REGULAMIN OCHRONY DANYCH OSOBOWYCH

Trails Center

Pobieranie danych osobowych od klientów

1. Pracownik upoważniony do przetwarzania danych osobowych klientów zwraca w szczególności uwagę aby:
    1. Pobierane dane były rzetelne i wolne od błędów
    2. W czasie uzyskania informacji dotyczących danych osobowych nie nastąpiło ich przypadkowe ujawnienie osobom postronnym
    3. Klient otrzymał informacje na temat przysługujących mu praw, danych administratora lub gdzie może znaleźć szczegóły w tym zakresie
2. Dostęp do danych zapisanych w systemie możliwy jest wyłącznie w celu realizacji obowiązków pracowniczych
3. Realizacja praw klienta w zakresie wglądu, edycji, usunięcia, przeniesienia albo zastrzeżenia danych odbywa się po weryfikacji tożsamości osoby która zwraca się z takim wnioskiem (np. poprzez sprawdzenie danych podawanych przez tę osobę).
4. W zakresie realizacji uprawnień o których mowa w pkt 3 stosuje się odpowiednie procedury

Sprzęt teleinformatyczny i oprogramowanie

2. Każdy użytkownik przetwarzający dane osobowe korzystający ze sprzętu elektronicznego i komputerowego zabezpiecza go przed zniszczeniem lub uszkodzeniem.
3. Użytkownik jest zobowiązany zgłosić każdy przypadek zagubienia, utraty lub zniszczenia sprzętu
4. Nie wolno samodzielnie instalować sprzętu ani oprogramowania
5. Sprzęt komputerowy zabezpiecza się przed nieautoryzowanym dostępem osób nieuprawnionych: klientów, pracowników innych działów jak również przed wglądem w wyświetlane na ekranach
6. Opuszczając stanowisko pracy, nawet czasowo, należy się wylogować lub włączyć wygaszacz ekranu zabezpieczony hasłem
7. Po zakończeniu pracy:
    a. pracownik wylogowuje się z systemu informatycznego, oraz wyłącza sprzęt komputerowy o ile jest to wymagane na danym stanowisku pracy
    b. pracownik zabezpiecza stanowisko pracy, w szczególności wszelkie nośniki z danymi osobowymi
8. Pliki z danymi osobowymi na sprzęcie współużytkowanym przez kilku pracowników należy zabezpieczać hasłem (bezpiecznym, tj, o długości minimum 8 znaków zawierającym duże i małe litery opcjonalnie także cyfry oraz znaki specjalne)
9. Użytkownicy komputerów przenośnych zobowiązani są do stosowania zasad bezpieczeństwa w tym w szczególności do zabezpieczania plików z danymi hasłem;
10. W przypadku konieczności zapisu danych osobowych na nośniku wymiennym dane osobowe wynoszone poza siedzibę firmy muszą być szyfrowane (hasło wymagane do otwarcia)

Uprawnienia i praca z systemem

1. Każdy użytkownik musi posiadać swój unikatowy identyfikator (login) zapewniający dostęp do systemu oraz hasło
2. Nowe konta tworzą wyznaczeni informatycy lub inne osoby na polecenie przełożonych
3. Czynności obsługi kont wykonują informatycy lub administrator systemów informatycznych
4. Zabrania się samodzielnej modyfikacji uprawnień do systemów informatycznych

