ZARZĄDZENIE NR 66 /2015
WOJEWODY ŚWIĘTOKRZYSKIEGO
z dnia 29 lipca 2015 r.

w sprawie powołania Administratora Bezpieczeństwa Informacji i organizacji ochrony danych osobowych w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach

Na podstawie art. 36 i 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r., poz. 1182 z późn.zm.), zarządzam co następuje:

§ 1.1. Administratorem Bezpieczeństwa Informacji zwanym dalej „ABI", w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach od dnia 1 lipca 2015r. jest Pani Agnieszka Lesiak Kierownik Oddziału ds. Organizacyjnych w Wydziale Organizacji i Kadr.

2. Stanowisko ABI podlega bezpośrednio Wojewodzie Świętokrzyskiemu, który pełni funkcję Administratora Danych Osobowych, zwanego dalej „ADO", dla przetwarzanych w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach zbiorów danych osobowych.

3. ABI realizując swoje zadania współpracuje z ADO, wyznaczonymi przez niego Lokalnymi Administratorami Danych Osobowych, zwanymi dalej „LADO", i Administratorami Systemów Informatycznych, zwanymi dalej „ASI" oraz Administratorami Bezpieczeństwa Zbiorów, zwanymi dalej „ABZ" .

4. Upoważniam LADO - kierowników komórek organizacyjnych Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach, wyznaczanych do wykonywania w moim imieniu zadań administratora danych osobowych, określonych w ustawie z dnia 29 sierpnia 1997r. o ochronie danych osobowych, zwanej dalej „u.o.d.o.", w odniesieniu do danych osobowych przetwarzanych w zbiorach danych osobowych prowadzonych w tych komórkach, zgodnie z wydanymi upoważnieniami oraz wydawania dalszych upoważnień dla osób, które przetwarzają dane osobowe.

5. Przetwarzanie danych osobowych w Urzędzie następuje zgodnie z Polityką bezpieczeństwa dla przetwarzanych w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach zbiorów danych osobowych oraz Instrukcją zarządzania systemem informatycznym.

6. Do przetwarzania danych osobowych mogą być dopuszczone osoby, które spełniają łącznie następujące warunki:

1) realizują zadania służbowe wymagające przetwarzania danych osobowych;
2) odbyły szkolenie lub instruktaż z zakresu ochrony danych osobowych;
3) posiadają upoważnienie do przetwarzania danych osobowych.

7. Upoważnienie do przetwarzania danych osobowych nadaje się osobie, która w ramach realizowanych zadań służbowych przetwarza dane osobowe.

8. Upoważnienie do przetwarzania danych osobowych traci ważność w przypadku:

1) zmiany przez osobę upoważnioną komórki organizacyjnej, w której jest zatrudniona;
2) zmiany zakresu obowiązków, w wyniku której osoba utraciła prawo do przetwarzania danych osobowych;
3) rozwiązania stosunku pracy;
4) zakończenia przez osobę upoważnioną świadczenia usług, zakończenia stażu lub praktyki;
5) odwołania upoważnienia;
6) upływu czasu, na który upoważnienie zostało udzielone.

9. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do:

1) zapoznania się z przepisami dotyczącymi ochrony danych osobowych, w tym zarządzeniami oraz z innymi dokumentami opisującymi sposób przetwarzania danych osobowych, do których przetwarzania zostały upoważnione oraz do ich przestrzegania;
2) dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności są obowiązane zapewnić, aby dane te były:
   a) przetwarzane zgodnie z prawem,
   b) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania, z uwzględnieniem przepisów odrębnych dotyczących zasad przechowywania informacji i danych osobowych;
3) zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia;
4) zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem, w szczególności po zakończeniu pracy;
5) korzystania z dostępu wyłącznie do tych zbiorów danych, w tym przetwarzanych w syste-

mach informatycznych, do których dostęp ten wynika z powierzonych jej przez przełożonego obowiązków służbowych i z zakresu upoważnienia;

6) nie tworzenia i nie przechowywania zbędnych kopii zbiorów danych oraz dokumentów zawierających dane osobowe;
7) zabezpieczenia dokumentów i informatycznych nośników danych z danymi osobowymi w przeznaczonych do tego szafach lub pomieszczeniach zgodnie z obowiązującymi w tym zakresie przepisami;
8) przetwarzania danych osobowych w taki sposób, aby osoby nieupoważnione nie widziały oraz nie słyszały treści danych osobowych;
9) opuszczania stanowiska pracy po aktywowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej;
10) informowania przełożonych oraz ABZ o przypadkach naruszenia zasad bezpieczeństwa przetwarzania danych osobowych, przyczynach ich powstania, podjętych działaniach mających na celu zapobieżenie powstania szkód, w tym w szczególności utraty poufności, integralności i dostępności danych osobowych oraz propozycjach mających na celu wyeliminowanie zagrożenia dla bezpieczeństwa danych osobowych w przyszłości;
11) udziału w organizowanych szkoleniach i instruktażach z zakresu ochrony danych osobowych, do odbycia których, zostali wyznaczeni.

10. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do przestrzegania tajemnicy, przez cały czas realizacji zadań, a także po ustaniu stosunku pracy, odwołaniu z pełnionej funkcji, zrealizowaniu umowy lub porozumienia.

§ 2. 1. ABI realizuje zadania z zakresu ochrony danych osobowych, w szczególności jest zobowiązany do:

1) koordynowania w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach czynności dotyczących ochrony danych osobowych wynikających z obowiązujących przepisów prawnych;
2) zapewniania przestrzegania przepisów o ochronie danych osobowych, w szczególności poprzez:
   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla ADO,
   b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 u.o.d.o. oraz przestrzegania zasad w niej określonych,
   c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
3) prowadzenia rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem

zbiorów, o których mowa w art. 43 ust. 1 u.o.d.o., zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7 u.o.d.o.;

4) sprawdzania i opracowywania sprawozdań dla Generalnego Inspektora Danych Osobowych zgodnie z art. 19 b u.o.d.o.;
5) opiniowania i inicjowania wdrażania skutecznych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w szczególności ochronę przed ich udostępnianiem osobom nieuprawnionym, przetwarzaniem z naruszeniem prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w tym opiniowanie i inicjowanie wdrażania skutecznych:
   a) zasad fizycznego zabezpieczenia pomieszczeń przetwarzania danych osobowych,
   b) procedur napraw, konserwacji i likwidacji urządzeń, na których zapisane są dane osobowe,
   c) procedur przydziału identyfikatorów, rejestracji i zarządzania hasłami użytkowników posiadających uprawnienia do przetwarzania danych,
   d) procedur tworzenia, przechowywania i weryfikowania przydatności kopii awaryjnych, na których zapisywane są dane osobowe,
   e) procedur transmisji danych osobowych w sieci komputerowej oraz przesyłania tych danych za pośrednictwem urządzeń teletransmisji,
   f) procedur obiegu oraz przechowywania dokumentów zawierających dane osobowe generowane przez system informatyczny;
6) w sytuacji wystąpienia naruszenia bezpieczeństwa danych prowadzenia analizy okoliczności i przyczyn, które do tego doprowadziły, a także przygotowywanie i przedstawianie ADO propozycji wprowadzenia odpowiednich zmian do Polityki Bezpieczeństwa Informacji, mających na celu wyeliminowanie lub ograniczenie wystąpienia podobnych sytuacji w przyszłości;
7) w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym, niezwłocznego informowania LADO o naruszeniu przepisów ustawy o ochronie danych osobowych oraz nakładania obowiązku naprawienia naruszenia;
8) opiniowania i przekazywania do Generalnego Inspektora Ochrony Danych Osobowych wniosków do rejestracji danych osobowych wrażliwych;
9) nadzoru nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe;
10) nadzoru nad prawidłowością archiwizacji oraz usuwania danych osobowych;
11) wdrażania szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz prowadzenie krótkiego instruktażu dla nowo zatrudnionych pracowników, którzy będą przetwarzać dane osobowe;
12) nadzorowania opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania

danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, oraz przestrzegania zasad w niej określonych;

13) prowadzenia korespondencji z Biurem GIODO w sprawach związanych z ochroną danych osobowych;

14) udzielania wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie prowadzonych sprawdzeń w celu dostosowania ochrony danych do stanu zgodnego z przepisami prawa;

15) podejmowania działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu jego zabezpieczeń lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych;

16) wykonywania innych zleconych przez ADO obowiązków, jeżeli nie narusza to prawidłowego wykonywania zadań wymienionych w § 2 ust.1.

2. ABI zabezpiecza przechowywane dane, dokumenty, materiały i opracowania przed dostępem osób nieuprawnionych oraz stosuje adekwatne środki bezpieczeństwa i ochrony przewidziane odpowiednimi przepisami.

