POLITYKA BEZPIECZEŃSTWA
DANYCH OSOBOWYCH

(PROJEKT)

Sławków, 01.06.2018 r.

Spis treści:

Postanowienia ogólne

1. Źródła prawa:

Niniejsza polityka bezpieczeństwa danych osobowych została opracowana w oparciu o powszechnie obowiązujące przepisy prawa z zakresu ochrony danych osobowych i jej treść odpowiada wymaganiom stawianym w szczególności przez przepisy:

- rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwanego dalej RODO;
- ustawy z dnia 10 maja 2018 r o ochronie danych osobowych (Dz.U.2018.1000), zwanej dalej UODO.

2. Cel polityki

Niniejsza polityka określa zasady, procedury oraz środki techniczne i organizacyjne niezbędne w celu zapewnienia ochrony danych osobowych przetwarzanych w „Euroterminal Sławków" sp. z o.o. z siedzibą w Sławkowie, przed wszelkiego rodzaju zagrożeniami.

Stosowanie zasad oraz wdrożenie procedur, określonych w niniejszej polityce ma na celu zapewnienie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe oraz utrzymania bezpieczeństwa ich przetwarzania.

Dane osobowe przetwarza się z zachowaniem zasad

- **zgodności z prawem, rzetelność i przejrzystości;**
- **ograniczenia celu;**
- **minimalizacji danych;**
- **prawidłowości;**
- **ograniczenia przechowywania;**
- **integralności i poufności;**
- **rozliczalności.**

3. Definicje

Użyte w treści niniejszej polityki bezpieczeństwa informacji określenia oznaczają:

- **administrator danych osobowych** – podmiot, który decyduje o środkach i celach przetwarzania danych osobowych – „Euroterminal Sławków" sp. z o.o. z siedzibą w Sławkowie, ul. Groniec 1, 41-260 Sławków;
- **inspektor ochrony danych (IOD)** – osoba wyznaczona przez administratora danych osobowych, odpowiedzialna w szczególności za zapewnienie przestrzegania przepisów o ochronie danych osobowych;

- **administrator systemu informatycznego (ASI)** – osoba wyznaczona przez administratora danych osobowych, odpowiedzialna w szczególności za wdrożenie i stosowanie zasad bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych;
- **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
- **zbiór danych osobowych** – każdy posiadający strukturę zestaw danych osobowych, dostępnych według określonych kryteriów;
- **przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, w tym zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
- **osoba upoważniona** – osoba posiadająca upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych lub inny podmiot do tego umocowany;
- **system informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych w celu przetwarzania danych;
- **sieć LAN/WAN** – sieć lokalna/rozległa umożliwiająca połączenie systemów informatycznych przy wykorzystaniu specjalistycznych dedykowanych urządzeń i sieci telekomunikacyjnych;
- **urządzenie przenośne –** urządzenie elektroniczne, pozwalające na przetwarzanie, odbieranie i wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią (m.in. notebook, smartfon);
- **nośnik danych** - przedmiot, na którym możliwe jest zapisanie oraz późniejsze odczytanie informacji, nośnik danych może być odczytany na dowolnym urządzeniu wyposażonym w odpowiedni napęd lub slot;
- **użytkownik** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym;
- **incydent** – każde zdarzenie, które zagraża lub może zagrozić bezpieczeństwu danych osobowych, w tym ich poufności, dostępności lub integralności.

4. Zakres stosowania

Niniejszą politykę stosuje się do wszelkich operacji przetwarzania danych osobowych, w tym do przetwarzania danych w systemach informatycznych oraz zapisanych w postaci elektronicznej na zewnętrznych nośnikach informacji.

Dopuszcza się możliwość przyjęcia i stosowania obok niniejszej polityki regulacji szczególnych.

5. Obowiązki administratora danych osobowych

Administrator danych osobowych obowiązany jest do zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym lub zabraniem przez te osoby oraz

przetwarzaniem z naruszeniem prawa, a w tym przed ich nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

Administrator danych osobowych, we współdziałaniu z IOD, jeżeli ten został powołany:

- zapewnia legalność procesów przetwarzania danych osobowych,
- sprawuje nadzór nad zabezpieczeniem danych osobowych,
- na bieżąco identyfikuje i analizuje zagrożenia oraz ryzyko związane z bezpieczeństwem przetwarzanych danych osobowych,
- kontroluje i monitoruje funkcjonowanie zabezpieczeń, wdrożonych w celu ochrony danych osobowych w systemach informatycznych oraz przetwarzanych poza systemami informatycznymi;
- podejmuje działania służące zapobieganiu naruszeń procedur z zakresu ochrony danych osobowych oraz usunięciu skutków tych naruszeń.

6. Inspektor ochrony danych osobowych

Powołuje się IOD. W przypadku niepowołania IOD, wszelkie jego zadania przewidziane niniejszą polityką wykonuje administrator danych osobowych.

Do podstawowych zadań IOD należy:

- sprawdzanie zgodności przetwarzania danych osobowych z przepisami prawa w drodze przeprowadzania okresowych audytów sprawdzających, w tym identyfikacja zagrożeń;
- opracowywanie sprawozdań dla administratora danych osobowych w zakresie zgodności przetwarzania danych osobowych z przepisami prawa;
- nadzorowanie opracowania i aktualizowania wymaganej przepisami prawa dokumentacji przestrzegania zasad przetwarzania danych osobowych;
- zapewnianie zapoznania osób upoważnionych z przepisami o ochronie danych osobowych;
- prowadzenie rejestru czynności przetwarzania, zgodnie z wzorem stanowiącym załącznik nr 1 do niniejszej polityki.

Możliwe jest powierzenie IOD przez administratora danych osobowych innych obowiązków, jeśli nie naruszy to prawidłowego wykonywania podstawowych zadań IOD.

