**Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w AVSI POLSKA**

Rozdział 1

Postanowienia ogólne

§ 1

Stosownie do postanowień art. 24 ust. 2 rozporządzeniu Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. oraz w ustawie z 10 maja 2018 r. o ochronie danych osobowych ustala się treść Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w AVSI POLSKA zwaną dalej Instrukcją.

§ 2

Instrukcja ma zastosowanie na obszarze wskazanym w Polityce bezpieczeństwa przetwarzania danych osobowych w AVSI POLSKA (dalej Polityka bezpieczeństwa), w którym przetwarzane są dane osobowe w systemie informatycznym.

§ 3

Administrator danych osobowych sprawuje ogólną kontrolę i nadzór nad przestrzeganiem postanowień instrukcji, a w szczególności:

1) sam lub z pomocą wyznaczonej przez siebie osoby sporządza kopie bezpieczeństwa dla baz sieciowych;

2) sam lub z pomocą wyznaczonej przez siebie osoby pozbawia urządzenia i inne nośniki informacji przeznaczone do likwidacji zapisu danych lub – gdy nie jest to możliwe – uszkadza je trwale w sposób uniemożliwiający odczytanie danych;

3) nadzoruje usuwanie awarii sprzętu komputerowego w sposób zapewniający bezpieczeństwo przetwarzanych danych osobowych;

4) sam lub z pomocą wyznaczonej przez siebie osoby zabezpiecza zbiory danych osobowych wysyłanych poza obszar określony w Polityce bezpieczeństwa;

5) sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe;

6) sam lub z pomocą wyznaczonej osoby sprawuje nadzór nad czynnościami związanymi z ochroną przeciwwirusową, czynnościami serwisowymi dotyczącymi systemu informatycznego, w którym przetwarzane są dane osobowe;

7) nadzoruje obieg i przetwarzanie wydruków z systemu informatycznego zawierających dane osobowe;

8) podejmuje i nadzoruje wszelkie inne działania zmierzające do zapewnienia bezpieczeństwa przetwarzanych w systemie informatycznym danych osobowych.

§ 4

Ilekroć w Instrukcji jest mowa o:

1) **systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
2) **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;

3) **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;
4) **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;
5) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
6) **użytkowniku** – rozumie się przez to upoważnionego przez administratora danych (w przypadku powołania administratora bezpieczeństwa informacji również przez ABI), wyznaczonego do przetwarzania danych osobowych pracownika;
7) **identyfikatorze użytkownika (login)** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
8) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
9) **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
10) **nośnikach danych osobowych** – rozumie się przez to dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/materiały służące do przechowywania plików z danymi.

## Rozdział 2

## Zakres przedmiotowy Instrukcji

§ 5

Niniejsza Instrukcja zawiera w szczególności:

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

§ 6

Działaniem Instrukcji objęci są:

1) osoby zatrudnione przy przetwarzaniu danych osobowych;
2) osoby, które mają dostęp do przetwarzania danych osobowych

## Rozdział 3

## NADAWANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH ORAZ ICH REJESTROWANIE W SYSTEMIE INFORMATYCZNYM

§ 7

1. Użytkownikiem systemu informatycznego może być jedynie osoba posiadająca odpowiednie upoważnienie i zarejestrowana w rejestrze użytkowników.

2. Rejestr użytkowników systemu jest prowadzony przez osobę odpowiedzialną i zapisany i aktualizowany jest w zabezpieczonym folderze.

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

4. Nadawanie identyfikatorów i przydzielanie haseł

1) Zalecane jest, aby hasło składało się z co najmniej 8 znaków; zawierało małe i wielkie litery oraz cyfry i znaki specjalne;
2) identyfikator użytkownika powinien być inny dla każdego użytkownika, a po jego wyrejestrowaniu z systemu informatycznego nie powinien być przydzielany innej osobie;
3) identyfikatory użytkowników ujawnione są w wykazie osób upoważnionych do przetwarzania danych osobowych;
4) hasła pozostają tajne, każdy użytkownik jest zobowiązany do zachowania w tajemnicy swego hasła, także po jego zmianie;
5) hasło, co do którego zaistniało choćby podejrzenie ujawnienia, powinno być niezwłocznie zmienione przez użytkownika;
6) utrata upoważnienia do przetwarzania danych osobowych powoduje natychmiastowe usunięcie z grona użytkowników systemu informatycznego.

