TOREC

# PROCEDURA OCHRONY DANYCH W „TOREC" SP. Z O.O.

**PROC125522 / A**
Sygn.: TOR/ORG/DP/4.13

Data zatwierdzenia: 2020/05/18
Obowiązuje od: 2020/05/18

## I CEL I ZAKRES

1.1 Niniejsza Procedura określa zasady przetwarzania danych osobowych w Przedsiębiorstwie Usługowo-Handlowym „TOREC" Sp. z o.o. oraz obowiązki osób przetwarzających dane osobowe, a także definiuje prawa osób, których dane osobowe są przetwarzane.

1.2 Celem Procedury jest opisanie zasad postępowania przy gromadzeniu i przetwarzaniu danych osobowych w Spółce, a w szczególności:

a. wskazanie obowiązków osób przetwarzających dane osobowe,
b. określenie organizacyjnych i technicznych środków bezpieczeństwa,
c. wskazanie działań, jakie należy wykonywać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki związane z ochroną danych osobowych,
d. określenie obszaru przetwarzania danych osobowych oraz sposobu ich przetwarzania w systemach informatycznych,
e. określenie praw osób, których dane osobowe są w Spółce przetwarzane,
f. dostosowanie do zasad związanych z ochroną danych osobowych regulowanych powszechnie obowiązującymi przepisami prawa.

## II ODPOWIEDZIALNOŚĆ

2.1 Za stosowanie niniejszej Procedury odpowiedzialny jest Zarząd Spółki.

## III DOKUMENTY POWIĄZANE

3.1 *Procedura „TOREC" sp. z o.o. w zakresie bezpieczeństwa IT*

## IV ZAŁĄCZNIKI

4.1 Zał.1 Wzór Rejestru Czynności Przetwarzania Danych
4.2 Zał.2 Wzór wykazu miejsc przetwarzania danych osobowych

## V SKRÓTY I DEFINICJE

*TOREC,*

*Administrator / Spółka; Dane; Dane Dzieci; Dane Karne; Dane Niezidentyfikowane; Dane Szczególnych Kategorii; Eksport Danych; Kontrola Zewnętrzna; Organ Nadzorczy; Osoba; Pracownik; Osoba Trzecia; Podmiot Przetwarzający oraz Przetwarzający; Prawa Jednostki; Procedura; Profilowanie; RCPD / Rejestr; RODO; Sprawdzenie*

***Skróty użyte na potrzeby niniejszego dokumentu:***

***RCPD*** - Rejestr Czynności Przetwarzania Danych

***Definicje pojęć użyte na potrzeby niniejszego dokumentu:***

5.1 ***Administrator / Spółka*** oznacza Przedsiębiorstwo Handlowo-Usługowe „TOREC" sp. z o.o., która w danym procesie przetwarzania Danych decyduje o celu i sposobach przetwarzania.

5.2 ***Dane*** oznaczają dane osobowe.

5.3 ***Dane Dzieci*** oznaczają Dane osób poniżej 13 roku życia.

5.4 ***Dane Karne*** oznaczają Dane wymienione w art. 10 RODO, tj. Dane dotyczące wyroków skazujących i naruszeń prawa.

5.5 ***Dane Niezidentyfikowane*** należy rozumieć jako Dane osób, których tożsamości Spółka nie zna (np. nagrania monitoringu wizyjnego) lub informacje, co do których Spółka nie wie, czy znajdują się w nich Dane, ale jest taka możliwość (np. zawartość serwera plików).

5.6 ***Dane Szczególnych Kategorii*** oznaczają Dane wymienione w art. 9 RODO, tj. Dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

5.7 ***Eksport Danych*** oznacza przekazanie Danych do państwa trzeciego (czyli poza Unię Europejską, Norwegię, Lichtenstein, Islandię) (dalej EOG) lub do organizacji międzynarodowych.

5.8 **Kontrola Zewnętrzna** oznacza kontrolę prowadzoną przez podmiot zewnętrzny, a w szczególności przez Organ Nadzorczy.

5.9 ***Organ Nadzorczy*** oznacza właściwy organ do wypełniania zadań i wykonywania uprawnień powierzonych mu zgodnie z RODO oraz przepisami krajowymi.

5.10 ***Osoba*** oznacza osobę, której Dane dotyczą.

5.11 ***Pracownik*** oznacza osobę, z którą Spółka nawiązała stosunek pracy w rozumieniu art. 22 k.p., oraz osoby zatrudnione na podstawie umowy cywilno-prawnej oraz na podstawie samozatrudnienia.

5.12 ***Osoba Trzecia*** oznacza pracownika firmy zewnętrznej realizującego określone zadania na rzecz Spółki.

5.13 **Podmiot Przetwarzający oraz Przetwarzający** oznacza organizację lub osobę, której Spółka powierzyła przetwarzanie Danych (np. usługodawca IT, zewnętrzna księgowość).

5.14 ***Prawa Jednostki*** oznaczają prawa przysługujące Osobie określone w art. 15-20 RODO tj, prawo dostępu do Danych, prawo do sprostowania Danych, prawo do usunięcia Danych, prawo do ograniczenia przetwarzania, prawo do bycia poinformowanym o sprostowaniu, usunięciu, lub ograniczeniu przetwarzania Danych, prawo do przenoszenia Danych.

5.15 ***Procedura*** oznacza niniejszą Procedurę Ochrony Danych.

5.16 ***Profilowanie*** oznacza dowolną formę zautomatyzowanego przetwarzania Danych, które polega na wykorzystaniu Danych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

5.17 ***RCPD / Rejestr*** oznacza Rejestr Czynności Przetwarzania Danych.

5.18 ***RODO*** oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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).

5.19 ***Sprawdzenie cykliczne*** sprawdzenie stanu zgodności przetwarzania Danych w Spółce przez osoby do tego wyznaczone w Spółce.

