administratora.

2. Urządzenia komputerowe i inne informatyczne nośniki danych przeznaczone do naprawy przez podmioty zewnętrzne będą amortyzowane z danych osobowych przed naprawą lub będą naprawiane pod nadzorem osoby upoważnionej przez Administratora.

3. Dane osobowe zostaną każdorazowo usunięte z nośników informatycznych, w przypadku przeznaczenia ich do likwidacji lub przekazania innemu podmiotowi, a jeżeli nie jest to możliwe, nośniki zostaną uszkodzone w sposób uniemożliwiający odczyt danych osobowych.

§13

[Komunikacja w sieci komputerowej]

1. Pliki zawierające dane osobowe mogą znajdować się tylko na serwerach, na których podlegają ochronie na poziomie systemu operacyjnego (uwierzytelnianie) lub innego systemu (w tym serwera zewnętrznego) chroniącego dane osobowe.

2. Nieuzasadnione kopiowanie przez Użytkowników plików z serwerów na stacje robocze Użytkowników i inne nośniki jest zabronione.

§14
[Fizyczna ochrona danych i metoda przechowywania nośników]

1. Wszystkie pomieszczenia, w których znajdują się informatyczne nośniki danych, urządzenia oraz jakiekolwiek wydruki i dokumenty zawierające dane osobowe powinny być wyposażone w systemy blokujące. W czasie, gdy nie ma w nich osób upoważnionych, pomieszczenia są zabezpieczane w sposób uniemożliwiający dostęp osobom nieupoważnionym do danych osobowych.

2. Dostęp do pomieszczeń, w których znajduje się sprzęt serwerowy i system pamięci masowej przetwarzania danych osobowych, powinien mieć co najmniej dwupoziomową kontrolę dostępu:

a. strefa przejściowa - dostęp do strefy możliwy jest dopiero po pozytywnej identyfikacji Administratora (weryfikacja na podstawie listy dostępu).
b. strefa przetwarzania danych - dostęp do strefy możliwy jest poprzez identyfikację w elektronicznym systemie dozoru lub za pomocą kluczy lub kodów, do których ma dostęp tylko Administrator.

3. Administrator może dodatkowo stosować inne metody ograniczenia dostępu do pomieszczeń stanowiących obszar przetwarzania danych osobowych.

4. Media informacyjne, w tym kopie informatyczne i wydruki, powinny być okresowo sprawdzane pod kątem ich dalszej użyteczności dla Administratora, co najmniej raz w tygodniu, a jeśli okaże się to niepotrzebne - należy natychmiast usuwać z nich dane osobowe lub zwracać je osobie, której dane dotyczą.

§15
[Obowiązek zapoznania się z instrukcją]

Przed rozpoczęciem prac związanych z przetwarzaniem danych osobowych każdy Użytkownik jest zobowiązany do zapoznania się z Instrukcją. Użytkownik podpisuje w tym zakresie odpowiednie oświadczenie, które jest przechowywane w jego osobistych plikach.

§16
[Moment wejścia w życie Instrukcji]

Niniejsza Instrukcja stanowi integralną część dokumentu „Polityka Prywatności” i wchodzi w życie wraz z przyjęciem jej obowiązywania.

Załącznik nr 2

do Polityki Prywatności

Role i obowiązki. Struktura organizacyjna Spółki

§1. Wstęp

1. Jednym z kluczowych atrybutów skutecznego podejścia do ochrony danych jest jasny podział ról, z których każda ma określone obowiązki. Każda z tych ról musi być przydzielona konkretnym osobom lub grupom w organizacji.

2. Jasne zdefiniowanie ról i obowiązków, pozwala zapobiec incydentom związanym z naruszeniem ochrony danych.

3. Obowiązki dotyczące wszystkich pracowników, wykonawców i innych Użytkowników są określone w odpowiednich zasadach organizacyjnych.

§2. Role ochrony danych

1. W ramach ochrony danych i zgodności z przepisami RODO należy zdefiniować i przydzielić następujące główne role:

- Inspektor ochrony danych
- Kierownicy działów
- Pracownicy / wykonawcy / współpracownicy

a. **Inspektor Ochrony Danych**

Inspektor Ochrony Danych jest to stanowisko wymagane zgodnie z ogólnym rozporządzeniem RODO i ma szczególne obowiązki w zakresie ochrony danych osobowych.

Inspektor Ochrony Danych ma następujące obowiązki:

- Raportowanie Administratorowi we wszystkich sprawach związanych z bezpieczeństwem danych osobowych regularnie i doraźnie, gdy jest to wymagane;

- Monitorowanie zgodności procesów przetwarzania z przepisami o ochronie danych oraz Polityką Prywatności;

- Przypisywanie obowiązków, podnoszenie świadomości i szkolenie personelu zaangażowanego w przetwarzanie danych osobowych i związane z tym kontrole;

- Udzielanie porad dotyczących oceny wpływu poszczególnych działań na ochronę danych i monitorowanie ich skuteczności;

- Współpraca ze wszystkimi właściwymi organami Administratora oraz kierownikami działów w celu ochrony danych;

- Działanie jako punkt kontaktowy dla organów Administratora oraz kierowników działów w kwestiach związanych z przetwarzaniem danych osobowych i konsultowanie się, w stosownych przypadkach, w odniesieniu do wszelkich innych spraw.

- Wdrożenie wymagań Polityki Prywatności;

- Zarządzanie ryzykiem związanym z dostępem do usługi lub systemów;

- Zapewnienie przeprowadzania i należytego udokumentowania kontroli bezpieczeństwa danych,

- Określanie ilościowo i monitorowanie rodzajów, ilości i skutków incydentów i awarii bezpieczeństwa;

- Zdefiniowanie planów i celów poprawy na rok budżetowy;

- Monitorowanie osiągnięć w stosunku do celów;

- Identyfikowanie incydentów bezpieczeństwa informacji i zarządzanie nimi zgodnie z przetwarzaniem danych osobowych.

b. **Kierownicy działów**

Kierownikami działów / kierownikami mogą być szefowie lub przełożeni jednostek operacyjnych w organizacji Spółki.

