Standardy Ochrony Danych Osobowych w Firmie

Securus Finanse sp. z o.o.

z siedzibą w Kaliszu, ul. W. Jabłkowskiego 3

Standardy Ochrony Danych Osobowych są dokumentem wewnętrznym w Securus Finanse sp. z o.o. (zwany dalej Administratorem) określającym reguły przetwarzania danych osobowych.

Dokument zawiera informacje o zabezpieczeniach, dlatego objęty jest ochroną na zasadzie tajemnicy przedsiębiorstwa (art. 11 ust. 4 ustawy z dnia 16.04.1993r. o zwalczaniu nieuczciwej konkurencji (t.j. z dnia 9 lutego 2018 r. Dz.U. z 2018 r. poz. 419). Treść dokumentu lub jego wybrane elementy mogą zostać udostępnione innym podmiotom po zawarciu umowy o zachowaniu poufności.

Standardy zawierają informacje niezbędne dla właściwego rozpoznania procesów przetwarzania danych, wprowadzenia adekwatnych rozwiązań organizacyjno - technicznych związanych z przetwarzaniem danych i ich ochroną, informowania osób zainteresowanych o przetwarzaniu danych osobowych, monitorowana poziomu ochrony danych, a w razie zaistnienia takiej potrzeby przedsięwzięcia odpowiednich środków w celu zminimalizowania ryzyka/niebezpieczeństwa naruszenia tych danych. Standardy wytyczają również reguły postępowania w zakresie zarządzania dostępem do procesów przetwarzania danych oraz osobami w procesie tym uczestniczącymi, określają osoby odpowiedzialne za bezpieczeństwo danych osobowych oraz reguły reagowania na ewentualne incydenty dotyczące danych osobowych.

Z treścią niniejszego dokumentu powinny być zapoznane wszystkie osoby upoważnione do przetwarzania danych osobowych, które z uwagi na zakres wykonywanych obowiązków i czynności mają dostęp do danych osobowych. Osoby odpowiedzialne w Firmie za nadzór nad ochroną danych osobowych są zobowiązane dołożyć starań, aby przyjęte reguły ochrony danych osobowych były stosowane i przestrzegane przez władze Firmy, pracowników, zleceniobiorców i innych współpracowników w zakresie w jakim przetwarzają dane osobowe w imieniu lub na rzecz Firmy.

Standardy Ochrony Danych Osobowych opracowane zostały na podstawie obowiązujących przepisów prawa, ze szczególnym uwzględnieniem przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. 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) które wejdzie w życie dnia 25.05.2018r.

Polityka bezpieczeństwa przetwarzania danych osobowych w firmie Securus Finanse sp. z o.o.

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy spełniony jest co najmniej jeden z poniższych warunków:
    - osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
    - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
    - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
    - przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
    - przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym;
    - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

2. Zasady przetwarzania danych
    - Zasada Ograniczenie celu- dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Takimi celami mogą być zawarcie umowy ubezpieczenia, proponowanie nowych produktów ubezpieczeniowych, odnowienie umowy ubezpieczenia.
    - Zasada minimalizacji danych- przetwarzane dane osobowe muszą być ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Niedozwolone jest zbieranie danych, które nie są związane z potrzebami ubezpieczeniowymi i finansowymi klienta.
    - Zasada prawidłowości danych - dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć działania, aby dane osobowe, które są nieprawidłowe zostały usunięte lub sprostowane.
    - Ograniczenie przechowywania dDane osobowe muszą być przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. W przypadku produktów ubezpieczeniowych i finansowych administrator przetwarza dane przez okres przedawnienia roszczeń oraz przez okresy wymagane przepisami o rachunkowości.