5. Użytkownikom nie wolno udostępniać nikomu loginu ani hasła. Praca na loginie innej osoby jest zabroniona.
6. Użytkownik rozpoczyna pracę wprowadzając identyfikator i hasło
7. Użytkownik ma obowiązek powiadamiać przełożonego o stwierdzonych próbach logowania się do systemu osoby nieupoważnionej
8. Przypadkowe zablokowanie systemu logowania wymaga powiadomienia przełożonego
9. Nakazuje się zabezpieczyć sprzęt komputerowy przed nieautoryzowanym dostępem osób nieuprawnionych: klientów, pracowników innych działów jak również wglądu w wyświetlane na ekranach dane (polityka czystego ekranu)
10. Opuszczając stanowisko pracy, nawet czasowo, należy się wylogować lub włączyć wygaszacz ekranu zabezpieczony hasłem
11. Zabrania się uruchamiania programów niezweryfikowanych przez pracowników odpowiedzialnych za wsparcie komputerowe
12. Kończąc pracę:
    a. pracownik wylogowuje się z systemu informatycznego, oraz wyłącza sprzęt komputerowy o ile jest to wymagane na danym stanowisku pracy
    b. pracownik zabezpiecza stanowisko pracy, w szczególności wszelkie nośniki z danymi osobowymi
13. Hasła powinny składać się z min 8 znaków, wśród których są litery duże, małe, w miarę możliwości także cyfry oraz znaki specjalne (np. #$%!@ &?)
14. Hasła nie mogą być łatwe do odgadnięcia (imiona, ciągi znaków z klawiatury, hasło o stałym członie i zmiennym fragmencie liczbowym itp.).
15. Zabrania się ujawniania haseł innym osobom bezpośrednio ani pośrednio a w przypadku ujawnienia hasła – należy niezwłocznie je zmienić
16. Hasła należy zmieniać co 30 dni
17. Użytkownik systemu w trakcie pracy w systemie może samodzielnie zmienić swoje hasło
18. Hasła używane do innych usług, rownież prywatnych celów pracownika, nie powinny być używane w czasie pracy z systemem informatycznym firmy;

Uzyskanie, zawieszenie i cofnięcie dostępu do systemów informatycznych

1. Uzyskanie dostępu do systemu informatycznego następuje na wniosek przełożonego zatrudniającego nowego pracownika po spełnieniu następujących warunków:
    a. podpisanie umowy o pracę
    b. odbycie przeszkolenia z zakresu ochrony danych osobowych
    c. zapoznanie się z niniejszym regulaminem i potwierdzenie przyjęcia jego wytycznych do realizacji
    d. realizacja przeszkolenia z zakresu podstaw obsługi systemu przez osobę zatrudniającą lub przez nią wskazaną
2. Uzyskanie dostępu w przypadku jego zawieszenia lub blokady następuje na wniosek przełożonego po weryfikacji warunków jak w pkt 1
3. Uzyskanie dostępu do systemu następuje po wskazaniu ważnego numeru telefonu kontaktowego
4. W przypadku nieobecności w pracy dłuższej niż 10 dni spowodowanej zwolnieniem lekarskim lub innymi przyczynami obiektywnymi dostęp do systemu może zostać zawieszony.

5. W przypadku uzasadnionego podejrzenia działania zmierzającego do uzyskania nieautoryzowanego dostępu do danych zawartych w systemach informatycznych poza zakresem niezbędnym do wykonywania zadań służbowych lub też w przypadku skali żądań dostępu do danych wykraczającego poza taki zakres dostęp do systemów może zostać zawieszony
6. Po ustaniu przyczyny wskazanej w pkt 5 lub złożeniu stosownych wyjaśnień dostęp jest ponownie udzielany
7. W przypadku zakończenia współpracy pomiędzy Pracodawcą a Pracownikiem, niezależnie od jej formy i przyczyn, dostęp do systemów informatycznych jak również do służbowej poczty internetowej jest cofany

Dokumenty papierowe

1. Papierowe dokumenty zawierające dane osobowe przechowuje się w absolutnie niezbędnym zakresie i jedynie przez minimalny niezbędny okres czasu uwzględniający realizację uprawnień osoby do której należą
2. Należy stosować politykę czystego biurka, czyli zabezpieczać dokumenty oraz nośniki z danymi przed nieuprawnionym dostępem lub kradzieżą w trakcie oraz po zakończeniu pracy. Dokumenty takie podczas nieobecności pracownika na stanowisku pracy powinny zostać zamknięte.
3. Niepotrzebne albo już wykorzystane dokumenty należy niszczyć w niszczarce lub inny bezpieczny sposób
4. Zabrania się pozostawiania dokumentów z danymi poza zabezpieczonymi pomieszczeniami, w przestrzeni publicznej niechronionej;
5. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik

Internet i poczta elektroniczna

1. Użytkownikom wolno korzystać z internetu wyłącznie w celach służbowych
2. Zabrania się pobierania programów nieautoryzowanych przez administratora systemów informatycznych, z podejrzanych lub pirackich źródeł.
3. Użytkownik ponosi pełną odpowiedzialność za ewentualne szkody wywołane samodzielnie pobranym i instalowanym oprogramowaniem
4. Zabrania się korzystania w sposób nieautoryzowany przez osobę odpowiedzialną za systemy komputerowe z managerów haseł i innych rozwiązań zapamiętujących wpisane loginy i hasła do serwisów
5. Każdorazowo należy weryfikować bezpieczne połączenie sprawdzając, czy w pasku adresu przeglądarki widoczna jest kłódka - symbol bezpiecznego połączenia.
6. W firmie nie stosuje się maili z prośbami o podanie hasła. Wszelkie tego typu działania są niemal na pewno działaniem nakierowanym na wyłudzenie hasła i/lub innych informacji niejawnych, co wymaga zgłoszenia przełożonemu
7. Zabrania się korzystania z nieautoryzowanych sposobów dostępu do internetu (przenośny internet lub udostępnienie internetu z telefonu) - bez polecenia przełożonego
8. W miarę możliwości technicznych dane osobowe wysyłane mailem należy wysyłać zaszyfrowane/spakowane
9. W przypadku zabezpieczenia plików hasłem, obowiązują wytyczne dotyczące rodzaju hasła jak opisano wcześniej
10. Wysyłając maila należy zwracać szczególną uwagę na poprawność adresów e-mail, zwłaszcza takich, które są uzupełniane półautomatycznie lub automatycznie
11. W przypadku korespondencji z zewnątrz należy zachować szczególną ostrożność w zakresie załączników typu exe, xls, xlsx, doc, docx, ppt, pptx, zip, rar i podobnych

12. Zachować szczególną ostrożność w przypadku hiperlinków w mailach z zewnątrz (spoza firmy)
13. Przypadki niejasne lub budzące wątpliwości należy niezwłocznie zgłaszać
14. Podczas wysyłania maili do wielu adresatów spoza firmy jednocześnie, zaleca się użyć metody „Ukryte do wiadomości – UDW" w polu DO wstawiając własny adres.
15. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych
16. Zakazuje się wysyłania bez zgody przełożonego korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób, w szczególności zawierającej jakiekolwiek dane osobowe.

Postępowanie z incydentami

1. W przypadku stwierdzenia wystąpienia któregokolwiek z poniższych przypadków należy powiadomić pracodawcę lub osobę upoważnioną w zakresie bezpieczeństwa przetwarzania danych
    a. brak zabezpieczenia systemów informatycznych
    b. niezamknięte pomieszczenia w których przetwarzane są dane osobowe
    c. ignorowanie zaleceń w zakresie przetwarzania danych osobowych
    d. wystąpienie zdarzenia losowego
    e. wystąpienie incydentu typu włamanie, kradzież, wyciek danych
    f. ujawnienie danych osobom nieupoważnionym
    g. celowe lub przypadkowe zniszczenie dokumentów osobowych
    h. awaria systemu informatycznego lub infekcja wirusem komputerowy
2. Pracownik który stwierdza jakąkolwiek sytuację mogącą grozić naruszeniem ochrony danych osobowych zgłasza ją do przełożonego
3. Administrator lub upoważniona osoba dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze
4. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

Zachowanie poufności

1. Każda osoba dopuszczona do przetwarzania danych osobowych w Trails Center zobowiązuje się do:
    a. przetwarzania danych osobowych wyłącznie w celach związanych z jej obowiązkami i stanowiskiem pracy
    b. zachowania w tajemnicy danych osobowych do których ma dostęp
    c. zachowania w tajemnicy stosowanych rozwiązań zabezpieczających
    d. ochrony danych osobowych przed zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, dostępem oraz przetwarzaniem
2. Każda osoba dopuszczona do przetwarzania danych osobowych w Trails Center odbywa ogólne szkolenie z zasad ochrony danych osobowych oraz zapoznaje się z Regulaminem Ochrony Danych Osobowych
3. Osoby przeszkolone w zakresie zasad przetwarzania danych osobowych podpisują oświadczenie o zachowaniu poufności;
4. Zabrania się przekazywania danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub w przypadku podejrzenia działania mającego na celu wyłudzenie danych osobowych

5. Zabrania się publicznego ujawniania, w tym w internecie, jakichkolwiek szczegółów dotyczących funkcjonowania firmy, stosowanych rodzajów zabezpieczeń, procedur bezpieczeństwa i podobnych

Odpowiedzialność karna

Za nieprzestrzeganie postanowień niniejszego regulaminu pracownikowi grozi odpowiedzialność z tytułu naruszenia obowiązków pracowniczych. Działania sprzeczne z Regulaminem mogą również naruszać przepisy karne określone w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.