Kierownik działu ma następujące obowiązki:

- Sprawdzać kompetencje pracowników oraz zarządzać potrzebne szkolenia, aby umożliwić im skuteczne wykonywanie swojej roli w obszarze ochrony danych,

- Upewniać się, że pracownicy są świadomi znaczenia i wpływu swoich działań oraz tego, w jaki sposób przyczyniają się do osiągnięcia celów ochrony danych,

- Uczestniczyć w dokonywaniu oceny wpływu ich obszaru działalności na ochronę danych.

c. Pracownicy

Obowiązki wszystkich pracowników są zdefiniowane w wielu politykach obowiązujących w całej organizacji i zostały streszczone w skrócie poniżej.

Pracownik ma następujące główne obowiązki w zakresie ochrony danych:

- Upewniać się, że inni pracownicy są świadomi konieczności przestrzegania Polityki Prywatności i przestrzegają wszystkich zasad ochrony danych organizacji istotnych z punktu widzenia ich roli biznesowej,
- Zgłaszać wszelkie faktyczne lub potencjalne naruszenia bezpieczeństwa,

- W razie potrzeby przyczyniać się do oceny wpływu Polityki Prywatności na ochronę danych.

Załącznik nr 3

do Polityki Prywatności w Spółce

Procedura dotycząca przetwarzania danych osobowych klientów Spółki

1. Aby zapewnić właściwą ochronę danych osobowych Klientów Spółki oraz spełnić warunki organizacyjne i techniczne określone przez obowiązujące prawo, w tym rozporządzenie Parlamentu Europejskiego i Rady 2016/679 (UE) 27 kwietnia 2016 r. W sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz uchylającej dyrektywę 95/46 / WE (RODO) i zawartych umów, Spółka zarządza:

Przetwarzając dane osobowe swoich klientów, Spółka zobowiązuje się do przestrzegania prawa i ustalonych zasad, w tym postanowień RODO, w szczególności:

- Wprowadzać w indywidualne obowiązki wynikające z przetwarzania danych osobowych użytkowników bazy danych,

- Przeprowadzać szkolenia Użytkowników w zakresie ochrony danych osobowych,

- Przygotować i wdrażać procedury postępowania w przypadku naruszenia ochrony danych osobowych i instrukcji dostępu do systemów informatycznych,

- Wyznaczyć Inspektora Ochrony Danych (IOD),

● Przechowywać rejestr Użytkowników upoważnionych do przetwarzania danych osobowych,

● Zmieniać hasła użytkowników systemu IT co najmniej raz w miesiącu,

● Zainstalować wygaszacze ekranu na komputerach, na których przetwarzane są dane osobowe,

● Zastosować ochronę antywirusową do powyższych systemów IT,

● Nie ujawniać systemów informatycznych ani nie ujawniać ich działania stronom trzecim,

● Z powoływanych systemów informatycznych korzystać tylko zgodnie z ich przeznaczeniem, tzn. tylko do obsługi klientów i potencjalnych klientów,

● Przetwarzać dane osobowe klientów (w tym tzw. potencjalnych klientów), które Użytkownicy otrzymają od klienta na podstawie umowy o powierzenie przetwarzania danych osobowych lub innej zgody klienta,

● Wykonywać kopie danych dla bezpieczeństwa,

● Prowadzić rejestr przetwarzania danych osobowych,

● Opracować procedurę zgłaszania naruszeń ochrony danych osobowych,

● Informować klientów o obowiązkach wynikających z RODO tj. Administratorze danych, źródle danych, celu przetwarzania danych osobowych, okresie, w którym będą przetwarzane dane osobowe, miejscach i podmiotach, do których przekazywane są dane osobowe, prawach podmiotu danych wynikających z RODO,

● Informować klientów, jeśli ich dane są poddawane automatycznemu przetwarzaniu, w tym profilowaniu,

● Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, klient ma prawo do uzyskania informacji o rozsądnych gwarancjach dotyczących transferu zgodnie z art. 46 rozporządzenia RODO.

Załącznik nr 4

do Polityki Prywatności

Rejestr przetwarzania danych osobowych w Spółce

1. **Wprowadzenie**

W codziennej działalności Spółka gromadzi i przechowuje rejestry i dane wielu typów i w różnych formatach. Względne znaczenie i wrażliwość tych zapisów również jest różna i podlega systemowi klasyfikacji bezpieczeństwa organizacji.

Ważne jest, aby te zapisy były chronione przed utratą, zniszczeniem, sfałszowaniem, nieautoryzowanym dostępem i nieautoryzowanym uwolnieniem dostępu, a do tego należy zapewnić szereg kontroli, w tym tworzenie kopii zapasowych, kontrolę dostępu i szyfrowanie.

Spółka jest również odpowiedzialna za zapewnienie, aby spełnione zostały wszystkie odpowiednie wymogi prawne, regulacyjne i umowne w zakresie gromadzenia, przechowywania, odzyskiwania i niszczenia zapisów. Szczególne znaczenie ma ogólne rozporządzenie o ochronie danych RODO i jego wymogi dotyczące przechowywania i przetwarzania danych osobowych.

Kontrola ta dotyczy wszystkich systemów, osób i procesów, które stanowią systemy informacyjne organizacji, w tym członków zarządu, dyrektorów, pracowników, dostawców i innych stron trzecich, które mają dostęp do systemów Spółki.

2. Zasady przechowywania rejestrów i Polityki Prywatności

Polityka ta rozpoczyna się od ustalenia głównych zasad, które należy przyjąć przy rozważaniu przechowywania i ochrony dokumentacji. Następnie określa rodzaje rejestrów posiadanych przez Spółkę i ich ogólne wymagania przed omówieniem ochrony rekordów, ich zniszczenia i zarządzania.

2.1 Ogólne zasady

Istnieje szereg kluczowych zasad ogólnych, które należy przyjąć przy rozważaniu polityki przechowywania rejestrów i ochrony dokumentacji, m.in.:

- Dane muszą być przechowywane zgodnie ze wszystkimi obowiązującymi wymogami prawnymi, regulacyjnymi i umownymi;
- Dane nie mogą być przechowywane dłużej niż jest to wymagane;
- Ochrona rejestrów pod względem ich poufności, integralności i dostępności musi być zgodna z ich klasyfikacją bezpieczeństwa;
- Zapisy muszą być zawsze dostępne zgodnie z wymogami biznesowymi;
- W stosownych przypadkach zapisy zawierające dane osobowe muszą być jak najszybciej poddane systemom zabezpieczania, które uniemożliwiają identyfikację osoby (szyfrowane/ anonimizowane).

