Regulamin Ochrony Danych Osobowych

w Centrum Edukacji Nauczycieli w Łomży

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

1. Pracowników, współpracowników, zleceniobiorców, stażystów;
2. Użytkowników systemów teleinformatycznych z dostępem do danych osobowych przetwarzanych przez Administratora.

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

SPIS TREŚCI

1 ZASADY OGÓLNE

1. Administrator przy współudziale IOD sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych, zapewniając ich bezpieczeństwo, a w szczególności przeciwdziałając dostępowi osób niepowołanych do systemów, w których przetwarzane są dane osobowe oraz podejmując odpowiednie działania w przypadku wykrycia naruszeń ochrony danych osobowych.
2. Administrator i IOD współpracują ze sobą przy realizacji zadań z zakresu ochrony danych osobowych.
3. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora.
4. Upoważnienie udzielane jest na czas wykonywania przez upoważnionego pracownika czynności na powierzonym stanowisku.
5. IOD ponosi odpowiedzialność za zapoznanie pracownika, który ma być dopuszczony do przetwarzania danych osobowych, z przepisami towarzyszącymi ochronie danych osobowych. Fakt zapoznania się z przepisami pracownik potwierdza własnoręcznym podpisem.
6. Za zapewnienie bezpieczeństwa dokumentów i wydruków odpowiedzialne są osoby przetwarzające dane osobowe.
7. Pracownik zobowiązany jest do przetwarzania danych osobowych zgodnie z przepisami prawa, a w szczególności:
    a. zapoznania się z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych;
    b. zachowania szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesu osób, których dane dotyczą;
    c. zachowania danych osobowych w tajemnicy;
    d. zabezpieczenia danych osobowych przed ich nieautoryzowaną zmianą, utratą, uszkodzeniem, zniszczeniem lub ujawnieniem osobom nieuprawnionym;
    e. przetwarzania danych osobowych zgodnie z celem, dla którego zostały zebrane;
    f. dokonywania okresowego przeglądu przetwarzanych danych w terminie do końca grudnia każdego roku kalendarzowego;
    g. uczestniczenia w szkoleniach z zakresu ochrony danych osobowych.

2 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, kserokopiarki, laptopy, służbowe tablety i smartfony.
2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
3. Samowolne instalowanie (demontaż) sprzętu IT, podłączanie przez użytkowników komputerów nośników używanych w urządzeniach pozostających poza kontrolą Administratora Systemów Informatycznych jest zabronione. W uzasadnionych przypadkach, dostarczony nośnik powinien zostać przed podłączeniem sprawdzony przez ASI w celu eliminacji ewentualnego zagrożenia.
4. Zabronione jest ładowanie telefonów komórkowych i innych urządzeń z portów USB komputerów służących do przetwarzania danych osobowych.

5. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.
6. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów typu: „Twój system jest zainfekowany! Zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie administratora lub informatyka.
7. Użytkownik jest zobowiązany do stosowania w praktyce tzw. Polityki czystego ekranu m. in. poprzez:
    a. uniemożliwienie osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych,
    b. niepozostawiania na monitorze otwartych dokumentów zawierających dane osobowe, w przypadku opuszczenia stanowiska pracy.
8. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu. Jeżeli tego nie uczyni, po upływie 2 minut system automatycznie aktywuje wygaszacz.
9. Użytkownik jest zobowiązany do powiadomienia administratora o próbach logowania do systemu przez osoby nieupoważnione, jeśli system to sygnalizuje.
10. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym informatyka.
11. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, a zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
12. 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).
13. 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 młotkiem).

3 ROZPOCZĘCIE, ZAWIESZENIE I ZAKOŃCZENIE PRACY

1. Każdy użytkownik systemu teleinformatycznego musi posiadać swój własny, indywidualny identyfikator (login) do logowania się oraz hasło.
2. Użytkownik rozpoczyna pracę z użyciem identyfikatora i hasła.
3. Tworzenie kont użytkowników oraz przydzielanie uprawnień dokonywane jest przez informatyka na polecenie przełożonych.
4. Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na swoim komputerze).
5. Zabrania się pracy wielu użytkowników na wspólnym koncie.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a. uruchomić procedury zapisujące zmodyfikowane dane, zamknąć używane aplikacje i odłączyć przenośne informatyczne nośniki danych używane w czasie pracy, wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy;
    b. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki informatyczne, na których znajdują się dane osobowe.

