

Polityka bezpieczeństwa danych osobowych

Realizując postanowienia: Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (Dz.U. UE L.2016.119.1 z dnia 4 maja 2016 r. oraz Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych wprowadza się do stosowania niniejszą Politykę bezpieczeństwa.

Jako minimum w powyższej normie ustala się, że dokument określający politykę bezpieczeństwa zawiera:

A.

1. Krótkie wyjaśnienie polityki bezpieczeństwa, zasad, norm i wymagań zgodności mających szczególne znaczenie dla organizacji, zawierające:
 - a) zgodność z prawem, regulacjami wewnętrznymi i wymaganiami wynikającymi z umów;
 - b) wymagania dotyczące kształcenia, szkoleń i uświadamiania w dziedzinie bezpieczeństwa;
 - c) zarządzanie ciągłością działania biznesowego;
 - d) konsekwencje naruszenia polityki bezpieczeństwa;
2. Definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania incydentów związanych z bezpieczeństwem informacji;
3. Odsyłacze do dokumentacji mogącej uzupełniać politykę, np. bardziej szczegółowych polityk bezpieczeństwa i procedur dotyczących poszczególnych systemów informatycznych lub zalecanych do przestrzegania przez użytkowników zasad bezpieczeństwa.

B.

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
2. Wykaz procesów przetwarzania danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3. Sposób przepływu danych pomiędzy poszczególnymi systemami;
4. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych.

I. Wstęp

Administrator danych, świadomy wagi zagrożeń prywatności, w tym zwłaszcza zagrożeń danych osobowych przetwarzanych w związku z wykonywaniem zadań administratora danych, deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania zagrożeniom, m. in. takim jak:

1. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu;
2. niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych;
3. awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie serwisantów, w tym pozostawienie serwisantów bez nadzoru, a także przyzwoleń na naprawę sprzętu zawierającego dane poza siedzibą administratora danych;
4. podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania, próby stosowania nie swojego hasła i identyfikatora przez osoby upoważnione;
5. celowe lub przypadkowe rozproszenie danych w Internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego administratora danych;
6. ataki z Internetu;
7. naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem procedur ochrony danych, w tym zwłaszcza:
 - a) niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlania treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu),
 - b) naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
 - c) ujawnienie osobom nieupoważnionym procedur ochrony danych stosowanych u administratora danych,
 - d) ujawnienie osobom nieupoważnionym danych przetwarzanych przez administratora danych, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach administratora danych,
 - e) niewykonywanie stosownych kopii zapasowych,
 - f) przetwarzanie danych osobowych w celach prywatnych,
 - g) wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez zgody administratora systemu.

II. Postanowienia ogólne

1. Definicje

Ilekoć w polityce bezpieczeństwa jest mowa o:

- a) **Administratorze Danych** – rozumie się przez to EXCHORD Spółkę Akcyjną z siedzibą w Białymstoku przy ul. Kombatantów 4/110, reprezentowaną przez Prezesa Zarządu Roberta Tarantowicza,
- b) **Podmiocie Przetwarzającym Dane** – rozumie się przez to podmiot zewnętrzny

- przetwarzający dane osobowe,
- c) **Hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
 - d) **Identyfikatorze** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
 - e) **Integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
 - f) **Odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
 - osoby, której dane dotyczą,
 - osoby upoważnionej do przetwarzania danych,
 - przedstawiciela, o którym mowa w art. 31a ustawy,
 - podmiotu, o którym mowa w art. 31 ustawy,
 - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
 - g) **Osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych zgodnie z zasadą reprezentacji,
 - h) **Poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
 - i) **Raportcie** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
 - j) **Rozliczalności** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
 - k) **Rozporządzeniu** – rozumie się przez to Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (Dz.U. UE L.2016.119.1 z dnia 4 maja 2016 r.,
 - l) **Publicznej sieci telekomunikacyjnej** – rozumie się przez to sieć publiczną telekomunikacyjną w rozumieniu art. 2 pkt. 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. 2017 poz. 1907),
 - ł) **Sieci telekomunikacyjnej** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt. 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. 2017 poz. 1907),
 - m) **Serwisancie** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,
 - n) **Systemie informatycznym administratora danych** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,
 - o) **Teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
 - p) **Ustawie** – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych,
 - r) **Uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
 - s) **Użytkownikowi** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

2. Cel

Wdrożenie polityki bezpieczeństwa u administratora danych ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych, w tym danych przetwarzanych w systemie informatycznym administratora danych i poza nim, poprzez wykonanie obowiązków wynikających z ustawy i rozporządzenia.