2.2 Typy rejestrów i wytyczne

Aby umożliwić stworzenie wytycznych dotyczących przechowywania i ochrony zapisów, dokumenty Spółki są pogrupowane w kategorie wymienione w tabeli na następnej stronie. Dla każdej z tych kategorii podaje się wymagany lub zalecany okres przechowywania oraz dopuszczalne nośniki wraz z uzasadnieniem.

Należy pamiętać, że są to tylko wytyczne i mogą istnieć szczególne okoliczności, w których dane muszą być przechowywane przez dłuższy lub krótszy okres czasu. Powinno to zostać ustalone indywidualnie dla każdego przypadku w ramach projektowania elementów bezpieczeństwa informacji nowych lub znacząco zmienionych procesów i usług.

Kategoria rekordu	Opis	Okres przechowywania	Przyczyna dla konkretnego okresu przechowywania	Dopuszczalne nośniki pamięci
Rachunkowość	Faktury, zamówienia zakupu, rachunki i inne historyczne zapisy finansowe	10 lat	Obowiązujące przepisy o rachunkowości	Elektroniczne / papierowe
Klienci	Dane osobowe, w tym nazwy klientów, adresy, historia zamówień, dane karty kredytowej i dane bankowe	10 lat po ostatnim zalogowaniu	Wymóg ochrony danych, AML, MGA - maksymalny okres	Elektroniczne / papierowe
Dostawcy	Nazwy dostawców, adresy, dane firmy	5 lat po zakończeniu dostaw	Maksymalny okres, w którym może wystąpić spór	Elektroniczny / papierowy
Zasoby ludzkie	Nazwiska pracowników, adresy, dane bankowe, kody podatkowe, historia zatrudnienia	10 lat po zakończeniu zatrudnienia	Wymóg ochrony danych; Prawo pracy; przepisy o rachunkowości	Elektroniczne / papierowe
Umowy	Umowy prawne, warunki, umowy najmu	5 lat po zakończeniu umowy	Maksymalny okres, w którym może wystąpić spór	Elektroniczne / papierowe

2.3 Korzystanie z kryptografii

W stosownych przypadkach do klasyfikacji informacji i nośnika danych należy stosować techniki kryptograficzne w celu zapewnienia poufności i integralności zapisów.

Należy zadbać o to, aby klucze szyfrowania używane do szyfrowania zapisów były bezpiecznie przechowywane przez cały okres istnienia odpowiednich zapisów i były zgodne z zasadami organizacji dotyczącymi kryptografii.

2.4 Wybór mediów

Wybór długoterminowych nośników danych musi uwzględniać fizyczne cechy medium i czas, w którym będzie on używany.

W przypadku gdy zapisy są prawnie (lub praktycznie) wymagane do przechowywania na papierze, należy podjąć odpowiednie środki ostrożności, aby zapewnić, że warunki środowiskowe pozostaną odpowiednie dla stosowanego rodzaju papieru. Tam, gdzie to możliwe, kopie zapasowe takich zapisów powinny być wykonywane metodami takimi jak skanowanie lub mikrofichowanie. Regularne kontrole muszą być przeprowadzane w celu oceny stopnia pogorszenia papieru i działań podjętych w celu zachowania zapisów, jeśli jest to wymagane.

W przypadku zapisów przechowywanych na nośnikach elektronicznych należy podjąć podobne środki ostrożności, aby zapewnić trwałość materiałów, w tym prawidłowe przechowywanie i kopiowanie na bardziej odporne nośniki, jeśli to konieczne. Możliwość odczytywania zawartości określonego formatu nośnika musi być zachowana dzięki zachowaniu urządzenia zdolnego do jego przetwarzania. Jeśli jest to niepraktyczne, zewnętrzna strona trzecia może zostać zatrudniona do konwersji nośnika na alternatywny format.

2.5 Pobieranie rekordów

Zachowywanie zapisów nie ma sensu, jeśli nie można uzyskać do nich dostępu zgodnie z wymogami biznesowymi lub prawnymi. Wybór i konserwacja urządzeń do przechowywania danych musi zapewnić, że rekordy będą mogły być pobierane w użytecznym formacie w akceptowalnym okresie czasu. Należy zachować odpowiednią równowagę między kosztem przechowywania a szybkością wyszukiwania, tak aby cele zabezpieczenia i przechowywania mogły być realizowane.

2.6 Usuwanie rejestrów

Gdy rekordy osiągają koniec swojej żywotności, zgodnie ze zdefiniowaną polityką, muszą być bezpiecznie zniszczone w sposób, który uniemożliwia ich wykorzystanie. Procedura zniszczenia musi umożliwiać prawidłowe zapisanie tylko tych szczególnych zapisów, które należy zachować jako dowód.

2.7. Przegląd rekordów

Przechowywanie i archiwizowanie danych musi podlegać regularnemu procesowi przeglądu przeprowadzanemu przez kierownictwo / kierowników działów, aby zapewnić, że:

- polityka dotycząca przechowywania i ochrony rejestrów pozostaje aktualna;
- zapisy są przechowywane zgodnie z polityką prywatności;
- zapisy są bezpiecznie usuwane, gdy nie są już potrzebne;
- wymogi prawne, regulacyjne i umowne są spełnione;
- procesy pobierania rekordów spełniają wymagania biznesowe.

Wyniki tych przeglądów muszą zostać zarejestrowane.

