

Z/P-072/192/13/21010

**Generalny Inspektor
Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa**

W odpowiedzi na pismo z dnia 03.09.2013r. DOLiS-035-2245/13/HH/56279, uprzejmie informuję, iż w Zakładzie Karnym w [] informacje oraz dane osobowe gromadzone są przede wszystkim w Centralnej Bazie Danych Osób Pozbawionych Wolności Noe.NET oraz aktach ewidencyjnych i teczkach osobopoznawczych osób pozbawionych wolności. Ponadto dane adresowe osób innych niż pozbawione wolności zamieszczane są zgodnie ze wzorami druków m.in. w „Książce doręczeń paczek”, „Książce ruchu osób i pojazdów”, prośbach o wydanie sprzętu z magazynu (osadzony podaje w prośbie imię i nazwisko oraz dokładny adres osoby, która dokona odbioru sprzętu).

W tutejszej jednostce stosowana jest Polityka Bezpieczeństwa Danych Osobowych Przetwarzanych, która obejmuje przetwarzanie danych osobowych przez Zakład Karny w [] oraz zawiera informacje, dotyczące rozpoznania procesów, ich przetwarzania oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.

Dane osobowe przetwarzane w Zakładzie Karnym w [] zabezpieczane są zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Zakład Karny w [] stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. Zabezpiecza dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, zmianę, utratę, uszkodzenie, lub zniszczenie.

Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przed administratorem danych osobowych – Dyrektora Jednostki. Osoby, które zostały upoważnione, są obowiązane zachować w tajemnicy te dane oraz sposób ich zabezpieczania. Osoby przetwarzające dane osobowe mają obowiązek zabezpieczać dane osobowe, a w szczególności:

- chronić dane osobowe przed osobami nieupoważnionymi do ich przetwarzania,
- zabezpieczać przetwarzane dane osobowe w formie papierowej, stosować „politykę czystego biurka” tak aby osoby nieupoważnione wchodzące do pomieszczenia nie miały możliwości zapoznać się z dokumentami zawierającymi dane osobowe,

- przed wyjściem z pomieszczenia zabezpieczyć dokumenty zawierające dane osobowe umieszczając je w zamykanej na klucz szafie, biurku lub innym przeznaczonym do tego celu bezpiecznym miejscu,
- po opuszczeniu pomieszczenia, jeżeli pozostaje ono puste, zamknąć drzwi na klucz,
- przeznaczone do niszczenia dokumenty zawierające dane osobowe niszczyć w sposób uniemożliwiający odczytanie zawartych w nich danych, w przeznaczonych do tego celu niszczarkach dokumentów,
- nie wnosić dokumentów zawierających dane osobowe poza obszar przetwarzania bez zgody ABI lub ADO i WZDO

Osoby przetwarzające dane osobowe w systemie informatycznym mają obowiązek zabezpieczać dane osobowe, a w szczególności:

- uniemożliwiać odczytanie danych osobowych zawartych w systemie informatycznym osobom przebywającym w pomieszczeniu i nieupoważnionym do ich przetwarzania poprzez zamykanie dokumentów i aplikacji zawierających dane osobowe lub ustawienie monitora w sposób uniemożliwiający ich odczytanie
- zabezpieczać system informatyczny na czas nieobecności w pomieszczeniu poprzez wyłączenie, zablokowanie komputera lub wylogowanie się z systemu, a po zakończeniu pracy każdorazowe wyłączenie komputera zgodnie z obowiązującymi w Zakładzie procedurami,
- nie kopiować dane osobowe na nośniki zewnętrzne,
- nie wnosić danych osobowych znajdujących się na komputerach przenośnych lub nośnikach zewnętrznych poza obszar przetwarzania,
- nie używać zewnętrznych nośników danych, nie będących nośnikami służbowymi,
- przed użyciem w systemie informatycznym zewnętrznego nośnika danych, każdorazowo sprawdzić go programem antywirusowym,

Wszelkie pliki z danymi osobowymi przesyłane na zewnątrz, przez łącza publiczne są chronione w sposób uniemożliwiający ich odczytanie osobom nieupoważnionym. Komunikacja użytkowników, łączących się z systemem informatycznym przez Internet odbywa się przy pomocy bezpiecznych protokołów sieciowych w szczególności: szyfrowanie dedykowane połączenia, fizyczne i logiczne zabezpieczenia komunikacji w sieci teleinformatycznej.

W Zakładzie Karnym w [] nie dopuszcza się, aby osoby postronne miały wgląd do dokumentacji zawierającej dane osobowe osób pozbawionych wolności. Udzielanie informacji lub udostępnienie danych osobowych o osobach pozbawionych wolności może nastąpić wyłącznie na podstawie pisemnego wniosku uprawnionego wnioskodawcy – osoby najbliższej albo podmiotu ustawowo uprawnionego. Szczegółowo regulują to przepisy art 24 ust. 3 i 4 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej, oraz rozporządzenia Ministra Sprawiedliwości z dnia 29 lipca 2010 r. w sprawie trybu składania oraz wzoru wniosku o udzielenie informacji lub udostępnienia danych osobowych o osobie obecnie lub uprzednio pozbawionej wolności w areszcie śledczym lub zakładzie karnym.

Zasady przechowywania, sposób archiwizowania i likwidacji dokumentów papierowych, odbywają się zgodnie z obowiązującymi przepisami i są to: przepisy kancelaryjne, rzeczowy wykaz akt oraz instrukcja archiwalna.

W toku prowadzonych czynności wyjaśniających ustalono ponadto, iż przeznaczone do niszczenia dokumenty zawierające dane osobowe, wytworzone przez poszczególne działy i służby, są niszczone w sposób uniemożliwiający odczytanie zawartych w nich danych. Dokumenty niszczone są trwale w przeznaczonych do tego celu niszczarkach dokumentów.