## VI REALIZACJA

### 6.1 ZASADY OCHRONY DANYCH

6.1.1 Następujące zasady stanowią filary ochrony Danych w Spółce:

6.1.1.1 Spółka dba o ochronę prywatności i przetwarza Dane zgodnie z prawem (Legalność).

6.1.1.2 Spółka zapewnia odpowiedni poziom bezpieczeństwa Danych podejmując stale działania w tym zakresie (Bezpieczeństwo).

6.1.1.3 Spółka umożliwia osobom, których Dane przetwarza, wykonywanie swoich praw i prawa te realizuje (Prawa Jednostki).

6.1.1.4 Spółka dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność z zasadami ochrony Danych (Rozliczalność).

6.1.2 Spółka przetwarza Dane z poszanowaniem następujących zasad:

6.1.2.1 w oparciu o podstawę prawną i zgodnie z prawem (legalizm)

6.1.2.2 rzetelnie i uczciwie (rzetelność)

6.1.2.3 w sposób przejrzysty dla Osoby (transparentność)

6.1.2.4 w konkretnych celach i nie „na zapas" (minimalizacja)

6.1.2.5 nie więcej niż potrzeba (adekwatność)

6.1.2.6 z dbałością o prawidłowość Danych (prawidłowość)

6.1.2.7 nie dłużej niż potrzeba (czasowość)

6.1.2.8 zapewniając odpowiednie bezpieczeństwo Danych (bezpieczeństwo)

6.1.3 System ochrony Danych w Spółce składa się z następujących elementów:

6.1.3.1 Inwentaryzacja danych. Spółka dokonuje identyfikacji czynności przetwarzania Danych w Spółce, w tym:

a. przypadków przetwarzania Danych Szczególnych Kategorii i Danych Karnych,
b. przypadków przetwarzania Danych Niezidentyfikowanych,
c. przypadków przetwarzania Danych Dzieci i innych osób wymagających szczególnej opieki,
d. profilowania i automatycznego podejmowania decyzji,
e. współadministrowania Danymi.

6.1.3.2 Rejestr. Spółka opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych jako Administrator i Kategorii Czynności Przetwarzania jako Podmiot Przetwarzający (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną Danych w Spółce.

6.1.3.3 Podstawy prawne. Spółka zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania Danych i rejestruje je w Rejestrze, oraz:

a. zarządza zgodami na przetwarzanie Danych i komunikację marketingową na odległość,
b. inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Spółka przetwarza Dane na podstawie prawnie uzasadnionego interesu Spółki.

6.1.3.4 Obsługa Praw Jednostki. Spółka spełnia obowiązki informacyjne względem osób, których Dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania.

6.1.3.5 Obowiązki informacyjne. Spółka przekazuje osobom prawem wymagane informacje przy zbieraniu Danych i w innych sytuacjach oraz organizuje zapewnia udokumentowanie realizacji tych obowiązków.

6.1.3.6 Możliwość wykonania żądań. Spółka weryfikuje i zapewnia możliwość efektywnego wykonania Praw Jednostki przez siebie i swoich przetwarzających.

6.1.3.7 Obsługa żądań. Spółka zapewnia odpowiednie nakłady i procedury, aby żądania Osób były realizowane w terminach i w sposób wymagany przez RODO i rzetelnie dokumentowane.

6.1.3.8 Minimalizacja. Spółka zarządza minimalizacją (privacy by default), a w tym:

a. adekwatnością Danych
b. dostępem do Danych
c. okresem przechowywania Danych

6.1.3.9 Bezpieczeństwo. Spółka zapewnia odpowiedni poziom bezpieczeństwa Danych, w tym:

a. przeprowadza analizy ryzyka przetwarzania Danych,
b. przeprowadza oceny skutków dla ochrony Danych tam, gdzie ryzyko naruszenia praw i wolności Osób jest wysokie,
c. dostosowuje środki ochrony Danych do ustalonego ryzyka,

6.1.3.10 stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony Danych Organowi Nadzorczemu - zarządza incydentami,

6.1.3.11 stosuje procedury pozwalające na ustalenie konieczności zawiadomienia Osób dotkniętych zidentyfikowanym naruszeniem ochrony Danych.

6.1.3.12 Przetwarzający. Spółka stosuje wymogi co do warunków powierzenia przetwarzania Danych.

6.1.3.13 Privacy by design. Spółka zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Spółce uwzględniają konieczność oceny wpływu zmiany na ochronę Danych, zapewnienie legalność (a w tym: zgodności celów przetwarzania, bezpieczeństwa Danych i minimalizacji) już w fazie projektowania zmiany, inwestycji, czy na początku nowego projektu.

6.1.3.14 Eksport danych. Spółka weryfikuje, czy nie dokonuje się Eksportu Danych oraz zapewnia zgodne z prawem warunki takiego przekazywania, jeśli ma ono miejsce.

6.1.3.15 Odpowiedzialność. Za przestrzeganie zasad ochrony danych osobowych w komórkach organizacyjnych Spółki odpowiadają odpowiedni kierownicy tych komórek organizacyjnych.

## 6.2 Dane Szczególnych Kategorii i Dane Karne

6.2.1 Spółka przetwarza Dane Szczególnych Kategorii tylko:

6.2.1.1 gdy Osoba, wyraziła wyraźną zgodę na przetwarzanie tych Danych,

6.2.1.2 gdy przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń,

6.2.1.3 przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub Osobę w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, na podstawie przepisu prawa lub porozumienia zbiorowego,

6.2.1.4 gdy przetwarzanie jest niezbędne do ochrony żywotnych interesów Osoby lub innej osoby fizycznej, a Osoba jest fizycznie lub prawnie niezdolna do wyrażenia zgody (np. nieprzytomna),

6.2.1.5 gdy przetwarzanie dotyczy Danych w sposób oczywisty upublicznionych przez Osobę,

6.2.1.6 gdy przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w RODO,

6.2.1.7 w innych przypadkach wymienionych w art. 9 ust. 2 RODO.

