

Zarządzenie nr 39
Dyrektora Generalnego Lasów Państwowych
z dnia 18 września 2014 r.

w sprawie polityki bezpieczeństwa danych osobowych
w Dyrekcji Generalnej Lasów Państwowych

Znak spr.: GK-1241- 1 /14

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) i rozporządzenia 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) oraz § 6 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe, nadanego zarządzeniem nr 50 Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 18 maja 1994 r. zarządzam, co następuje:

§ 1

W celu:

- 1) ochrony danych osobowych przetwarzanych - przez osoby upoważnione - w formie tradycyjnej oraz w systemach informatycznych;
- 2) zabezpieczenia danych osobowych przed dostępem osób nieuprawnionych;
- 3) ochrony danych osobowych przed ich zabraniem przez osoby nieuprawnione, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

wprowadza się do stosowania w Dyrekcji Generalnej Lasów Państwowych politykę bezpieczeństwa danych osobowych, zwaną w dalszej części „Polityką bezpieczeństwa”, która stanowi zbiór zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych, określonych niniejszym zarządzeniem.

§ 2

1. Zakres „Polityki bezpieczeństwa” obejmuje wszystkie obszary, w których przetwarzane są dane osobowe, tj. jakiejkolwiek operacje wykonywane na danych osobowych, czyli utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
2. „Polityka bezpieczeństwa” opisuje procedury bezpieczeństwa danych osobowych zawartych w zbiorach tradycyjnych (papierowych) oraz w systemach informatycznych Dyrekcji Generalnej Lasów Państwowych, które określają granice dopuszczalnego zachowania wszystkich użytkowników systemu informatycznego Dyrekcji Generalnej Lasów Państwowych. Polityka bezpieczeństwa zawiera również opis konsekwencji, jakie mogą ponieść osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

§ 3

„Polityka bezpieczeństwa” zapewnia ochronę wszystkich danych osobowych przetwarzanych w Dyrekcji Generalnej Lasów Państwowych przez osoby upoważnione.

§ 4

„Polityka bezpieczeństwa” zawiera:

- 1) wykaz budynków oraz pomieszczeń stanowiących obszar, gdzie przetwarzane są dane osobowe (załącznik nr 1);
- 2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz struktury zbiorów danych osobowych (załącznik nr 2);
- 3) sposób przepływu danych pomiędzy poszczególnymi systemami (załącznik nr 3);
- 4) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (załącznik nr 4);
- 5) wzór upoważnienia do przetwarzania danych osobowych (załącznik nr 5);
- 6) wzór ewidencji osób upoważnionych do przetwarzania danych osobowych (załącznik nr 6);
- 7) instrukcję postępowania w sytuacji naruszenia bezpieczeństwa przetwarzania danych osobowych (załącznik nr 7);
- 8) wzór raportu z naruszenia bezpieczeństwa danych osobowych w Dyrekcji Generalnej Lasów Państwowych (załącznik nr 8).

§ 5

Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowią instrukcje SILP.

§ 6

1. Administratorem danych jest Dyrekcja Generalna Lasów Państwowych reprezentowana przez Dyrektora Generalnego Lasów Państwowych.
2. Administrator danych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:
 - 1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych,
 - 2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnym zakresie, odpowiadającym zakresowi ich obowiązków,
 - 3) odrębnym dokumentem wyznacza Administratora Bezpieczeństwa Informacji,
 - 4) odrębnym dokumentem wyznacza Administratora Systemu Informatycznego,
 - 5) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpieczeństwa przetwarzania danych osobowych.

§ 7

Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych w Dyrekcji Generalnej Lasów Państwowych, tj.:

- 1) sprawuje nadzór nad wdrożeniem stosownych środków technicznych, tj.:
 - a) prawidłowego wydawania kluczy do pomieszczeń przetwarzania danych;
 - b) prawidłowego zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe;
 - c) prawidłowego zabezpieczenia danych w formie papierowej;
- 2) sprawuje nadzór nad stosowaniem środków organizacyjnych, tj.:
 - a) prowadzi ewidencję osób upoważnionych, zgodnie z załącznikiem nr 6;
 - b) przygotowuje upoważnienia do przetwarzania danych osobowych zgodnie z załącznikiem nr 5;
- 3) koordynuje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych,
- 4) przygotowuje projekty zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz odpowiada za korespondencję z Generalnym Inspektorem oraz Biurem Generalnego Inspektora Ochrony Danych Osobowych,
- 5) przygotowuje projekty zmian niniejszego zarządzenia, w szczególności w przypadku zmian organizacyjnych w Dyrekcji Generalnej Lasów Państwowych oraz zmian przepisów o ochronie danych osobowych,
- 6) zapoznaje pracowników z procedurami przetwarzania danych osobowych.

