# POLITYKA BEZPIECZEŃSTWA

obowiązuje od 25 maja 2018 r.

## SPIS TREŚCI

## Część I
## Postanowienie ogólne

### § 1

Celem Polityki bezpieczeństwa przetwarzania danych osobowych w MKPUBLIKACJE Marek Kaniewski zwanej dalej „Polityką bezpieczeństwa", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych sposobu przetwarzania informacji zawierających dane osobowe.

### § 2

Zgodnie z art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 Nr 133 poz. 883, tekst jedn.: Dz.U. z 2016 r. poz. 922), zwanej dalej „ustawą" oraz z ROZPORZĄDZENIEM PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem oraz z § 3 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 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), zwanego dalej „rozporządzeniem", ustanawia się „Politykę Bezpieczeństwa".

### § 3

Administratorem danych osobowych jest firma MKPUBLIKACJE Marek Kaniewski.

### § 4

Administrator danych osobowych powołuje Inspektora Ochrony Danych, którego zadania określa Część V Polityki Bezpieczeństwa.

## Część II
## Definicje

### § 1

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1) Administrator danych osobowych – rozumie się jako MKPUBLIKACJE Marek Kaniewski.
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 jednolity: 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) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
6) 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;
7) 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;
8) system informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

9) 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;
10) zabezpieczenie danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
11) administrator systemu informatycznego – rozumie się przez to osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi;
12) użytkownik – rozumie się przez to upoważnionego przez administratora danych osobowych lub administratora bezpieczeństwa informacji (o ile został powołany), wyznaczonego do przetwarzania danych osobowych pracownika;
13) identyfikator użytkownika (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
14) hasło – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

## Część III
## Zasady przetwarzania i ochrony danych osobowych

### § 1

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

### § 2

Utrzymanie bezpieczeństwa przetwarzanych danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.

### § 3

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
4) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
5) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
6) zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

### § 4

Każda osoba, mająca dostęp do danych osobowych przetwarzanych w jednostce organizacyjnej jest zobowiązana do zapoznania się z niniejszym dokumentem.

### § 5

Wymagany przez rozporządzenie wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe (zwany dalej „obszarem przetwarzania”) stanowi załącznik nr 1 do niniejszego dokumentu.

### § 6

Wymagany przez rozporządzenie wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, stanowi załącznik nr 2 do niniejszego dokumentu.

**§ 7**

Osoby, które przetwarzają w jednostce organizacyjnej dane osobowe, muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez Administratora Danych Osobowych (załącznik nr 3 do niniejszego dokumentu).

**§ 8**

Każda osoba posiadająca upoważnienie do przetwarzania danych osobowych posiada swój identyfikator oraz hasło, pozwalające na zalogowanie się do systemu informatycznego, w którym przetwarzane są dane osobowe. Techniczne wymagania, jakie musi spełniać hasło, określone zostały w części II § 2 Instrukcji Zarządzania Systemem Informatycznym.

**§ 9**

W przypadku konieczności dostępu do obszaru przetwarzania osób, nieposiadających upoważnienia, o jakim mowa w § 4 (załącznik nr 3 do niniejszego dokumentu), które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują oni oświadczenie o zachowaniu poufności (załącznik nr 4 do niniejszego dokumentu), chyba że czynności odbywają się pod nadzorem osoby upoważnionej do przetwarzania danych.

**§ 10**

Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych.

**§ 11**

Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia, przez co rozumie się w szczególności pisemny wniosek podmiotu uprawnionego.

**§ 12**

Dokumenty zawierające dane osobowe przechowywane w formie papierowej, upoważnione osoby przechowują je w obszarze przetwarzania danych w szafach zamykanych na klucz.

W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenie dokonuje się poprzez pocięcie w niszczarce.

**§ 13**

Zasady przetwarzania danych osobowych w systemie informatycznym określone są w „Instrukcji zarządzania systemem informatycznym” służącym do przetwarzania danych osobowych.

**§ 14**

Osoby upoważnione do przetwarzania danych mają obowiązek:

1) przetwarzać je zgodnie z obowiązującymi przepisami, w szczególności z ustawą i rozporządzeniem,
2) nie udostępniać ich oraz uniemożliwiać dostęp do nich osobom nieupoważnionym,
3) zabezpieczać je przed zniszczeniem.

**§ 15**

W przypadku otrzymania wniosku o udostępnienie danych osobowych od osoby, której one dotyczą, osoba wyznaczona przez osobę nadzorującą przetwarzanie danych przygotowuje odpowiedź w ciągu 30 dni.

**§ 16**

1) W przypadku zbierania danych osobowych od osoby, której one dotyczą, osoba nadzorująca przetwarzanie danych jest zobowiązana poinformować tę osobę w przystępnej dla niej formie (w szczególności może to być informacja ustna, zapis w umowie lub regulaminie) o:
   - adresie swojej siedziby i pełnej nazwie, (lub odpowiednio imieniu, nazwisku i miejscu zamieszkania Administratora Danych Osobowych, jeżeli działa on jako osoba fizyczna),
   - celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
   - prawie dostępu do treści swoich danych oraz ich poprawiania,
   - dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
2) Rejestr czynności przetwarzania danych osobowych prowadzony jest przez administratora danych (załącznik nr 10 do niniejszego dokumentu).

## Część IV
## Środki techniczne i organizacyjne zabezpieczenia danych osobowych

### § 1

Zabezpieczenia organizacyjne:
1) sporządzono i wdrożono Politykę bezpieczeństwa;
2) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
3) wyznaczono Inspektora Ochrony Danych*;*
4) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych bądź osobę przez niego upoważnioną;
5) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;
6) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
7) osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy;
8) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
9) 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;
10) 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.