§ 8

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

1) niepowołanym dostępem;
2) nieuzasadnioną modyfikacją lub zniszczeniem;
3) nielegalnym ujawnieniem;

4) pozyskaniem – w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.

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

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

## Rozdział 4

## Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

### § 9

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

1) 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 obowiązana jest uczynić to w taki sposób, aby utrudnić jego ewentualne odczytanie, poprzez wprowadzenie do hasła: znaków szczególnych, cyfr, dużych liter itd.,
2) sprawdzenia prawidłowości funkcjonowania sprzętu komputerowego i systemów, na swoim stanowisku pracy,
3) w razie stwierdzenia nieprawidłowości, do powiadomienia o tym fakcie bezpośredniego przełożonego
4) 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.

2. Przerywając przetwarzanie danych, użytkownik powinien co najmniej: aktywować wygaszasz ekranu lub w inny sposób zablokować możliwość korzystania ze swego konta użytkownika przez inne osoby. Zalecane jest w takich przypadkach:

1) skorzystanie z mechanizmu czasowej blokady dostępu do komputera poprzez uruchomienie wygaszacza ekranu z hasłem (hasło powinno być zbieżne z hasłem logowania do systemu);

2) zakończenie pracy w systemie informatycznym – wylogowanie się z systemu.

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

1) zakończenia pracy w systemie informatycznym;

2) wylogowania się z systemu informatycznego;

3) wyłączenia sprzętu komputerowego oraz zamknięcia szaf, w których przechowuje się nośniki, na których utrwalone są dane osobowe;

4) zamknięcia pomieszczeń.

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

## Rozdział 5

## Kopie bezpieczeństwa

### § 10

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych wskutek awarii zasilania lub zakłóceń w sieci zasilającej. Zabezpieczenie to powinno być tak skonstruowane, by

umożliwiało zapisanie danych we wszystkich uruchomionych aplikacjach i wykonanie kopii bezpieczeństwa.

§ 11

1. Kopie bezpieczeństwa wykonywane są w różnych odstępach czasu w zależności od systemu, o którym mowa, nie rzadziej jednak niż raz w tygodniu.
2. Tworzenie kopii bezpieczeństwa odbywa się automatycznie przez zaplanowane zadania w systemie informatycznym
3. Osobą odpowiedzialną za tworzenie kopii zapasowych jest Informatyk.
4. Tworzone kopie bezpieczeństwa powinny być opisane w sposób pozwalający na określenie ich zawartości.
5. Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne, pozbawia się zapisu danych w sposób uniemożliwiający ich odtworzenie.
6. Jeżeli pozbawienie zapisu nie jest możliwe, kopie są niszczone w sposób uniemożliwiający odczytanie bądź odtworzenie danych zawartych na nośniku kopii.

## Rozdział 6

## Sposób i czas przechowywania oraz zasady likwidacji nośników informacji

§ 12

1. Wydruki komputerowe z systemu, zawierające dane osobowe są sporządzane jedynie do celów operacyjnych.
2. Wydruk komputerowy z systemu, zawierający dane osobowe, po odpowiednim opisaniu i oznaczeniu, podlega zasadom ochrony danych osobowych przetwarzanych metodami tradycyjnymi.
3. Wydruki ze zbiorów danych osobowych tworzone i używane do celów roboczych (operacyjnych) przechowywane są w zamykanych szafach.
4. Nośniki magnetyczne, optyczne i inne nośniki informatyczne, zawierające dane osobowe, przechowywane są w odpowiednich, przeznaczonych do tego zamykanych szafach.