§ 8

Administrator Systemu Informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Dyrekcji Generalnej Lasów Państwowych, w tym zwłaszcza:

- 1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z poziomu administratora,
- 2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego,
- 3) zakłada konta oraz przydziela uprawnienia upoważnionym użytkownikom zgodnie z przekazanym wnioskiem i na podstawie wewnętrznych regulacji dotyczących zarządzania systemami informatycznymi,
- 4) dokonuje wyrejestrowania użytkowników z systemu informatycznego zgodnie z przekazanym wnioskiem i na podstawie wewnętrznych regulacji dotyczących zarządzania systemami informatycznymi,
- 5) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
- 6) w sytuacjach stwierdzenia naruszenia zabezpieczeń systemu informatycznego, informuje Administratora Bezpieczeństwa Informacji o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,

- 7) sprawuje nadzór nad:
 - a) wykonywaniem napraw, konserwacji oraz likwidacji urządzeń komputerowych,
 - b) wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
- 8) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

§ 9

Kierownicy komórek organizacyjnych Dyrekcji Generalnej Lasów Państwowych:

- 1) nadzorują bezpieczeństwo przetwarzania danych osobowych w swoich komórkach organizacyjnych,
- 2) informują Administratora Bezpieczeństwa Informacji o przetwarzaniu nowych zbiorów danych osobowych – nie ujętych w załączniku nr 2,
- 3) kierują do Administratora Bezpieczeństwa Informacji wnioski o zgłoszenie zbiorów danych osobowych do Generalnego Inspektora Ochrony Danych Osobowych,
- 4) składają wniosek (w formie pisemnej lub mailem), do Administratora Bezpieczeństwa Informacji o przygotowanie upoważnienia dla pracownika przystępującego do pracy na stanowisku, na którym przetwarzane są dane osobowe,
- 5) zgłaszają potrzebę odwołania lub zmiany upoważnienia do przetwarzania danych osobowych do Administratora Bezpieczeństwa Informacji.

§ 10

Każdy pracownik zobowiązany jest do:

- 1) przestrzegania zasad przetwarzania danych osobowych zapisanych w Polityce bezpieczeństwa,
- 2) przekazywania Administratorowi Bezpieczeństwa Informacji wszelkich problemów związanych z ochroną danych osobowych,
- 3) informowania Administratora Bezpieczeństwa Informacji o zmianach zaistniałych w przetwarzanych zbiorach,
- 4) niezwłocznego powiadomienia Administratora Bezpieczeństwa Informacji w sytuacji, gdy pracownik uzna, że dane osobowe zostały bądź są bezprawnie przetwarzane.

§ 11

1. Wewnętrzne audyty, o których mowa w § 7 pkt 3, przeprowadzane są nie częściej niż raz w roku.
2. Audyt przeprowadza się w celu:
 - 1) stwierdzenia stanu wykonania przepisów o ochronie danych osobowych,

- 2) identyfikacji i oceny istniejących mechanizmów ochrony pod kątem ich zgodności z obowiązującymi wymaganiami prawnymi.
3. Audyt stanowi przegląd i ocenę działania środków organizacyjnych, fizycznych oraz technicznych w celu:
 - 1) weryfikacji adekwatności zastosowanych środków,
 - 2) sprawdzenia, czy system ochrony danych osobowych działa zgodnie z wprowadzonymi procedurami,
 - 3) porównania zgodności z aktualnymi wymaganiami prawnymi,
 - 4) oceny funkcjonowania przyjętych procedur.
4. Po czynnościach audytowych tworzy się raport obejmujący wskazanie rozbieżności pomiędzy stanem faktycznym a wymaganiami przepisów o ochronie danych osobowych.

§ 12

Udostępnianie danych osobowych poza Dyрекcyję Generalną Lasów Państwowych odbywa się na wniosek, po uprzednim pisemnym wyrażeniu zgody przez osoby, których dane dotyczą, chyba że obowiązek ten wynika z przepisów prawa.

§ 13

1. O wszystkich przypadkach naruszenia lub podejrzenia naruszenia ochrony danych osobowych użytkownik (pracownik) zobowiązany jest powiadomić Administratora Bezpieczeństwa Informacji, zgodnie z „Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych” (załącznik nr 7).
2. Osoby, które w przypadku naruszenia ochrony danych osobowych, zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia, nie podjęły działania określonego w niniejszym zarządzeniu, a w szczególności nie powiadomiły odpowiedniej osoby zgodnie z tymi zasadami, ponoszą konsekwencje prawne.
3. Przypadki nieuzasadnionego niewykonania obowiązków wynikających z niniejszego zarządzenia mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.
4. Procedury i zasady zawarte w niniejszym zarządzeniu oraz w jego załącznikach obowiązują wszystkich pracowników Dyrekcyj Generalnej Lasów Państwowych. Obowiązują one także stażystów, praktykantów, zleceniobiorców oraz inne osoby, które mają dostęp do przetwarzania danych osobowych w Dyrekcyj Generalnej Lasów Państwowych, jeżeli zobowiązały się pisemnie do ich przestrzegania.

§ 14

Załączniki do niniejszego zarządzenia nie podlegają publikacji.

§ 15

Traci moc zarządzenie nr 37 Dyrektora Generalnego Lasów Państwowych z dnia 14 maja 2008 r. w sprawie ustanowienia „Polityki bezpieczeństwa danych osobowych w Dyrekcji Generalnej Lasów Państwowych”.

§ 16

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR GENERALNY
LASÓW PAŃSTWOWYCH

mgr inż. Adam Wasiak