Niniejsza **Polityka bezpieczeństwa** służy zapewnieniu wysokiego poziomu bezpieczeństwa i opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

3. Zakres stosowania

- a) Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.
- b) Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. wolontariuszy, praktykantów.

III. Organizacja przetwarzania danych osobowych

1. Administrator danych osobowych

Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

- a) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych;
- b) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
- c) wyznacza pracownika działu spraw pracowniczych właściwego do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oraz pozostałej dokumentacji z zakresu ochrony danych, o ile jako właściwy do jej prowadzenia nie zostanie wskazany w niniejszym dokumencie inny podmiot;
- d) prowadzi rejestr czynności przetwarzania danych osobowych;
- e) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych;
- f) sprawuje nadzór nad wdrożeniem stosownych środków fizycznych, a także organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa danych;
- g) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych;
- h) nadzoruje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych;
- i) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom;
- j) zatwierdza wzory dokumentów (odpowiednie klauzule w dokumentach) dotyczących ochrony danych osobowych, przygotowywane przez pracowników administratora danych;
- k) nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych

osobowych przez upoważnionego pracownika ds. pracowniczych;

- l) prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych;
- m) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego;
- n) przygotowuje wyciągi z polityki bezpieczeństwa, dostosowane do zakresów obowiązków osób upoważnionych do przetwarzania danych osobowych;
- o) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnionych do przetwarzania danych osobowych.

2. Upoważniony pracownik ds. pracowniczych

Upoważniony pracownik ds. pracowniczych realizuje przede wszystkim następujące zadania w zakresie ochrony danych osobowych:

- a) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych;
- b) występuje z wnioskiem do administratora danych o nadanie upoważnienia do przetwarzania danych osobowych;
- c) występuje z wnioskiem do administratora systemu o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych;
- d) występuje z wnioskiem o odwołanie upoważnienia do przetwarzania danych osobowych i/lub wyrejestrowania użytkownika z systemu informatycznego.

3. Osoba upoważniona do przetwarzania danych osobowych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

- a) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;
- b) musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
- c) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
- d) stosuje określone przez administratora danych procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;
- e) korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;
- f) zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym.

IV. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

1. Przetwarzaniem danych osobowych jest wykonywanie jakichkolwiek operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemie informatycznym.
2. Dane osobowe przetwarzane są tylko i wyłącznie na terenie budynku przy ul. Kombatantów nr 4, lok. 114, 15-102 Białystok.

V. Procesy przetwarzania danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Tabela 1. Procesy przetwarzania danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych w Spółce

Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych			
Lp.	Proces przetwarzania danych	Programy zastosowane do przetwarzania danych	Miejsce przetwarzania danych
1.	Proces rekrutacji	E-mail	Kombatantów 4 lok. 110
2.	Proces zatrudniania	E-mail	Kombatantów 4 lok. 110
3.	Proces marketingowy	E-mail	Kombatantów 4 lok. 110
4.	Proces przetwarzania danych pracowników	Akta osobowe	Kombatantów 4 lok. 110
5.	Proces sprzedaży	E-mail, Excell	Kombatantów 4 lok. 110
6.	Proces zakupów	E-mail, Excell	Kombatantów 4 lok. 110
7.	Proces dostawy	E-mail, Excell	Kombatantów 4 lok. 110
8.	Proces windykacji	E-mail	Kombatantów 4 lok. 110
9.	Proces archiwizacji	E-mail	Kombatantów 4 lok. 110

VI. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych

1. Hasła dla indywidualnych użytkowników;
2. Uprawnienia dostępu dla indywidualnych użytkowników przyznawane na poziomie systemu;
3. Ochrona fizyczna pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych;

4. Pisemne zobowiązanie pracowników mających dostęp do danych osobowych do zachowania poufności.

VII. Strategia zabezpieczenia danych osobowych (działania niezbędne do zapewnienia poufności przetwarzanych danych)

A. Bezpieczeństwo osobowe

1. Zachowanie poufności

- a) Ryzyko utraty bezpieczeństwa danych przetwarzanych przez administratora danych pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci), jest minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych;
- b) Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia administratora danych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń.