6.2.2 Przetwarzanie Danych Karnych jest dopuszczalne jedynie na podstawie konkretnego przepisu prawa lub zezwolenia lub innej decyzji uprawnionego organu.

### 6.3 Zasady przetwarzania Danych Szczególnych Kategorii w Spółce

6.3.1 Spółka oceni przypadki, w których dotychczas zwykle przetwarzała Dane Szczególnych Kategorii (np. przy usprawiedliwianiu nieobecności w pracy, przy udzielaniu świadczeń z Zakładowego Funduszu Świadczeń Socjalnych).

6.3.2 Jeżeli Spółka ustali, że zwykle w ramach swojej działalności Spółka przetwarza Dane Szczególnych Kategorii lub Dane Karne:

6.3.2.1 Spółka zweryfikuje, czy zachodzi jedna z przesłanek dopuszczalności przetwarzania Danych Szczególnych Kategorii lub Danych Karnych.

6.3.2.2 W razie braku podstawy przetwarzania Spółka zaprzestaje przetwarzania pozbawionego podstawy i postanawia o usunięciu Danych, ewentualnie uzupełnia brakującą podstawę prawną (np. uzyskuje stosowne zgody), a w razie wątpliwości zasięga opinii, co do zgodności z prawem dotychczasowego sposobu przetwarzania Danych Szczególnych Kategorii lub Danych Karnych jak i rekomendacji w związku z RODO.

6.3.2.3 Spółka określa rekomendacje lub instrukcje dla Pracowników w celu uniknięcia niezgodnego z prawem przetwarzania Danych Szczególnych Kategorii (np. wskazuje, że przy ocenie zasadności udzielenia urlopu w związku ze złym stanem zdrowia członka rodziny nie należy żądać ani udzielać informacji, kogo dotyka zły stan zdrowia ani przede wszystkim, na czym konkretnie polega, o ile nie zostanie to dopuszczone przepisami prawa pracy. W przypadku gdy tego typu informacje zostały jednak udzielone, Spółka dba aby nie były one dalej przekazywane przez osobę, która je uzyskała).

6.3.2.4 Spółka przeprowadza ocenę skutków dla ochrony Danych (DPIA), o której mowa w art. 35 RODO oraz wyznaczy Inspektora Ochrony Danych, o którym mowa w art. 37 RODO, jeżeli przetwarza Dane Szczególnych Kategorii na dużą skalę.

6.3.3 Niedozwolone jest automatyczne podejmowanie decyzji, w tym profilowanie w oparciu o Dane Szczególnych Kategorii, chyba że Spółka przetwarza Dane Szczególnych Kategorii w oparciu o zgodę lub o ważny interes publiczny, oraz zapewniła właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów Osoby.

6.3.4 Ryzyko przetwarzania Danych Szczególnych Kategorii i Danych Karnych powinno zostać uwzględnione przy ocenie zastosowania odpowiednich technicznych i organizacyjnych środków ochrony Danych.

6.3.5 Techniczne środki ochrony Danych powinny zostać dostosowane do ryzyka przetwarzania Danych Szczególnych Kategorii i Danych Karnych, o którym mowa powyżej.

6.3.6 Organizacyjne środki ochrony Danych powinny zostać dostosowane do ryzyka przetwarzania Danych Szczególnych Kategorii i Danych Karnych, o którym mowa powyżej. W szczególności:

6.3.6.1 Osoby przetwarzające Dane Szczególnych Kategorii lub Dane Karne lub które z dużym prawdopodobieństwem mogą przypadkowo przetwarzać takie Dane, powinny zostać (i) zaznajomione z wymaganiami dotyczącymi przetwarzania Danych Szczególnych Kategorii i Danych Karnych, w tym z niniejszą Procedurą; (ii) zobowiązane na piśmie do przestrzegania tych wymagań.

6.3.6.2 Co najmniej raz do roku przeprowadzane są przeglądy dokumentacji przetwarzania Danych Szczególnych Kategorii i Danych Karnych oraz mechanizmy ich zabezpieczania.

6.3.7 Do Przetwarzających zasady powyższe stosuje się odpowiednio. W szczególności umowa powierzenia przetwarzania Danych precyzuje, czy przedmiotem powierzenia są Dane Szczególnych Kategorii oraz w miarę możliwości, czy w ramach powierzenia może dojść do przetwarzania Danych Szczególnych Kategorii, oraz sposób postępowania i obowiązki Przetwarzającego w tych sytuacjach.

### 6.4 Dane Niezidentyfikowane

6.4.1 Spółka weryfikuje przypadki, w których dochodzi do przetwarzania lub może dochodzić do przetwarzania Danych Niezidentyfikowanych, a w szczególności: monitoringu wizyjnego, poczty e-mail oraz innych obszarów wymiany i przechowywania plików, gdzie struktura przechowywania nie jest narzucona tzn. nie są one skatalogowane wg. Danych (np. nazwisk klientów, wieku Osób, czy innych cech) i utrzymuje mechanizmy ułatwiające realizację praw Osób. Skatalogowanie należy rozumieć nie tylko jako strukturę hierarchiczną samych katalogów Danych, ale także listy wyszukiwania pozwalające na przeszukiwanie katalogów według Danych.

6.4.2 Spółka nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania Osoby, jeżeli do przetwarzania Danych nie jest wymagana wiedza o tożsamości Osoby.

6.4.3 Spółka w przypadku przetwarzania Danych Niezidentyfikowanych, ma obowiązek poinformowania Osoby o niemożliwości ustalenia tożsamości Osoby (w miarę możliwości) oraz poinformowania o przetwarzaniu Danych (np. tabliczki informacyjne w miejscach objętych monitoringiem wizyjnym).