3. Ogólne zasady bezpieczeństwa przetwarzania danych osobowych:

- dane osobowe, które są wykorzystywane do przetwarzania muszą być prawidłowe. Jeżeli istnieje informacja o nieaktualnych danych osobowych, nie należy ich przetwarzać. W takim przypadku należy je zaktualizować.
- podczas wysyłki korespondencji należy zwrócić szczególną uwagę na poprawność adresów Klientów, zawsze należy zweryfikować poprawność danych adresata przed wysyłką,
- wszelkie wiadomości uzyskane w związku z wykonywaniem czynności służbowych należy chronić przed nieuprawnionym ujawnieniem,
- każdorazowo po wyjściu z biura zamykaj drzwi. Po zakończonym dniu pracy uruchom alarm antywłamaniowy,
- klucze do biura należy nosić przy sobie, nie należy pożyczać nikomu kluczy,
- po zakończonym spotkaniu w salach ogólnodostępnych dla innych osób należy uprzątnąć wszystkie materiały, skasować pliki w ogólnodostępnym sprzęcie elektronicznym, wyczyścić tablicę.

4. Ochrona przetwarzanych danych osobowych w formie elektronicznej:
    - każdy sprzęt elektroniczny należy wyposażyć w hasło dostępu,
    - jeżeli w czasie pracy następuje opuszczenie miejsca pracy należy zablokować komputer,
    - nie należy zapisywać haseł do systemów informatycznych, w których znajdują się dane osobowe. Zarówno własnych, jaki i tych udostępnionych przez Towarzystwa Ubezpieczeniowe,
    - jeżeli istnieje przypuszczenie, ze mogło dojść do ujawnienia hasła, należy je niezwłocznie zmienić,
    - ekran monitora komputera należy ustawić w taki sposób, aby uniemożliwić osobą postronnym wgląd w widoczne na nim dane osobowe,
    - wprowadza się zakaz tworzenia nieautoryzowanych kopii danych osobowych,
    - wprowadza się zakaz tworzenia kopii danych osobowych na zewnętrznych nośnikach danych (np. pendrive, płyta CD itp.)
    - każdy komputer oraz sprzęt przenośny wyposażony jest w legalne oprogramowanie antywirusowe
    - dane osobowe, które są przesyłane e-mailem należy zaszyfrować, dostęp do danych przesyłanych (hasło do poliku) należy przekazać odbiorcy odrębny źródłem
    - należy zachować szczególną ostrożność po otrzymaniu wiadomości e-mail od nieznajomego nadawcy, szczególnie jeśli zawiera załączniki,
    - poczta elektroniczna może być wykorzystywana tylko i wyłącznie do celów służbowych,
    - sprzęt mobilny należy przechowywać w miejscu niedostępnym dla osób trzecich.

5. Ochrona przetwarzanych danych osobowych na dokumentach/wydrukach itp.
    - zasada czystego biurka/ czystej drukarki/kopiarki – nie należy pozostawiać bez nadzoru dokumentów zawierających dane osobowe na biurku, drukarce, czy kopiarce ani innych miejscach dostępnych dla osób postronnych,

- po zakończeniu pracy należy umieścić dokumenty w przeznaczonych dla nich szafach zamykanych na klucz, klucz należy schować w uzgodnionym miejscu,
- w trakcie dnia pracy należy odkładać dokumenty zawierające dane osobowe w takie miejsce i w taki sposób, aby osoby postronne nie mogły się z nimi zapoznać,
- w razie konieczności zniszczenia dokumentów zawierających dane osobowe należy zrobić to w sposób bezpieczny i skuteczny, np. w niszczarce. Bezwzględny zakaz wyrzucania takich danych do kosza na śmieci.

6. Ochrona przetwarzanych danych osobowych w trakcie rozmowy:
    - podczas rozmowy z Klientem należy zachować szczególną ostrożność w pozyskiwanych danych osobowych. Upewnij się, czy osoby postronne nie słyszą rozmowy. Jeżeli istnieje możliwość należy posługiwać się przekazanymi przez klienta dokumentami (np. dowodem rejestracyjnym),
    - nie należy przekazywać przez telefon informacji dotyczących Klienta, jeżeli nie ma pewności, że rozmówca jest uprawniony do tego, by je otrzymać,
    - zakaz rozmowy o klientach z osobami postronnymi, nieupoważnionymi do otrzymywania takich informacji,
    - prowadząc służbową rozmowę w miejscu publicznym należy zachować dyskrecję i unikać możliwości jej podsłuchania.

