Krajowy Ośrodek Psychiatrii Sądowej
dla Nieletnich w Garwolinie

Regulamin Ochrony Danych Osobowych

ZATWIERDZAM

……

Maj 2018

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników Krajowego Ośrodka Psychiatrii Sądowej dla Nieletnich w Garwolinie
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora Danych
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora Danych

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych.

SPIS TREŚCI

1 PODSTAWOWE DEFINICJE

Ilekroć w niniejszym dokumencie jest mowa o:

1. **Ośrodku**, **Administratorze Danych** lub **Pracodawcy** – należy rozumieć Krajowy Ośrodek Psychiatrii Sądowej dla Nieletnich w Garwolinie.
2. **Administratorze Systemów Informatycznych (ASI)** – należy rozumieć osobę odpowiedzialną za funkcjonowanie systemów informatycznych w ośrodku oraz stosowanie technicznych i organizacyjnych środków ochrony.
3. **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
4. **identyfikatorze użytkownika (login)** – rozumie się ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
5. **Inspektorze Ochrony Danych (IOD)** – należy rozumieć osobę formalnie wyznaczoną przez Administratora Danych w celu informowania i doradzania jemu, pracownikom i współpracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego – Urzędu Ochrony Danych Osobowych.
6. **uwierzytelnianiu** — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
7. **sprzęcie IT** – rozumie się przez to: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony.

2 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW I PROGRAMÓW

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem.
2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
3. Samowolne instalowanie otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
5. Użytkownicy komputerów przenośnych bez zgody przełożonego nie mogą wynosić komputerów na zewnątrz Ośrodka;
6. Wynoszenie komputerów przenośnych odbywa się tylko w uzasadnionych celach służbowych po sprawdzeniu i zabezpieczeniu danych przez ASI;
7. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, osoba upoważniona zobowiązana jest do chronienia wyświetlanych danych osobowych na monitorze przed wglądem osób nieupoważnionych.
8. W przypadku kradzieży/zgubienia lub naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest zgłosić zdarzenie problem IOD.
9. Osoba upoważniona zobowiązana jest do zabezpieczenia komputera przenośnego w czasie transportu, a przede wszystkim: zaleca się przenoszenie komputera przenośnego w zwykłej

teczce, aktówce, zabrania się pozostawiania komputera przenośnego w samochodzie podczas nieobecności osoby upoważnionej.

10. Gdy komputer przenośny jest pozostawiony w miejscu dostępnym dla osób nieupoważnionych, konieczne jest zabezpieczenie hasłem. Dotyczy to przede wszystkim zabezpieczenia komputera przenośnego na stanowisku pracy, podczas przedstawiania prezentacji, szkolenia.

3 ZARZĄDZANIE UPRAWNIENIAMI – PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Każdy użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów, w których użytkownik pracuje, poczty elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
2. Tworzenie kont użytkowników wraz z uprawnieniami (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) oraz wyrejestrowanie użytkownika dokonuje Administrator Systemu (ASI) lub serwis programu na podstawie upoważnienia do przetwarzania danych osobowych.
3. Czynności, o których mowa w pkt. 2, mogą mieć charakter czasowy lub trwały.
4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:
    a. nieobecność w pracy trwająca dłużej niż 2 miesiące kalendarzowe,
    b. zawieszenie w pełnieniu obowiązków służbowych,
    c. zwolnienie z pełnienia obowiązków służbowych.
5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.
6. Użytkownik nie może samodzielnie zmieniać swoich kont.
7. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
8. Zabrania się pracy wielu użytkowników na wspólnym koncie.
9. Użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę z użyciem identyfikatora i hasła.
10. Użytkownik jest zobowiązany do powiadomienia Administratora Systemów Informatycznych (ASI) o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
11. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić ASI.
12. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. **Polityka czystego ekranu**.
13. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
14. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana przez ASI. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
15. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,

b. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki elektroniczne, magnetyczne i optyczne, na których znajdują się dane osobowe.

4 POLITYKA HASEŁ

1. Hasła powinny składać się z minimum 8 znaków.
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy natychmiast je zmienić.
6. Hasła muszą być zmieniane co 30 dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
8. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
9. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
10. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym Ośrodka.
11. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
12. Zaleca się niedefiniowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

5 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „Polityki czystego biurka”. Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np. na terenach publicznych miejskich lub w lesie.

