Zgłoszenie zbioru danych
do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych

Zgodnie z obowiązującymi przepisami wynikającymi z Ustawy o ochronie danych osobowych przygotowaliśmy dla Państwa wzór, który może stanowić pomoc w wypełnianiu części E i części F ze ZGŁOSZENIA ZBIORU DANYCH DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH.

Zestawienie dotyczy *Opisu środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* stosowanych przez firmę SOKRATES-software dla bibliotek powierzających przetwarzanie danych osobowych (wypożyczalnia)i korzystających z usługi hostingu.

Firma SOKRATES-software, w oparciu o umowę świadczenia usług dostępu do baz danych zawartą z Państwem staje się – z mocy ustawy Art. 31.1 – podmiotem przetwarzającym dane osobowe.

Niniejszy dokument jest informacją o środkach, jakie stosuje firma SOKRATES-software dla spełnienia wymogów zawartych w Art. 36 do 39 ustawy. W tym zakresie ponosimy odpowiedzialność taką jak administrator danych (Art. 31.3).

Nadal jednak administratorem danych pozostaje Biblioteka. To na niej spoczywa odpowiedzialność za przestrzeganie przepisów ustawy (Art. 31.4).

Wybrane opcje oznaczono poprzez podkreślenie i **pogrubienie.**

15. Zbiór danych osobowych jest prowadzony:

a)

centralnie,

w architekturze rozproszonej,

b)

wyłącznie w postaci papierowej,

z użyciem systemu informatycznego,

c)

z użyciem co najmniej jednego urządzenia systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną (np. Internetem),

bez użycia żadnego z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną (np. Internetem).

16. Zostały spełnione wymogi określone w art. 36-39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych:

a)

został wyznaczony administrator bezpieczeństwa informacji nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych,

administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji,

b)

do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych

c)

prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,

d)

została opracowana i wdrożona polityka bezpieczeństwa,

e)

została opracowana i wdrożona instrukcja zarządzania systemem informatycznym,

f)

inne środki, oprócz wymienionych w ppkt a - e, zastosowane w celu zabezpieczenia danych:

Środki ochrony fizycznej danych:

Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).

Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min.

Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.

Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.

Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.

Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu.

Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.

Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.

Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez cała dobę jest nadzorowany przez służbę ochrony.

Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie.

Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie.

Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym sejfie lub kasie pancernej.

Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie.

Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej metalowej szafie.

Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej.

Zbiory danych osobowych przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach.

Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.

Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego.

Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.

Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.

Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.

Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena.

Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej.

Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.

Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.

Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.

Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.

Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.

Zastosowano procedurę oddzwonienia (callback) przy transmisji realizowanej za pośrednictwem modemu.

Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.

Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.

Użyto system Firewall do ochrony dostępu do sieci komputerowej.

Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

Środki ochrony w ramach narzędzi programowych i baz danych:

Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.

Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.

Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

Dostęp do zbioru danych osobowych wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN lub tokena.

Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem technologii biometrycznej.

Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.

Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.

Zastosowano kryptograficzne środki ochrony danych osobowych.

Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Środki organizacyjne:

Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.

Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.

Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.

Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

Administrator danych prowadzący zbiór w systemie tradycyjnym (papierowym) zobowiązany jest do zastosowania środków określonych w pkt 16 ppkt a - d, a w przypadku prowadzenia zbioru w systemie informatycznym ponadto środka określonego w pkt 16 ppkt e.

Część F.

Informacja o sposobie wypełnienia warunków technicznych i organizacyjnych, o których mowa w rozporządzeniu 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 (Dz. U. Nr 100, poz. 1024)

17. Zastosowano środki bezpieczeństwa na poziomie:

podstawowym,

podwyższonym,

wysokim,