7. Administrator Systemów Informatycznych

Powołuje się ASI. W przypadku niepowołania ASI, wszelkie jego zadania przewidziane niniejszą polityką wykonuje administrator danych osobowych.

Do podstawowych zadań ASI należy:

- zarządzanie kontrolą dostępu do systemów informatycznych;
- weryfikacja zdarzeń systemowych;
- zarządzanie kontami użytkowników;

- wdrażanie mechanizmów bezpieczeństwa przetwarzania danych osobowych;
- kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym;
- regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania tych kopii zapasowych

Możliwe jest powierzenie ASI przez administratora danych osobowych innych obowiązków, jeśli nie naruszy to prawidłowego wykonywania podstawowych zadań ASI.

I. Procesy przetwarzania danych osobowych

1. Rejestr czynności przetwarzania

Prowadzi się rejestr czynności przetwarzania. Za prowadzenie rejestru, o którym mowa w zdaniu poprzednim odpowiada IOD.

Rejestr czynności przetwarzania prowadzi się w formie papierowej lub elektronicznej i zamieszcza się w nim:

- nazwę i dane kontaktowe administratora danych osobowych oraz ewentualnych współadministratorów;
- nazwy zbiorów danych osobowych;
- cele przetwarzania;
- opis kategorii osób, których danych dotyczą, oraz kategorii danych osobowych;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
- gdy ma to zastosowanie, informację o przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
- planowane terminy usunięcia poszczególnych kategorii danych;
- opis występujących ryzyk;
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Wzór rejestru czynności przetwarzania stanowi załącznik nr 1 do niniejszej polityki.

2. Aktualizacja rejestru

Dokonuje się, nie rzadziej niż raz na 12 miesięcy, okresowych przeglądów rejestru przetwarzania danych osobowych pod kątem jego zgodności ze stanem faktycznym.

Osoby odpowiedzialne za procesy biznesowe (kierownicy komórek organizacyjnych), zarządzające zbiorami danych osobowych obowiązane są do IOD wszelkich planowanych zmian struktur zarządzanych przez siebie zbiorów danych osobowych oraz utworzenia nowego zbioru danych.

3. Sposób odnotowania informacji o udostępnieniu danych osobowych odbiorcom

Za odbiorcę danych uznaje się każdy podmiot, któremu udostępnia się dane osobowe, z wyłączeniem:

- osoby, której dane dotyczą;
- osoby upoważnionej do przetwarzania danych osobowych;
- podmiotu przetwarzającego dane na zlecenie administratora danych osobowych w oparciu o umowę powierzenia przetwarzania danych osobowych;
- organów państwowych lub samorządowych, którym dane udostępniane są w związku z prowadzonym postępowaniem.

Działania użytkowników systemów informatycznych w zakresie udostępnienia danych są rozliczalne, tj. możliwe do weryfikacji.

Dla systemów informatycznych uniemożliwiających odnotowanie udostępnienia danych odbiorcy, a także dla odnotowania przypadków udostępnienia danych odbiorcy poza systemem informatycznym prowadzi się rejestr udostępnienia danych osobowych. Użytkownik udostępniający dane osobowe obowiązany jest do odnotowania każdorazowego udostępnienia w rejestrze, wskazując odbiorcę danych oraz zbiór danych, którego udostępnienie dotyczy.

Nadzór nad prowadzonym rejestrem udostępnienia danych osobowych sprawują IOD oraz ASI.

4. Polityki *privacy by design/privacy by default*

Wprowadza się polityki privacy by design oraz privacy by default.

Celem realizacji polityk, o których mowa powyżej, administrator danych osobowych wyznacza osobę odpowiedzialną za zapewnienie odpowiedniego poziomu ochrony danych osobowych w fazie projektowania nowych narzędzi informatycznych, procedur oraz produktów (*privacy by design*).

Jako zasadę przyjmuje się domyślną ochronę danych (*privacy by default*). W celu zapewnienia odpowiedniego poziomu ochrony danych w projektowanym narzędziu, procedurze oraz produkcie stosuje się możliwie najdalej posunięte zabezpieczenia w ich ustawieniach początkowych. Zmniejszenie zakresu ochrony danych uzależnia się od wyraźnego działania osoby, której dane dotyczą i zgody na zmianę tych ustawień w ramach konkretnego procesu przetwarzania.

Osoba wyznaczona przez administratora danych osobowych odpowiada za zapewnienie odpowiedniego poziomu ochrony danych osobowych w fazie projektowania poprzez dobór odpowiednich środków technicznych i organizacyjnych przeznaczonych do stosowania w projektowanym narzędziu informatycznym, procedurze lub produkcie. Przy doborze środków, o których mowa w zdaniu poprzednim uwzględnia się charakter, zakres, kontekst i cel przetwarzania oraz ryzyka naruszenia praw lub wolności osób, których dane dotyczą i prawdopodobieństwo ich wystąpienia.

W zakresie wykonywanych zadań, o których mowa w ust 2 – 4, osoba wyznaczona do realizacji polityk, o których mowa powyżej, odpowiada bezpośrednio przed administratorem danych osobowych. Osoba ta sporządza i przedstawia administratorowi danych osobowych raport z realizacji zadań, o których mowa powyżej. Raport, o którym mowa w zdaniu poprzednim zawiera w szczególności:

- informację na temat narzędzia, procedury lub produktu będącego przedmiotem projektowania;
- informację o charakterze, zakresie, kontekście i celu przetwarzania oraz ryzykach naruszenia praw lub wolności osób, których dane dotyczą i prawdopodobieństwie ich wystąpienia;
- informację o podjętych działaniach służących zapewnieniu odpowiedniego poziomu ochrony danych.

Raport, o którym mowa w powyżej sporządza się w formie pisemnej lub elektronicznej.

