

ZARZĄDZENIE NR 6/2020
STAROSTY TUCHOLSKIEGO
z dnia 23 stycznia 2020 r.

w sprawie wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji Starostwa Powiatowego w Tucholi.

Na podstawie art. 34 ust.1 i art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (t. j. Dz. U. z 2019 r., poz. 511 z późn. zm.), art. 24 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz § 20 ust. 1 i 2 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t. j. Dz.U z 2017 r., poz. 2247 z późn. zm.).

zarządza się, co następuje:

§ 1

W Starostwie Powiatowym w Tucholi wprowadza się:

- 1) Politykę bezpieczeństwa informacji Starostwa Powiatowego w Tucholi, stanowiącą załącznik nr 5 do zarządzenia;
- 2) Instrukcję zarządzania systemami informatycznymi Starostwa Powiatowego w Tucholi, stanowiącą załącznik nr 2 do zarządzenia;
- 3) Politykę ochrony danych osobowych Starostwa Powiatowego w Tucholi, stanowiącą załącznik nr 1 do zarządzenia;
- 4) Metodykę szacowania ryzyka i oceny skutków dla ochrony danych osobowych Starostwa Powiatowego w Tucholi, stanowiącą załącznik nr 4 do zarządzenia;
- 5) Procedurę identyfikacji wymagań Starostwa Powiatowego w Tucholi, stanowiącą załącznik nr 3 do zarządzenia;
- 6) Plan awaryjny reakcji na incydenty ciągłości działania Starostwa Powiatowego w Tucholi, stanowiący załącznik nr 6 do zarządzenia;
- 7) Deklarację stosowania Systemu Zarządzania Bezpieczeństwem Informacji Starostwa Powiatowego w Tucholi, stanowiącą załącznik nr 7 do zarządzenia;
- 8) Procedurę audytu wewnętrznego Starostwa Powiatowego w Tucholi, stanowiącą załącznik nr 8 do zarządzenia;
- 9) Procedurę działań naprawczych Starostwa Powiatowego w Tucholi, stanowiącą załącznik nr 9 do zarządzenia;
- 10) Regulamin przestrzegania zasad i procedur korzystania z legalnego oprogramowania oraz ochrony własności intelektualnej.

§ 2

Zobowiązuje się wszystkich pracowników Starostwa Powiatowego w Tucholi do zapoznania się z niniejszym zarządzeniem i załącznikami do zarządzenia oraz do przestrzegania zasad zawartych w tych dokumentach. Oświadczenie stanowi załącznik nr 11 do zarządzenia.

§ 3

Nadzór nad wykonaniem zarządzenia powierzam Zespołowi ds. Systemu Zarządzania Bezpieczeństwem Informacji.

§ 4

Traci moc Zarządzenie Nr 30/2018 Starosty Tucholskiego z dnia 24 maja 2018 r. w sprawie wprowadzenia „Dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych w Starostwie Powiatowym w Tucholi” zmienione Zarządzeniem Nr 34/2019 Starosty Tucholskiego z dnia 11 czerwca 2019 r.

§ 5

Określenia i skróty użyte w Zarządzeniu oraz jego załącznikach:

- 1) Administrator – Starostwo Powiatowe w Tucholi reprezentowane przez Starostę Tucholskiego, decydujący o celach i środkach przetwarzania danych osobowych;
- 2) Administrator systemów informatycznych (ASI) – osoba wyznaczona przez Administratora, odpowiedzialna za infrastrukturę techniczną systemów;
- 3) Administrator systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;
- 4) Baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;
- 5) Bezpieczeństwo informacji – zapewnienie poufności, integralności oraz dostępności informacji;
- 6) Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
- 7) Dostępność – właściwość informacji zapewniająca możliwość dostępu do tej informacji przez uprawnione osoby w każdym czasie, gdy dana informacja jest potrzebna;
- 8) Hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
- 9) Identyfikator - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- 10) Integralność – właściwość informacji zapewniająca możliwość dokonywania w niej zmian tylko przez uprawnione osoby lub procesy w dozwolony sposób;
- 11) Inspektor ochrony danych (IOD) - osoba powołana przez Administratora w Starostwie Powiatowym w Tucholi, odpowiedzialna za nadzorowanie całokształtu spraw związanych z ochroną danych osobowych oraz za zapewnienie przetwarzania danych zgodnie z odpowiednimi przepisami ustawy i rozporządzenia;
- 12) Instrukcja – Instrukcja zarządzania systemami informatycznymi Starostwa Powiatowego w Tucholi;