5. Likwidacja z systemu wydruków zawierających dane osobowe odbywa się za pomocą niszczarki do dokumentów lub w inny sposób, trwale uniemożliwiający odczytanie danych.
6. Z urządzeń, dysków lub innych nośników informatycznych, które zostały przeznaczone do przekazania innemu podmiotowi, usuwa się zapisane na nich dane.

## Rozdział 7

## Ochrona antywirusowa

### § 13

1. Ochrona antywirusowa jest realizowana poprzez zainstalowanie odpowiedniego oprogramowania antywirusowego.
2. W przypadku wykrycia wirusa komputerowego użytkownik systemu zobowiązany jest do natychmiastowego poinformowania o tym fakcie administratora danych osobowych
3. System informatyczny w tym stacje robocze i serwery, podlegają stałemu monitoringowi i okresowym pełnym skanom pod kątem obecności wirusów komputerowych.
4. Wykryte zagrożenia usuwane są niezwłocznie z systemu informatycznego.
5. Przed przystąpieniem do unieszkodliwienia wirusa należy zabezpieczyć dane zawarte w systemie przed ich utratą.
6. Osobą odpowiedzialną za powyższe działania jest Informatyk

## Rozdział 8

## Konserwacja i naprawa systemu przetwarzającego dane osobowe

### § 14

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. czynności przedsiębiorcy zajmującego się zawodowo ich wykonywaniem, są one wykonywane pod bezpośrednim nadzorem administratora danych osobowych lub Informatyka.

2. Urządzenia komputerowe, dyski twarde, lub inne informatyczne nośniki danych przeznaczone do naprawy pozbawia się przed tymi czynnościami zapisu zgromadzonych na nich danych osobowych.

## Rozdział 9

## Sposoby postępowania w zakresie komunikacji w sieci komputerowej

### § 15

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

## Rozdział 10

## Zasady korzystania z komputerów przenośnych

### § 16

1. Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem przeznaczonym do przetwarzania danych osobowych, wskazanym w Polityce bezpieczeństwa.
2. W celu zapobieżenia dostępowi do tych danych osobie niepowołanej należy:
   1) zabezpieczyć dostęp do komputera hasłem (w przypadku systemu operacyjnego Windows – w sposób, który umożliwia to oprogramowanie);

2) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych;
3) zabezpieczyć aplikacje przetwarzające dane osobowe hasłem.

## Rozdział 11

## Postępowanie w sytuacji stwierdzenia naruszenia ochrony danych osobowych

### § 17

Naruszeniem zabezpieczeń systemu informatycznego są w szczególności:

1) naruszenie lub próby naruszenia integralności systemu przeznaczonego do przetwarzania danych osobowych – przez osoby nieuprawnione do dostępu do sieci lub aplikacji ze zbiorem danych osobowych;
2) naruszenie lub próba naruszenia integralności danych osobowych w systemie przetwarzania (wszelkie dokonane lub usiłowane modyfikacje, zniszczenia, usunięcia danych osobowych przez nieuprawnioną do tego osobę);
3) celowe lub nieświadome przekazanie zbioru danych osobowych osobie nieuprawnionej do ich otrzymania;
4) nieautoryzowane logowanie do systemu;
5) nieuprawnione prace na koncie użytkownika dopuszczonego do przetwarzania danych osobowych przez osobę do tego nieuprawnioną;
6) istnienie nieautoryzowanych kont dostępu do danych osobowych;
7) włamanie lub jego usiłowanie z zewnątrz sieci;
8) nieautoryzowane zmiany danych w systemie;
9) niezablokowanie dostępu do systemu przez osobę uprawnioną do przetwarzania danych osobowych w czasie jej nieobecności;
10) ujawnienie indywidualnych haseł dostępu użytkowników do systemu;
11) brak nadzoru nad serwisantami lub innymi pracownikami przebywającymi w pomieszczeniach, w których odbywa się przetwarzanie danych osobowych;

12) nieuprawniony dostęp lub próba dostępu do pomieszczeń, w których odbywa się przetwarzanie danych osobowych;
13) kradzież nośników, na których zapisane są dane osobowe;
14) nieautoryzowana zmiana lub usunięcie danych zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;
15) niewykonanie kopii bezpieczeństwa w odpowiednim terminie;
16) niewłaściwe bądź nieuprawnione uszkadzanie, niszczenie nośników zawierających dane osobowe.

