Polityka bezpieczeństwa
ochrony danych osobowych i zarządzania systemem informatycznym
w CSMART

Polityka bezpieczeństwa ochrony danych osobowych i zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych użytkowników serwisów i aplikacji internetowych należących do CSMART Katarzyna Meyza (dalej CSMART), zwana dalej „Polityką bezpieczeństwa", określa sposób zarządzania i zabezpieczania danych osobowych użytkowników oraz zasady administrowania systemem informatycznym służącym do przetwarzania tych danych osobowych, dla celów świadczonych przez CSMART usług.

1.

Podstawa prawna.

Polityka bezpieczeństwa stworzona została na podstawie następujących obowiązujących przepisów:

1. ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;

2. rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

2.

Szczegółowe regulacje.

Polityka bezpieczeństwa określa:

1. Miejsca przechowywania i przetwarzania danych osobowych.
2. Wykaz zbiorów danych osobowych. Programy wykorzystywane do przetwarzania danych.
3. Struktura zbiorów. Sposób przepływu danych między zbiorami.
4. Sposób przechowywania dokumentów zawierających dane osobowe. Zabezpieczenia i organizacja dla potrzeb zapewnienia poufności danych osobowych.
5. Zasady tworzenia i posługiwania się hasłami dostępu do systemów informatycznych.
6. Sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności.
7. Obowiązki administratora danych osobowych.
8. Procedury pracy w systemie informatycznym.
9. Sposób i miejsce przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.
10. Zasady niszczenia i sposoby dokumentowania procesu niszczenia nośników informacji zawierających dane osobowe. Zasady postępowania w zakresie komunikacji sieciowej.
11. Zasady zabezpieczenia, wykonywanie przeglądów i konserwacji systemów służących do przetwarzania danych osobowych.
12. Zasady rejestrowania i wyrejestrowania użytkowników systemu informatycznego, zakres odpowiedzialności administratora systemu, zasady dopuszczania pracowników do eksploatacji systemów informatycznych przetwarzających zbiory danych osobowych, zasady prowadzenia ewidencji

pracowników, którzy wykonują czynności związane z przetwarzaniem danych osobowych.

13. Procedury tworzenia kopii zapasowych.

3.

Terminologia

Użyte w Polityce bezpieczeństwa terminy oznaczają:

1. dane osobowe – każda informacja dotycząca zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
2. zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie czy zestaw ten jest rozproszony czy podzielony funkcjonalnie, w którym dane są przetwarzane, w szczególności w:
   a) kartotekach,
   b) skorowidzach,
   c) księgach,
   d) wykazach,
   e) rejestrach,
   f) systemach informatycznych itp.;
3. przetwarzanie danych – wszelkie operacje wykonywane na danych osobowych i ich zbiorach, w szczególności: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, także w formie elektronicznej;
4. usuwanie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalanie tożsamości osoby, której dane dotyczą;
5. administrator danych osobowych (administrator) – podmiot zajmujący się przetwarzaniem danych osobowych;
6. administrator bezpieczeństwa informacji (ABI) – podmiot, którego zadaniem jest zastępowanie administratora danych osobowych we wszelkich sprawach dotyczących ochrony danych osobowych;
7. system informatyczny – zespół współpracujących ze sobą urządzeń, programów i procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
8. zabezpieczanie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
9. odbiorca danych – każdy komu udostępnia się dane osobowe z wyłączeniem:
   a) osoby której dane dotyczą,
   b) osoby upoważnionej do przetwarzania danych,
   c) podmiotu przetwarzającego dane w drodze umowy zawartej na piśmie,
   d) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

4.

Miejsca przechowywania i przetwarzania danych osobowych.

Sposób przechowywania dokumentów zawierających dane osobowe.

Zabezpieczenia i organizacja dla potrzeb zapewnienia poufności danych osobowych.