Osoba wyznaczona do realizacji polityk *privacy by design* i *privacy by default* współpracuje przy wykonywaniu zadań związanych z realizacją tych polityk z IOD i ASI.

5. Ocena skutków dla ochrony danych

Dokonuje się oceny skutków w odniesieniu do przetwarzania, którego charakter, zakres, cel i kontekst powodować może z dużym prawdopodobieństwem powodować ryzyko dla praw i wolności osób, których dane dotyczą, w tym w szczególności w przypadku:

- systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
- przetwarzania na dużą skalę danych wrażliwych;
- systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Dokonuje się oceny skutków przetwarzania również w przypadkach określonych decyzją organu nadzorczego, wydanych na podstawie powszechnie obowiązujących przepisów prawa.

Oceny skutków dla ochrony danych dokonuje się przed przystąpieniem do realizacji operacji przetwarzania.

Dla podobnych operacji przetwarzania danych osobowych, wiążących się z podobnym ryzykiem, dopuszcza się przeprowadzenie pojedynczej oceny. Za operacje podobne uznaje się operacje dokonywane z użyciem podobnej technologii, w sytuacji gdy w jej ramach przetwarzane są dane należące do podobnych kategorii i odnoszące się do podobnych kategorii osób, których dotyczą, a przetwarzanie służy realizacji celu tożsamego lub podobnego.

Dokonując oceny skutków sporządza się raport obejmujący:

- opis planowanych operacji przetwarzania i celów przetwarzania;

- opis prawnie usprawiedliwionych celów realizowanych przez administratora danych osobowych, jako podstawę przetwarzania – w sytuacji, gdy ma to zastosowanie;
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne do celów;
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
- opis środków planowanych w celu zaradzenia ryzyku naruszenia praw lub wolności osób, których dane dotyczą.

Raport, o którym mowa powyżej sporządza się w formie pisemnej lub elektronicznej.

II. Zarządzanie dostępem do danych osobowych

1. Upoważnienie do przetwarzania danych osobowych oraz ewidencja osób upoważnionych

Do przetwarzania danych osobowych dopuszcza się wyłącznie osoby upoważnione, wpisane do ewidencji osób upoważnionych. Osoby upoważnione zobowiązane są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.

Upoważnienia do przetwarzania danych osobowych wydawane są przez administratora danych osobowych lub pośrednio, przez upoważnione przez niego osoby, na wniosek bezpośredniego przełożonego.

Powyższą procedurę stosuje się odpowiednio w sprawach modyfikacji zakresu wydanych już upoważnień.

Zakres upoważnienia związany jest z zajmowanym stanowiskiem lub pełnioną funkcją oraz zakresem obowiązków służbowych ciążących na osobie upoważnionej. Upoważnienia do przetwarzania danych osobowych udzielane są na czas wykonywania obowiązków służbowych związanych z przetwarzaniem danych osobowych.

Ewidencja osób upoważnionych prowadzona jest w formie pisemnej lub elektronicznej i zawiera:

- imię i nazwisko osoby upoważnionej;
- datę nadania i ustalenia oraz zakres upoważnienia do przetwarzania danych osobowych;
- identyfikator/y w systemie/ach informatycznym/ch, jeżeli upoważnienie obejmuje przetwarzanie danych w systemie informatycznym.

Ewidencję osób upoważnionych prowadzi administrator danych osobowych lub upoważnione przez niego osoby.

Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 3 do niniejszej polityki.

Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 4 do niniejszej polityki.

2. Identyfikator użytkownika w systemie informatycznym

Wszystkim użytkownikom nadaje się w systemach informatycznych odpowiednie identyfikatory. Identyfikator użytkownika w systemie informatycznym nadawany jest przez ASI, na wniosek bezpośredniego przełożonego użytkownika.

Identyfikator użytkownika w systemie informatycznym tworzony jest zgodnie z formatem:

*XXXXXYYY**

**gdzie, XXXXX to 5 pierwszych liter nazwiska, YYY to pierwsze 3 litery imienia, bez znaków diakrytycznych*

Dopuszcza się odstępstwo od powyższej zasady w uzasadnionych przypadkach, w tym w odniesieniu do systemów informatycznych, dla których przewidziano odmienne zasady tworzenia identyfikatorów.

Nadawane identyfikatory są unikalne. Identyfikator użytkownika, który utracił uprawnienia nie może zostać przydzielony innej osobie, w tym nowemu użytkownikowi.

Identyfikator użytkownika w systemie informatycznym odnotowuje się w prowadzonym rejestrze upoważnień do przetwarzania danych osobowych.

3. Nadawanie uprawnień do przetwarzania danych osobowych w systemie informatycznym

Uprawnienia do przetwarzania danych osobowych w systemie Informatycznym oraz dostępu do jego zasobów nadawane są przez ASI, na wniosek bezpośredniego przełożonego użytkownika, na podstawie wydanego uprzednio upoważnienia do przetwarzania danych osobowych.

Zakres uprawnień nadawanych użytkownikom jest związany z zakresem upoważnienia do przetwarzania danych osobowych przypisanego dla danej kategorii użytkowników, co skorelowane jest z zaszeregowaniem użytkownika w ramach określonej kategorii uprawnień oraz zajmowanym stanowiskiem lub pełnioną funkcją oraz zakresem obowiązków służbowych ciążących na użytkowniku. W uzasadnionych przypadkach ASI może odmówić nadania uprawnień i zwrócić się o podjęcie decyzji w tej sprawie do IOD.

W uzasadnionych przypadkach, w tym w szczególności z uwagi na delegowanie użytkownika do wykonywania określonych zadań, możliwa jest czasowa zmiana zakresu uprawnień użytkownika. Zmiana, o której mowa w zdaniu poprzednim dokonywana jest na wniosek bezpośredniego przełożonego użytkownika po uzyskaniu zgody administratora danych osobowych.