3. Stanowisko ABI powinno znajdować się w osobnym pomieszczeniu, ograniczającym dostęp osobom nieuprawnionym oraz zapewniającym bezpieczne przechowywanie dokumentów w szafach zabezpieczonych zamkami.

§ 3.1. LADO w zakresie właściwości, realizują zadania Wojewody Świętokrzyskiego jako Administratora Danych Osobowych.

2. Do głównych zadań LADO w szczególności należy:

1) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, utratą, uszkodzeniem lub zniszczeniem, poprzez zapewnienie:
   a) zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe oraz kontrola przebywających w nich osób,
   b) nadzoru nad zarządzaniem hasłami użytkowników, zgodnie z wytycznymi zawartymi w instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,

c) nadzoru nad naprawami oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,

d) nadzoru nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych wg instrukcji zarządzania systemem informatycznym,

e) nadzoru nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,

f) nadzoru nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,

g) nadzoru nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,

h) nadzoru nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe generowane przez system informatyczny;

2) podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu, w tym: analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło) i przygotowanie we współdziałaniu z ABI oraz przedstawienie ADO propozycji odpowiednich zmian do instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;

3) monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych;

4) zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych;

5) zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru danych wprowadzone oraz komu zostały przekazane;

6) prowadzenie rejestru nadanych upoważnień do przetwarzania danych osobowych oraz ewidencji, o której mowa w art. 39 ust. 1 u.o.d.o.;

7) wykonywanie obowiązku informacyjnego wynikającego z realizacji praw osób, których dane dotyczą;

8) wyznaczanie obszarów, w których mogą być przetwarzane dane osobowe;

9) zapewnienie prowadzenia w formie pisemnej wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe oraz niezwłocznego jego aktualizowania;

10) niezwłoczne przekazywanie do ABI informacji i wymaganych dokumentów niezbędnych do:

a) rejestracji nowych zbiorów,

b) aktualizowania zbiorów,

c) wykreślania zbiorów z prowadzonego rejestru;

11) zapewnienie szkolenia osób upoważnionych do przetwarzania danych osobowych w zakresie ochrony danych osobowych;

12) występowania za pośrednictwem ABI do ADO o:

a) utworzenie zbioru danych przed rozpoczęciem przetwarzania w nim danych osobowych,

b) zmianę struktury zbioru danych przed dokonaniem zmian w zbiorze danych,

c) likwidację zbioru danych w przypadku zaprzestania przetwarzania danych osobowych w zbiorze danych;

13) udzielanie ABI niezbędnej pomocy w zakresie realizacji jego zadań, a w szczególności do opracowania i przekazania dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych oraz jej aktualizacji;

14) wykonywanie innych uwag i zaleceń ABI w zakresie ochrony danych osobowych;

15) przekazywanie ABI:

a) nazwisk osób, które przetwarzają dane osobowe w rozumieniu art. 7 pkt 2 u.o.d.o., tj. dokonują jakichkolwiek operacji wykonywanych na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemach informatycznych,

b) informacji o zagrożeniach i/lub niedociągnięciach systemu ochrony przetwarzanych danych osobowych wynikających z przepisów prawa w tym zakresie lub innych napotykanych w procesach przetwarzania danych, wraz z sugestiami wskazującymi metody eliminowania takich zagrożeń,

c) kopi podpisanych umów, których skutkiem jest dostęp podmiotów zewnętrznych do danych osobowych gromadzonych w systemie informatycznym Urzędu.

§ 4. Do zadań ASI należy:

1) realizacja decyzji ADO i/lub LADO odnośnie nadania osobom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania, w środowisku IT Urzędu tj.:

a) tworzenie kont użytkowników w systemach informatycznych,

b) przypisywanie do kont startowych haseł uwierzytelniających użytkowników tych kont,

c) przypisywanie określonych wymogów co do jakości haseł i częstotliwości ich zmiany,

d) resetowanie utraconych haseł,

e) usuwanie kont i uprawnień dla kont osób które zakończyły pracę w Urzędzie,

f) dostarczanie ABI informacji i materiałów potrzebnych do oceny prawidłowości funkcjonowania systemów, w których przetwarzane są dane osobowe;

2) planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w Urzędzie;
3) planowanie i wykonywanie zadań związanych z tworzeniem kopii bezpieczeństwa systemów i danych;
4) automatyzacja zadań konserwacyjnych w systemie – w tym wykonywania kopii zapasowych oprogramowania i danych;
5) monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników;
6) monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych;
7) zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych;
8) systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego;
9) zapewnienie eksploatowanym systemom usługi serwisowej producenta – zawieranie umów regulujących formy tej usługi;
10) rozwiązywanie, samodzielnie i we współpracy z pozostałym personelem IT, problemów towarzyszących eksploatacji systemów informatycznych;
11) prowadzenie szkoleń na temat bezpiecznych zachowań użytkowników w środowisku systemów IT;
12) dokumentowanie wykonywanych czynności.

