POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

LEX-ECONOMIC
KANCELARIA RADCY PRAWNEGO
ZBIGNIEW PIOTR BĄK

BIAŁYSTOK, 2022 R.

SPIS TREŚCI

I. POSTANOWIENIA OGÓLNE

§1.

Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, w tym z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 20126/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [dalej zwane RODO] sposobu przetwarzania w LEX-ECONOMIC Kancelarii Radcy Prawnego Zbigniew Piotr Bąk grupy informacji zawierającej dane osobowe.

§2.

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

- Kancelaria — LEX-ECONOMIC Kancelaria Radcy Prawnego Zbigniew Piotr Bąk
- Administrator — administrator w rozumieniu art. 4 pkt 7 RODO
- dane osobowe — dane osobowe w rozumieniu art. 4 pkt 1 RODO
- naruszenie ochrony danych osobowych — naruszenie ochrony danych osobowych w rozumieniu aft. 4 pkt 12 RODO
- podmiot przetwarzający — podmiot przetwarzający w rozumieniu art. 4 pkt 8 RODO
- przetwarzanie — przetwarzanie danych osobowych w rozumieniu art. 4 pkt 2 RODO
- RODO - Rozporządzenia Parlamentu Europejskiego i Rady (UE) 20126/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

II. DEFINICJA BEZPIECZEŃSTWA INFORMACJI

§3.

1. Utrzymanie bezpieczeństwa przetwarzanych przez Kancelarię informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.

2. Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji:
   - Poufność informacji — rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
   - Integralność informacji — rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,

- Dostępność informacji — rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
- Zarządzanie ryzykiem — rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.

3. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
   - Niezaprzeczalności odbioru — rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,
   - Niezaprzeczalności nadania — rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie,
   - Rozliczalności działań — rozumianej, jako zapewnienie, że wszystkie działania istotne dla
   - przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

III. ZAKRES I CEL

§4.

1. W systemie informacyjnym Kancelarii przetwarzane są informacje służące do wykonywania zadań niezbędnych dla zrealizowania umów zawartych z Klientami Kancelarii, uprawnień lub spełnienia obowiązku wynikającego z przepisów prawa (w tym ustawy o podatku od Towarów i Usług, Kodeksu Pracy, RODO),

2. Informacje te są przetwarzane i składowane zarówno w postaci papierowej jak i elektronicznej.

§5.

Politykę Bezpieczeństwa stosuje się do:

— danych osobowych przetwarzanych w systemie informatycznym,
— wszystkich informacji dotyczących danych pracowników Kancelarii, w tym danych osobowych personelu i treści zawieranych umów o pracę,
— wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,
— informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
— rejestru osób dopuszczonych do przetwarzania danych osobowych,
— innych dokumentów zawierających dane osobowe.

§6.

Zakres gromadzonych danych osobowych obejmuje:

— W przypadku klientów: Imię nazwisko, adres, numery PESEL, NIP, numery telefonów, adresy mail, inne dane wynikające ze specyfiki danej umowy, jeżeli jest to niezbędne dla realizacji celu danej umowy,
— W przypadku pracowników: imię, nazwisko, treści zawieranych umów o pracę, adres, numery PESEL, NIP, numery telefonów, adresy mail, inne dane jeżeli pracownik poda je po uprzednim wyrażeniu zgody.

§7.

Okres przechowywania danych osobowych Klientów Kancelarii wynosi do 10 lat licząc od dnia zakończenia danego zlecenia — odpowiednio do okresu przedawnienia dochodzenia przed sądem ewentualnych roszczeń klienta wynikających z umowy. Okres ten ulega skróceniu odpowiednio do ogólnego terminu przedawnienia roszczeń wynikających z przepisów Kodeksu cywilnego. Wskazany okres jest maksymalny. Minimalny okres przechowywania dokumentów wynosi 5 lat.

§8.

1. Zakresy określone przez dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Jednostki w szczególności do:
   a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
   b) wszystkich lokalizacji — budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
   c) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, zleceniobiorców, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, zleceniobiorcy, konsultanci, współpracujący z Kancelarią Radcowie Prawni i Adwokaci, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

§9.