Powyższą procedurę stosuje się odpowiednio w sprawach modyfikacji i cofnięcia nadanych już uprawnień.

O fakcie nadania, modyfikacji lub cofnięciu uprawnień użytkownika ASI informuję drogą elektroniczną bezpośredniego przełożonego użytkownika, których zmiana w zakresie nadanych uprawnień dotyczy oraz IOD.

Uprawnienia użytkowników w zakresie administrowania systemami informatycznymi, w tym uprawnienia ASI nadawane, modyfikowane i wycofywane są za zgodą administratora danych osobowych, wyłącznie przez osobę wyznaczoną przez administratora danych osobowych.

Uprawnienia nadawane są na czas trwania stosunku zatrudnienia u administratora danych osobowych lub innego stosunku prawnego stanowiącego podstawę przyznania uprawnień. W uzasadnionych przypadkach administrator danych osobowych może zdecydować o pozostawieniu aktywnych uprawnień po ustaniu zatrudnienia lub innego stosunku prawnego stanowiącego podstawę przyznania uprawnień.

4. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

Uwierzytelnianie użytkowników w systemie informatycznym następuje za pomocą indywidualnych, przypisanych do identyfikatorów użytkowników, haseł dostępu, karty RFID lub danych biometrycznych. Stosuje się dwustopniowe uwierzytelnienie:

- na poziomie dostępu do domeny;
- na poziomie dostępu do systemu informatycznego;

Pierwotne hasło dostępu przydzielane jest użytkownikowi przez ASI na etapie przyznawania uprawnień do przetwarzania danych osobowych w systemie informatycznym oraz dostępu do jego zasobów i sieci LAN. Hasło pierwszego logowania przekazywane jest użytkownikowi bezpośrednio, w sposób zwyczajowo przyjęty sposób, powszechnie uznawany za bezpieczny.

Po otrzymaniu pierwotnego hasła dostępu, użytkownik jest obowiązany do jego zmiany, niezwłocznie po zalogowaniu się do systemu informatycznego. Pierwsza i kolejne zmiany hasła dokonywane są przez użytkownika. Zmiana hasła następuje co 90 dni. Użytkownik zobowiązany jest do zmiany hasła co 90 dni również w odniesieniu do systemów informatycznych, które nie wymuszają tego rodzaju zmiany.

Hasło winno składać się co najmniej z 8 znaków i zawierać małe oraz wielkie litery, a także cyfry.

Login i hasło użytkownika może być używane wyłącznie przez tego użytkownika, któremu zostały nadane. Przekazywanie loginu i hasła innym osobom jest zabronione. Dotyczy to również haseł, które utraciły swą ważność.

Hasła mogą być przez użytkowników przechowywane wyłącznie w formie zaszyfrowanej, zabezpieczonej hasłem głównym spełniającym ogólne wymogi dotyczące haseł. Zabrania się przechowywania haseł w postaci jawnej.

Na potrzeby wykonywania zadań związanych z administrowaniem systemami informatycznymi, ASI uprawniony jest do uzyskiwania informacji o hasłach dostępu użytkownika w systemach informatycznych. ASI nadaje użytkownikowi nowe hasło w przypadku utraty hasła obowiązującego.

III. Organizacja procesów przetwarzania danych osobowych w systemach informatycznych

1. Procedury rozpoczęcia, zawieszenia i zakończenia pracy z systemem informatycznym

Rozpoczęcie pracy z systemem informatycznym:

Przystępując do pracy z systemem informatycznym użytkownik zobowiązany jest do zweryfikowania, w miarę posiadanej wiedzy i istniejących możliwości, stanu zabezpieczeń stacji roboczej oraz systemu informatycznego.

Zawieszenie pracy z systemem informatycznym:

Użytkownik zobowiązany jest do dokonania blokady stacji roboczej w przypadku tymczasowego zaprzestania pracy z systemem informatycznym połączonego z opuszczeniem stanowiska pracy oraz w każdym przypadku, gdy zachodzi niebezpieczeństwo uzyskania przez osoby nieupoważnione wglądu w wyświetlone na monitorze dane osobowe.

Odblokowanie stacji roboczej następuje po wprowadzeniu identyfikatora użytkownika oraz hasła dostępu lub innego środka uwierzytelniania.

Zakończenie pracy z systemem informatycznym:

Zakończenie pracy z systemem informatycznym odbywa się poprzez zamknięcie wszelkich uruchomionych programów i aplikacji oraz przeprowadzenie operacji wylogowania.

Pozostałe zalecenia

Monitory urządzeń służących do przetwarzania danych osobowych znajdujące się w pomieszczeniach, do których dostęp mają osoby nieupoważnione, winny być ustawione w sposób uniemożliwiający tym osobom uzyskanie wglądu do wyświetlanych danych osobowych.

Przetwarzane w systemie informatycznym dane osobowe winny być przechowywane na nośnikach sieciowych (serwer), przy jednoczesnym minimalizowaniu przypadków przechowywania danych osobowych na nośnikach lokalnych.

2. Praca z urządzeniami przenośnymi

Użytkownicy wykorzystujący urządzenia przenośne służące do przetwarzania danych osobowych są zobowiązani do:

- transportowania urządzeń przenośnych w sposób minimalizujący ryzyko ich kradzieży, zagubienia lub uszkodzenia;
- przechowywania urządzeń przenośnych w sposób minimalizujący ryzyko ich kradzieży lub uszkodzenia, w tym pod nadzorem osób upoważnionych lub w zamykanych na klucz pomieszczeniach;

- zabezpieczenia urządzeń przenośnych przed dostępem osób nieupoważnionych, w tym pracy z urządzeniami przenośnymi w sposób uniemożliwiający uzyskanie wglądu do przetwarzanych danych osobowych przez osoby nieupoważnione;
- przetwarzania, w tym przechowywania danych osobowych na nośnikach sieciowych (serwer), przy jednoczesnym minimalizowaniu przypadków przechowywania danych osobowych na nośnikach lokalnych (np. dysk twardy urządzenia przenośnego).