Załącznik nr 5

do Polityki Prywatności w Spółce

Polityka mianowania Inspektora Ochrony Danych (IOD)

POWOŁYWANIE Inspektora Ochrony Danych (IOD)

1. **Obowiązek powołania IOD:**

Zgodnie z art. 37 RODO obowiązek wyznaczenia Inspektora Ochrony Danych ma zawsze miejsce, gdy:

- główna działalność Administratora lub Podmiotu Przetwarzającego polega na operacjach przetwarzania, które ze względu na ich charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania podmiotów danych na dużą skalę

- główną działalnością Administratora lub Podmiotu Przetwarzającego jest przetwarzanie na dużą skalę „danych wrażliwych";

Po przeanalizowaniu postanowień rozporządzenia RODO i na podstawie audytu wewnętrznego w zakresie przetwarzania danych osobowych, Spółka spełnia wymogi przewidziane w art. 37 RODO i kwalifikuje się do spełnienia obowiązku wyznaczenia IOD zgodnie z obowiązującymi przepisami prawa i procedurami przyjętymi w Spółce.

2. Kwalifikacje i doświadczenie Inspektora Ochrony Danych:

Kandydat na Inspektora Ochrony Danych musi wykazać się odpowiednimi kwalifikacjami zawodowymi, w szczególności wiedzą zawodową na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wykonywania zadań spoczywających na IOD.

IOD może:

- być członkiem personelu Administratora lub Podmiotu Przetwarzającego,

- wykonywać zadania na podstawie umowy o świadczenie usług,

- wykonywać zadania w grupie przedsiębiorstw, chyba że utrudni to nawiązanie kontaktu lub uniemożliwi skuteczne wykonywanie swoich obowiązków.

IOD ma obowiązek:

- władać językiem lub językami używanymi przez organy nadzoru i osoby, których dane dotyczą,

- posiadać pełną zdolność do czynności prawnych, cieszyć się pełnymi prawami publicznymi i nie być karanym za umyślne przestępstwo.

3. Konflikt interesów

Inspektor ochrony danych może wykonywać inne zadania i obowiązki, chyba że powoduje to konflikt interesów. Pojęcie konfliktu interesów należy interpretować w odniesieniu do zadań Inspektora ochrony danych i jego niezależności w wykonywaniu zadań. Inspektor ochrony danych nie może zajmować stanowiska w organizacji Spółki, co pociąga za sobą określenie metod i celów przetwarzania danych. Stanowiska zarządzania przedsiębiorstwem (np. członkowie zarządu, dyrektor generalny, dyrektor operacyjny, dyrektor finansowy, kierownik ds. marketingu, kierownik działu kadr, kierownik działu IT) będą uważane za sprzeczne interesy, a także zasiadanie na niższych stanowiskach, jeśli będą one zaangażowane w definiowanie celów i metod przetwarzania danych. Profesjonalny przedstawiciel (np. adwokat, radca prawny) może działać jako Inspektor ochrony danych, chyba że reprezentuje Spółkę w sprawach przed sądem dotyczących ochrony danych osobowych.

Poniżej znajdują się funkcje, których nie można łączyć z funkcją IOD:

- Prezes Zarządu;
- Członek Rady Nadzorczej;
- Prokurent;
- Dyrektor operacyjny;
- Dyrektor finansowy;
- Kierownik działu IT;
- Kierownik działu marketingu.

Spółka na etapie rekrutacji Inspektora ochrony danych jest zobowiązana do jej przeprowadzenia z uwzględnieniem zasad określonych w niniejszej Polityce.

Jeżeli Administrator zdecyduje się nałożyć nowe obowiązki na Inspektora ochrony danych, które nie są związane z przetwarzaniem danych osobowych, jest on zobowiązany ocenić, czy w wyniku takich działań nie dojdzie do konfliktu interesów lub trudności w skutecznym wykonaniu obowiązków Inspektora ochrony danych.

4. Sposób powołania Inspektora ochrony danych w Spółce:

IOD jest mianowany do wykonywania swojej funkcji w ramach jednego z wymienionych trybów:

- uchwała Zarządu,
- zarządzenie dyrektora, jeśli ma on skuteczne upoważnienie,
- decyzja o powierzeniu wykonania zadań,
- zawarcie umowy o pracę,
- zawarcie umowy cywilnoprawnej (w tym outsourcing).

Niniejsza Polityka jest obowiązkowym załącznikiem do wyżej wymienionych form nawiązania współpracy.

5. Zgłaszanie Inspektora ochrony danych organowi nadzorczemu i publikowanie danych.

Firma publikuje dane kontaktowe Inspektora ochrony danych i powiadamia o tym organ nadzoru w ciągu 14 dni od daty wyznaczenia Inspektora ochrony danych.

Publikacja danych IOD oznacza umieszczenie informacji o IOD na stronie internetowej Spółki (numer telefonu, adres e-mail). Ponadto informacje o Inspektorze ochrony danych powinny być przekazywane wszystkim współpracownikom, pracownikom i podmiotom współpracującym.

Powiadomienie organu nadzorczego jest rozumiane jako elektroniczne powiadomienie właściwego organu.

5. Zasady współpracy z IOD:

Inspektor ochrony danych zostaje natychmiast i odpowiednio zaangażowany we wszystkich sprawach dotyczących ochrony danych osobowych. Wszystkie osoby w organizacji Spółki są zobowiązane do przestrzegania określonych zasad współpracy z IOD i dobrych praktyk związanych z dostarczaniem informacji IOD.

Administrator lub podmiot przetwarzający nie może usunąć, dyscyplinować ani ukarać Inspektora ochrony danych za wypełnianie swoich zadań.

IOD podlega bezpośrednio najwyższemu kierownictwu Administratora lub Podmiotu Przetwarzającego.

Osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych i korzystać z praw przysługujących im na mocy rozporządzenia RODO.

Administrator i podmiot przetwarzający wspierają IOD w wypełnianiu jego zadań, zapewniając mu zasoby niezbędne do wykonywania tych zadań i dostępu do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego profesjonalnej wiedzy.

6. Obowiązki IOD

- Informowanie Administratora, Podmiotu Przetwarzającego / Użytkownika i pracowników przetwarzających dane osobowe o obowiązkach spoczywających na nich zgodnie z wymaganiami RODO i innymi obowiązującymi przepisami dotyczącymi ochrony danych osobowych.