Prawa osób, których dane dotyczą

1. Prawo dostępu do danych

Jest to uprawnienie osoby do dostępu do danych na swój temat oraz do informacji o procesie ich przetwarzania. Klient na prawo poprosić o zestawienie zawierające wykaz danych osobowych przetwarzanych w firmie lub towarzystwie ubezpieczeniowym.

2. Prawo do sprostowania danych osobowych

Osoba, której dane dotyczą ma prawo w każdym momencie żądać sprostowania nieprawidłowych danych o sobie.

3. Prawo do bycia zapomnianym

Jest to prawo do usunięcia danych osobowych. Prawo to, co do zasady może być zrealizowane wobec potencjalnych klientów, których dane są zbierane w celach marketingowych, którzy nie złożyli wniosku o ubezpieczenie, z którymi nie została zawarta umowa ubezpieczenia. W przeciwnym razie żądanie nie to nie może zostać zrealizowane do upływu okresu przedawnienia roszczeń.

4. Prawo do sprzeciwu wobec przetwarzania danych w celach marketingowych

Po złożeniu takiego sprzeciwu, dalsze przetwarzanie danych osobowych w celach marketingowych jest niedozwolone.

5. Prawo do przenoszenia danych

Jest to prawo uzyskania wszystkich swoich danych osobowych w ustrukturyzowanym, powszechnie używanym formacie, nadającym się do odczytu maszynowego. Prawo to polega na uzyskaniu treści przetwarzanych danych w formie elektronicznej które przekazał nam wcześniej klient i które przetwarzamy w systemie informatycznym.

6. Prawo do cofnięcia zgody

Zgoda na przetwarzanie danych osobowych w każdym czasie może zostać wycofana. Wycofanie zgody nie powoduje nieważności wcześniej przetwarzanych danych.

7. Prawo niepodlegania automatycznej decyzji, w tym profilowania

Prawo, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu i wywołuje wobec osoby skutki prawne

8. Prawo wniesienia skargi do organu nadzorczego

W przypadku uznania, że dane osobowe mogły zostać naruszone, każdy ma prawo wniesienia skargi do organu nadzorczego.

Procedura w przypadku naruszenia

1. Administrator w przypadku naruszenia ochrony danych osobowych, przeprowadza wewnętrzne postępowanie w celu ustalenia okoliczności w których doszło do naruszenia oraz jego skutków, a także podejmuje niezwłoczne działania mające na celu naprawę lub zapobieżenie skutkom naruszenia.
2. W przypadku stwierdzenia naruszenia ochrony danych osobowych należy niezwłocznie, lecz nie później niż w ciągu 72 godzin od stwierdzenia naruszenia zgłosić stwierdzone naruszenia organ nadzorczy (PUODO). Zgłoszenie o którym mowa w ust. 2 powinno:
    - opisywać okoliczności zdarzenia stanowiącego naruszenie oraz jego ustalone lub podejrzewane przyczyny,
    - opisywać charakter naruszenia danych osobowych, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą, oraz przybliżoną liczbę wpisów (rekordów) danych osobowych
    - opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
    - zawierać wstępną analizę ryzyka naruszenia praw i wolności osób, których dane dotyczą i informacje niezbędne do zawiadomienia tych osób,
    - opisywać środki podjęte oraz proponowane w celu zaradzenia naruszeniu danych osobowych, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków,
    - zawierać datę i czas wystąpienia incydentu,
    - zawierać datę i czas dowiedzenia się przez Securus Finanse sp. z o.o. o naruszeniu.
3. Securus Finanse sp. z o.o. dokumentuje w formie rejestru wszelkie stwierdzone naruszenia ochrony danych osobowych w tym ich okoliczności, skutki oraz podjęte działania zaradcze