3. Praca z urządzeniami drukującymi oraz skanującymi

Użytkownicy korzystający ze współdzielonych urządzeń drukujących i skanujących zobowiązani są do:

- notyfikowania bezpośrednim przełożonym wszelkich awarii urządzeń drukujących;
- nadzorowania procesu wydruku lub skanowania dokumentów (zakaz pozostawiania dokumentów bez nadzoru po zakończeniu procesu ich wydruku lub skanowania).

4. Zarządzanie kopiami zapasowymi danych osobowych oraz systemów informatycznych służących do ich przetwarzania

– Rodzaj i struktura informacji podlegających zabezpieczeniu poprzez proces tworzenia kopii zapasowych.

Pliki użytkowników oraz baza danych i system napisanych przez firmę BCS do obsługi płyty kontenerowej. Baza danych i system WinsadlB. Bazy danych i programy do obsługi wag. Systemy kontroli dostępu oraz rejestracji czasu pracy RCP i KD (Unis oraz RCP Access Net+), system Druku SafeQ

– Urządzenia i nośniki służące do wykonywania kopii.

Kopie zapasowe wykonywane są przy pomocy programu dostarczonego wraz z systemem operacyjnym MS Windows 2003 server (kopia zapasowa). Wykonywane są na taśmy LTO 200/400 GB przy pomocy streamera Tandberg TS400 SCSI Sequential Device. Głowica streamera jest czyszczona w momencie gdy urządzenie sygnalizuje, że czyszczenie jest wymagane. Czyszczenie głowicy odbywa się przy pomocy taśmy przeznaczonej do tego celu.

Kopia zapasowa danych wykonywana jest dodatkowo na macierz dyskową znajdującą się w serwerowni spółki.

Dodatkowo raz w tygodniu kopia danych wykonywana jest do odrębnej lokalizacji (Serwerownia Grupy CZH S.A., Katowice, Ul. Lompy 14) przez szyfrowany kanał IPSec VPN Site-to_site.

– Zakres danych objętych instrukcją wykonywania kopii zapasowych.

a) Dane znajdujące się na serwerze: stan systemu (rejestry i pliki startowe), baza danych i system do obsługi płyty kontenerowej BCS Tiger, pliki użytkowników.
b) Dane z wag (samochodowa, kolejowa, magazyn),
c) Dane z systemu WinsadlB

d) Systemy RCP, KD Unis oraz RCP Access Net+

System druku SafeQ

- Czas i częstotliwość wykonywania kopii.

a) Dane na serwerze - kopie wykonywane są pn-pt w nocy od godz. 21:00 do godz. 01:00 programem kopia zapasowa systemu win server 2003.
b) Wagi - archiwizacja przy pomocy programu kopia zapasowa na stacji, na której znajduje się baza z danymi. Lokalizacją docelową archiwizacji jest serwer.
c) Dane WinsadlB - archiwizacja przy pomocy programu WinsadlB.

d) Cały zakres danych - kopie na macierz dyskową wykonywane są automatycznie codziennie w nocy od godziny 23:59

e) Kopia tygodniowa danych do odrębnej lokalizacji wykonywana jest w każdą sobotę od godz 19:59

- Osoby odpowiedzialne za wykonywanie kopii i sposób dokumentowania wykonywanych kopii.

Za wykonywanie kopii odpowiedzialna jest podmiot, z którym Spółka ma zawartą umowę outsourcingową. Za wymianę tasiemki i sprawdzenie poprawności wykonanej kopii odpowiedzialny jest podmiot, z którym Spółka ma zawartą umowę outsourcingową- Grupa CZH S.A. Wszelkie zdarzenia zapisywane są w logach serwera i podlegają stałej analizie.

- Miejsce przechowywania kopii zapasowych oraz sposób oznaczania kopii.

Kopie przechowywane są w serwerowni w stalowej szafie pancernej. Taśmy oznaczone są dniami tygodnia.
Miejsce przechowywania danych macierzy dyskowej to serwerownia Euroterminal Sławków Sp. z.o.o. oraz zapasowa lokalizacja – serwerownia Grupy CZH S.A., Katowice, ul. Lompy 14.

- Sprawdzanie wykonania kopii oraz dokumentacja czynności sprawdzających.

Sprawdzanie wykonania kopii polega na odzyskaniu losowo wybranego pliku do lokalizacji testowej. W przypadku problemów z odzyskaniem danych wykonywana jest ponowna archiwizacja na innym nośniku. Stary nośnik jest opisywany jako uszkodzony, następnie jest kasowany i niszczony tak, aby niemożliwe było dotworzenie danych. Pozostałości po uszkodzonym nośniku są utylizowane zgodnie z ustawą dotyczącą utylizacji odpadów niebezpiecznych.

- Odzyskiwanie danych z kopii zapasowych.

Odzyskiwanie danych następuje na wniosek użytkowników sieci komputerowej, po uprzednim sprawdzeniu czy dany użytkownik ma prawo dostępu do danych, o których odzyskanie się ubiega. Odzyskanie danych jest wykonywane do lokalizacji alternatywnej, w której następuje zmiana nazwy pliku. Następnie plik z nową nazwą jest kopiowany do lokalizacji macierzystej, aby użytkownik mógł dokonać jego weryfikacji. Po weryfikacji uszkodzona nazwa pliku jest zmieniana do jego pierwotnej wartości. W przypadku danych archiwalnych decyzja o odzyskaniu pliku jest podejmowana na podstawie informacji od kierownika zainteresowanego działu.