1. Dane osobowe przechowywane są i przetwarzane w siedzibie CSMART, tj. 7 Kings Avenue, M8 5AS Manchester, United Kingdom. Dane przechowywane są zarówno w formie papierowej, jak i elektronicznej.
2. Dokumenty zawierające dane osobowe przechowywane są w formie elektronicznej na dyskach komputerowych lub w formie papierowej w teczkach osobowych, w sposób uniemożliwiający osobom niepowołanym dostęp do danych osobowych innych osób, w miejscach odpowiednio zabezpieczonych przed nieuprawnionym ich przejęciem, modyfikacją lub zniszczeniem.
3. Dane osobowe znajdujące się w siedzibie CSMART nie mogą być wynoszone przez użytkowników poza jej obszar bez pisemnego upoważnienia administratora danych osobowych. Upoważnienie to nie może być wyrażone w formie ogólnej, a wyłącznie do poszczególnego, każdorazowo uzasadnionego okolicznościami przypadku.
4. Podmioty współpracujące z CSMART zobowiązane są umownie do przestrzegania poufności przekazywanych im danych i wykorzystywania ich wyłącznie w celach związanych z realizacją umów.
5. Dostęp do danych osobowych CSMART mają wyłącznie osoby pisemnie do tego upoważnione przez administratora danych osobowych.
6. Osoby upoważnione do dostępu do danych osobowych i ich przetwarzania zobowiązane są do:
   a) wykorzystywania danych osobowych zgodnie z prawem,
   b) zbierania danych osobowych wyłącznie dla celów określonych Polityce bezpieczeństwa,
   c) aktualizowania danych osobowych i dbania by ich treść była zgodna ze stanem faktycznym,
   d) wykorzystywania danych osobowych nie dłużej, niż wymaga tego realizacja celu dla którego zostały zgromadzone.
7. Obsługa interesantów CSMART odbywa się w sposób uniemożliwiający dostęp do danych osobowych osób innych niż sam zainteresowany. Dotyczy to zarówno sposobu pracy z dokumentami zawierającymi dane osobowe wyłącznie w danej chwili niezbędnymi, jak i odpowiedniego usytuowania monitorów komputerowych w sposób uniemożliwiający dostęp do danych osobom nieupoważnionym.
8. W przypadku chwilowego opuszczania pomieszczeń, w których przetwarzane są dane osobowe, powinny być one zamykane w sposób uniemożliwiający dostanie się osobie nieuprawnionej.
9. W pomieszczeniach, w których przetwarzane są dane osobowe osoby trzecie mogą przebywać wyłącznie w obecności osób upoważnionych przez administratora.
10. Pomieszczenia, w których przechowywane są dane osobowe muszą być zamykane w przypadku opuszczania pomieszczenia przez osoby uprawnione, chyba że zbiory danych osobowych umieszczone są w miejscu niedostępnym, jak np. kasa pancerna, sejf itp. Miejsca takie muszą być każdorazowo po użyciu zamykane, a klucze przechowywane w sposób niedostępny dla osób nieuprawnionych.
11. Dane archiwizowane nie mogą być przechowywane w tych samych miejscach co dane wykorzystywane do bieżącej działalności CSMART.

5.

Wykaz zbiorów danych osobowych.

Programy wykorzystywane do przetwarzania danych.

Struktura zbiorów. Sposób przepływu danych między zbiorami.

1. CSMART prowadzi zbiory danych osobowych w postaci:

a) *wykazu osób korzystających z usług oferowanych przez należące do CSMART serwisy internetowe,*

b) *danych niezbędnych do obliczania opłat za korzystanie z serwisów internetowych należących do CSMART,*

c) *indywidualnych rozliczeń pomiędzy użytkownikami serwisów internetowych należących do CSMART a CSMART,*

d) …

2. Dane pomiędzy zbiorami przekazywane są zarówno w formie papierowej, jak i elektronicznej.

3. Dla potrzeb przetwarzania danych w CSMART wykorzystuje się następujące programy komputerowe:

a) ...

6.

Zasady tworzenia i posługiwania się hasłami dostępu do systemów informatycznych.

Sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany

oraz osoby odpowiedzialne za te czynności.

1. Użytkownik posiada bezpośredni dostęp do danych osobowych w systemie informatycznym po podaniu nazwy użytkownika, tzw. „loginu” oraz właściwego hasła.
2. Stworzone hasło powinno składać się z co najmniej 8 znaków, w tym jednej dużej litery i cyfry.
3. Użytkownicy nie mogą korzystać z innych nazw użytkowników niż te, do których są upoważnieni.
4. Zmiana hasła następuje co najmniej raz na pół roku. O każdorazowej zmianie hasła Użytkownik jest informowany przez administratora danych osobowych lub ABI.