Rejestr naruszeń ochrony danych osobowych - WZÓR

(dokument prowadzony w formie elektronicznej)

Lp.	Data i czas naruszenia	Data i czas identyfikacji naruszenia	Opis naruszenia	Przyczyna naruszenia	Kategorie osób	Ilość osób	Zastosowane środki	Proponowane środki	Czy zgłoszono do ZU	Data i godzina zgłoszenia do ZU

Zarządzanie systemami informatycznymi służącymi do przetwarzania danych osobowych

1. Celem instrukcji jest określenie sposobu zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.
2. Zawarte z instrukcji procedury i wytyczne są przekazywane osobom odpowiedzialnym za ich realizację stosownie do przyznanych uprawnień i zakresu obowiązków.
3. Ilekroć w Instrukcji jest mowa o:
   - **systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
   - **zabezpieczeniu systemu informatycznego** – należy przez to rozumieć zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, mające na celu w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą uszkodzeniem lub zniszczeniem.
   - **zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
   - **przetwarzaniu 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;
   - **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
   - **administratorze danych osobowych –** rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych;
   - **administratorze bezpieczeństwa informacji –** rozumie się przez to osobę wyznaczoną przez administratora danych, 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;
   - **użytkowniku** – rozumie się przez to osobę upoważnioną przez administratora danych, wyznaczoną do przetwarzania danych osobowych;
   - **identyfikator użytkownika (login)** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
   - **hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
   - **uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
   - **nośniki danych osobowych** – rozumie się przez to urządzenia/materiały służące do przechowywania plików z danymi.

4. Administrator danych osobowych lub administrator bezpieczeństwa informacji sprawuje ogólną kontrolę i nadzór nad przestrzeganiem postanowień instrukcji, a w szczególności:

- sam lub za pomocą wyznaczonej przez siebie osoby sporządza kopie bezpieczeństwa dla baz danych;

- pozbawia urządzenia i inne nośniki informacji przeznaczonych do likwidacji zapisu danych lub – gdy nie jest to możliwe – uszkadza je trwale w sposób uniemożliwiający odczytanie danych;
- nadzoruje usuwanie awarii sprzętu komputerowego w sposób zapewniający bezpieczeństwo przetwarzanych danych osobowych;
- zabezpiecza zbiory danych osobowych wysyłanych poza obszar określony w polityce bezpieczeństwa;
- sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe;
- sam lub za pomocą wyznaczonej osoby lub firmy sprawuje nadzór nad czynnościami związanymi z ochroną przeciwwirusową, czynnościami serwisowymi dotyczącymi systemu informatycznego, w którym przetwarzane są dane osobowe;
- podejmuje i nadzoruje wszelkie inne działania zmierzające do zapewnienia bezpieczeństwa przetwarzanych w systemie informatycznym danych osobowych.

5. Zakres przedmiotowy Instrukcji

Niniejsza Instrukcja zawiera w szczególności:

- sposób przydziału haseł dla użytkowników i częstotliwości ich zmiany oraz wskazania osób odpowiedzialnych za te czynności;
- sposób rejestrowania i wyrejestrowywania użytkowników oraz wskazania osób odpowiedzialnych za te czynności;
- procedury rozpoczęcia, zawieszenia i zakończenia pracy;
- metody i częstotliwość tworzenia kopii awaryjnych;
- metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania;
- sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków;
- sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych;
- sposób postępowania w zakresie komunikacji w sieci komputerowej.

6. Działaniem Instrukcji objęci są:

- administrator danych osobowych;
- administrator bezpieczeństwa informacji;
- osoby zatrudnione przy przetwarzaniu danych osobowych;
- osoby, które przetwarzają dane osobowe.

7. Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym

7.1. Użytkownikiem systemu informatycznego może być wyłącznie osoba posiadająca odpowiednie upoważnienie i zarejestrowana w rejestrze użytkowników.

