Polityka bezpieczeństwa przetwarzania danych osobowych

Obowiązuje od	15 maja 2018	
Opracował:	Inspektor Ochrony Danych	ZSK Sp. z o.o. Prokurent Adam Tarnawski
Zatwierdził	Prezes Zarządu	„ZSK" Sp. z o.o. Prezes dr inż. Andrzej Poślednik

KARTA ZMIAN

LP.	WPROWADZONO	ANULOWANO	DATA ZMIANY	WPROWADZAJACY ZMIANĘ
1	WYDANIE 02	WYDANIE 01	03.12.2012	Adam Tarnawski
2	WYDANIE 03	WYDANIE 02	27.06.2013	Adam Tarnawski
3	WYDANIE 04	WYDANIE 03	01.07.2015	Adam Tarnawski
4	WYDANIE 05	WYDANIE 04	01.01.2017	Adam Tarnawski
5	WYDANIE 06	WYDANIE 05	25.05.2018	Adam Tarnawski

ROZDZIELNIK

LP	OTRZYMUJĄCY PROCEDURĘ	NR EGZ.	DATA OTRZYMANIA
1	Wersja elektroniczna	1	25.05.2018
2	Dział administracji	2	25.05.2018

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

ZAKŁAD SYSTEMÓW KOMPUTEROWYCH ZSK spółka z o.o.

ul. Wadowicka 12, 30-415 Kraków

ROZDZIAŁ 1

Postanowienia ogólne

§ 1

Celem Polityki Bezpieczeństwa Przetwarzania Danych Osobowych zwaną dalej „Polityką bezpieczeństwa", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

§ 2

Polityka bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922) oraz Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024). Rozporządzenie Parlamentu Europejskiego poz. 2016/679 w sprawie ogólnego rozporządzenia ochrony danych osobowych (RODO). W przypadku zmiany obowiązujących przepisów prawa powodujących niezgodność niniejszego dokumentu z nimi Polityka bezpieczeństwa zostanie dostosowana do obowiązujących przepisów.

§ 3

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników.

ROZDZIAŁ 2

Definicje

§ 4

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1. **administrator danych osobowych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę decydującą o celach i środkach przetwarzania danych osobowych;
2. **inspektor ochrony danych** – rozumie się przez to osobę wyznaczoną przez administratora danych osobowych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
3. **ustawa** – rozumie się przez to ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2016 r. poz. 922);
4. **rozporządzenie** – rozporządzenie ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024);
5. **rodo** – rozporządzenie Parlamentu Europejskiego i Rady (UE) z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych ... (poz. 2016/679).
6. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
7. **zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
8. **przetwarzanie danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
9. **system informatyczny** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
10. **system tradycyjny** – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
11. **zabezpieczenie danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
12. **administrator systemu informatycznego** – rozumie się przez to osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi;

13. **użytkownik** – rozumie się przez to upoważnionego przez administratora danych osobowych wyznaczonego do przetwarzania danych osobowych pracownika;
14. **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
15. **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

ROZDZIAŁ 3

Zakres i cel stosowania

§ 5

1. Administrator Danych Osobowych to:

Zakład Systemów Komputerowych ZSK sp. z o.o.

Administrującym w imieniu podmiotu jest Zarząd Spółki pod przewodnictwem:

Andrzeja Poślednika - Prezesa Zarządu

2. Administrator danych osobowych powołuje:
Inspektora ochrony danych, do którego zadań należy:
a) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
b) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki bezpieczeństwa,
c) nadzorowanie wydawania i anulowania upoważnień do przetwarzania danych osobowych,
d) nadzorowanie prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych,
e) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
f) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
g) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

§ 6

1. Celem Polityki bezpieczeństwa jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   - **poufność danych** – rozumianą, jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   - **integralność danych** – rozumianą, jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   - **rozliczalność danych** – rozumianą, jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;

- **integralność systemu** – rozumianą, jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
- **dostępność informacji** – rozumianą, jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;

3. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych, a **zarządzanie ryzykiem** rozumiane jest, jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 7

1. Zapisy polityki bezpieczeństwa przetwarzania danych zobowiązane są stosować wszystkie osoby, które w podmiocie mają dostęp do danych osobowych.
2. Polityka bezpieczeństwa dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (system tradycyjny, systemy informatyczne).
3. Polityka bezpieczeństwa ma zastosowanie wobec wszystkich komórek organizacyjnych w tym oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.

§ 8

Politykę bezpieczeństwa stosuje się w szczególności do:

a) danych osobowych przetwarzanych w systemach informatycznych;
b) wszystkich informacji dotyczących danych osobowych zawartych w przetwarzanych zbiorach;
c) wszystkich lokalizacji – budynków i pomieszczeń, w których są przetwarzane dane (wykaz miejsc przetwarzania danych stanowi **zał. nr 1** do niniejszej Polityki bezpieczeństwa);
d) wszystkich informacji danych zawartych w opisie struktury zbiorów;
e) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych;
f) rejestru osób dopuszczonych do przetwarzania danych osobowych;
g) innych dokumentów zawierających dane osobowe.