### 6.5 Profilowanie

6.5.1 Spółka nie dokonuje profilowania przetwarzanych Danych.

### 6.6 Współadministrowanie

6.6.1 Spółka weryfikuje przypadki, w których dochodzi do współadministrowania Danymi. W przypadku zidentyfikowania sytuacji współadministrowania Danymi Spółka wraz z współadministratorami dokonuje wspólnych uzgodnień, które w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez Osobę przysługujących jej praw. W szczególności Spółka zawrze stosowną umowę o współadministrowanie oraz opracuje klauzule informacyjną w przypadku współadministrowania Danymi.

### 6.7 Rejestr Czynności Przetwarzania Danych (RCPD)

6.7.1 RCPD stanowi formę dokumentowania czynności przetwarzania Danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony Danych, czyli zasady rozliczalności.

6.7.2 Spółka prowadzi Rejestr, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje Dane. Rejestr cechuje się czytelnością, użytecznością i zarządzalnością zarówno dla organizacji jak i dla Organu Nadzorczego.

6.7.3 W Rejestrze, dla każdej czynności przetwarzania Danych, Spółka odnotowuje co najmniej:

a. nazwę czynności,
b. cel przetwarzania,
c. opis kategorii Osób,
d. opis kategorii Danych,
e. podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Spółki, jeśli podstawą jest uzasadniony interes,
f. sposób zbierania Danych,
g. opis kategorii odbiorców Danych (w tym Przetwarzających),
h. informację o przekazaniu poza EOG (wzór Rejestru stanowi załącznik nr 1 do niniejszej Procedury).

6.7.4 Rejestr prowadzony jest w formie elektronicznej.

### 6.8 Podstawy przetwarzania

6.8.1 Spółka dokumentuje w Rejestrze podstawy prawne przetwarzania Danych dla poszczególnych czynności przetwarzania.

6.8.2 Spółka zarządza zgodami w sposób umożliwiający rejestrację i weryfikację posiadania zgody Osoby na przetwarzanie jej konkretnych Danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, inne) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie etc.).

### 6.9 Sposób obsługi Praw Jednostki i obowiązków informacyjnych

6.9.1 Spółka dba o czytelność i styl przekazywanych informacji i komunikacji z Osobami.

6.9.2 Spółka ułatwia Osobom korzystanie z ich praw poprzez różne działania np. zamieszczenie na stronie internetowej Spółki informacji lub odwołań (linków) do informacji o prawach Osób, sposobie skorzystania z nich w Spółce, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu ze Spółką w tym celu, ewentualnym cenniku żądań „dodatkowych", etc.

6.9.3 Spółka dba o dotrzymywanie prawnych terminów realizacji obowiązków względem Osób.

6.9.4 Spółka dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań Osób.

### 6.10 Obowiązki informacyjne oraz inne obowiązki Spółki

6.10.1 Spółka określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

6.10.2 Spółka informuje:

6.10.2.1 Osobę o przetwarzaniu jej Danych, przy pozyskiwaniu tych Danych,

6.10.2.2 Osobę o przetwarzaniu jej Danych, przy pozyskiwaniu jej Danych niebezpośrednio od danej Osoby,

6.10.2.3 Osobę o przetwarzaniu Danych Niezidentyfikowanych tam, gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym),

6.10.2.4 Osobę o planowanej zmianie celu przetwarzania Danych,

6.10.2.5 Osobę przed uchyleniem ograniczenia przetwarzania,

6.10.2.6 Odbiorców Danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania Danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe),

6.10.2.7 Osobę o prawie sprzeciwu względem przetwarzania Danych najpóźniej przy pierwszym kontakcie z tą Osobą,

6.10.3 Spółka bez zbędnej zwłoki zawiadamia Osobę o naruszeniu ochrony Danych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej Osoby.

6.10.4 Nieprzetwarzanie. Spółka informuje Osobę, w ciągu miesiąca od otrzymania żądania, o tym, że nie przetwarza Danych jej dotyczących, jeśli taka Osoba zgłosiła żądanie dotyczące jej praw.

6.10.5 Odmowa. Spółka informuje Osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania (np. wobec nieudanej weryfikacji tożsamości) i o prawach Osoby z tym związanych.

6.10.6 Dostęp do Danych. Na żądanie Osoby dotyczące dostępu do jej Danych, Spółka informuje Osobę, czy przetwarza jej Dane oraz informuje Osobę o szczegółach przetwarzania zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela Osobie dostępu do Danych jej dotyczących. Dostęp do Danych może być zrealizowany przez wydanie kopii Danych, z zastrzeżeniem, że kopii Danych wydanej w wykonaniu prawa dostępu do Danych Spółka nie uzna za pierwszą nieodpłatną kopię Danych dla potrzeb opłat za kopie Danych.

6.10.7 Kopie Danych. Na żądanie Spółka wydaje Osobie kopię Danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii Danych.

6.10.8 Sprostowanie Danych. Spółka dokonuje sprostowania nieprawidłowych Danych na żądanie Osoby. Spółka ma prawo odmówić sprostowania Danych, chyba że Osoba w rozsądny sposób wykaże nieprawidłowości Danych, których sprostowania się domaga. W przypadku sprostowania Danych Spółka informuje Osobę o odbiorcach danych, na żądanie tej Osoby.