7.2. Rejestr użytkowników systemu prowadzi administrator danych osobowych.

7.3. Każdy zarejestrowany użytkownik korzysta z przydzielonego mu konta użytkownika, opatrzonego unikalnym identyfikatorem i hasłem dostępu.

7.4. Użytkownicy nie mogą używać tych samych identyfikatorów, ani wymieniać się identyfikatorami.

7.5. Identyfikator użytkownika powinien być inny dla każdego użytkownika, a po jego wyrejestrowaniu z systemu informatycznego, nie powinien być przydzielany innej osobie.
7.6. Identyfikatory użytkowników ujawnione są w wykazie osób upoważnionych do przetwarzaniu danych osobowych.
7.7. Hasła pozostają tajne, każdy użytkownik jest zobowiązany do zachowania w tajemnicy swego hasła, także po jego zmianie oraz upływie ważności.
7.8. Hasło, co do którego zaistniało choćby podejrzenie ujawnienia powinno być niezwłocznie zmienione przez użytkownika.
7.9. Przy tworzeniu identyfikatora użytkownika administrator systemu ustawia losowe hasło i przekazuje to hasło w formie pisemnej użytkownikowi
7.10. Użytkownik jest zobowiązany zmienić hasło, o ile system na to pozwala, przy pierwszym dostępie do systemu.
7.11. Użytkownicy są zobowiązani do przestrzegania reguł odnośnie długości i złożoności hasła oraz częstotliwości jego zmiany
7.12. Hasło składa się z co najmniej 8 znaków, zalecane jest, aby zawierało małe i wielkie litery oraz cyfry i znaki specjalne
7.13. Zmiana hasła powinna być wykonywana nie rzadziej niż co 30 dni.
7.14. Hasło użytkownika jest jego własnością i zna je wyłącznie dany użytkownik. Zabronione jest przekazywania hasła innym osobom.
7.15. Utrata upoważnienia do przetwarzania danych osobowych, powoduje natychmiastowe zablokowanie użytkowników systemu informatycznego.

8. Indywidualny zakres czynności osoby upoważnionej przy przetwarzaniu danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę tych danych przed:

- niepowołanym dostępem;
- nieuzasadnioną modyfikacją lub zniszczeniem;
- nielegalnym ujawnieniem;
- pozyskaniem – w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.

Jeżeli istnieje taka możliwość, ekrany monitorów, na których możliwy jest dostęp do danych osobowych, powinny być automatycznie wyłączane po upływie ustalonego czasu nieaktywności użytkownika.

Monitory komputerów powinny być tak ustawione, aby uniemożliwić osobom postronnym wgląd do danych osobowych.

9. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

9.1. Przed rozpoczęciem pracy w systemie informatycznym użytkownik zobowiązany jest do:

- zalogowania się do systemu z wykorzystaniem zastrzeżonych tylko dla siebie: identyfikatora i hasła w sposób uniemożliwiający ich ujawnienie osobom postronnym – hasło nie może zawierać mniej niż 8 znaków, osoba je tworząca zobowiązana jest uczynić to w taki sposób, aby utrudnić jego ewentualne odczytanie, poprzez wprowadzenie do hasła: znaków szczególnych, cyfr, dużych liter itd.,
- sprawdzenia prawidłowości funkcjonowania sprzętu komputerowego i systemów, na swoim stanowisku pracy,
- w razie stwierdzenia nieprawidłowości, do powiadomienia o tym fakcie bezpośredniego przełożonego oraz administratora bezpieczeństwa informacji,
- w razie stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub stanu wskazującego na istnienie takiej możliwości, do podjęcia odpowiednich kroków

stosownie do zasad postępowania w sytuacji naruszenia zabezpieczenia danych osobowych.