§ 9

1. Zakresy ochrony danych osobowych określone przez dokumenty Polityki bezpieczeństwa mają zastosowanie do systemów informatycznych, w których są przetwarzane dane osobowe, a w szczególności do:

a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;
b) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;

c) wszystkich pracowników, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez dokumenty Polityki bezpieczeństwa zobowiązani są wszyscy pracownicy, w tym inne osoby mające dostęp do informacji podlegających ochronie.

ROZDZIAŁ 4

Zbiory danych osobowych

§ 10

Dane osobowe gromadzone są w zbiorach danych. Wykaz zbiorów danych wraz ze wskazaniem systemu informatycznego służącego do przetwarzania danych stanowi **zał. nr 2** do niniejszej Polityki bezpieczeństwa.

§ 11

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych określona została w **zał. nr 3** do niniejszej Polityki bezpieczeństwa.

ROZDZIAŁ 5

Nadawanie upoważnień do przetwarzania danych osobowych

§ 13

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych osobowych. Upoważnienie stanowi **zał. nr 4** do niniejszej Polityki bezpieczeństwa.

Administrator danych osobowych nadając uprawnienia pracownikom, którzy przetwarzają dane odbiera od pracownika oświadczenie o zachowaniu danych w poufności oraz o zapoznaniu się z dokumentami określającymi zasady zabezpieczania i przetwarzania danych osobowych w podmiocie.

Administrator danych osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która stanowi **zał. nr 5** do niniejszej Polityki bezpieczeństwa.

ROZDZIAŁ 6
Udostępnienie i powierzanie danych osobowych

§ 14

1. Administrator danych osobowych jest uprawniony do udostępnienia danych osobie wnioskującej z zachowaniem zasady, że udostępnienie danych osobowych nie może naruszać praw i wolności osoby, których dane dotyczą. Wzór wniosku o udostępnienie danych stanowi **zał. nr 6** do niniejszej Polityki bezpieczeństwa. Każdorazowe udostępnienie danych musi być odnotowane w rejestrze udostępnienia, który stanowi **zał. nr 7** do niniejszej Polityki bezpieczeństwa.
2. Dopuszczalne jest powierzenie przez administratora danych przetwarzania danych podmiotom zewnętrznym.
3. Powierzenie przetwarzania danych może mieć miejsce na podstawie pisemnej umowy określającej w szczególności zakres i cel przetwarzania danych. Umowa musi określać też zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy oraz sposób rozwiązania umowy. Wzór umowy powierzenia danych stanowi **zał. nr 8** do niniejszej Polityki bezpieczeństwa.
4. Powierzenie przetwarzania danych osobowych musi uwzględniać ponadto wymogi określone w obowiązujących ustawach i rozporządzeniu UE. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych do podjęcia środków zabezpieczających zbiór danych.
5. Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności administratora danych za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w umowach stanowiących podstawę powierzenia przetwarzania danych umieszczenia prawa administratora danych do kontroli wykonania przedmiotu umowy w siedzibie podmiotu zewnętrznego m. in. w zakresie przestrzegania Polityki bezpieczeństwa, Instrukcji zarządzania systemem informatycznym oraz właściwych przepisów prawa.
6. Wykaz podmiotów, którym powierzono przetwarzanie danych stanowi **zał. nr 9** do niniejszej Polityki bezpieczeństwa.
7. Powierzenie przetwarzania danych uregulowane w Polityce bezpieczeństwa nie ma zastosowania do przekazywania danych podmiotom upoważnionym do ich przetwarzania na mocy przepisów prawa, w tym w szczególności ZUS, Prokuraturze, Policji, Sądom, Komornikom, itd.