4 POLITYKA HASEŁ

1. Hasła powinny składać się z co najmniej 8 znaków, zawierać wielkie i małe litery oraz cyfry lub znaki specjalne. Hasło nie może być jednakowe z identyfikatorem użytkownika.
2. 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 (np. 123456, qwerty, itp.).
3. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
4. W przypadku ujawnienia hasła – należy powiadomić administratora oraz IOD i natychmiast je zmienić.
5. Hasła muszą być zmieniane nie rzadziej, niż co 30 dni.
6. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
7. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
8. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
9. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym firmy.
10. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
11. Zabrania się przesyłania haseł jawnym tekstem w wiadomościach e-mail.
12. Zabrania się definiowania 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 jeden z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

5 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Pracownicy są zobowiązani do stosowania tzw. Polityki czystego biurka, polegającej na niepozostawianiu dokumentów na biurku podczas nieobecności w trakcie godzin pracy oraz na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach, biurkach po godzinach pracy, w celu ochrony przed kradzieżą lub wglądem osób nieupoważnionych.
2. Pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, pomieszczeniach konferencyjnych, na kserokopiarkach lub drukarkach.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz.

6 ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA ORGANIZACJĘ

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych informatycznych nośników z zapisanymi danymi osobowymi bez zgody administratora. Do takich nośników zalicza się: wymienne twarde dyski, pendrivy, płyty CD, DVD.

2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej.
4. Przy przesyłaniu dokumentów zawierających dane osobowe za pośrednictwem firm kurierskich, należy uprzednio zawrzeć umowę powierzenia przetwarzania danych osobowych.
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest on do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.
6. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji można stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce,
    b. dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą,
    c. należy stosować bezpieczne koperty depozytowe,
    d. przesyłkę należy przesyłać przez kuriera.

7 ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu bez zgody administratora.
4. 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).
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.
8. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych (np. w celu ładowania) i innych urządzeń dostępowych.

8 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem e-maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.

2. W przypadku przesyłania danych osobowych poza organizację należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy telefonicznie lub SMS.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: wielkie i małe litery oraz cyfry lub znaki specjalne.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych e-mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. **WAŻNE:** Nie otwierać załączników (.zip, .xlsm, .pdf, .exe) zawartych w mailach. Są to zwykle „wirusy", które infekują komputer oraz często pozostałe komputery w sieci. Pociąga to za sobą wysokie ryzyko bezpowrotnej utraty danych.
7. **WAŻNE:** Nie wolno „klikać" na hiperlinki w e-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 administratorowi i informatykowi przypadki podejrzanych e-maili.
9. Użytkownicy nie powinni rozsyłać „niezawodowych" e-maili w formie tzw. „łańcuszków szczęścia" lub życzeń świątecznych adresowanych do np. 100 osób.
10. Podczas wysyłania e-maili do wielu adresatów jednocześnie, należy użyć metody **„Ukryte do wiadomości – Bcc lub UDW"**.
11. Użytkownicy powinni okresowo kasować niepotrzebne e-maile.
12. Konta pocztowe firmowe powinny być odseparowane od poczty prywatnej. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
13. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
14. Użytkownicy mają prawo korzystać z poczty elektronicznej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
15. Korzystanie z e-maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej pracy oraz na prawidłowe i rzetelne wykonywanie obowiązków służbowych.
16. Przy korzystaniu z e-maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
17. Użytkownicy nie mają prawa korzystać z poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
18. Użytkownik bez zgody administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

9 SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia przełożonego, Administratora Systemu Informatycznego lub Inspektora Ochrony Danych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych. Zgłoszenia można dokonać w formie elektronicznej

poprzez formularz umieszczony na stronie internetowej administratora, w zakładce ochrona danych osobowych.

2. Do sytuacji wymagających powiadomienia, należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
    b. niewłaściwe zabezpieczenie sprzętu IT czy oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / czystego 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 komputerów, twardych dysków, oprogramowania, pomyłki użytkowników, utrata / zagubienie danych);
    c. umyślne incydenty (włamanie do systemu teleinformatycznego 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 komputera przenośnego lub CD, twardych dysków, pendrive z danymi osobowymi;
    j. e-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.
5. Kompletną procedurę postępowania w przypadku naruszenia ochrony danych osobowych zawiera Załącznik Nr 5 do PB CEN w Łomży.

10 OBOWIĄZEK OCHRONY DANYCH OSOBOWYCH, ZACHOWANIE POUFNOŚCI

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 dostęp w związku z wykonywaniem powierzonych zadań;
    c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań;
    d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych;

e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym do nich dostępem.

2. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować.
3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
4. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania organizacji, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta organizacja oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.
5. Osoby zapoznane z treścią niniejszego Regulaminu i przeszkolone z zasad ochrony danych osobowych, zobowiązane są podpisać Oświadczenie o poufności.

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 sprzeczne z powyższymi zobowiązaniami, może też być podstawą do dochodzenia roszczeń na drodze cywilnoprawnej, a także może zostać uznane za naruszenie przepisów karnych zawartych w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r., poz. 1000 ze zm.).