9.2. Przerywając przetwarzanie danych użytkownik powinien zablokować możliwość korzystania ze swego konta użytkownika przez inne osoby. Zalecane jest w takich przypadkach:

- skorzystanie z mechanizmu czasowej blokady dostępu do komputera poprzez uruchomienie wygaszacza ekranu z hasłem (hasło powinno być zbieżne z hasłem logowania do systemu);
- zakończenie pracy w systemie informatycznym – wylogowanie się z systemu.

9.3. Po zakończeniu przetwarzania danych osobowych w danym dniu, osoba upoważniona zobowiązana jest do:

- zakończenia pracy w systemie informatycznym;
- wylogowania się z systemu informatycznego;
- wyłączenia sprzętu komputerowego oraz zamknięcia szaf, w których przechowuje się nośniki, na których utrwalone są dane osobowe;
- zamknięcia pomieszczeń.

9.4. Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.

10. Kopie bezpieczeństwa

10.4. Kopie bezpieczeństwa powinny być wykonywane co najmniej raz w tygodniu.

10.5. Tworzenie kopii bezpieczeństwa odbywa się poprzez automatyczne zgranie danych na dysk zewnętrzny.

10.6. Osobą odpowiedzialną za tworzenie kopii zapasowych jest administrator danych osobowych.

10.7. Tworzone kopie bezpieczeństwa powinny być opisane w sposób pozwalający na określenie ich zawartości.

10.8. Kopie bezpieczeństwa należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu oraz bezzwłocznie usuwać po ustaniu ich użyteczności.

10.9. Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych w sposób uniemożliwiający ich odtworzenie.

10.10. Jeżeli pozbawienie zapisu nie jest możliwe, kopie są niszczone w sposób uniemożliwiający odczytanie bądź odtworzenie danych zawartych na nośniku kopii.

11. Sposób i czas przechowywania oraz zasady likwidacji nośników informacji

11.4. Wydruki komputerowe z systemu, zawierające dane osobowe są sporządzane jedynie dla celów operacyjnych.

11.5. Wydruk komputerowy z systemu, zawierający dane osobowe, po odpowiednim opisaniu i oznaczeniu, podlega zasadom ochrony danych osobowych przetwarzanych metodami tradycyjnymi.

11.6. Wydruki ze zbiorów danych osobowych tworzone i używane do celów roboczych, (operacyjnych) przechowywane są w zamykanych szafach.

11.7. Nośniki magnetyczne, optyczne i inne nośniki informatyczne, zawierające dane osobowe, przechowywane są w odpowiednich, przeznaczonych do tego zamykanych szafach.

11.8. Likwidacja wydruków z systemu, zawierających dane osobowe odbywa się za pomocą niszczarki do dokumentów lub w inny sposób, trwale uniemożliwiający odczytanie danych.

11.9. Z urządzeń, dysków lub innych nośników informatycznych, które zostały przeznaczone do przekazania innemu podmiotowi, usuwa się zapisane na nich dane.

12. Ochrona antywirusowa

12.4. Ochrona antywirusowa jest realizowana poprzez zainstalowanie odpowiedniego oprogramowania antywirusowego.
12.5. W przypadku wykrycia wirusa komputerowego, użytkownik systemu zobowiązany jest do natychmiastowego poinformowania o tym fakcie administratora danych osobowych lub administratora bezpieczeństwa informacji.
12.6. System informatyczny podlega regularnej kontroli pod kątem obecności wirusów komputerowych.
12.7. Wykryte zagrożenia usuwa się niezwłocznie z systemu informatycznego.
12.8. Przed przystąpieniem do unieszkodliwienia wirusa, należy zabezpieczyć dane zawarte w systemie przed ich utratą.
12.9. Osobą odpowiedzialną za powyższe działania jest administrator danych osobowych.

