REGULAMIN OCHRONY

DANYCH OSOBOWYCH

PORADNIA PSYCHOLOGICZNO-PEDAGOGICZNA NR 2

UL. MAZOWIECKA 35, 15-301 BIAŁYSTOK

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

- Pracowników
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający

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

ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. Każdy użytkownik upoważniony do korzystania ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy
2. Użytkownik ma obowiązek natychmiast zgłosić zniszczenie powierzonego mu Sprzętu IT
3. Niedozwolone jest podłączanie do komputerów prywatnych nośników danych (pendrive, płyty CD/DVD, telefony komórkowe itd
4. Nośniki danych w postaci dysków twardych powinny być przechowywane w odpowiednich warunkach środowiskowych, gwarantujących ich trwałość
5. Użytkownik jest zobowiązany do stosowania tzw Polityki czystego ekranu - czyli uniemożliwienia osobom niepowołanym (np. interesntom, pracownikom nieupoważnionym) wgląd do danych wyświetlanych na monitorach komputerowych, a w przypadku opuszczenia stanowiska pracy zobowiązany jest do wylogowania się z aplikacji lub zablokowania dostępu do pulpitu stacji roboczej (WINDOWS+L)
6. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego, a następnie wyłączyć komputer
7. Upoważniony użytkownik niszczy nośniki w sposób trwały poprzez np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive młotkiem

2 ZARZĄDZANIE UPRAWNIENIAMI

1. Każdy użytkownik przetwarzający dane w systemie informatycznym posiada indywidualny login i hasło. W organizacji funkcjonuje poczta firmowa.
2. Użytkownik upoważnienie do przetwarzania danych osobowych od Administratora Danych. Identyfikator, hasło i odpowiednie uprawnienia w aplikacji zostają nadane przez operatora monitorów ekranowych
3. Uprawnienia nadawane są w zakresie wykonywanych obowiązków służbowych.
4. Jeśli dostęp do przetwarzania danych w systemie informatycznym posiadają co najmniej dwie osoby, dla każdego użytkownika systemu nadawany jest unikalny identyfikator, dzięki któremu możliwa jest jednoznaczna identyfikacja
5. Użytkownicy nie mogą samodzielnie zmieniać uprawnień.
6. Każdy z użytkowników pracuje na swoim koncie. Niedopuszczalna jest praca na koncie innego użytkownika.
7. Zabrania się nadawania identyfikatorów użytkowników, którzy stracili upoważnienia do przetwarzania danych.
8. W przypadku zwolnienia bądź zmian uprawnień użytkownika (pracownika) za aktualizację dostępu do aktywów i urządzeń przetwarzania informacji odpowiada jego przełożony. Przełożony powiadomienia operator monitorów ekranowych, który jest odpowiedzialny za wycofanie wszystkich uprawnień użytkownika do dostępu do systemów informatycznych (dezaktywacja identyfikatorów).
9. Uprawnienia do przetwarzania danych osobowych w formie papierowej nadawane są i odwoływane przez Administratora.
10. Użytkownik, który przetwarza dane osobowe w formie papierowej chroni je przed użytkownikami nie mającymi do nich dostępu.

3 POLITYKA HASEŁ

1. Hasło składa się z 8 znaków, zawiera małe i duże litery oraz znaki specjalne lub cyfry;
2. Zmiana haseł następuje co 30 dni;
3. Do haseł dostępu nie stosuje się znaków słownikowych i łatwych do odgadnięcia;
4. Osoba upoważniona zobowiązuje się do nie udostępnia haseł osobom trzecim;

5. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie
6. W przypadkach stwierdzenia naruszenia bezpieczeństwa danych osobowych konto dostępowe zostaje zablokowane.

4 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**". W przypadku dłuższej nieobecności przy stanowisku pracy lub po jej zakończeniu pracownik jest zobowiązany do umieszczenia wszelkich dokumentów i nośników zawierających dane osobowe w bezpiecznym miejscu, np. zamykanej szafce, w celu uniemożliwienia dostęp do nich osobom nieuprawnionym. Nie należy również zostawiać dokumentów i nośników w łatwo dostępnych miejscach, np. przy urządzeniach drukujących
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza obszarem przetwarzania np. w korytarzach
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

5 ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA FIRMĘ/ORGANIZACJĘ

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi.