### § 2

Zabezpieczenia techniczne:
1) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą zapory ogniowej wbudowanej w router,
2) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
3) 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:
1) obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest zamkniętym pomieszczeniem z podwójnym zamkiem patentowym typu „Gerda”,
2) obszar, na którym przetwarzane są dane osobowe objęty jest całodobowym monitoringiem,
3) urządzenia służące do przetwarzania danych osobowych umieszcza się w zamykanych pomieszczeniach,
4) dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych szafach.

**§ 4**

Zabezpieczenia organizacyjne:

1) opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych,
2) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w firmie,
3) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,
4) opracowano i bieżąco prowadzi się rejestr czynności przetwarzania,
5) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych bądź osobę przez niego upoważnioną,
6) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
7) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
8) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
9) 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,
10) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.

**§ 5**

Zabrania się przenoszenia niezabezpieczonych danych poufnych poza teren firmy. W szczególności zabrania się przenoszenia danych poufnych na nośnikach elektronicznych (np.: pendrive, nośniki CD, DVD) poza teren firmy.

## Część V
## Zadania administratora bezpieczeństwa informacji

**§ 1**

Do najważniejszych obowiązków administratora danych osobowych lub administratora bezpieczeństwa informacji należy:

1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa,
3) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
5) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych, prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
6) nadzór nad bezpieczeństwem danych osobowych,
7) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
8) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

**§ 2**

Inspektor Ochrony Danych prowadzi również następujące wykazy:

1) ewidencję osób, którym nadano upoważnienia do przetwarzania danych osobowych (załącznik nr 6 do niniejszego dokumentu),
2) wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania (załącznik nr 1 do niniejszego dokumentu),
3) wykaz podmiotów i osób, którym udostępniono dane (załączniki nr 7 i nr 9 do niniejszego dokumentu),
4) wykaz podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych osobowych w rozumieniu art. 31 ustawy (załącznik nr 8 do niniejszego dokumentu).

## Część VI
## Zadania administratora systemu informatycznego

### § 1

Administrator systemu informatycznego odpowiedzialny jest za:

1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2) optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
3) instalacje i konfiguracje oprogramowania systemowego, sieciowego,
4) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
5) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
6) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
7) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
8) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
10) przyznawanie na wniosek administratora danych osobowych lub administratora bezpieczeństwa informacji ściśle określonych praw dostępu do informacji w danym systemie,
11) wnioskowanie do administratora danych osobowych lub administratora bezpieczeństwa informacji w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
12) zarządzanie licencjami oraz procedurami ich dotyczącymi,
13) prowadzenie profilaktyki antywirusowej.

### § 2

Praca administratora systemu informatycznego jest nadzorowana pod względem przestrzegania ustawy o ochronie danych osobowych, rozporządzenia ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych, Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz Polityki bezpieczeństwa przez administratora danych lub administratora bezpieczeństwa informacji.

## Część VII
## Szkolenia użytkowników

**§ 1**

Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.

**§ 2**

Za przeprowadzenie szkolenia odpowiada administrator danych osobowych.

**§ 3**

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, a także o zobowiązaniu się do ich przestrzegania.

**§ 4**

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.

**§ 5**

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.

## Część VIII
## Zakres stosowania

**§ 1**

1) W jednostce organizacyjnej przetwarzane są dane osobowe: imię i nazwisko, adres zamieszkania, nr telefonu oraz adres email, zebrane w zbiorach danych osobowych,
2) Informacje te są przetwarzane wyłącznie w postaci dokumentacji elektronicznej,
3) Polityka bezpieczeństwa zawiera m.in. uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych,
4) Innymi dokumentami regulującymi ochronę danych osobowych w firmie są:
   - Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w firmie,
   - Ewidencja osób upoważnionych do przetwarzania danych osobowych,
   - Rejestr czynności przetwarzania danych osobowych,
   - Procedura postępowania w przypadku naruszenia ochrony danych osobowych,

**§ 2**

Politykę bezpieczeństwa stosuje się w szczególności do:
1) danych osobowych przetwarzanych w: systemie Windows 10, pakiecie Microsoft Office, programie do fakturowania – Faktura Small Business),
2) wszystkich informacji dotyczących danych klientów,
3) odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia (tj. biuro rachunkowe, placówki pocztowe, kurierzy, firmy hostingowe),
4) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5) innych dokumentów zawierających dane osobowe.

**§ 3**

Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie,
2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
3) wszystkich pracowników, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

Do stosowania zasad określonych przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty zobowiązani są wszyscy pracownicy oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.

## Część IX
## Wykaz zbiorów danych osobowych

**§ 1**

Dane osobowe gromadzone są w zbiorach:

1) Ewidencja osób upoważnionych do przetwarzania danych osobowych,
2) Umowy zawierane z kontrahentami,
3) Rejestr klientów,
4) Dokumenty archiwalne,

## Część X
## Postanowienia końcowe

**§ 1**

Administrator danych osobowych lub administrator bezpieczeństwa informacji ma obowiązek zapoznać z treścią Polityki każdego użytkownika.

**§ 2**

Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

**§ 3**

Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce bezpieczeństwa.

**§ 4**

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.

**§ 5**

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.

**§ 6**

Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z art. 49-54a ustawy o ochronie danych osobowych.

**§ 7**

W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy ustawy o ochronie danych osobowych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 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.

**§ 8**

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