13. Konserwacja i naprawa systemu przetwarzającego dane osobowe

13.1. Prace bieżące w dziedzinie konserwacji i naprawy systemu przetwarzającego dane osobowe prowadzi osoba odpowiedzialna za te czynności lub w wypadku konieczności zaangażowania do w/w czynności przedsiębiorcy zajmującego się zawodowo ich wykonywaniem, są one wykonywane pod bezpośrednim nadzorem administratora danych osobowych. W uzasadnionych przypadkach zostaje podpisana stosowna umowa o poufności.
13.2. Urządzenia komputerowe, dyski twarde, lub inne informatyczne nośniki danych przeznaczone do naprawy, pozbawia się przed tymi czynnościami zapisu zgromadzonych na nich danych osobowych, a jeśli nie jest to możliwe, czynności te wykonuje się w obecności i pod nadzorem administratora danych osobowych. W uzasadnionych przypadkach zostaje podpisana stosowna umowa o poufności.

14. Sposoby postępowania w zakresie komunikacji w sieci komputerowej

14.1. Wszelkie pliki zawierające kopie danych osobowych zawartych w systemie, wysyłanych poza system, muszą być zabezpieczone hasłem.
14.2. W miarę możliwości, dane osobowe zawarte na serwerze sieciowym nie mogą być przechowywane na stacjach roboczych. Należy dane te umieszczać na dysku sieciowym.
14.3. Nieuzasadnione kopiowanie danych z serwera na stacje robocze bądź na nośniki informatyczne jest zabronione.

15. Zasady korzystania z komputerów przenośnych

15.1. Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, zobowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem, przeznaczonym do przetwarzania danych osobowych.
15.2. W celu zapobieżenia dostępowi do tych danych osobie niepowołanej, należy:

- zabezpieczyć dostęp do komputera hasłem;
- nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych;
- zabezpieczyć aplikacje przetwarzające dane osobowe hasłem.

16. Postępowanie w sytuacji stwierdzenia naruszenia ochrony danych osobowych

Naruszeniem zabezpieczeń systemu informatycznego są w szczególności:

- naruszenie lub próby naruszenia integralności systemu przeznaczonego do przetwarzania danych osobowych – przez osoby nieuprawnione do dostępu do sieci lub aplikacji ze zbiorem danych osobowych;
- naruszenie lub próba naruszenia integralności danych osobowych w systemie przetwarzania (wszelkie dokonane lub usiłowane modyfikacje, zniszczenia, usunięcia danych osobowych przez nieuprawnioną do tego osobę);
- celowe lub nieświadome przekazanie zbioru danych osobowych osobie nieuprawnionej do ich otrzymania;
- nieautoryzowane logowanie do systemu;
- nieuprawnione prace na koncie użytkownika dopuszczonego do przetwarzania danych osobowych przez osobę do tego nieuprawnioną;
- istnienie nieautoryzowanych kont dostępu do danych osobowych;
- włamanie lub jego usiłowanie z zewnątrz sieci;
- nieautoryzowane zmiany danych w systemie;
- nie zablokowanie dostępu do systemu przez osobę uprawnioną do przetwarzania
- danych osobowych w czasie jej nieobecności;
- ujawnienie indywidualnych haseł dostępu użytkowników do systemu;
- brak nadzoru nad serwisantami lub innymi pracownikami przebywającymi w pomieszczeniach, w których odbywa się przetwarzanie danych osobowych;
- nieuprawniony dostęp lub próba dostępu do pomieszczeń, w których odbywa się przetwarzanie danych osobowych;
- kradzież nośników, na których zapisane są dane osobowe lub ich zagubienie;
- nieautoryzowana zmiana lub usunięcie danych zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;
- niewykonanie kopii bezpieczeństwa w odpowiednim terminie;
- niewłaściwe bądź nieuprawnione uszkadzanie, niszczenie nośników zawierających dane osobowe.