- Monitorowanie przestrzegania zasad wynikających z RODO i innych obowiązujących przepisów dotyczących ochrony danych osobowych, a także Polityki Prywatności;

- Zgłaszanie do organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych) jakiegokolwiek naruszenia ochrony danych osobowych w Spółce, w ciągu 72 godzin od ujawnienia naruszenia.

- Współpraca z właściwymi organem nadzoru w imieniu Spółki.

● Pełnienie funkcji punktu kontaktowego dla osób fizycznych składających wnioski i skargi dotyczące przetwarzania ich danych osobowych i wykonywania ich praw przez Spółkę.

● Prowadzenie szkoleń personelu zaangażowanego w operacje przetwarzania danych.

● Podnoszenie świadomości w zakresie ochrony danych osobowych.

● Przeprowadzanie audytów dotyczących ochrony danych osobowych

● Wydawanie zaleceń dotyczących oceny skutków w zakresie ochrony danych i monitorowanie ich wdrażania zgodnie z RODO.

● Pełnienie funkcji punktu kontaktowego dla organu nadzorczego i innych organów ochrony danych w sprawach związanych z przetwarzaniem, w tym wcześniejszych konsultacji, o których mowa w RODO i w stosownych przypadkach, konsultowanie się we wszystkich innych sprawach.

7. Zespół ds. Ochrony Danych Osobowych (dalej jako "Zespół")

Jeśli Inspektor Ochrony Danych uzna, że do skutecznego wykonywania jego obowiązków konieczne jest utworzenie Zespołu ochrony danych osobowych, wyznaczy odpowiednie osoby z organizacji Administratora i podmiotu przetwarzającego, które będą częścią wyznaczonego Zespołu. Sposób i tryb działania Zespołu zostanie określony przez wewnętrzną regulację IOD, z uwzględnieniem praktyk organizacyjnych i skuteczności operacji.

8. Ocena wpływu i wyniku określonych działań Spółki na ochronę danych osobowych

a. Jeśli dany rodzaj przetwarzania - w szczególności przy użyciu nowych technologii - ze względu na jego charakter, zakres, kontekst i cele może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Spółka jest zobowiązana do oceny skutków planowanych operacji przed rozpoczęciem przetwarzania, w celu ochrony danych osobowych.
b. Pojedyncza ocena może zostać przeprowadzona w przypadku podobnych operacji przetwarzania danych obejmujących podobne wysokie ryzyko.
c. Przeprowadzając ocenę wpływu na ochronę danych, firma konsultuje się z Inspektorem ochrony danych.
d. Ocena wpływu na ochronę danych jest wymagana w szczególności dla:
    - systematycznej, wszechstronnej oceny czynników osobowych odnoszących się do osób fizycznych, opartych na zautomatyzowanym przetwarzaniu, w tym profilowaniu, stanowiących podstawę decyzji, które wywołują skutki prawne dla osoby fizycznej lub w podobny sposób znacząco wpływają na osobę fizyczną;

- przetwarzania wrażliwych danych osobowych na dużą skalę (tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej związanej ze zdrowiem, seksualnością lub orientacją seksualną) lub dane osobowe dotyczące wyroków skazujących, innych orzeczeń sądowych i naruszeń prawa.

9. Procedura informowania IOD o naruszeniach lub ryzyku naruszenia

W przypadku wystąpienia któregokolwiek z warunków opisanych w punkcie 8 powyżej, wyznaczone osoby odpowiedzialne za przetwarzanie danych i Administrator są zobowiązane do informowania i konsultowania się z Inspektorem Ochrony Danych zgodnie z następującą procedurą:

Nr:	Odpowiedzialna osoba:	Działania podjęte
1.	**Administrator**	Prośba osób odpowiedzialnych o wdrożenie nowego / zmienionego projektu i przeprowadzenie oceny skutków planowanych operacji zgodnie z RODO
2.	**Administrator / osoba odpowiedzialna za projekt**	Sprawdzanie, czy projekt jest związany z przetwarzaniem danych osobowych
3.	**Administrator / osoba odpowiedzialna za projekt**	Oświadczenie, że projekt jest związany z przetwarzaniem danych osobowych ub brak jasnej odpowiedzi - przejście do następnego punktu procedury. Oświadczenie, że projekt nie jest związany z przetwarzaniem danych osobowych - zakończenie procedury.
4.	**Administrator / osoba odpowiedzialna za projekt**	Natychmiastowe poinformowanie IOD o szczegółach projektu

5.	**IOD**	Odpowiedź do Administratora / osoby odpowiedzialnej za projekt co do przyjętego przez IOD stanowiska. lub Jeśli projekt wymaga dalszych konsultacji, Inspektor ochrony danych konsultuje się z Zespołem ds. Ochrony danych osobowych (jeśli został wyznaczony). Po konsultacji, Odpowiedź do Administratora / osoby odpowiedzialnej za projekt co do przyjętego przez IOD i zespół stanowiska.
6.	**Administrator / osoba odpowiedzialna za projekt**	Uwzględnienie wytycznych Inspektora ochrony danych, zastosowanie ich do projektu, poinformowanie Inspektora ochrony danych. Koniec procedury. Jeśli nie zgadzasz się z opinią Inspektora ochrony danych: - Osoba odpowiedzialna za projekt - przejdź do punktu 7. - Administrator - przejdź do punktu 8.
7.	**Osoba odpowiedzialna za projekt**	Osoba odpowiedzialna za projekt - przekazuje wątpliwości i przyjęte stanowisko Administratorowi. Informuje Inspektora ochrony danych.
8.	**Administrator**	Podejmuje decyzję i informuje Inspektora ochrony danych oraz osobę odpowiedzialną za projekt wraz z uzasadnieniem. Koniec procedury.

Załącznik nr 6

do Polityki Prywatności w Spółce

Procedura zgłaszania incydentów podczas przetwarzania danych osobowych

§ 1
Wstęp

Niniejsza procedura zgłaszania incydentów podczas przetwarzania danych osobowych w Spółce jest przeznaczona do wykorzystania w przypadku, wystąpienia ryzyka naruszenia ochrony danych osobowych („Procedura„).