6 ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z Internetu głównie w celach związanych z pracą.
2. Zabrania się instalowania na komputerach programów z Internetu bez zgody ADO
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo
5. Zabrania się z korzystania z prywatnych portali społecznościowych i serwisów aukcyjnych
6. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł
7. 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
8. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

7 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych przy użyciu poczty elektronicznej może odbywać się tylko przez osoby upoważnione

2. W przypadku przesyłania danych osobowych poza organizację stosuje się zabezpieczenia kryptograficzne
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 12 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać SMS-em lub podać telefonicznie
4. Dopuszcza się możliwość korzystania z poczty prywatnej za zgodą ADO
5. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu
6. W przypadku wysyłania informacji do kilku odbiorców należy skorzystać z opcji „kopia ukryta"
7. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata
8. Zabrania się otwierania załączników niewiadomego pochodzenia., które mogą zawierać w sobie złośliwe oprogramowanie wykradające lub szyfrujące dane. Otworzenie takiego załącznika niesie za sobą wysokie ryzyko utraty danych osobowych.
9. Każdy przypadek z podejrzanym mailem należy zgłosić ASI lub ADO
10. Użytkownik bez zgody Pracodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej

8 OCHRONA ANTYWIRUSOWA

1. Użytkownicy, którzy dostali zgodę ADO na używanie nośników zewnętrznych zobowiązani są do skanowania plików wprowadzanych z tych nośników programem antywirusowym
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe
3. Użytkownicy zobowiązani są do natychmiastowego zgłaszania podejrzenia zainfekowania komputera przez wirusa operatorowi monitorów ekranowych
4. Zaleca się aktualizację oprogramowanie antywirusowego i nie odkładanie „na później"
5. Zabrania się wprowadzania dysków zewnętrznych przynoszonych przez osoby trzecie.

9 SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Przez naruszenie zasad ochrony danych osobowych należy rozumieć:
- nieuprawniony dostęp lub próbę dostępu do systemu lub pomieszczeń (widoczne uszkodzenia bądź naruszenia zabezpieczeń),
- nieupoważniony dostęp, modyfikację, kopiowanie lub zniszczenie/usunięcie danych osobowych, zarówno w systemie informatycznym, jak i na nośnikach papierowych i elektronicznych,
- udostępnianie danych osobowych nieuprawnionym podmiotom lub osobom,
- kradzież nośników zawierających dane osobowe lub oprogramowanie,
- kradzież sprzętu służącego do przetwarzania danych osobowych.

2. W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu
2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie zabezpieczeń systemu informatycznego należy natychmiast przerwać pracę na komputerze.
3. Osoba odpowiedzialna za ochronę danych osobowych:

- ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane, stan urządzeń i zbioru danych oraz identyfikuje wielkość negatywnych następstw naruszenia ochrony danych osobowych,
- ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,
- niezwłocznie zapewnia przywrócenie prawidłowego stanu działania systemu
- lokalizuje źródło problemu (przeprowadza analizę posiadanych danych).

5. W przypadku stwierdzenia, że podejrzenie nie świadczy o naruszeniu zasad ochrony danych, Administrator Danych Osobowych po przeanalizowaniu sytuacji i wyeliminowaniu możliwości wystąpienia ich w przyszłości, podejmuje decyzję o dalszej pracy.
6. Po przywróceniu normalnego funkcjonowania systemu informatycznego należy podjąć działania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości, a w szczególności:
a) jeżeli przyczyną zdarzenia był błąd użytkownika należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych osobowych,
b) jeżeli przyczyną była infekcja wirusowa należy ustalić źródło i wykonać zabezpieczenie systemowe i organizacyjne,
c) jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika należy wyciągnąć konsekwencje dyscyplinarne.

10 OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
    a. zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora
    b. niewykorzystywania danych osobowych w celach pozasłużbowych o ile nie są one jawne
    c. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne
    d. korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych
    e. wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora
    f. należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją ochrony danych osobowych
    g. zachowania w tajemnicy sposobów zabezpieczeń danych osobowych
2. Każda osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych
3. Osoby zapoznane z treścią niniejszego Regulaminu ODO 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

11 POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy
2. Postępowanie jest prowadzone po zgromadzeniu dowodów, po upewnieniu się, że nastąpiło naruszenie zasad oraz stopniowane w zależności od rodzaju, wagi naruszenia, okoliczności itd.
3. Postępowanie prowadzi się zgodnie z obowiązującymi przepisami w tym. m.in. zgodnie z Kodeksem Pracy, Kodeksem Cywilnym i Rozporządzeniem o ochronie danych osobowych
4. W przypadku poważnego naruszenia zasad bezpieczeństwa przez pracownika możliwe jest jego natychmiastowe zwolnienie oraz odebranie praw dostępu
5. W przypadku gdy naruszenie zasad bezpieczeństwa prowadzi do szkody po stronie Pracodawcy/Zleceniodawcy, może on dochodzić odszkodowań zgodnie z przepisami prawa pracy lub kodeksu cywilnego. Jeżeli naruszenie bezpieczeństwa jest jednocześnie czynem zabronionym, pracodawca/zleceniodawca jest zobowiązany zgłosić zawiadomienie o popełnieniu przestępstwa do właściwych organów
6. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę / Zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.
7. W przypadku gdy działania podejmowane po wystąpieniu incydentu bezpieczeństwa wymagają użycia kroków prawnych, należy gromadzić, przechowywać oraz przedstawić materiał dowodowy zgodny z obowiązującym prawem

DYREKTOR
Poradni Psychologiczno-Pedagogicznej Nr 2
w Białymstoku
mgr Barbara Jocz