- 13) Incydent bezpieczeństwa – problem, który może mieć wpływ na utratę poufności, dostępności lub integralności informacji albo może powodować przerwę lub zakłócenie realizacji zadań publicznych;
- 14) Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- 15) Nośnik komputerowy (wymienny) - nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde, dyski flash, pendrive;
- 16) Odbiorca danych - osoba fizyczna, lub prawna, organ publiczny lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane w ramach konkretnego postępowania nie są jednak uznawane za odbiorców. Przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych osobowych mającymi zastosowanie stosowne do celów przetwarzania;
- 17) Podatność - słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie;
- 18) Podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora, czyli działającym na jego zlecenie;
- 19) Poufność – właściwość informacji zapewniająca jej dostęp wyłącznie dla osób uprawnionych;
- 20) PODO – Polityka ochrony danych osobowych;
- 21) Polityka - Polityka Bezpieczeństwa Informacji Starostwa Powiatowego w Tucholi;
- 22) Prezes Urzędu Ochrony Danych Osobowych (PUODO) – rozumie się przez to organ nadzorujący przestrzeganie przepisów ochrony danych osobowych;
- 23) Przetwarzanie danych - operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
- 24) RCPDO lub Rejestr – oznacza Rejestr czynności przetwarzania danych osobowych;
- 25) Rozporządzenie lub RODO - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
- 26) Ryzyko – niepewność osiągnięcia zamierzonych celów;
- 27) System informatyczny (system) - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- 28) System Zarządzania Bezpieczeństwem Informacji (SZBI) – część zintegrowanego systemu zarządzania odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymania i doskonalenia bezpieczeństwa informacji;
- 29) Szacowanie ryzyka – proces identyfikowania, analizowania i oceniania ryzyka;

- 30) Szczególne kategorie danych osobowych (tzw. dane wrażliwe) – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby, a także dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa;
- 31) Usuwanie danych - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
- 32) Użytkownik - pracownik Starostwa Powiatowego w Tucholi posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;
- 33) Właściciel ryzyka – konkretna osoba, której przypisano własność poszczególnych ryzyk, osoba odpowiedzialna za plany działań, ograniczenie prawdopodobieństwa wystąpienia ryzyka lub naprawę zmaterializowanego ryzyka. Osoba odpowiedzialna za zarządzanie ryzykiem, mająca kompetencje do podjęcia działań zaradczych w stosunku do obszaru, którym zarządza;
- 34) Zabezpieczenie systemu informatycznego - wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
- 35) Zagrożenie - potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub urzędu;
- 36) Załączniki – należy przez to rozumieć wzory dokumentów. Administrator może przedmiotowe wzory zastąpić wydrukami z systemów komputerowych lub innymi dokumentami o treści zgodnej z przepisami powszechnie obowiązującego prawa;
- 37) Zarządzanie ryzykiem – skoordynowane postępowanie, którego celem jest identyfikacja, kontrolowanie i minimalizowanie ryzyka związanego z bezpieczeństwem informacji i ciągłością działania;
- 38) Zbiór danych - zestaw danych osobowych posiadający określoną strukturę, prowadzony według określonych kryteriów oraz celów;
- 39) Zespół ds. SZBI – zespół odpowiedzialny za inicjowanie i wspieranie wszelkich działań związanych z bezpieczeństwem informacji i ciągłością działania.
- 40) Zgoda osoby, której dane dotyczą - oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorożumiana z oświadczenia woli o innej treści;

§ 6

Zarządzenie wchodzi w życie z dniem 23 stycznia 2020 r.

STAROSTA TUCHOLSKI

Michał Mróz