Wymogiem RODO jest powiadomienie organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych (UODO) przez Administratora lub Inspektora ochrony danych o zdarzeniach mających wpływ na bezpieczeństwo danych osobowych, jeżeli zdarzenie mogło spowodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą. Organ nadzorczy powinien zostać powiadomiony bez zbędnej zwłoki - jeśli to możliwe - w okresie nie dłuższym niż 72 godziny od momentu wykrycia zdarzenia. Po 72 godzinach należy wyjaśnić powody opóźnienia.

W sytuacji, gdy występujemy jako podmiot przetwarzający dane, Administrator / Inspektorzy danych osobowych powinni być powiadamiani bez zbędnej zwłoki o naruszeniu danych.

W sytuacji, gdy działamy jako Administrator danych, należy podjąć decyzję dotyczącą zakresu, ram czasowych i treści komunikacji z osobami, których dane dotyczą. Zgodnie z postanowieniami rozporządzenia RODO, osoba, której dane dotyczą, powinna być poinformowana „bez zbędnej zwłoki", jeżeli naruszenie ochrony danych skutkuje „ryzykiem naruszenia praw lub wolności osób fizycznych".

Działania opisane w tej procedurze powinny służyć jedynie jako wskazówki dotyczące reagowania na naruszenia danych. Ze względu na fakt, że niemożliwe jest przewidzenie dokładnego charakteru zdarzenia i jego konsekwencji, konieczne jest zastosowanie zdrowego rozsądku, aby podjąć właściwe działania. Jednak przestrzeganie niniejszej Procedury gwarantuje, że Spółka wypełnia należycie swoje zobowiązania wobec stosowania przepisów rozporządzenia RODO.

§ 2

Procedura zgłaszania naruszenia ochrony danych osobowych

1. W przypadku naruszenia ochrony danych osobowych, należy poinformować następujące strony:
    a. Administrator danych;
    b. IOD;
    c. organ nadzorczy - Prezes UODO;
    d. osoby poszkodowane.

2. Powiadomienie o naruszeniu ochrony danych osobowych zależy od oceny ryzyka naruszenia „praw i wolności osób fizycznych", dlatego nie należy go zakładać z góry. Procedura ta zawiera informacje, które pozwolą Ci zdecydować o konieczności powiadomienia i instrukcje, jak postępować w razie konieczności.

§3

Powiadomienie Administratora Danych i Inspektora Ochrony Danych

1. W przypadku naruszenia lub podejrzenia o naruszeniu ochrony danych osobowych należy natychmiast poinformować Administratora i Inspektora Ochrony Danych. Następnie Inspektor decyduje, czy istnieje potrzeba zgłoszenia naruszenia i podjęcia dalszych działań.

2. Aby Administrator mógł działać zgodnie z postanowieniami RODO, Użytkownik musi podać następujące informacje:
- data i godzina wykrycia naruszenia danych,
- data i godzina, uważane za moment, kiedy prawdopodobnie miało miejsce naruszenie danych;
- jakich danych dotyczyło przetwarzanie (np. imię i nazwisko, adres, dane bankowe, numer PESEL itp.),
- zakres danych, których dotyczy naruszenie,
- liczba poszkodowanych osób, których dane dotyczą,
- charakter naruszenia, np. kradzież, przypadkowe zniszczenie,
- informacja, czy dane osobowe zostały zaszyfrowane,
- jaki był poziom siły szyfrowania danych,
- podjęte działania zaradcze,
- dane kontaktowe osoby zajmującej się ochroną danych osobowych w organizacji,
- inne czynniki uznane za istotne.

§4

Organ nadzoru

Jeżeli Inspektor Ochrony Danych lub Administrator stwierdzi, że naruszenie wymaga powiadomienia organu nadzorczego zgodnie z postanowieniami rozporządzenia RODO, Inspektor Ochrony Danych składa sprawozdanie następującemu organowi:

Nazwa organu :	Prezes Urzędu Ochrony Danych Osobowych (UODO) https://uodo.gov.pl;
Adres:	ul. Stawki 2 00-193 Warszawa
Telefon:	606-950-000
Faks:	+48 (22) 531-03-01
E-mail:	kancelaria@uodo.gov.pl

§5

Decyzja o zgłoszeniu naruszenia organowi nadzorczemu

1. Zgodnie z postanowieniami RODO naruszenia danych osobowych należy zgłaszać organowi nadzorczemu, „chyba że jest mało prawdopodobne, że naruszenie skutkowałoby ryzykiem naruszenia praw lub wolności osób fizycznych" (art. 33 rozporządzenia RODO). Dlatego też IOD musi ocenić poziom ryzyka przed podjęciem decyzji, czy zgłoszenie naruszenia organowi nadzorczemu jest konieczne.

2. Ocena ryzyka powinna uwzględniać następujące czynniki:

a. czy dane osobowe zostały zaszyfrowane,
b. jaka jest siła szyfrowania danych,
c. jaki jest stopień, w jakim dane zostały pseudonimizowane (np. czy osoby można zidentyfikować na podstawie tych danych),
d. dane, których to dotyczy (np. imię i nazwisko, adres, dane bankowe, PESEL),
e. zakres danych, których dotyczy naruszenie,
f. liczba poszkodowanych osób, których dane dotyczą,
g. charakter naruszenia, np. kradzież, przypadkowe zniszczenie,
h. inne czynniki uznane za istotne.

3. Metodę oceny ryzyka, uzasadnienie i podsumowanie należy udokumentować i przedstawić Administratorowi do podpisu.
Wyniki oceny ryzyka powinny spowodować podjęcie jednej z następujących decyzji:

a. uznanie, że powiadomienie o naruszeniu danych osobowych nie jest konieczne;
b. uznanie, że naruszenie ochrony danych osobowych należy zgłosić wyłącznie organowi nadzorczemu;
c. uznanie, że naruszenie ochrony danych osobowych należy zgłosić zarówno organowi nadzoru, jak i osobom, których dotyczy naruszenie.

4. Podjęte decyzje mogą ulec zmianie ze względu na informacje zwrotne od organu nadzorczego i dalsze informacje uzyskane podczas badania okoliczności naruszenia danych osobowych.