5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

Elektroniczne nośniki informacji zawierające dane osobowe, w tym pamięci flash, dyski optyczne, taśmy magnetyczne i dyski twarde przechowywane są w serwerowni „Euroterminal Sławków". Pozostałe nośniki, które są w posiadaniu pracowników powinny być przechowywane zgodnie z poniższymi wytycznymi.

Po zakończeniu pracy z danym nośnikiem, użytkownik zobowiązany jest do jego zabezpieczenia poprzez umieszczenie w zamykanej szafie lub kasetce.

Elektroniczne nośniki informacji zawierające dane osobowe oznacza się w sposób umożliwiający ich identyfikację.

Elektroniczne nośniki informacji zawierające dane osobowe mogą być przekazywane osobom upoważnionym do przetwarzania danych osobowych w odpowiednim zakresie oraz innym podmiotom wyłącznie za uprzednią zgodą administratora danych osobowych.

Dane osobowe przenoszone z wykorzystaniem elektronicznych nośników informacji usuwa się z tych nośników po ich poprawnym przeniesieniu do miejsca docelowego.

Nośniki sieciowe (serwer) przechowywane są w odrębnych, zamkniętych pomieszczeniach, specjalnie do tego przeznaczonych, do których dostęp posiadają wyłącznie osoby upoważnione.

Kopie zapasowe danych osobowych oraz systemów informatycznych służących do ich przetwarzania przechowuje się w sposób uniemożliwiający dostęp do tych danych i systemów przez osoby nieupoważnione. Dostęp do kopii zapasowych posiada wyłącznie administrator danych osobowych, IOD oraz ASI.

6. Procedury wykonywania przeglądów i konserwacji systemów informatycznych oraz nośników informacji służących do przetwarzania danych osobowych

Prawidłowość działania systemów informatycznych służących przetwarzaniu danych osobowych jest monitorowana na bieżąco przez ASI. Niezależnie od powyższego ASI dokonuje cyklicznych sprawdzeń prawidłowości wykonywanych kopii zapasowych.

Prace serwisowe związane z naprawami i konserwacją systemów informatycznych wykonywane są przez ASI lub podmioty trzecie – autoryzowanych dostawców oprogramowania, na podstawie umów łączących te podmioty z administratorem danych osobowych, zawierających odpowiednie postanowienia w przedmiocie powierzenia przetwarzania danych osobowych. Nadzór nad pracami serwisowymi wykonywanymi przez podmioty trzecie, o których mowa w zdaniu poprzednim sprawuje ASI.

Przeglądy urządzeń oraz nośników elektronicznych służących do przetwarzania danych osobowych dokonywane są zgodnie z warunkami gwarancji producentów tych urządzeń i nośników.

Prace serwisowe związane z naprawami i konserwacją urządzeń oraz nośników służących do przetwarzania danych osobowych wykonywane są przez podmioty trzecie, pod nadzorem ASI.

W przypadku konieczności przeprowadzenia prac serwisowych, o których mowa powyżej, w siedzibie podmiotu trzeciego, usuwa się z urządzenia przeznaczonego do konserwacji lub naprawy wszelkie nośniki danych zawierające dane osobowe, a jeżeli nie jest to możliwe, dokonuje się usunięcia przechowywanych na tych nośnikach danych osobowych oraz systemów informatycznych służących do przetwarzania danych osobowych. Przed przeprowadzeniem operacji usunięcia danych i systemów informatycznych sporządza się kopię zapasową tych danych.

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane, w tym dane osobowe, przeznaczone do:

- likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

Odzyskanie utraconych danych z uszkodzonych nośników odbywa się przy udziale ASI. Operacja odzyskiwania utraconych danych może zostać wykonana jedynie przez wyspecjalizowany podmiot zewnętrzny.

Zabrania się dokonywania napraw uszkodzonych elektronicznych nośników danych (np. dysków twardych).

Niedozwolone jest dokonywanie samodzielnych napraw sprzętu służącego do przetwarzania danych osobowych przez osoby nieupoważnione. Każda powstała usterka powinna być zgłoszona kierownikowi odpowiedniej komórki organizacyjnej oraz ASI. Naprawy dokonywane są przez ASI lub wyspecjalizowany podmiot zewnętrzny.

IV. Bezpieczeństwo danych osobowych

1. Ocena zagrożeń i ryzyk

Identyfikuje się następujące kategorie zagrożeń bezpieczeństwa przetwarzania danych osobowych oraz towarzyszących tym zagrożeniom ryzyk:

- zagrożenia losowe zewnętrzne, obejmujące w szczególności klęski żywiołowe i przerwy w dostawie energii elektrycznej niezależne od administratora danych osobowych, mogą prowadzić do utraty danych lub naruszenia ich integralności;
- zagrożenia losowe wewnętrzne, obejmujące w szczególności błędy ludzkie, awarie sprzętowe, błędy oprogramowania, mogą prowadzić do utraty danych lub naruszenia ich integralności oraz do naruszenia poufności przetwarzanych danych osobowych;
- zagrożenia związane z działaniem zamierzonym osób trzecich, obejmujące wszelkie działania osób trzecich, w tym pracowników administratora danych osobowych, nakierowane na dokonanie czynności naruszających bezpieczeństwo danych osobowych, mogą prowadzić do utraty danych lub naruszenia ich integralności oraz do naruszenia poufności przetwarzanych danych osobowych.

Dokonuje się, nie rzadziej niż raz na 12 miesięcy, okresowego przeglądu ryzyk. Przeglądu ryzyk dokonuje się również w przypadku:

- wprowadzenia do użytku nowych narzędzi służących przetwarzaniu danych osobowych;
- dokonania zmiany procesów biznesowych, których elementem pozostaje przetwarzanie danych osobowych.