7.

Obowiązki Administratora danych osobowych.

1. Administratorem danych osobowych jest CSMART, a w jej imieniu Zarząd spółki.
2. Administrator zapoznaje użytkowników z przepisami o ochronie danych osobowych oraz wykazem akt i wiadomości, które stanowią tajemnicę służbową.
3. Administrator prowadzi ewidencję osób posiadających dostęp do danych osobowych w jednostce.
4. Administrator posiada hasła do systemu, które podlegają szczególnej ochronie.
5. Administrator przyznaje użytkownikowi indywidualne hasło przed pierwszym logowaniem do systemu zawierającego dane osobowe. Hasło jest zmieniane przez administratora co najmniej raz na pół roku, o czym informuje on poszczególnych użytkowników.
6. Administrator danych osobowych wyznacza administratora bezpieczeństwa informacji (ABI) w CSMART, którego zadaniem jest zastępowanie administratora danych

osobowych we wszelkich sprawach dotyczących ochrony danych osobowych, a w szczególności:

a) nadzorowanie przestrzegania zasad ochrony danych w CSMART;
b) prowadzenie ewidencji użytkowników systemu informatycznego;
c) rejestracja i wyrejestrowanie użytkownika systemu informatycznego;
d) zapewnienie bezpieczeństwa i poufności danych, w tym zabezpieczenie ich przed ujawnieniem;
e) zabezpieczenie danych przed nieuprawnionym dostępem;
f) zabezpieczenie danych przed nieuprawnionym pozyskaniem;
g) zabezpieczenie przed utratą danych;
h) zabezpieczenie przed uszkodzeniem lub zniszczeniem danych oraz przed ich nielegalną modyfikacją.

7. Administratorem bezpieczeństwa informacji (ABI) w CSMART jest Michał Meyza..

8.

Procedury pracy z systemem informatycznym.

1. Dostęp do systemu informatycznego może mieć wyłącznie użytkownik wpisany do ewidencji obowiązującej w jednostce i dopuszczony przez administratora.

2. Użytkownik podejmujący pracę z systemem winien jest przestrzegać procedur, które mają na celu zabezpieczenie przetwarzanych danych osobowych. Procedury te polegają w szczególności na:

a) obowiązku każdorazowego zamknięcia aplikacji i wylogowania się z pracy w sieci przed opuszczeniem stanowiska;
b) obowiązku każdorazowego zamknięcia pomieszczenia, w którym przechowywane są dane osobowe po zakończeniu pracy;
c) zakazie samowolnego tworzenia kopii danych z systemu informatycznego.

3. Komputery służące do przetwarzania danych osobowych muszą być zabezpieczone przed utratą danych osobowych spowodowaną awarią zasilania.

4. Komputery służące do przetwarzania danych osobowych muszą być zabezpieczone przed dostępem osób trzecich, w tym poprzez połączenia sieciowe, a także przed zagrożeniami elektronicznymi takimi jak wirusy, programy szpiegujące itp.

9.

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

1. Kopie zapasowe i elektroniczne nośniki informacji zawierające dane osobowe powinny być przechowywane w siedzibie spółki lub w specjalnie wyznaczonym do tego celu miejscu poza jej siedzibą.
2. Miejsce, w którym przechowywane są kopie zapasowe i elektroniczne systemy danych, musi być odpowiednio zabezpieczone przed nieuprawnionym ich przejęciem, modyfikacją lub zniszczeniem.
3. Komputery przenośne znajdujące się w siedzibie lub oddziale jednostki nie mogą być wynoszone przez użytkowników poza jej obszar, bez wyraźnego upoważnienia administratora danych. Upoważnienie to może być wyrażone wyłącznie w formie pisemnej.

10.

Zasady niszczenia i sposoby dokumentowania procesu niszczenia nośników informacji zawierających dane osobowe. Zasady postępowania w zakresie komunikacji sieciowej.