§ 6

Zgłoszenie naruszenia organowi nadzorczemu]

1. Jeśli zostanie podjęta decyzja o powiadomieniu organu nadzorczego, zgodnie z postanowieniami RODO, należy to zrobić „bez zbędnej zwłoki - w miarę możliwości, nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia" (art. 33 rozporządzenia RODO). Powiadomienie złożone organowi nadzorczemu, po upływie tego okresu, musi zawierać wyjaśnienie powodów opóźnienia.

2. Należy przesłać powiadomienie za pomocą odpowiednich, bezpiecznych środków do odpowiedniego organu nadzorczego opisanego w powyższej tabeli, dokonując raportowania naruszenia danych osobowych, poprzez formularz dostępny w Spółce, jako szablon.

3. Powiadomienie powinno zawierać następujące informacje:

a. charakter naruszenia ochrony danych osobowych, w tym, jeśli to możliwe:
   - kategorie i przybliżona liczba osób, których dane dotyczą;

- kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie;

b. imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenia innej osoby, od której można uzyskać więcej informacji;

c. opis możliwych konsekwencji naruszenia danych osobowych;

d. opis środków podjętych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym, w stosownych przypadkach, środki mające na celu zminimalizowanie jego potencjalnych niekorzystnych skutków;

e. wyjaśnienie powodów opóźnienia (w przypadku powiadomienia przesłanego organowi nadzorczemu po 72 godzinach).

4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia danych osobowych, ich skutki i podjęte działania naprawcze. Ta dokumentacja musi umożliwić organowi nadzorczemu sprawdzenie zgodności z przepisami RODO.

5. Potwierdzenie pisemne otrzymania powiadomienia o naruszeniu ochrony danych powinno określać datę i godzinę otrzymania powiadomienia. W uzasadnionych przypadkach przepisy rozporządzenia RODO nakazują przekazywanie informacji sukcesywnie, bez zbędnej zwłoki.

§ 7

Osoby, których dane dotyczą

1. Zgodnie z postanowieniami rozporządzenia o ochronie danych osobowych RODO osoby, których dane dotyczą, powinny być informowane o naruszeniu ochrony danych osobowych „jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych” (art. 34 RODO).

2. Wcześniejsza ocena ryzyka pozwoli ustalić, czy ryzyko naruszenia praw lub wolności osób, których dane dotyczą, jest wystarczająco wysokie, aby uzasadnić powiadomienie tych osób.

3. W sytuacji, gdy z powodzeniem podjęto działania w celu zminimalizowania ryzyka dla osób, których dane dotyczą, eliminując prawdopodobieństwo wysokiego ryzyka, zgodnie z wymogami rozporządzenia w sprawie RODO, nie ma potrzeby powiadamiania tych osób.

4. Zgodnie z przepisami rozporządzenia RODO powiadomienie osób, których dane dotyczą, nie jest wymagane w przypadku, gdy „wymagałoby to nieproporcjonalnie dużego wysiłku”. W takiej sytuacji pojawia się komunikat publiczny, np. za pośrednictwem strony internetowej.

5. Podjęta decyzja może ulec zmianie ze względu na informacje zwrotne od organu nadzorczego i dalsze informacje uzyskane podczas badania okoliczności naruszenia danych osobowych.

6. Jeżeli zostanie podjęta decyzja o powiadomieniu osób, których dane dotyczą zgodnie z postanowieniami RODO, należy to zrobić bez zbędnej zwłoki.

7. Powiadomienie pokrzywdzonych osób, których dotyczy naruszenie, powinno być napisane „jasnym i prostym językiem opisującym charakter naruszenia danych osobowych” (art. 34 RODO) i musi zawierać następujące informacje:

a. pełne imię i nazwisko oraz dane kontaktowe Administratora, IOD lub innej osoby upoważnionej, od której można uzyskać więcej informacji,
b. opis możliwych konsekwencji naruszenia ochrony danych osobowych,
c. opis środków podjętych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym, w stosownych przypadkach, środków mających na celu zminimalizowanie jego potencjalnych negatywnych skutków.

8. Oprócz informacji wymaganych w przepisach rozporządzenia RODO zaleca się udzielenie osobie, której dane dotyczą, porady w sprawie działań, jakie osoba ta może podjąć, aby zmniejszyć ryzyko związane z naruszeniem jej danych osobowych.

9. W większości przypadków wskazane jest powiadomienie osób, których dane dotyczą, o naruszeniach ochrony danych, za pośrednictwem tradycyjnej poczty lub poczty elektronicznej - w celu zapewnienia, że wiadomość została odebrana - a osoba, której dane dotyczą, ma możliwość podjęcia odpowiednich działań.

10. Procedura powiadamiania stanowi załącznik do Polityki Prywatności i wchodzi w życie z dniem przyjęcia Polityki.

Formularz zgłaszania naruszenia danych osobowych

Imię i nazwisko:	
Tytuł:	
Nazwa organizacji:	
Adres organizacji:	
Telefon:	
Adres e-mail:	
Data i godzina powiadomienia:	
Data i godzina wykrycia naruszenia danych osobowych:	
Czas między wykryciem a powiadomieniem:	

Opis charakteru naruszenia ochrony danych osobowych:

Możliwe konsekwencje naruszenia danych osobowych:

Środki podjęte w celu zaradzenia naruszeniu ochrony danych osobowych:

Proponowane środki w celu dalszego przeciwdziałania naruszeniom ochrony danych osobowych:

Wyjaśnienie przyczyn opóźnienia w zawiadomieniu, jeśli dotyczy:

PROJEKT POWIADOMIENIA

_____, _____

Spółka …….. sp. z o.o.

Dane spółki

[nazwa odbiorcy]

Szanowna / y Pani / Panie

Jako Administrator Państwa danych osobowych, Spółka ….. dokłada wszelkich starań, aby gromadzone i przetwarzane dane były pod najlepszą ochroną.

Niestety czujemy się zobowiązani do poinformowania Pani/Pana o incydencie, który może wpłynąć na bezpieczeństwo Pani /Pana danych osobowych, które przechowujemy.