6 ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA OŚRODEK

1. Dane osobowe wynoszone poza Ośrodek powinny być zarchiwizowane i zabezpieczone hasłem

2. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach i teczkach.
3. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.
4. W sytuacji przekazywania nośników z danymi osobowymi poza obszar Ośrodka można stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce,
    b. dane przed wysłaniem powinny zostać zabezpieczone hasłem, a hasło podane adresatowi inną drogą,
    c. jeśli ma to zastosowanie to należy stosować bezpieczne koperty depozytowe.

7 ZASADY KORZYSTANIA Z INTERNETU

1. Zabrania się pobierania na dysk twardy komputera oraz uruchamia jakichkolwiek nielegalnych programów oraz plików pochodzących z niewiadomego źródła.
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
3. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
4. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
5. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
6. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

8 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza Ośrodek może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza Ośrodek należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne, a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. **WAŻNE:** Nie wolno otwierać załączników od nieznanych podmiotów zwłaszcza załączniki z rozszerzeniem np.zip, .xlsm, .pdf, .exe w mailach! Są to zwykle „wirusy”, które infekują

komputer oraz często pozostałe komputery w sieci. WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH.

7. **WAŻNE:** Nie wolno „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami". Użytkownik „klikając" na taki hiperlink infekuje komputer oraz inne komputery w sieci. WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH.
8. Należy zgłaszać IOD lub ASI przypadki podejrzanych maili.
9. Użytkownicy nie powinni rozsyłać „niezawodowych" maili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 230 osób. Może to spowodować zablokowanie konta mailowego.
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!
11. Użytkownicy powinni okresowo kasować niepotrzebne maile.
12. Konta pocztowe służbowe są odseparowane od poczty prywatnej.
13. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
14. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
15. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
16. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
17. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
18. Przy korzystaniu z maila, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
19. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
20. Użytkownik bez zgody przełożonego nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Ośrodka, jego pracowników, pacjentów, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

9 OCHRONA ANTYWIRUSOWA

1. Do zabezpieczenia systemu stosuje się oprogramowanie AVAST ANTYWIRUS PROFESSIONAL lub inny program zatwierdzony przez Administratora Systemów Informatycznych.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów np.: „Twój system jest zainfekowany!, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie ASI lub IOD.
4. Administrator Systemów Informatycznych zobowiązany jest do dopilnowania, aby zainstalowany program antywirusowy był tak skonfigurowany, by co najmniej raz w tygodniu dokonywał aktualizacji bazy wirusów oraz co najmniej raz w tygodniu dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów komputerowych oraz oprogramowania złośliwego.

5. Oprogramowanie powyższe powinno być skonfigurowane w taki sposób że:
    a. w przypadku wykrycia wirusa w pliku przysyłanym z sieci zewnętrznej plik usuwany jest automatycznie, a użytkownik informowany o jego wykryciu,
    b. w przypadku wykrycia wirusa w innych wypadkach użytkownik jest informowany o jego wykryciu,
    c. użytkownik może podjąć próbę usunięcia wirusa, bez usuwania zainfekowanego pliku,
    d. usunięcie wirusa wraz z zainfekowanym plikiem możliwe jest wyłącznie po uzyskaniu zgody Administratora Systemów Informatycznych (ASI).
6. Fizyczne nośniki informacji takie jak: dyski przenośne, pamięci typu flash, płyty CD/DVD/BD itp. należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie.
7. W przypadku zauważenia komunikatu oprogramowania zabezpieczającego system wskazującego na zaistnienie zagrożenia lub rozpozna tego typu zagrożenie, użytkownik zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z Administratorem Systemów Informatycznych (ASI).
8. Zabrania się użytkownikom komputerów wyłączania, blokowania, odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.

10 KOPIE ZAPASOWE

1. Zabezpieczenie danych osobowych dokonywane jest poprzez tworzenie pełnej kopii zapasowej.
2. Dla systemów finansowo-kadrowo-magazynowo-płacowych kopię bezpieczeństwa wykonuje się co dwa dni. Wykonywana jest ona automatycznie przez program. Raz w tygodniu następuje ręczna archiwizacja programu na zewnętrzny komputer lub inny nośnik informacji Administratora Systemów Informatycznych.
3. Kopie programu dokumentacji medycznej sporządzane są codziennie automatycznie i raz w tygodniu zgrywane na nośnik.
4. Nośniki informacji przechowywane są w pomieszczeniu informatyka zabezpieczonym systemem kontroli dostępu.
5. Zabezpieczenie programów służących do przetwarzania danych osobowych dokonywane jest poprzez sporządzenie kopii zapasowej przed zainstalowaniem nowego programu oraz po dokonaniu jakichkolwiek zmian w programie. Kopia zapasowa sporządzana jest w jednym egzemplarzu.
6. Dla systemu monitoringu kopie sporządzane są codziennie na bieżąco i przechowywane w serwerowni.
7. Pomieszczenia przeznaczone do przechowywania kopii zapasowych:
    a. pomieszczenie kadr i płac – sejf,
    b. pomieszczenie informatyka,
    c. serwerownia.
8. Pełna kopia zapasowa z danymi osobowymi przechowywana jest na nośniku nie dłużej niż do czasu sporządzenia następnej kopii zapasowej.
9. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się przed utratą danych osobowych spowodowana awarią zasilania lub zakłóceniami w sieci poprzez wyposażenie serwerów oraz stacji roboczych w zasilacze awaryjne (UPS).

10. Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych, ma wyłącznie Administrator Systemów Informatycznych, a w zakresie monitoringu wizyjnego Kierownik Sekcji Ochrony.
11. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.
12. W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych.
13. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby postronne. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie (niszczarka dokumentów).

11 FIZYCZNE I ORGANIZACYJNE ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Gwarancją zapewnienia bezpieczeństwa systemu informatycznego Ośrodka oraz przetwarzanych i przechowywanych danych jest zapewnienie bezpieczeństwa fizycznego. Bezpieczeństwo fizyczne zapewnione jest przez specyfikę pracy placówki. Pracuje ona w systemie całodobowym z całodobową ochroną fizyczną oraz monitoringiem. Budynek otoczony jest murem o wysokości 4,5 m. Nie ma możliwości nieuzasadnionego wejścia lub opuszczenia budynku oraz poruszania się w sposób niekontrolowany i samodzielny (tj. bez opieki osoby upoważnionej).
2. Dane osobowe przetwarzane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi zamykanymi na indywidualny klucz lub dodatkowo zabezpieczone elektronicznym systemem kontroli dostępu (KD).
3. Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych.
4. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
5. Powołano IOD.
6. Opracowano i wdrożono Politykę Bezpieczeństwa.
7. Opracowano i wdrożono Regulamin Ochrony Danych Osobowych.
8. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz zostały do zachowania ich w tajemnicy.
9. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.
10. Pomieszczenia, w których przetwarzane są dane, z reguły nie są dostępne dla osób postronnych – interesantów, pacjentów, itp., tam gdzie jest to konieczne wydzielona jest specjalna strefa przeznaczona (poprzez odpowiednie ustawienie mebli biurowych, barierki lub tzw. linie demarkacyjne).
11. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się komputer, na którym dane osobowe przetwarzane są na bieżąco.
12. Zbiory danych osobowych przetwarzanych tradycyjnie (kartoteki, skorowidze, księgi, wykazy i inne zbiory ewidencyjne), przechowywane są w szafach zamkniętych na klucz, ewentualnie w oddzielnych pomieszczeniach specjalnie zabezpieczonych przed dostępem osób nieupoważnionych.
13. Wszystkie pomieszczenia Ośrodka, są zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego, dodatkowo hydrantów lub wolnostojącej gaśnicy.
14. Dokumenty zawierające dane osobowe, po ustaniu przydatności, niszczone są w sposób mechaniczny za pomocą niszczarek dokumentów.