1. Nośniki papierowe nie przeznaczone do ponownego użytku oraz nie archiwizowane należy natychmiast niszczyć w sposób trwały i uniemożliwiający odczytanie.

2. Jeżeli usunięcie danych osobowych z nośników magnetycznych nie jest możliwe, wówczas nośniki muszą zostać uszkodzone w sposób uniemożliwiający ich odczytanie.

3. Proces niszczenia kopii zapasowych powinien odbywać się komisyjnie i musi być dokumentowany. W przypadku tworzenia kopii awaryjnych nakazuje się niszczyć je bez zbędnej zwłoki po ustaniu ich użyteczności.

4. Przeglądarka internetowa oraz program do obsługi poczty elektronicznej muszą być ustawione w taki sposób, by nie zapamiętywały nazwy użytkownika oraz hasła.

11.

Zasady zabezpieczenia, wykonywanie przeglądów i konserwacji systemów służących do przetwarzania danych.

1. Na wszystkich komputerach wykorzystywanych w danej jednostce musi być zainstalowane oprogramowanie posiadające aktualne licencje, aktualizacje, certyfikaty legalności itp.

2. Za legalność użytkowanego oprogramowania specjalistycznego odpowiedzialny jest użytkownik systemu.

3. Do usuwania wirusów, używa się programów antywirusowych, które są dostępne w danej jednostce.

12.

Zasady rejestrowania i wyrejestrowania użytkowników systemu informatycznego. Zasady dopuszczania pracowników do eksploatacji systemów informatycznych przetwarzających zbiory danych osobowych. Zasady prowadzenia ewidencji pracowników, którzy wykonują czynności związane z przetwarzaniem danych osobowych.

1. Rejestracji i wyrejestrowania użytkownika systemu informatycznego dokonuje administrator w prowadzonej przez niego ewidencji.
2. Ewidencja osób posiadających dostęp do danych osobowych zawiera m.in.: dane personalne pracownika, oznaczenie komórki organizacyjnej, nazwę użytkowanego programu, datę wprowadzenia do rejestru, datę usunięcia z rejestru, ważność upoważnienia itp. Zmiana danych użytkownika podlega odnotowaniu w ewidencji.
3. Każdy użytkownik upoważniony do pracy w systemie informatycznym, w którym przetwarzane są dane osobowe, powinien posiadać własny odrębny identyfikator i hasło dostępu.
4. Rozwiązanie stosunku pracy, bądź zmiana zakresu obowiązków powoduje utratę dostępu do przetwarzania danych i natychmiastowe wyrejestrowanie użytkownika z systemu oraz wykreślenie z ewidencji.
5. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, które służą do zbierania lub przetwarzania danych osobowych zostają dopuszczeni wyłącznie pracownicy, którzy posiadają

ważne upoważnienia.

13.

Procedury tworzenia kopii zapasowych

1. Kopie zapasowe zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania powinny być wykonywane przynajmniej raz na tydzień przez administratora.

2. Kopie zapasowe powinny być zarejestrowane nośnikach magnetycznych, odpowiednio opisanych, oznakowanych i ewidencjonowanych a każdy proces wykonywania kopii zapasowej powinien być osobno dokumentowany.

3. Administrator zobowiązany jest przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odtworzenia danych zapisanych na tych kopiach pod kątem ewentualnej przydatności w sytuacji awarii systemu.

4. Dane z kopii zapasowych powinny być odtwarzane wyłącznie przez administratora.

14.

Postanowienia końcowe

1. Osoba wpisana do ewidencji zobowiązana jest do odbycia szkolenia w zakresie ochrony danych osobowych oraz zapoznania się z Polityką bezpieczeństwa i aktami prawnymi w niej wymienionymi.
2. Wykonanie powyższych zobowiązań użytkownik potwierdza oświadczeniem własnoręcznie podpisanym, które wraz z upoważnieniem umieszcza się w aktach osobowych pracownika.
3. W kwestiach nieuregulowanych w Polityce bezpieczeństwa zastosowanie mają odpowiednie przepisy obowiązujących aktów prawnych.
4. Niniejsza Polityka bezpieczeństwa wchodzi w życie w dniu jej uchwalenia przez Zarząd spółki CSMART.