§ 5. 1. LADO wyznaczają dla zbiorów przetwarzanych elektronicznie Administratora Bezpieczeństwa Zbioru (ABZ), który jest odpowiedzialny za zapewnienie bezpieczeństwa przetwarzanych danych osobowych w ramach określonego zbioru lub zbiorów danych w komórce organizacyjnej, w której został wyznaczony.

2. Do jego zadań należy w szczególności:

1) przygotowywanie, we współpracy z ABI instrukcji dla użytkowników systemów informatycznych zgodnych z celami i metodologią wdrożonej polityki bezpieczeństwa informacji;
2) wykonywanie poleceń LADO oraz realizacja zadań przez niego wskazanych, w szczególności wynikających z innych dokumentów opracowanych dla konkretnych zbiorów danych oraz systemów informatycznych, w których są przetwarzane dane osobowe;
3) wdrażanie zasad bezpieczeństwa określonych w przepisach dotyczących ochrony danych osobowych, w szczególności w decyzji oraz nadzór nad ich przestrzeganiem;

4) przyjmowanie informacji o przypadkach naruszenia bezpieczeństwa przetwarzania danych osobowych, niezwłoczne podejmowanie działań zmierzających do zapobieżenia powstania szkód, w tym w szczególności utraty poufności, integralności i dostępności danych osobowych oraz ustalenia przyczyn ich powstania;
5) informowanie LADO o naruszeniach zasad bezpieczeństwa przetwarzania danych osobowych, podjętych działaniach, dokonanych ustaleniach oraz propozycjach mających na celu wyeliminowanie zagrożenia w przyszłości;
6) prowadzenie szkoleń instruktażowych z zakresu obsługi zbioru danych osobowych oraz bezpieczeństwa systemów informatycznych, w przypadku posiadania w tym zakresie niezbędnej wiedzy i doświadczenia;
7) wykonywanie zaleceń ABI w zakresie ochrony danych osobowych;
8) prowadzenie dziennika działań i ewidencjonowanie w nim wykonywanych czynności;
9) konfiguracja stanowisk komputerowych zgodnie z wymaganiami, instalacja i aktualizacja oprogramowania, w tym antywirusowego;
10) utrzymywanie w aktualności haseł przydzielonych przez ASI;
11) współdziałanie z ASI w zakresie zakładania, blokowania i zamykania kont użytkownikom do systemu informatycznego w zakresie zgodnym z upoważnieniem do przetwarzania danych osobowych;
12) podejmowanie czynności związanych z bieżącą naprawą, konserwacją i rozbudową systemu informatycznego w zakresie umożliwiającym utrzymywanie go w stałej sprawności technicznej oraz funkcjonalnej;
13) dokonywanie oględzin sprzętu odebranego z naprawy przed zainstalowaniem w systemie informatycznym, pod kątem spełnienia wymogów bezpieczeństwa;
14) prowadzenie ewidencji osób uprawnionych do przetwarzania danych osobowych w systemie informatycznym, którego jest administratorem, zawierającej informacje, o których mowa w art. 39 ust. 1 u.o.d.o.;
15) stosowanie procedury nadawania oraz odbierania uprawnień do przetwarzania zbiorów danych;
16) przyjmowanie od użytkowników uwag o stwierdzonych nieprawidłowościach w działaniu systemu informatycznego oraz podejmowanie działań zmierzających do zapewnienia sprawności systemu informatycznego;
17) nadzór nad przekazywaniem przez użytkowników informatycznych nośników danych osobowych do Archiwum Zakładowego.

§ 6. Traci moc Zarządzenie Nr 42/2013 Wojewody Świętokrzyskiego z dnia 14 maja 2013 r. w sprawie powołania Administratora Bezpieczeństwa Informacji w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach oraz określenia jego zakresu odpowiedzialności.

§. 7. Zarządzenie wchodzi w życie z dniem podpisania.

WOJEWODA ŚWIĘTOKRZYSKI

Bożentyna Pałka-Koruba