6.10.9 Uzupełnienie Danych. Spółka uzupełnia i aktualizuje Dane na żądanie Osoby. Spółka ma prawo odmówić uzupełnienia Danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania Danych (np. Spółka nie musi przetwarzać Danych, które są Spółce zbędne). Spółka może polegać na oświadczeniu Osoby co do uzupełnianych Danych, chyba że będzie to niewystarczające w świetle przyjętych przez Spółkę procedur (np. co do pozyskiwania takich Danych), przepisów prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

6.10.10 Usunięcie Danych – prawo do bycia zapomnianym. Na żądanie osoby, Spółka usuwa Dane, gdy:

6.10.10.1 Dane nie są niezbędne do celów, w których zostały zebrane ani nie są przetwarzane w innych celach zgodnie z prawem,

6.10.10.2 zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

6.10.10.3 Osoba wniosła skuteczny sprzeciw względem przetwarzania tych Danych,

6.10.10.4 Dane były przetwarzane niezgodnie z prawem,

6.10.10.5 konieczność usunięcia wynika z obowiązku prawnego.

Osoba powinna zostać niezwłocznie poinformowana o uwzględnieniu jej żądania.

6.10.11 Odmowa usunięcia Danych. Danych nie usuwa się w zakresie w jakim jest to niezbędne:

6.10.11.1 do korzystania z prawa do wolności wypowiedzi i informacji,

6.10.11.2 do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa polskiego, któremu podlega Administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi,

6.10.11.3 z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego,

6.10.11.4 do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych o ile prawdopodobne jest, że usunięcie Danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania,

6.10.11.5 do ustalenia, dochodzenia lub obrony roszczeń.

Osoba powinna zostać niezwłocznie poinformowana o nieuwzględnieniu jej żądania, w miarę możliwości – z krótkim uzasadnieniem

### 6.11 Ograniczenie przetwarzania

6.11.1 Spółka dokonuje ograniczenia przetwarzania Danych na żądanie Osoby, gdy:

6.11.1.1 Osoba kwestionuje prawidłowość Danych – na okres pozwalający sprawdzić ich prawidłowość,

6.11.1.2 przetwarzanie jest niezgodne z prawem, a Osoba sprzeciwia się usunięciu Danych, żądając w zamian ograniczenia ich wykorzystywania,

6.11.1.3 Spółka nie potrzebuje już Danych, ale są one potrzebne Osobie do ustalenia, dochodzenia lub obrony roszczeń,

6.11.1.4 Osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Spółki zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

6.11.2 W trakcie ograniczenia przetwarzania Spółka przechowuje Dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody Osoby chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Ograniczenie przetwarzania nie oznacza całkowitego zakazu wykorzystywania Danych wnioskodawcy – nie należy jedynie korzystać z Danych w taki sposób, jaki Osoba objęła żądaniem ograniczenia.

### 6.12 Realizacja pozostałych praw Osoby

6.12.1 Przenoszenie Danych. Na żądanie Osoby Spółka wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, Dane dotyczące tej Osoby, które dostarczyła ona Spółce, przetwarzane na podstawie zgody tej Osoby lub w celu

zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Spółki. Osoba może żądać, aby jej Dane zostały przesłane przez Spółkę bezpośrednio innemu administratorowi, w takiej formie, że Dane nadają się do wprowadzenia do systemu nowego administratora, czy też do własnego systemu informatycznego Osoby.

6.12.2 Sprzeciw. Sprzeciw wobec przetwarzania jest możliwy, gdy:

a. przetwarzanie odbywa się na podstawie interesu publicznego administratora lub prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią,
b. sprzeciw opiera się na szczególnej sytuacji osoby,
c. nie istnieją ważne, prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą,
d. nie istnieją podstawy do ustalenia, dochodzenia lub obrony roszczeń,
e. Dane przetwarzane są na potrzeby marketingu bezpośredniego. W sytuacji gdy okaże się, że Dane przetwarzane są w oparciu o inną podstawę prawną niż na podstawie przesłanki interesu publicznego administratora lub prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, sprzeciw nie opiera się na szczególnej sytuacji osoby oraz istnieją ważne, prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą lub istnieją podstawy do ustalenia, dochodzenia lub obrony roszczeń, a dane nie są przetwarzane wyłącznie na potrzeby marketingu bezpośredniego, wniosek o sprzeciw uznawany jest za bezzasadny.

6.12.3 Sprzeciw w szczególnej sytuacji. Jeżeli Osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej Danych, a Dane przetwarzane są przez Spółkę w oparciu o uzasadniony interes Spółki lub o powierzone Spółce zadanie w interesie publicznym, Spółka uwzględni sprzeciw, o ile nie zachodzą po stronie Spółki ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności Osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

6.12.4 Sprzeciw względem marketingu bezpośredniego. Jeżeli Osoba zgłosi sprzeciw względem przetwarzania jej Danych przez Spółkę na potrzeby marketingu bezpośredniego, Spółka uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

### 6.13 Minimalizacja

6.13.1 Spółka w ramach procesu utworzenia Rejestru zweryfikowała zakres pozyskiwanych Danych, zakres ich przetwarzania i ilość przetwarzanych Danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

6.13.2 Spółka dokonuje okresowego przeglądu ilości przetwarzanych Danych i zakresu ich przetwarzania.

6.13.3 Spółka przetwarza Dane jedynie niezbędne do osiągnięcia celu przetwarzania.

6.13.4 Spółka stosuje kontrolę dostępu fizycznego do pomieszczeń i urządzeń, w których przetwarzane są Dane i sporządza Wykaz miejsc przetwarzania danych osobowych (wzór Wykazu stanowi załącznik nr 2 do niniejszej Procedury).

6.13.5 Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów Spółki jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Spółkę. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia Danych a w tym wymogi usuwania Danych.

6.13.6 Osoby przetwarzające Dane oraz mające dostęp do tych danych powinny zostać na piśmie upoważnione do przetwarzania Danych. Upoważnienie do przetwarzania danych zawiera ponadto zobowiązanie do zachowania poufności zarówno w trakcie, jak i po ustaniu stosunku pracy.