15. Dokumenty zawierające dane osobowe, przesyłane do innych jednostek organizacyjnych powinny być zabezpieczone w kopercie (zaklejonej lub w inny sposób zabezpieczonej przed przypadkowym otwarciem). Wysyłane pocztą muszą być spakowane w koperty wzmocnione folią; natomiast przekazywane przez uprawnione osoby, muszą być przewożone w zamykanej teczce. Niedopuszczalne jest przewożenie w otwartej siatce lub w samej kopercie.
16. Dokumenty zawierające dane osobowe, w tym dane wrażliwe, przenoszone pomiędzy komórkami organizacyjnymi mieszczącymi się w tym samym budynku lub pomiędzy pomieszczeniami tej samej komórki organizacyjnej, muszą być zabezpieczone przed wglądem osób postronnych.
17. W przypadku stwierdzenia, że zostały naruszone zabezpieczenia urządzeń powiadamia Administratora Danych lub inną upoważnioną przez niego osobę, która podejmie odpowiednie kroki w celu wyjaśnienia sprawy.
18. Za przechowywanie zbiorów danych, przetwarzanie i udostępnianie informacji ze zbioru danych osobowych odpowiada bezpośrednio pracownik upoważniony do przetwarzania danych osobowych, a w przypadku jego nieobecności osoba upoważniona przez Administratora Danych.
19. Po zakończeniu pracy pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest zabezpieczyć należycie zbiory danych (kartoteki, skorowidze, księgi, wykazy i inne zbiory ewidencyjne) przed dostępem osób trzecich.
20. Administrator Danych podejmuje odpowiednie przedsięwzięcia mające na celu należyte zabezpieczenie danych osobowych w czasie remontu pomieszczeń, naprawy urządzeń i sprzętu oraz w czasie zmiany lokalizacji jednostki organizacyjnej lub w trakcie opuszczania pomieszczeń, jak również w czasie innych okoliczności zakłócających normalny tok pracy.
21. Administrator Danych musi dopilnować, aby każdy użytkownik powinien miał świadomość zagrożeń wpływających na bezpieczeństwo systemu informatycznego, z którego korzysta. Nowy pracownik powinien być zapoznany z ogólnymi zasadami i przepisami dotyczącymi bezpieczeństwa systemów teleinformatycznych, a szczególnie wynikających z ustawy o ochronie danych osobowych. Raz w roku należy przeprowadzać szkolenia z udziałem wszystkich pracowników Ośrodka omawiające problematykę bezpieczeństwa teleinformatycznego, ze szczególnym uwzględnieniem nowych uregulowań prawnych. Szkolenie to powinno uzmysłowić pracownikom skalę zagrożeń oraz rangę zabezpieczeń, zwłaszcza stosowanych na poziomie użytkownika.

12 PRZEGLĄD I KONSERWACJA SYSTEMU I ZBIORU DANYCH OSOBOWYCH

1. Przeglądy i konserwacje systemu oraz zbiorów danych wykonuje Administrator Systemów Informatycznych na bieżąco, lecz nie rzadziej niż raz w miesiącu. Sprawdzana jest spójność danych, indeksów oraz stan nośników informacji, np. dysków twardych oraz urządzeń peryferyjnych.
2. W celu zapewnienia właściwego funkcjonowania systemu informatycznego służącego do przetwarzania danych osobowych:
    a. każdorazowo po sporządzeniu kopii sprawdza się stan zapisu poprzez odtworzenie dowolnie wybranego pliku,
    b. nie rzadziej niż raz w miesiącu sprawdza się stan zapisu kopii oprogramowania służącego do przetwarzania danych osobowych,
    c. Administrator Systemów Informatycznych przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.

3. W przypadku awarii urządzeń zawierających nośniki z danymi osobowymi, wszelkie prace konserwacyjne prowadzone są w warunkach zapewniających ochronę przed udostępnieniem danych osobowych osobom nie dopuszczonym do ich używania.
4. Naprawa urządzeń zawierających nośniki z danymi osobowymi odbywa się po usunięciu danych w sposób uniemożliwiający ich odczytanie lub gdy jest to niemożliwe naprawa odbywa się pod nadzorem ASI.
5. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale ASI nie rzadziej niż raz w miesiącu.
6. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy dopiero po podpisaniu umowy o powierzeniu danych osobowych.
7. W przypadku konieczności naprawy poza miejscem użytkowania, sprzęt komputerowy, przed oddaniem do serwisu, powinien być odpowiednio przygotowany.

13 SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy zostaje stwierdzone naruszenie zabezpieczeń ochrony danych osobowych przetwarzanych w systemie informatycznym lub w sposób tradycyjny.
2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia bezpośredniego przełożonego lub Inspektora Ochrony Danych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
3. Do sytuacji wymagających powiadomienia, należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
4. Do incydentów wymagających powiadomienia, należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
5. Typowe przykłady incydentów wymagające reakcji:
    a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
    b. dokumentacja jest niszczona bez użycia niszczarki,
    c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
    d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
    e. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,
    f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz Ośrodka bez upoważnienia przełożonego,

g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
h. telefoniczne próby wyłudzenia danych osobowych,
i. kradzież, zagubienie komputerów lub CD, twardych dysków, pendrive'ów z danymi osobowymi,
j. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
l. hasła do systemów przyklejone są w pobliżu komputera.

6. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator Danych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – Administrator Danych zgłasza je organowi nadzorczemu.
7. Szczegółowy zakres postępowanie opisany jest w Polityce Bezpieczeństwa Informacji.

14 OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę-Administratora Danych zadaniach,
   b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę,
   c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę,
   d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.
3. Osoby zapoznane z treścią niniejszego Regulaminu lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
6. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania Ośrodka, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta placówka, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.

15 POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.
3. Naruszenie obowiązków wynikających z niniejszego dokumentu może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.