17. W przypadkach, o których mowa w § 16, należy podjąć czynności zmierzające do zabezpieczenia miejsca zdarzenia, zabezpieczenia ewentualnych dowodów przestępstwa i minimalizacji zaistniałych szkód, w tym w szczególności:

17.1. zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności:

- dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
- dane osoby zgłaszającej,
- opis miejsca zdarzenia,
- opis przedstawiający stan techniczny sprzętu służącego do przetwarzania lub przechowywania danych osobowych,
- wszelkie ustalone okoliczności zdarzenia;

17.2. Na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem;

17.3. Dokonać identyfikacji zaistniałego zdarzenia, poprzez ustalenie w szczególności:

- rozmiaru zniszczeń,
- sposobu, w jaki osoba niepowołana uzyskała dostęp do danych osobowych,
- rodzaju danych, których dotyczyło naruszenie;

17.4. Wyeliminować czynniki bezpośredniego zagrożenia utraty danych osobowych;
17.5. Sporządzić protokół z wyżej wymienionych czynności;
17.6. Poinformować właściwe organy ścigania w przypadku podejrzenia popełnienia przestępstwa.

18. Administrator danych osobowych lub osoba przez niego upoważniona zobowiązani są do niezwłocznego podjęcia działań mających na celu powstrzymanie lub ograniczenie osobom niepowołanym dostępu do danych osobowych w szczególności przez:
    - zmianę hasła dla administratora i użytkowników;
    - fizyczne odłączenie urządzeń i tych segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej;
    - wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.

19. Po przeanalizowaniu przyczyn i skutków zdarzenia powodującego naruszenie bezpieczeństwa przetwarzanych danych osobowych, osoby odpowiedzialne za bezpieczeństwo danych osobowych zobowiązane są podjąć wszelkie inne działania mające na celu wyeliminowanie podobnych naruszeń w przyszłości oraz zmniejszenie ryzyka występowania ich negatywnych skutków. W szczególności, jeżeli przyczyną naruszenia są:
    - błąd osoby upoważnionej do przetwarzania danych osobowych związany z przetwarzaniem danych osobowych – należy przeprowadzić dodatkowe szkolenie (indywidualne lub grupowe);
    - uaktywnienie wirusa komputerowego – należy ustalić źródło jego pochodzenia oraz wykonać test zabezpieczenia antywirusowego;
    - zaniedbanie ze strony osoby upoważnionej do przetwarzania danych osobowych – należy wyciągnąć konsekwencje zgodnie z przepisami z zakresu prawa pracy o odpowiedzialności pracowników;
    - włamanie – należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających;
    - zły stan urządzenia lub sposób działania programu lub inne niedoskonałości informatycznego systemu przetwarzania danych osobowych – należy niezwłocznie przeprowadzić kontrolne czynności serwisowo – programowe.

20. W przypadku uszkodzenia urządzeń służących do przetwarzania danych, utraty danych, lub ich zniekształcenia, odtwarza się bazy danych osobowych z ostatniej kopii bezpieczeństwa.

21. Administrator danych osobowych zobowiązany jest sporządzić raport ze zdarzenia naruszającego zabezpieczenia systemu informatycznego, obejmujący wnioski dotyczące całokształtu procesu teleinformatycznego przetwarzania danych osobowych, a w szczególności:
    - stanu urządzeń wykorzystywanych do przetwarzania danych osobowych;
    - zawartości zbioru danych osobowych;
    - prawidłowości działania systemu informatycznego i teleinformatycznego, w którym przetwarzane są dane osobowe z uwzględnieniem skuteczności stosowanych do chwili wystąpienia naruszenia, środków zabezpieczających przed dostępem osób niepowołanych;
    - jakości działania sieci informatycznej;
    - wykluczenia obecności wirusów komputerowych;

- ustalenia przyczyny i przebiegu zdarzenia;
- wyciągnięcia wniosków co do uniknięcia podobnych naruszeń w przyszłości.

Raport, o którym mowa w ust. 1, jest przekazywany administratorowi danych w terminie 30 dni od dnia potwierdzenia zdarzenia naruszenia zabezpieczenia systemu informatycznego.

Rejestr użytkowników systemów informatycznych – WZÓR

(prowadzony w formie elektronicznej)