ROZDZIAŁ 7

Wynoszenie akt i dokumentacji

§ 15

1. Poza miejsca przetwarzania danych wskazanych w zał. nr 4 nie wolno wynosić żadnej dokumentacji ani akt związanych z wykonywaniem czynności służbowych, a zwłaszcza dokumentów zawierających dane osobowe.
2. Przepis powyższy nie dotyczy tych pracowników, których zakres obowiązków wymaga dokonywania czynności służbowych z dokumentacją zawierającą dane osobowe poza obszarem przetwarzania danych, a także czynności związanych z przesyłaniem i transportem korespondencji.
3. Pracownicy, o których mowa w punkcie powyżej, są zobowiązani stosować środki zapewniające ochronę powierzonych danych osobowych podczas ich transportu, przechowywania i użytkowania poza obszarem siedziby pracodawcy, a w szczególności zabezpieczyć te dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Pracownicy tacy ponoszą pełną odpowiedzialność za powierzony im sprzęt oraz dokumentację znajdującą się poza siedzibą administratora.
5. Każdy pracownik, który podejrzewa, iż mogło nastąpić naruszenie bezpieczeństwa ochrony danych osobowych lub próba dokonania takiego naruszenia przez osoby nieupoważnione, jest zobowiązany do niezwłocznego poinformowania o powyższym Administratora **Danych Osobowych – Prezesa Zarządu Spółki,** który prowadzi postępowanie kontrolne, pod kątem wyjaśnienia okoliczności ewentualnego naruszenia bezpieczeństwa danych osobowych.
6. Odpowiedzialność za bezpieczeństwo dokumentacji lub akt wynoszonych poza obszar przetwarzania danych ponosi pracownik, który te akta wynosi, z chwilą ich pobrania. Odpowiedzialność ta dotyczy również danych znajdujących się na nośnikach cyfrowych.
7. Po zwrocie akt i dokumentacji (lub przenośnych komputerów) przez pracownika, przełożony zobowiązany jest do jej sprawdzenia pod kątem zgodności ze stanem sprzed wypożyczenia.
8. Pozostawanie w pracy po godzinach pracy może mieć miejsce tylko w związku z pełnionymi obowiązkami i za zgodą Prezesa lub osoby przez niego upoważnionej.

ROZDZIAŁ 8
Zasady korzystania z komputerów przenośnych

§ 16

Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.

§ 17

Użytkownik komputera przenośnego zobowiązany jest do:

a) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności: transportowania komputera w bagażu podręcznym, nie pozostawiania komputera w samochodzie, przechowalni bagażu, itp.,

b) przenoszenia komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych,

c) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,

d) nie zezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe,

e) blokowanie dostępu przed użyciem przez osoby postronne,

f) kopiowania danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych,

g) zmiany haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.

ROZDZIAŁ 9
Środki techniczne i organizacyjne zabezpieczenia danych osobowych

§ 18

1. <u>Zabezpieczenia organizacyjne:</u>

a) sporządzono i wdrożono Politykę bezpieczeństwa;

b) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;

c) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych, bądź osobę przez niego upoważnioną;

d) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;

e) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
f) osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy;
g) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
h) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
i) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
j) wprowadzono zasadę „czystego biurka" i „białej kartki";
k) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób;
l) informacji telefonicznych nie udziela się, względnie udziela się po zidentyfikowaniu rozmówcy i stwierdzeniu jego upoważnienia do uzyskania danych.

2. Zabezpieczenia techniczne:
a) sprzęt komputerowy zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą **zapory sieciowej.**
b) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową
c) konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym wyłącznie za pośrednictwem używanych aplikacji;
d) zastosowano wygaszenie ekranu po 600 sekundach nieaktywności użytkownika, wznowienie pracy możliwe jest po wprowadzeniu hasła
e) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła.

3. Środki ochrony fizycznej:
a) urządzenia służące do przetwarzania danych osobowych i dokumentację zawierającą dane osobowe umieszcza się w zamykanych pomieszczeniach;
b) obszar, na którym przetwarzane są dane osobowe, chroniony jest poprzez:
- **MAGAZYN:** kraty w oknach, zamki patentowe, domofon, kontrola dostępu przy użyciu kart zbliżeniowych;
- **SKŁADZIK:** zamki patentowe, kraty w oknach;
- **STREFA ADMINISTRACYJNA:** grupa interwencyjna, system alarmowy, kontrola dostępu przy użyciu kart zbliżeniowych, wideo domofon, dziennik wejść/wyjść, monitoring wizyjny, rolety antywłamaniowe.

ROZDZIAŁ 10

Szkolenia użytkowników

§ 19

Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej zostaje poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
Za zorganizowanie szkolenia odpowiada **Inspektor Ochrony Danych.**
Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u administratora danych osobowych.
Zgodnie z wymogami ustawy pracownicy zostają zapoznani z przepisami z zakresu ochrony danych osobowych w każdym przypadku istotnych zmian w przepisach dotyczących przetwarzania danych.
Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

ROZDZIAŁ 11

Postanowienia końcowe

§ 20

Wszyscy pracownicy zobowiązani są do zapoznania się z niniejszym dokumentem oraz do stosowania zawartych w nim reguł.
Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
W sprawach nieuregulowanych w polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.
Dokumentem powiązanym z niniejszą polityką jest Instrukcja zarządzania systemem informatycznym.

§ 21

Niniejszy dokument wchodzi w życie z dniem 25 maja 2018 r.

Inspektor Danych Osobowych
Adam Tarnawski

Prezes Zarządu
Andrzej Poślednik