2. Bezpieczeństwo środowiskowe

Lokalizację przechowywania nośników danych osobowych dobiera się z uwzględnieniem wymaganych aspektów bezpieczeństwa przetwarzanych danych osobowych. W szczególności należy rozważyć aspekty dotyczące:

- zasilania energią elektryczną;
- klimatyzacji i wentylacji;
- wykrywania oraz ochrony przed pożarem i powodzią;
- fizycznej kontroli dostępu.

Pomieszczenia wchodzące w skład obszaru przetwarzania danych osobowych wyposaża się w odpowiednie środki ochrony fizycznej i organizacyjnej chroniące przed nieautoryzowanym lub nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami pracy.

Kopie zapasowe zawierające dane osobowe przechowuje się w drugiej fizycznej lokalizacji w bezpiecznej odległości od lokalizacji podstawowej.

3. Niszczenie nośników danych osobowych

Nośniki zawierające nieaktualne dane osobowe oraz nośniki uszkodzone niszczy się w sposób uniemożliwiający odzyskanie zawartych na nich danych z wykorzystaniem przeznaczonych do tego urządzeń specjalistycznych (niszczarki) lub poprzez przekazanie nośników do wyspecjalizowanego podmiotu trzeciego.

Przekazywanie nośników informacji służących do przetwarzania danych osobowych podmiotowi trzeciemu odbywa się na podstawie protokołu podpisanego przez właściwych użytkowników, a w przypadku nośników elektronicznych, również przez ASI. Protokół przekazuje się do IOD.

4. Środki techniczne służące zapewnieniu bezpieczeństwa przetwarzania danych osobowych

Stosuje się określone w tabelach poniżej środki techniczne i organizacyjne służące zapewnieniu bezpieczeństwa przetwarzanych danych osobowych.

Środki techniczne

Środki techniczne	Zabezpieczony obszar	Uwagi
Zamykane szafy	Wszystkie budynki	Dokumentacja przechowywana jest w zamykanych szafach.
Zamykane pomieszczenia	Wszystkie budynki	Wszystkie pomieszczenia tworzące obszar przetwarzania danych osobowych posiadają w drzwiach zamki i są zamykane na klucz po godzinach pracy.
Monitoring	Wszystkie budynki	W budynku głównym oraz wokół budynków zamontowane są urządzenia rejestrujące obraz, do których dostęp ma ochrona.

Środki organizacyjne

Środki organizacyjne	Dotyczy	Uwagi
Rejestr kluczy	Wszystkie lokalizacje.	Rejestry kluczy oraz ewidencja wejść i wyjść prowadzone w pomieszczeniach portierni na bramie wjazdowej
Ewidencja wejść i wyjść		
Karty pracownicze	Budynek główny.	Wejście do biura zarządu możliwe jest za pomocą karty RFID.

Ochrona	Wszystkie lokalizacje	Ochronę wykonuje firma zewnętrzna. Ochrona prowadzi rejestr wjazdów i wyjazdów z terenu Spółki. Ochrona ponadto prowadzi księgę kluczy. W dyżurce ochrony znajduje się ponadto księga wejść i wyjść

Okresowo, nie rzadziej jednak niż raz na 12 miesięcy, dokonuje się przeglądu stosowanych środków bezpieczeństwa.

5. Obszar przetwarzania danych osobowych

Obszar przetwarzania danych osobowych tworzą:

- pomieszczenia, w których zlokalizowane są stacje robocze lub serwery służące do przetwarzania danych osobowych;
- pomieszczenia, w których przechowywane są dokumenty stanowiące nośniki danych osobowych;
- pomieszczenia, w których przechowywane są sprawne i uszkodzone elektroniczne nośniki informacji oraz kopie zapasowe zawierające dane osobowe.

Pomieszczenia tworzące obszar przetwarzania danych osobowych objęte są kontrolą dostępu.

Pomieszczenia tworzące obszar przetwarzania danych osobowych zamyka się na czas nieobecności osób upoważnionych do przetwarzania danych osobowych, czyniąc to w sposób ograniczający możliwość dostępu do tych pomieszczeń przez osoby nieupoważnione.

6. Zasada „czystego biurka”

W celu ograniczenia ryzyka nieautoryzowanego lub nieuprawnionego dostępu do danych osobowych przez osoby nieupoważnione wprowadza się zasadę „czystego biurka”.

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przechowywania na biurku wyłącznie dokumentacji, nośników innego rodzaju i narzędzi służących do przetwarzania danych osobowych wykorzystywanych do wykonywania bieżącego zadania. Po godzinach pracy narzędzia, o których mowa w zdaniu poprzednim, a także nośniki danych osobowych, w tym dokumentację zawierającą dane osobowe zabezpiecza się poprzez ich umieszczenie w zamykanych szafach.

7. Polityka kluczy

W celu ograniczenia ryzyka nieautoryzowanego lub nieuprawnionego dostępu do danych osobowych przez osoby nieupoważnione wprowadza się politykę kluczy.

Po zakończeniu pracy osoby upoważnione przekazują klucze do pomieszczeń tworzących obszar przetwarzania danych osobowych do ochrony.

Klucze zapasowe przechowuje się oddzielnie od kluczy głównych. Dostęp do kluczy zapasowych udzielany jest za zgodą administratora danych osobowych lub osoby przez niej upoważnionej.

Nadzór nad depozytami kluczy sprawują osoby upoważnione przez administratora danych osobowych.

8. Zarządzanie incydentami bezpieczeństwa danych osobowych

Osoba upoważniona oraz każdy inny pracownik zobowiązani są do zgłaszania wszelkich wykrytych incydentów lub niepożądanych zdarzeń związanych z bezpieczeństwem przetwarzania danych osobowych, w trybie i na zasadach określonych niniejszą polityką.