2. Szkolenia w zakresie ochrony danych osobowych

- a) Administrator danych uwzględnia następujący plan szkoleń:
 - szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych,
 - szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych,
 - przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.
- b) Tematyka szkoleń obejmuje:
 - przepisy i procedury dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
 - sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą,
 - obowiązki osób upoważnionych do przetwarzania danych osobowych,
 - odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych,
 - zasady i procedury określone w polityce bezpieczeństwa.

B. Strefy bezpieczeństwa

Miejsca przetwarzania danych należą do pierwszej strefy bezpieczeństwa.

1. Serwer jest zlokalizowany w pomieszczeniu gdzie mogą przebywać wyłącznie pracownicy do tego uprawnieni, inne osoby upoważnione do przetwarzania tylko w ich towarzystwie.
2. Informatycy wskazują użytkownikom, jak postępować, aby zapewnić prawidłową eksploatację systemu informatycznego, a zwłaszcza:
 - ochronę nośników przenośnych – w tym także nośników danych, na których przechowywane są kopie zapasowe,
 - wszystkie urządzenia systemu informatycznego administratora danych są zasilane za pośrednictwem zasilaczy awaryjnych (UPS).
3. Bieżąca konserwacja sprzętu wykorzystywanego przez administratora danych do

przetwarzania danych prowadzona jest tylko przez jego pracowników. Natomiast poważne naprawy wykonywane przez personel zewnętrzny realizowane są w siedzibie administratora danych po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszenie bezpieczeństwa danych.

4. Administrator systemu dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi także zawiera się umowy powierzenia przetwarzania danych.

C. Zabezpieczenia we własnym zakresie

Niezwykle ważne dla bezpieczeństwa danych jest wyrobienie przez każdą osobę upoważnioną do przetwarzania danych lub użytkownika nawyku:

1. ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
2. niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych oraz w samochodach;
3. pilnego strzeżenia akt, dysków CD/DVD, pamięci przenośnych i komputerów przenośnych;
4. kasowania po wykorzystaniu danych na dyskach przenośnych;
5. nieużywania powtórnie dokumentów zawierających dane osobowe zadrukowanych jednostronnie;
6. niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;
7. powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
8. przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji;
9. opuszczania stanowiska pracy dopiero po aktywowaniu wygaszacza ekranu zabezpieczonego hasłem lub po zablokowaniu stacji roboczej w inny sposób;
10. kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;
11. udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;
12. niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;
13. wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;

14. kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera;
15. niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
16. niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
17. zachowania tajemnicy danych, w tym także wobec najbliższych;
18. chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
19. umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
20. zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
21. zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
22. zamykania drzwi na klucz po zakończeniu pracy w danym dniu.

D. Postępowanie z nośnikami i ich bezpieczeństwo

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

1. dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, niedostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone;
2. uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie;
3. zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;
4. po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych.

E. Wymiana danych i ich bezpieczeństwo

1. Sporządzanie kopii zapasowych następuje w trybie opisanym w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
2. Inne wymogi bezpieczeństwa systemowego są określone w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach administratora danych oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”.
3. Poczta elektroniczną można przysyłać tylko jednostkowe dane, a nie całe bazy lub

szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed „przesłuchami” na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie.

4. Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora systemu. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora danych oraz umożliwić mu monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.
5. Administrator systemu dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.
6. Należy stosować następujące sposoby kryptograficznej ochrony danych:
 - przy przesyłaniu danych za pomocą poczty elektronicznej stosuje się szyfrowanie połączenia,
 - przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się stron zabezpieczonych protokołem HTTPS.

F. Kontrola dostępu do sieci

1. System informatyczny posiada szerokopasmowe połączenie z Internetem.
2. Administrator danych wykorzystuje centralną zaporę sieciową w celu separacji lokalnej sieci od sieci publicznej.
3. Korzystanie z zasobów sieci wewnętrznej (intranet) jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.
4. Operacje za pośrednictwem rachunku bankowego administratora danych może wykonywać wyłącznie pracownik działu księgowości, upoważniony przez Administratora danych, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

G. Komputery przenośne i praca na odległość

1. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby administratora danych nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Komputery przenośne należy przewozić w przeznaczonych do tego torbach.
2. Nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych ani też w samochodach.
3. Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu.
4. Wykorzystywanie komputerów przenośnych administratora danych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona

do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione. W konsekwencji korzystanie z komputera przenośnego będzie z reguły niedozwolone w restauracjach czy środkach komunikacji publicznej.