W dniu [data] …… zauważyliśmy, że …… [opis zdarzenia naruszającego ochronę danych osobowych] . Mamy podstawy, aby twierdzić, że w wyniku tego zdarzenia Pani /Pama dane osobowe, w tym …… .. [lista danych osobowych, na przykład imię i nazwisko, adres, dane bankowe] zostały skradzione lub udostępnione [lub w inny sposób naruszone, np. utracone] . To naruszenie może spowodować zwiększone ryzyko ……. [opis możliwych konsekwencji naruszenia ochrony danych osobowych osoby, której dane dotyczą].

Rozpoczęliśmy działania wyjaśniające okoliczności naruszeń ochrony danych, aby dotrzeć do źródła problemu i uniknąć podobnych sytuacji w przyszłości. Od momentu stwierdzenia naruszenia ochrony danych osobowych …… .. [opis podjętych dotychczas działań naprawczych] . Planujemy również ……. [opis dodatkowych działań zaradczych, które zostaną podjęte].

Skontaktujemy się z Panią / Panem ponownie, gdy otrzymamy nowe informacje dotyczące tej kwestii. Pozostajemy w ścisłej współpracy z organem nadzorczym - Prezesem Urzędu Ochrony Danych Osobowych w celu podjęcia działań prawnych w tej sprawie.

W razie chęci uzyskania dodatkowych informacji zachęcamy do kontaktu z [wpisz osobę upoważnioną przez administratora danych] na [adres e-mail] lub pocztą na [adres pocztowy].

Z poważaniem,

_____

Administrator danych

Załącznik nr 7

do Polityki Prywatności w Spółce

Oświadczenie pracownika / współpracownika

Ja niżej podpisany …….. (imię i nazwisko pracownika/współpracownika) niniejszym oświadczam, że zapoznałem się z przepisami dotyczącymi ochrony danych osobowych w Spółce …… , w szczególności z Polityką Prywatności wraz z załącznikami oraz przepisami rozporządzenia 2016/679 Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz uchylenie dyrektywy 95/46 / WE („RODO") i zobowiązuję się je przestrzegać.

W związku z powyższym zobowiązuję się do:

● przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w zadaniach powierzonych przez Administratora, w tym na podstawie upoważnienia udzielonego przez Administratora do przetwarzania danych osobowych;

● poufności danych osobowych, do których uzyskałem lub uzyskuję dostęp w związku z wykonywaniem zadań powierzonych przez Administratora;

● nie wykorzystywania danych osobowych do celów niezgodnych z zakresem i celem zadań powierzonych przez Administratora;

● utrzymywania w tajemnicy sposobu ochrony danych osobowych przetwarzanych przez Administratora;

● ochrony danych osobowych przed przypadkowym lub bezprawnym zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych i ich przetwarzaniem.

Jednocześnie jestem zobowiązany powiadomić Administratora i Inspektora Ochrony Danych o każdym naruszeniu przepisów RODO lub wewnętrznych procedur dotyczących danych osobowych w ciągu 24 godzin na adres e-mail IOD : iod@.....

Rozumiem, że zachowanie sprzeczne z wyżej wymienionymi zobowiązaniami może zostać uznane przez Administratora za naruszenie postanowień GDPR. Zdaję sobie sprawę z obowiązku zachowania w tajemnicy danych osobowych, ich zabezpieczenia, także po zakończeniu współpracy.

……(data i podpis)

Załącznik nr 8

do Polityki Prywatności w Spółce

Upoważnienie pracownika / współpracownika

do przetwarzania danych osobowych

Spółka _____

(dalej jako **“Administrator")**

UPOWAŻNIENIE

DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, zgodnie z art. 29 Rozporządzenie 2016/679 Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz uchylające dyrektywę 95/46 / EC („RODO”), upoważniam:

Panią / Pana …… na stanowisku …… (dalej jako **„Osoba upoważniona”),**

do przetwarzania danych osobowych, w celach związanych z wykonywaniem zobowiązań wynikających z zawartej umowy między Administratorem a Osobą Upoważnioną („Umowa”), polegająca na gromadzeniu, nagrywaniu, organizowaniu, przechowywaniu, dostosowywaniu, modyfikowaniu, pobieraniu, przeglądaniu, używaniu, ujawnianiu poprzez wysyłanie lub inne rodzaje udostępniania, dopasowywania lub łączenia, ograniczenie w zakresie niezbędnym do prawidłowego wykonywania czynności zleconych przez Administratora.

Upoważnienie to obejmuje przetwarzanie danych osobowych zarówno w formie tradycyjnej, jak i elektronicznej.

Upoważnienie wygasa wraz z wygaśnięciem Umowy pomiędzy Stronami.

Jednocześnie informuję, że Osoba Upoważniona jest zobowiązana do zachowania powyższych informacji w poufności. Osoba upoważniona jest zobowiązana do przestrzegania zasad obowiązujących u Administratora w zakresie ochrony danych osobowych, w tym wynikających z obowiązujących procedur, zasad i przepisów RODO, w tym do zapoznania się z Polityką Prywatności. Obowiązek zachowania tajemnicy istnieje również po wygaśnięciu Umowy.

_____ w imieniu Administratora

Załącznik nr 9

do Polityki Prywatności w Spółce

Rejestr naruszeń ochrony danych osobowych

nr	Data i godzina incydentu	Opis okoliczności naruszenia	Skutki naruszenia	Opis działań naprawczych	Data i godzina powiadomienia administratora danych / inspektora ochrony danych	Naruszenie i incydent powodujący ryzyko naruszenia praw lub wolności osób fizycznych wymaga powiadomienia Prezesa Urzędu Ochrony Danych Osobowych	Koniec realizacji działań - data	Osoba odpowiedzialna za realizację działań	Naruszenie ochrony danych powodujące wysokie ryzyko naruszenia praw i wolności osób wymaga powiadomienia osoby, której dane dotyczą.

Załącznik nr 10

do Polityki Prywatności w Spółce

REJESTR OSÓB

UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Imię i nazwisko / stanowisko pracy	Data uzyskania autoryzacji od Administratora *(załącznik 8 Polityki Prywatności)*	Data wygaśnięcia autoryzacji (wygaśnięcie Umowy)	Data odbycia szkoleń z zakresu RODO	Plik PDF z podpisanym oświadczeniem RODO *(załącznik 7 Polityki Prywatności)*