### 6.14 Bezpieczeństwo

6.14.1 Spółka zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności Osób wskutek przetwarzania Danych.

6.14.2 Spółka zapewnia bezpieczeństwo Danych zgodnie z przyjętymi regulacjami w tym zakresie, obejmującymi metodykę w zakresie analizy ryzyka ochrony danych.

6.14.3 Spółka przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania Danych lub ich kategorii. Spółka analizuje możliwe sytuacje i scenariusze naruszenia ochrony Danych.

6.14.4 Spółka ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania.

6.14.5 Spółka stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony Danych.

6.14.6 Dane w wersji papierowej przetwarza się w sposób uniemożliwiający wgląd do nich osób nieupoważnionych oraz przechowuje się w szafach lub szufladach zamykanych na klucz. Dokumenty archiwalne przechowywane są w archiwum. Zasady dostępu do archiwum reguluje „Instrukcja składnicy akt".

6.14.7 Spółka, szczególnie planując nowe rozwiązania informatyczne, weryfikuje możliwość wykorzystania pseudonimizacji lub anonimizacji do ograniczenia dostępu do Danych i zwiększenia ich bezpieczeństwa. W szczególności, gdy znajomość tożsamości konkretnych Osób nie jest konieczna (np. przy budowie założeń nowej kampanii marketingowej), Spółka w miarę możliwości ogranicza dostęp do Danych poprzez ich pseudonimizowanie lub zanonimizowanie.

6.14.8 Spółka tworzy kopie zapasowe Danych z uwzględnieniem następujących podstawowych zasad:

6.14.9 zasadniczo powinny być tworzone kopie zapasowe Danych,

6.14.10 zdolność przywrócenia Danych z kopii zapasowych powinna być testowana,

6.14.11 kopie archiwalne również uważa się za kopie zapasowe,

6.14.12 okres przydatności (przechowywania) kopii zapasowych powinien być ograniczony – w szczególności nie wolno przechowywać kopii zapasowych Danych, co do których nie istnieje już podstawa prawna przetwarzania,

6.14.13 kopie zapasowe po upływie okresu przydatności powinny być niszczone,

6.14.14 dostęp do kopii zapasowych powinien być ograniczony,

6.14.15 kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.

6.14.16 Należy unikać przechowywania Danych na nośnikach zewnętrznych takich jak pendrive'y. W przypadku konieczności przechowywania Danych Szczególnej Kategorii na nośnikach należy stosować wobec tych danych środki ochrony kryptograficznej. Zabrania się przenoszenia Danych Szczególnej Kategorii na prywatne komputery, prywatne telefony, pendrive'y lub inne urządzenia mogące służyć do ich przechowywania.

6.14.17 Zabrania się automatycznego przekierowania służbowej skrzynki pocztowej na prywatną skrzynkę pocztową. W wyjątkowych przypadkach Prezes Zarządu może udzielić pisemnej zgody Pracownikowi na automatyczne przekierowanie poczty.

6.14.18 Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające Dane, które są przekazywane do naprawy lub utylizacji, pozbawia się przed przekazaniem wszelkich Danych lub – w sytuacji utylizacji – uszkadza się w sposób uniemożliwiający ich odczytanie.

6.14.19 Dostęp do modułów systemów informatycznych, w których przetwarzane są Dane jest przyznawany wyłącznie Pracownikom, którzy są upoważnieni do przetwarzania Danych w zakresie tego upoważnienia. W systemach informatycznych stosuje się mechanizmy kontroli dostępu (indywidualny identyfikator i hasło). Hasło powinno być zmieniane co najmniej raz na pół roku.

6.14.20 Niedozwolone jest podejmowanie działań mogących być zagrożeniem dla systemów informatycznych, a w szczególności próby łamania haseł, dokonywanie włamań na konta innych użytkowników, zakłócanie działania usług, omijanie i badanie zabezpieczeń, doprowadzanie do rozprowadzania wirusów, robaków, koni trojańskich oraz niechcianej poczty (spam), praca na koncie innego użytkownika, udostępnianie identyfikatora i hasła innym osobom.

6.14.21 Pracownik upoważniony do przetwarzania Danych, wychodząc z pomieszczenia, w którym Dane są przetwarzane jest zobowiązany do zamykania drzwi na klucz oraz zablokowania komputera. Blokada komputera powinna być ustawiona w trybie automatycznym. Odblokowanie powinno nastąpić po podaniu hasła użytkownika (polityka czystego ekranu). Po zakończeniu pracy Pracownik jest zobowiązany do wyłączenia komputera.

6.14.22 Przebywanie osób trzecich w pomieszczeniu możliwe jest wyłącznie w obecności Pracownika upoważnionego do przetwarzania Danych.

6.14.23 W pomieszczeniach, w których przetwarzane są dane osobowe, monitory ekranowe komputerów powinny być tak usytuowane, by osoby trzecie nie miały możliwości wglądu do wyświetlanych informacji.

6.14.24 Sporządzane wydruki i kserokopie należy natychmiast odbierać z urządzeń. W miejscach ogólnodostępnych w trakcie drukowania i kopiowania nie należy urządzeń zostawiać bez nadzoru osób upoważnionych.

6.14.25 Niepotrzebne dokumenty oraz wydruki zawierające Dane niszczy się w taki sposób, aby uniemożliwić ich odczytanie (w niszczarkach).

6.14.26 Służbowy komputer przenośny należy transportować w sposób minimalizujący ryzyko kradzieży lub zniszczenia. W trakcie podróży nie należy pozostawiać komputera bez nadzory. Komputera nie mogą używać osoby nieupoważnione. Służbowy komputer przenośny musi być szyfrowany.

6.14.27 Utratę lub uszkodzenia służbowego komputera przenośnego lub służbowego telefonu komórkowego należy niezwłocznie zgłosić bezpośredniemu przełożonemu.