5. W domu niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do administratora danych. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym administratora danych.
6. Administrator systemu w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa zasady zwrotu sprzętu w razie zakończenia pracy u administratora danych.
7. W zakresie nieuregulowanym w polityce bezpieczeństwa stosuje się do pracy z wykorzystaniem komputerów przenośnych postanowienia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

H. Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych

1. Administrator danych przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania.
2. Administrator danych może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych administratora danych.
3. Z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez administratora danych.
4. Administrator danych przygotowuje wykaz procesów przetwarzania danych, w którym poszczególnym kategoriom danych osobowych przypisane zostaną okresy ich przechowywania. Wykaz ten zostanie sporządzony po przeanalizowaniu przepisów wyznaczających m.in. obowiązek przechowywania dokumentacji czy też okresy przedawnienia roszczeń udokumentowanych z wykorzystaniem danych osobowych. Przed sporządzeniem takiego wykazu przygotowany zostanie wykaz przepisów, na mocy których przetwarzane są dane osobowe, na podstawie wykazów cząstkowych, sporządzonych przez poszczególne komórki organizacyjne.

I. Udostępnianie danych osobowych

1. Udostępnianie danych osobowych

Udostępnianie danych osobowych odbiorcom danych może nastąpić wyłącznie po złożeniu pisemnego wniosku.

2. Udostępnianie danych osobowych na podstawie ustaw szczególnych

I. Udostępnianie informacji Policji

1. Udostępnianie danych osobowych funkcjonariuszom policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien

mieć formę pisemną i zawierać:

- oznaczenie wnioskodawcy,
 - wskazanie przepisów uprawniających do dostępu do informacji,
 - określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,
 - wskazanie imienia, nazwiska i stopnia służbowego policjanta upoważnionego do pobrania informacji lub zapoznania się z ich treścią.
2. Udostępnianie danych osobowych na podstawie ustnego wniosku zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.
 3. Osoba udostępniająca dane osobowe jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji. Policjant jest obowiązany do pokwitowania lub potwierdzenia.
 4. Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.
 5. Jeśli policjant pouczył osobę udostępniającą informacje o konieczności zachowania w tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze udostępnień niezależnie od odnotowania faktu udostępnienia informacji.

II. Udostępnianie danych osobowych innym służbom

Ustawy o innych służbach dają im szczególne uprawnienia. Posiadają one szerokie kompetencje do pozyskiwania informacji, co więcej, wszelkie inne instytucje zobligowane są do podporządkowania się przedmiotowym służbom. W zakresie swojej właściwości mogą zbierać, także niejawnie dane osobowe, w tym również, jeżeli jest to uzasadnione charakterem realizowanych zadań, dane wskazane w art. 27 i 28 ustawy o ochronie danych osobowych, a także korzystać z danych osobowych i innych informacji użytkowych w wyniku wykonywania czynności operacyjno-rozpoznawczych oraz przetwarzać je, w rozumieniu ww. ustawy, bez wiedzy i zgody osoby, której te dane dotyczą. Administrator zbiorów danych jest zobowiązany udostępnić dane o osobie. Od strony proceduralnej udostępnianie danych osobowych tym służbom przez administratora zbioru danych wymaga przedłożenia pisemnego imiennego upoważnienia, okazanego wraz z legitymacją służbową.

J. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.

Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 266 Kodeksu karnego. Przykładowo przestępstwo można popełnić wskutek:

1. stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej;
2. niezabezpieczenia nośnika lub komputera przenośnego;
3. zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym administratora danych.

VIII. Postanowienia końcowe

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści. Każdej osobie upoważnionej do przetwarzania danych administrator danych przekazuje wyciąg z polityki bezpieczeństwa, a użytkownikom dodatkowo z instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, przygotowany z uwzględnieniem stanowiska tej osoby (obowiązków). Polityka bezpieczeństwa wchodzi w życie 25.05.2018 r.