Ocena bezpieczeństwa przetwarzania danych osobowych winna być dokonywana w szczególności na podstawie oceny:

- stanu zabezpieczeń technicznych zastosowanych w celu zabezpieczenia danych osobowych;
- stanu technicznego budynków i pomieszczeń tworzących obszar przetwarzania danych osobowych oraz stanu technicznego ich wyposażenia;
- zawartości zbiorów danych osobowych.

Wszelkie wykryte incydenty winny niezwłocznie zostać zgłoszone bezpośredniemu przełożonemu w formie pisemnej, elektronicznej (e-mail), telefonicznej lub ustnej wraz z określeniem sytuacji i czasu, w jakim zostały one zauważone. O stwierdzonych incydentach informuje się również IOD oraz ASI, jeżeli incydent dotyczy przetwarzania danych w systemie informatycznym. Informację o stwierdzonym incydencie przekazuje do IOD i ASI bezpośredni przełożony osoby zgłaszającej incydent.

Jeżeli istnieje taka możliwość, osoba zgłaszająca incydent winna podjąć akcję korekcyjną, polegającą na doraźnym wyeliminowaniu skutków incydentu. Bezpośredni przełożony osoby zgłaszającej incydent we współdziałaniu z IOD i ASI:

- podejmują czynności niezbędne dla powstrzymania niepożądanych skutków zdarzenia;
- podejmują czynności niezbędne dla ustalenia przyczyn i sprawców zdarzenia;
- podejmują decyzję o wstrzymaniu bieżącej pracy w celu zabezpieczenia miejsca zdarzenia;
- uprawnieni są do uzyskania wyjaśnień od świadków zdarzenia;
- powiadamiają administratora danych osobowych o zaistniałym zdarzeniu.

Jako incydenty kwalifikować należy w szczególności:

- odnotowany brak zabezpieczenia przetwarzanych danych osobowych lub obszaru przetwarzania danych osobowych;

- ujawnienie stosowanych zabezpieczeń danych osobowych osobom trzecim;
- uzyskanie dostępu do przetwarzanych danych przez osobę nieupoważnioną;
- kradzież nośników zawierających dane osobowe;
- nieautoryzowane usunięcie danych osobowych, przy jednoczesnym braku aktualnej kopii zapasowej.

Po wyeliminowaniu bezpośredniego zagrożenia bezpieczeństwa danych osobowych administrator danych osobowych we współdziałaniu z IOD i ASI przeprowadza analizę stanu zabezpieczeń danych osobowych w celu potwierdzenia lub wykluczenia możliwości wystąpienia dalszych naruszeń ochrony danych osobowych, a w szczególności:

- kontroluje stan urządzeń wykorzystywanych do przetwarzania danych osobowych;
- kontroluje zawartość zbioru danych osobowych, którego incydent dotyczył;
- kontroluje sposób działania systemu informatycznego przeznaczonego do przetwarzania danych osobowych, którego incydent dotyczył;
- kontroluje stan zabezpieczeń.

Po przywróceniu prawidłowego stanu zabezpieczeń danych osobowych sporządza się raport zawierający informacje na temat:

- charakteru incydentu wraz ze wskazaniem kategorii i przybliżonej ilości osób, których dane dotyczą oraz kategorii i przybliżonej liczby wpisów danych osobowych, których dotyczy naruszenie;
- miejsca i czasu stwierdzenia wystąpienia incydentu;
- możliwych konsekwencji naruszenia ochrony danych osobowych;
- podjętych środków mających na celu zaradzeniu naruszenia ochrony danych osobowych lub zminimalizowaniu jego ewentualnych skutków;
- rekomendacji środków służących minimalizacji ryzyka wystąpienia tożsamych incydentów w przyszłości.

Wzór raportu stanowi załącznik nr 5 do niniejszej polityki.

9. Szkolenia z zakresu ochrony danych osobowych

IOD opracowuje elektroniczne materiały szkoleniowe z zakresu ochrony danych osobowych. Materiały te udostępnia się osobom upoważnionym w zwyczajowo przyjęty sposób.

Osoby upoważnione obowiązane są do zapoznania się z materiałami szkoleniowymi udostępnionymi im w zwyczajowo przyjęty sposób.

Dopuszcza się możliwość podejmowania również innych działań o charakterze szkoleniowym niż opisane powyżej.

V. Postanowienia końcowe

Niniejsza polityka wchodzi w życie z dniem 01 czerwca 2018 r.

Do zapoznania się z niniejszą polityką i jej stosowania zobowiązany jest administrator danych osobowych, IOD oraz wszyscy pracownicy, w tym osoby świadczące usługi na podstawie umów cywilnoprawnych.

Administrator danych osobowych oraz IOD mają prawo do kontroli stosowania określonych niniejszą polityką zasad ochrony danych osobowych w każdym czasie. W zakresie stosowania zasad odnoszących się do pracy w systemach informatycznych, prawo kontroli przysługuje również ASI.

Kierownicy poszczególnych komórek organizacyjnych uprawnieni są do skierowania odpowiedniego wniosku do administratora danych osobowych albo IOD, jeżeli ten został powołany, w przypadku zaistnienia potrzeby wprowadzenia zmian w niniejszej polityce i zmiany obowiązujących zasad przetwarzania danych osobowych.

W zakresie nieuregulowanym w niniejszej polityce, zastosowanie znajdują postanowienia RODO i UODO. Dokonuje się okresowych przeglądów zgodności niniejszej polityki z powszechnie obowiązującymi przepisami prawa, nie rzadziej jednak niż raz na 6 miesięcy.

Następujące dokumenty stanowią integralną część niniejszej polityki:

- Załącznik nr 1 - wzór rejestru czynności przetwarzania;
- Załącznik nr 2 - wzór upoważnienia do przetwarzania danych osobowych;
- Załącznik nr 3 – wzór ewidencji osób upoważnionych do przetwarzania danych osobowych;
- Załącznik nr 4 – wzór raportu o stwierdzonym incydencie.