6.14.28 Pracownik upoważniony do przetwarzania Danych opuszczając swoje stanowisko pracy jest zobowiązany do schowania i zabezpieczenia dokumentów w formie papierowej, w szczególności poprzez zamknięcie ich w zabezpieczonych szafach (polityka czystego biurka).

6.14.29 Pracownicy upoważnieni do przetwarzania Danych są zobowiązani do podjęcia wszelkich działań, które zapewnią, aby do Danych nie mieli dostępu Pracownicy nieupoważnieni do przetwarzania Danych oraz inne osoby.

6.14.30 Procedura w zakresie bezpieczeństwa IT została uregulowana w dokumencie Procedura „TOREC" sp. z o.o. w zakresie bezpieczeństwa IT.

### 6.15 Zgłaszanie naruszeń

6.15.1 Spółka stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony Danych Organowi Nadzorczemu w terminie 72 godzin od ustalenia naruszenia.

6.15.2 Naruszenie ochrony Danych ma miejsce w szczególności, gdy:

6.15.2.1 stwierdzono naruszenie zabezpieczenia systemu informatycznego,

6.15.2.2 stan urządzenia, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci teleinformatycznej mogą wskazywać na naruszenie poufności, integralności lub dostępności tych danych,

6.15.2.3 stan pomieszczeń lub szaf, bądź innych miejsc przechowywania danych osobowych, zawartość dokumentacji lub nośników informacji może wskazywać na uzyskanie dostępu do nich przez osoby nieupoważnione,

6.15.2.4 miało miejsce nieuprawnione przekazanie lub ujawnienie danych osobowych.

6.15.3 Na naruszenie ochrony Danych mogą wskazywać w szczególności:

6.15.3.1 widoczne uszkodzenia bądź naruszenia powierzchni szaf lub innych mebli, ścian, drzwi okien lub zamków,

6.15.3.2 uszkodzenia dokumentacji,

6.15.3.3 utrata komputera przenośnego lub telefonu umożliwiającego dostęp do Danych,

6.15.3.4 nieuprawniony dostęp do systemów informatycznych lub pomieszczeń,

6.15.3.5 naruszenie lub próba naruszenia integralności systemu informatycznego,

6.15.3.6 zmiana danych zapisanych na kopiach zapasowych dokonana w sposób nieuprawniony lub ich utrata,

6.15.3.7 zniszczenie lub próba zniszczenia w sposób nieuprawniony Danych,

6.15.3.8 inny stan pomieszczeń lub systemu informatycznego niż pozostawiony po zakończeniu pracy lub przerwie w pracy w systemie informatycznym,

6.15.3.9 informacja uzyskana od pracownika lub z zewnątrz Spółki,

6.15.3.10 zadziałanie systemu sygnalizacji włamania.

6.15.4 W przypadku stwierdzenia lub podejrzenia naruszenia ochrony Danych pracownik ma obowiązek:

6.15.4.1 powiadomić bezpośredniego przełożonego,

6.15.4.2 powstrzymać się od wszelkich działań mogących utrudnić ustalenie okoliczności naruszenia,

6.15.4.3 zabezpieczyć pomieszczenie do czasu przybycia kierownika komórki organizacyjnej,

6.15.4.4 podjąć inne działania stosownie do zaistniałej sytuacji, niezbędne do zapobieżenia dalszym zagrożeniom dla danych.

6.15.5 Kierownik komórki organizacyjnej, w której nastąpiło naruszenie ochrony Danych:

6.15.5.1 zabezpiecza ślady nieprawidłowych działań,

6.15.5.2 niezwłocznie informuję o naruszeniu Prezesa Zarządu Spółki,

6.15.5.3 ocenia zakres oraz rodzaj naruszenia zasad ochrony Danych,

6.15.5.4 określa przyczyny oraz skutki naruszenia, w szczególności przez wysłuchanie i zapisanie relacji osoby, która odkryła naruszenie ochrony Danych, wykonanie notatek, szkicu sytuacyjnego miejsca zdarzenia, ewentualnie fotografii,

6.15.5.5 w przypadku Danych przetwarzanych w systemie informatycznym: sprawdza, z którego stanowiska nastąpiło włamanie i czy użytkownik pracujący przy stanowisku, z którego nastąpiło włamanie, dostatecznie zabezpieczył stanowisko pracy,

6.15.5.6 określa działania i środki, jakie należy podjąć w celu przywrócenia prawidłowego funkcjonowania systemu zabezpieczeń i przybliżony czas jego odtworzenia,

6.15.5.7 określa działania i środki, jakie należy podjąć w celu uniemożliwienia naruszenia ochrony Danych osobowych w przyszłości oraz sporządza szczegółowy raport z przeprowadzonego postępowania.

6.15.6 Prezes Zarządu Spółki podejmuje decyzję o poinformowaniu Organu nadzorczego o naruszeniu ochrony Danych oraz o poinformowaniu właściwych organów ścigania o podejrzeniu popełnienia przestępstwa.

6.15.7 Spółka przywraca normalne działanie systemów informatycznych, w szczególności przez odtworzenie bazy z kopii zapasowej, z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania nieuprawnionego dostępu tą samą drogą.

6.15.8 Jeżeli przyczyną zdarzenia był błąd użytkownika systemu, przeprowadzane jest szkolenie dla osób bezpośrednio związanych z zaistniałą sytuacją. Wnioski wynikające ze zdarzenia są przekazywane wszystkim kierownikom komórek organizacyjnych w celu poinformowania pracowników o konieczności unikania podobnych zagrożeń.

### 6.16 Przetwarzający

6.16.1 Spółka korzysta wyłącznie z Przetwarzających Dane, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji Praw Jednostki i innych obowiązków ochrony Danych spoczywających na Spółce.

