INSTRUKCJA
WYMOGI JAKIM PODLEGAJĄ OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH W ZAKRESIE ZAPEWNIENIA BEZPIECZEŃSTWA DANYCH

Osoby upoważnione do czynności związanych z przetwarzaniem danych osobowych zobowiązane są do zachowania następujących reguł bezpieczeństwa:

1) powstrzymywania się od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu oraz instalowania nieautoryzowanego oprogramowania, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
2) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);
3) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);
4) zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
5) przestrzegania indywidualnych uprawnień i realizacji obowiązków w zakresie przetwarzania danych osobowych, w szczególności właściwego korzystania z powierzonych sprzętów i udostępnionych zasobów oraz używania wyłącznie własnego identyfikatora i hasła;
6) odpowiedniego zabezpieczenia identyfikatora i hasła wymaganego do uwierzytelnienia się w systemie oraz nieudostępniania go innym osobom;
7) zachowania danych osobowych i sposobu ich zabezpieczenia w tajemnicy, w tym także wobec osób najbliższych;
8) ustawiania ekranów komputerowych tak, by osoby nieuprawnione nie widziały treści wyświetlanych na ekranie;
9) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
10) niepozostawiania bez kontroli włączonych urządzeń zawierających dane osobowe oraz niezabezpieczonych dokumentów (czasowe opuszczania stanowiska pracy jest dopuszczalne dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu urządzenia w inny sposób);
11) niszczenia niepotrzebnych wydruków i kopii dokumentów po ich wykorzystaniu oraz kasowania po wykorzystaniu danych z dysków przenośnych;
12) przekazywania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;
13) zapisywanie plików lub wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;
14) kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;
15) zadbanie o odpowiednie zabezpieczenie wszelkich dokumentów i wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy (np. w szafie zamykanej na klucz) – tzw. polityka czystego biurka
16) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
17) zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
18) zamykania drzwi na klucz po zakończeniu pracy w danym dniu i złożenia klucza na portierni.

2. Komputery przenośne i praca poza siedzibą administratora

1) Wynoszenie poza obszar przetwarzania danych urządzeń i dokumentów zawierających dane osobowe jest dopuszczalne jedynie za wiedzą i zgodą inspektora ochrony danych lub bezpośredniego przełożonego, gdy konieczność taka została uzgodniona z inspektorem ochrony danych.
2) Urządzenia zawierające dane osobowe wynoszone poza obszar przetwarzania danych należy chronić przed uszkodzeniami fizycznymi. Należy też bezwzględnie przestrzegać zaleceń producentów dotyczących ochrony sprzętu. W szczególności należy pamiętać, że urządzenia elektroniczne mogą

ulec uszkodzeniu w skutek działanie silnego pola elektromagnetycznego i chronić je przed takim oddziaływaniem.

3) Urządzenia przenośne, nośniki danych oraz dokumenty wynoszone poza obszar przetwarzania danych nie powinny być pozostawiane bez nadzoru. W szczególności zabrania się pozostawiania urządzeń i dokumentów zawierających dane osobowe bez odpowiedniego zabezpieczenia w miejscach publicznych, pokojach hotelowych oraz w samochodach.

4) Wykorzystywanie urządzeń przenośnych, nośników danych oraz dokumentów zawierających dane osobowe w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko utraty, zniszczenia lub zapoznania się z danymi przez osoby nieupoważnione. Za miejsca szczególnego ryzyka należy uznać restauracje oraz środki komunikacji publicznej.

5) Niedozwolone jest udostępnianie urządzeń przenośnych i nośników danych należących do administratora danych osobom nieupoważnionym, w tym domownikom i osobom bliskim użytkownika. Użytkownik obowiązany jest zachować w tajemnicy wobec wszystkich osób, w tym wobec domowników i osób bliskich identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym administratora danych lub chroniącym dostęp do nośników danych.

6) Administrator systemu w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa termin i zasady zwrotu sprzętu.

Inspektor Ochrony Danych
Dr Marta Macełko