Informacje niejawne nie są objęte zakresem niniejszej Polityki.

IV. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA INFORMACJI

§10.

1. Dokumenty Polityki Bezpieczeństwa Informacji ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.

2. Zestaw dokumentów Polityki Bezpieczeństwa Informacji składa się z:
   a) Niniejszego dokumentu Polityki Bezpieczeństwa Informacji,
   b) Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych w Jednostce - załącznik nr l ,
   c) Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, opisującej tryb postępowania w sytuacjach naruszenia zabezpieczenia zasobów danych osobowych, zaobserwowanych prób naruszenia tego zabezpieczenia, a także uzasadnionego podejrzenia o przygotowywanej próbie naruszenia - załącznik nr 2.

V. DOSTĘP DO INFORMACJI

§11.

Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Kancelarii zasad ochrony danych osobowych.

§12.

Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

§13.

Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, mogą być udostępnione jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

§14.

Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§15.

Dane osobowe udostępnia się na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać zakres i przeznaczenie.

VI. ZARZĄDZANIE DANYMI OSOBOWYMI

§16.

Administratorem danych osobowych jest Właściciel LEX-ECONOMIC Kancelaria Radcy Prawnego Zbigniew Piotr Bąk.

§17.

1. Za bezpieczeństwo danych osobowych Kancelarii, odpowiada Administrator danych osobowych – Właściciel.
2. Administrator danych osobowych Jednostki realizując politykę bezpieczeństwa informacji ma prawo wydawać instrukcje regulujące kwestie związane z ochroną danych w strukturach Kancelarii.
3. W umowach zawieranych przez Kancelarii winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych udostępnionych przez Kancelarię, zgodnie z przepisami RODO.

§18.

Zapoznanie się z dokumentami określonymi w §8 pkt 2 pracownicy Kancelarii potwierdzają O podpisem na „Indywidualnym zakresie czynności osoby zatrudnionej przy przetwarzaniu danych osobowych” (wzór w załączniku nr 3) i przekazują Administratorowi danych osobowych.

§19.

Ochrona zasobów danych osobowych Kancelarii jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników Kancelarii.

VII. ZAKRESY ODPOWIEDZIALNOŚCI

§20.

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Kancelarii.

§21.

Administrator danych osobowych w Kancelarii:

1. odpowiada za realizację RODO,
2. sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób,
3. określa strategię zabezpieczania systemów informatycznych Kancelarii.

4. sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
5. sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe,
6. identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Kancelarii,
7. określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
8. sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, palmtopach, w których przetwarzane są dane osobowe,
9. sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe,
10. monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
11. 11 . sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych,
12. zatwierdza wnioski o przyznaniu danemu użytkownikowi identyfikatora oraz praw dostępu do informacji chronionych w danym systemie przetwarzania,
13. powiadamia administratora systemu o konieczności utworzenia identyfikatora użytkownika w systemie oraz zmianie/nadaniu uprawnień dostępu użytkownika do systemu,
14. prowadzi ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe,
15. prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych,
16. prowadzi ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych,
17. prowadzi rejestr zbiorów danych osobowych Kancelarii (przetwarzanych metodą tradycyjną lub w systemach informatycznych).

§22.

Administrator danych osobowych zobowiązany jest do przestrzegania wszystkich przepisów ustawy o ochronie danych, w szczególności poprzez:

1. określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z RODO,
2. określenie budynków, pomieszczeń lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,
3. zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
4. wdrażanie i nadzorowanie przestrzegania Polityki bezpieczeństwa informacji,

5. wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
6. działanie zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych,
7. stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania RODO,
8. odpowiedzialność za poprawność merytoryczną danych gromadzonych w systemach informacyjnych,
9. określanie, które osoby i na jakich prawach mają dostęp do danych informacji.

§23.