6.16.2 Z Przetwarzającymi Spółka zawiera umowy powierzenia przetwarzania.

### 6.17 Eksport Danych

6.17.1 Spółka rejestruje w Rejestrze przypadki Eksportu Danych, czyli przekazywania Danych poza Europejski Obszar Gospodarczy (Unia Europejska, Islandia, Lichtenstein i Norwegia) lub do organizacji międzynarodowej.

### 6.18 Projektowanie prywatności

6.18.1 Spółka zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa Danych, minimalizacji ich przetwarzania, zgodności celów przetwarzania.

6.18.2 W tym celu zasady prowadzenia projektów i inwestycji przez Spółkę odwołują się do zasad bezpieczeństwa Danych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę Danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania Danych od początku projektu lub inwestycji a także weryfikacji zgodności zamierzonego przetwarzania Danych z dotychczasowymi celami przetwarzania Danych.

6.18.3 Spółka umieszcza stosowne zapisy w swoich procedurach inicjowania i prowadzenia projektów i inwestycji.

### 6.19 Szkolenia

6.19.1 W Spółce są prowadzone szkolenia z zakresu przetwarzania Danych w świetle RODO, w szczególności w przypadku Pracowników upoważnionych do przetwarzania Danych.

### 6.20 Sprawdzenie

6.20.1 Zaleca się, aby Spółka przeprowadzała co najmniej raz w roku Sprawdzenie w zakresie ochrony Danych, z której sporządzone zostaje sprawozdanie. Sprawozdanie o stanie ochrony Danych powinno zawierać wszelkie informacje uzyskane podczas kontroli, zawierać krótki opis podjętych czynności, zidentyfikowane braki zgodności oraz zalecenia w zakresie uzupełnienia zidentyfikowanych braków zgodności z prawem w obszarze ochrony Danych.

6.20.2 Plan Sprawdzenia uwzględnia przede wszystkim konieczność weryfikacji zgodności z RODO następujących obszarów:

6.20.2.1 Zgodność przetwarzania z prawem

6.20.2.2 Obsługę Praw Jednostki

6.20.2.3 Wypełnianie obowiązków Spółki jako Administratora Danych

6.20.2.4 Bezpieczeństwo Danych, w tym w szczególności obsługa incydentów

6.20.2.5 Zgodność z Kodeksami postępowania, uzyskanymi certyfikatami oraz wiążącymi regułami korporacyjnymi, jeśli znajduje zastosowanie.

6.20.3 Sprawdzenie może być przeprowadzane w obiektach i urządzeniach Spółki oraz Przetwarzających.

### 6.21 Procedura na wypadek Kontroli Zewnętrznej

6.21.1 Osoba wyznaczona przez Spółkę do nadzorowania czynności kontrolnych powinna niezwłocznie zweryfikować upoważnienie Kontrolującego, w szczególności zakres upoważnienia do Kontroli. W razie potrzeby, osoba ta powinna zawiadomić zewnętrzną kancelarię prawną współpracującą ze Spółką w zakresie ochrony Danych oraz Zarząd Spółki.

6.21.2 Kontrolerzy mają prawo do:

6.21.2.1 Wstępu do wszystkich budynków, lokali oraz innych pomieszczeń Spółki, z zastrzeżeniem przepisów odrębnych.

6.21.2.2 Wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z przedmiotem Kontroli.

6.21.2.3 Przeprowadzania oględzin urządzeń, nośników i systemów informatycznych lub teleinformatycznych służących do przetwarzania Danych.

6.21.2.4 Żądania złożenia pisemnych lub ustnych wyjaśnień oraz wzywania i przesłuchiwania w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego.

6.21.3 Osoba wyznaczona jest stale obecna przy Kontrolerach.

6.21.4 Osoba wyznaczona umożliwia Kontrolerom przeprowadzenie przez nich kontroli, w szczególności wskazuje, gdzie znajdują się potrzebne Kontrolerom informacje oraz udziela żądanych wyjaśnień. W miarę możliwości, Osoba Wyznaczona powinna zapewnić, by Kontrolerzy przebywali na stale w wyznaczonym pomieszczeniu, do którego dostarczane będą im wymagane dokumenty, dostęp do systemów etc.

6.21.5 Osoba wyznaczona odpowiedzialna jest za sporządzenie wykazu przeglądanych przez Kontrolerów dokumentów z uwzględnieniem, czy dokument został przez Kontrolerów jedynie przejrzany, czy został skopiowany. W razie możliwości, w wykazie umieszcza się uwagi Kontrolerów dotyczące tych dokumentów. Osoba wyznaczona sporządza oprócz wykazu notatkę z Kontroli, w której na bieżąco dokumentuje czynności Kontrolerów.

6.21.6 Osoba wyznaczona zapewnia, by do wszystkich Pracowników Spółki została wysłana wiadomość e-mail zawierająca informację o trwającej Kontroli. W wiadomości powinna znaleźć się informacja o tym, że Pracownicy Spółki zobowiązani są współpracować z Kontrolerami, ale nie mają obowiązku dostarczać im informacji z własnej inicjatywy oraz, że zabronione jest niszczenie dokumentów, usuwanie informacji z systemów oraz podejmowanie wszelkich innych czynności, które mogą negatywnie wpłynąć na przebieg kontroli. Oprócz tego, pracownicy powinni zostać poinformowani o konieczności zachowaniu przeprowadzanej Kontroli w tajemnicy.

## 6.22 Postanowienia końcowe

6.22.1 W sprawach nieuregulowanych w niniejszej Procedurze zastosowanie mają odpowiednie przepisy prawa.

6.22.2 Niniejsza Procedura i powiązane z nią dokumenty podlegają przeglądom i aktualizacji, w szczególności w przypadku wystąpienia zmian w przepisach prawa lub w przypadku wprowadzenia zmian w działaniach Spółki.

PREZES ZARZĄDU
Waldemar Kozieł