§ 18

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

1) zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności:
   1) dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
   2) dane osoby zgłaszającej,
   3) opis miejsca zdarzenia,
   4) opis przedstawiający stan techniczny sprzętu służącego do przetwarzania lub przechowywania danych osobowych,
   5) wszelkie ustalone okoliczności zdarzenia;
2) na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem;
3) dokonać identyfikacji zaistniałego zdarzenia, poprzez ustalenie w szczególności:
   1) rozmiaru zniszczeń,
   2) sposobu, w jaki osoba niepowołana uzyskała dostęp do danych osobowych,
   3) rodzaju danych, których dotyczyło naruszenie;
4) wyeliminować czynniki bezpośredniego zagrożenia utraty danych osobowych;
5) sporządzić protokół z wyżej wymienionych czynności;

6) poinformować właściwe organy ścigania w przypadku podejrzenia popełnienia przestępstwa.

§ 19

Administrator danych osobowych lub osoba przez niego upoważniona obowiązana jest do niezwłocznego podjęcia działań mających na celu powstrzymanie lub ograniczenie osobom niepowołanym dostępu do danych osobowych w szczególności przez:

1) zmianę hasła dla administratora i użytkowników;
2) fizyczne odłączenie urządzeń i tych segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej;
3) wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.

§ 20

Po przeanalizowaniu przyczyn i skutków zdarzenia powodującego naruszenie bezpieczeństwa przetwarzanych danych osobowych osoby odpowiedzialne za bezpieczeństwo danych osobowych obowiązane 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:

1) błąd osoby upoważnionej do przetwarzania danych osobowych związany z przetwarzaniem danych osobowych – należy przeprowadzić dodatkowe szkolenie, indywidualne lub grupowe;
2) uaktywnienie wirusa komputerowego – należy ustalić źródło jego pochodzenia oraz wykonać test zabezpieczenia antywirusowego;
3) zaniedbanie ze strony osoby upoważnionej do przetwarzania danych osobowych – należy wyciągnąć konsekwencje zgodnie z przepisami z zakresu prawa pracy o odpowiedzialności pracowników;
4) włamanie – należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających;
5) zły stan urządzenia lub sposób działania programu lub inne niedoskonałości informatycznego systemu przetwarzania danych osobowych – należy niezwłocznie przeprowadzić kontrolne czynności serwisowo-programowe.

§ 21

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

§ 22

1. Administrator danych osobowych lub osoba przez niego upoważniona obowiązana jest sporządzić raport ze zdarzenia naruszającego zabezpieczenia systemu informatycznego, obejmujący wnioski dotyczące całokształtu procesu teleinformatycznego przetwarzania danych osobowych, a w szczególności:
   1) stanu urządzeń wykorzystywanych do przetwarzania danych osobowych;
   2) zawartości zbioru danych osobowych;
   3) 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;
   4) jakości działania sieci informatycznej;
   5) wykluczenia obecności wirusów komputerowych;
   6) ustalenia przyczyny i przebiegu zdarzenia;
   7) wyciągnięcia wniosków co do uniknięcia podobnych naruszeń w przyszłości.
2. Raport, o którym mowa w ust. 1, jest przekazywany administratorowi danych w terminie 30 dni od dnia potwierdzenia zdarzenia naruszenia zabezpieczenia systemu informatycznego.

Rozdział 12

Postanowienia końcowe

§ 23

W sprawach nieunormowanych stosuje się przepisy ustawy z 10 maja 2018r r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2018 r. poz. 1000) oraz przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r.