Administrator danych osobowych w ramach systemu informatycznego odpowiedzialny jest za:

1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2. optymalizację wydajności systemu informatycznego, baz danych,
3. instalacje i konfiguracje sprzętu sieciowego i serwerowego,
4. instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,
5. konfigurację i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
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 w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
10. przyznawanie ściśle określonych praw dostępu do informacji w danym systemie,
11. wszczynanie procedur bezpieczeństwa i standardów zabezpieczeń,
12. zarządzanie licencjami, procedurami ich dotyczącymi,
13. prowadzenie profilaktyki antywirusowej.

VIII. PRZETWARZANIE DANYCH OSOBOWYCH

§24.

1. Przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach zamykanych na klucz przez wyznaczone do tego celu osoby.

2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§25.

1. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć w stopniu uniemożliwiającym ich odczytanie.

2. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

XIX. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI PRZETWARZANYCH DANYCH

§26.

W Kancelarii rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:
   a) Pomieszczenia zamykane na klucz,
   b) szuflady zamykane na klucz,
   c) sejf pancerny z zamkiem szyfrowym,
   d) pomieszczenia zabezpieczone alarm antywłamaniowym z indywidualnymi kodami dostępu poszczególnych użytkowników do pomieszczeń, z rejestracją czasu dostępu poszczególnych dysponentów kodu,
   e) budynek, w którym znajdują się pomieszczenia zabezpieczony kodem indywidualnym dla danego lokalu,
3. Zabezpieczenia procesów przewarzania danych w dokumentacji papierowej:
   a) przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
   b) przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby,
   c) obieg korespondencji wchodzącej i wychodzącej zawierającej dane osobowe parafowany jest przez osobę wprowadzającą,
4. Zabezpieczenia organizacyjne:
   a) osobą odpowiedzialną za bezpieczeństwo danych jest Administrator danych osobowych,
   b) Administrator danych osobowych i wszyscy powołani przez niego administratorzy na bieżąco kontrolują pracę systemów informatycznych z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i obowiązującymi procedurami,
5. Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:
   a) Wykaz pracowników Kancelarii uprawnionych do przetwarzania danych osobowych, znajduje się u Administratora danych osobowych - zał. nr 6,

b) przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie przyznane przez Administratora danych osobowych- zał. Nr 5,
c) w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
d) przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszonego,
e) w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,
f) po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

XX. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§27.

Archiwizacja informacji zawierających dane osobowe odbywa się w formie elektronicznej oraz papierowej. Nośniki danych przechowywane są w wydzielonych pomieszczeniach, które są zabezpieczone przed dostępem osób nieupoważnionych (wykaz pomieszczeń załącznik nr 4).

Załącznik nr 2 do Polityki Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

LEX-EONOMIC KANCELARIA RADCY PRAWNEGO ZBIGNIEW PIOTR BĄK

§1.

Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych.

§2.

Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:

- -stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
- -stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

§3.

Każdy pracownik Kancelarii, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób) zobowiązany jest do niezwłocznego poinformowania o tym administratora tego systemu informatycznego lub w przypadku jego nieobecności administratora bezpieczeństwa informacji Kancelarii.

§4.

1. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.

2. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

§5.

1. Administrator bazy danych osobowych, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony tej bazy danych zobowiązany jest do niezwłocznego:
   a) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,
   b) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,
   c) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.
   d) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.
   e) fizycznego odłączenia urządzeń i segmentów sieci które mogły umożliwić dostęp do bazy danych osobie niepowołanej,
   f) wylogowania użytkownika podejrzanego o naruszenie ochrony danych, a jeżeli nie ma takiego uprawnienia, to zawiadomienia Administratora danych osobowych o konieczności dokonania wylogowania,
   g) zmianę hasła lub zablokowanie dostępu do konta administratora i użytkownika poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu, a jeżeli nie ma takiego uprawnienia, to zawiadomienia Administratora danych osobowych o konieczności dokonania wylogowania,
   h) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
   i) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

2. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

3. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.

4. Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.

5. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz RODO.

§6.

1. Administrator danych osobowych, w przypadku naruszenia ochrony danych osobowych przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia.

2. Administrator danych osobowych w Kancelarii przeprowadza analizę raportów i uwzględnia je w opracowywaniu corocznego raportu.