Regulamin Ochrony Danych Osobowych

Nazwa podmiotu wprowadzającego	Ośrodek Pomocy Społecznej w Ciepłowodach
Data wprowadzenia	24.05.2018
Numer zarządzenia wprowadzającego	7/2018
Podpis ADO	
Podpis IODO	

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad dotyczących ochrony danych osobowych dla:

- 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 wymienionych osób jest zobowiązana do zapoznania się z poniższym regulaminem oraz oświadczenia o stosowaniu zasad w nim zawartych własnoręcznym podpisem.

1. **Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów, nośników zewnętrznych**
    1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, kserokopiarki, laptopy, służbowe tablety i smartfony.
    2. Użytkownik ma obowiązek natychmiastowo zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
    3. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych przez administratora urządzeń (typu smartfon lub pendrive) do systemu informatycznego jest zabronione.

4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach komputerowych przez:
    a) odwrócenie monitora w taki sposób, aby nie był możliwy wgląd,
    b) niedopuszczenie osób niepowołanych do stanowiska.
5. Przed odejściem od stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) oraz wylogować się z programów.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a) wylogować się z systemu informatycznego, a jeśli to wymagane - następnie wyłączyć sprzęt komputerowy,
    b) zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe.
7. 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).
8. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien trwale zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive poprzez połamanie).

2. **Zarządzanie uprawnieniami**
    1. Każdy użytkownik posiadający dostęp do danych osobowych w systemie informatycznym (np. na swoim komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
    2. Osoba odpowiedzialna za nadawanie uprawnień do dostępu do danych w systemie informatycznym nadany login oraz pierwsze hasło podaje w formie ustnej.
    3. Użytkownik zobowiązany jest do niezwłocznej zmiany hasła po jego otrzymaniu.
    4. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonych i przy realizacji informatyków-administratorów.
    5. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień administratora w systemie.
    6. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest zatem umożliwianie innym osobom pracy na koncie innego użytkownika.

3. **Polityka haseł**
    1. Hasło użytkownika składa się z minimum 8 znaków.

2. Hasło użytkownika składa się z dużych liter + małych liter + minimum 1 cyfry lub znaku specjalnego.
3. Hasło nie może być łatwe do odgadnięcia. Nie można stosować powszechnie używanych słów.
4. Hasła nie mogą 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.

4. **Zabezpieczenie dokumentacji papierowej zawierającej dane osobowe**
   1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. polityki czystego biurka. Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
   2. Pomieszczenia, w których przetwarzane są dane osobowe muszą być każdorazowo zamykane na klucz.
   3. Klucze do drzwi nie mogą pozostawać w zamku.
   4. Klucze do szaf i biurek po godzinach pracy lub podczas nieobecności pracownika w trakcie godzin pracy nie mogą pozostawać w zamkach. Muszą one być schowane w miejsce niedostępne dla osób nieuprawnionych.
   5. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach.
   6. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych, na tablicach korkowych, biurkach itd.
   7. Zabrania się wyrzucania niezniszczonych dokumentów.
   8. Zabrania się zabierania dokumentów do domu w celu utylizacji ich w prywatnym systemie grzewczym (np. w piecu, kominku).

5. **Zasady wynoszenia nośników danych oraz dokumentów poza jednostkę**
   1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez pisemnej zgody administratora. Do takich nośników zalicz się: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash i inne dokumenty papierowe.
   2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki). Zapis nie dotyczy dokumentów papierowych.
   3. Należy korzystać ze sprawdzonych firm kurierskich.

4. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.

6. **Zasady korzystania z internetu**

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera, instalowania oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania systemem informatycznym i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi pełną odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. 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.
7. 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.

7. **Zasady korzystania z poczty elektronicznej**

1. Przesyłanie danych osobowych z użyciem poczty elektronicznej poza jednostkę może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza jednostkę należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać inną metodą, np. telefonicznie lub SMS-em. Zabrania się przesyłania hasła na ten sam adres mailowy, na który zostały wysłane pliki z danymi.

4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu, aby uniknąć przesłania plików do osób nieuprawnionych.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych za pomocą poczty elektronicznej zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata. W zastępstwie można użyć opcji automatycznego potwierdzenia otrzymania wiadomości w programie pocztowym.
6. Nie należy otwierać załączników (plików) w e-mailach nawet od rzekomo znanych nam nadawców bez weryfikacji nadawcy. Tego typu maile mogą zawierać załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem systemu informatycznego przez kryptowirusy.
7. Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w e-mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy.
8. Należy zgłaszać administratorowi przypadki podejrzanych e-maili.
9. Użytkownicy nie powinni rozsyłać e-maili niezwiązanych z pracą w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do wielu osób.
10. Podczas wysyłania e-maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie e-maili do wielu adresatów z użyciem opcji „Do wiadomości".
11. Użytkownicy nie powinni rozsyłać, e-maili zawierających załączniki o dużym rozmiarze. Jest to możliwe tylko w wyjątkowych sytuacjach.
12. Użytkownicy powinni minimum raz w miesiącu kasować niepotrzebne wiadomości.
13. E-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 elektronicznej dla celów prywatnych wyłącznie okazjonalnie i za zgodą administratora.
16. Korzystanie z poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

17. Przy korzystaniu z poczty elektronicznej, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
18. Użytkownik bez zgody administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące administratora, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

8. **Ochrona antywirusowa**
    1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.
    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!, Wykryto zagrożenie!”, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie administratora lub osobę upoważnioną.
9. **Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych**
    1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do niezwłocznego powiadomienia administratora lub inspektora w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
    2. 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).
    3. 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).

4. 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 organizacji bez upoważnienia administratora,
    g) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej,
    h) telefoniczne próby wyłudzenia danych osobowych,
    i) kradzież, zagubienie komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi,
    j) e-maile zachęcające do ujawnienia identyfikatora i/lub hasła,
    k) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów.

10. **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 administratora zadaniach,

b) zachowania w tajemnicy danych osobowych do których ma lub będzie miał/a dostęp w związku z wykonywaniem zadań powierzonych przez administratora,

c) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez administratora,

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. Każda osoba dopuszczona do przetwarzania zostaje zaznajomiona z zasadami ochrony danych osobowych przed rozpoczęciem ich przetwarzania.

3. 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.
4. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.

11. Zapisy końcowe

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 administratora lub inspektora za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.
3. Z naruszenia obowiązków wynikających z niniejszego dokumentu lub z postępowania sprzecznego mogą zostać wyciągnięte konsekwencje dyscyplinarne w postaci pisemnego upomnienia, nagany lub kary finansowej.