ZARZĄDZENIE NR 38/2018

STAROSTY ŁOWICKIEGO

z dnia 23 maja 2018 r.

w sprawie wprowadzenia Regulaminu postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w Starostwie Powiatowym w Łowiczu

Na podstawie art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 679/2016 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 (Dz. Urz. UE L 119/1) oraz art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz. U. z 2017 r. poz. 1868; z 2018 r., poz. 130), zarządzam, co następuje:

§1. Wprowadzam *Regulamin postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w Starostwie Powiatowym w Łowiczu*, zwany dalej Regulaminem, stanowiący załącznik do niniejszego Zarządzenia.

§2. Nadzór nad wykonaniem zarządzenia powierzam Inspektorowi Ochrony Danych Osobowych w Starostwie Powiatowym w Łowiczu.

§3. Do stosowania postanowień zawartych w Regulaminie zobowiązani są wszyscy pracownicy i współpracownicy Administratora.

§4. Zarządzenie wchodzi w życie z dniem 25 maja 2018 r.

STAROSTA ŁOWICKI

Krzysztof Figat

RADCA PRAWNY

Anna Moduk

Łd-M-1619

Administrator Bezpieczeństwa Informacji

Martyna Bogucka

Załącznik
do Zarządzenia Nr 38/2018
Starosty Łowickiego
z dnia 23 maja 2018 r.
w sprawie wprowadzenia
Regulaminu postępowania w sytuacji
naruszenia bezpieczeństwa danych
osobowych w Starostwie Powiatowym
w Łowiczu

Regulamin postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w Starostwie Powiatowym w Łowiczu

Postanowienia ogólne

§1. Ilekroć w Regulaminie postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w Starostwie Powiatowym w Łowiczu jest mowa o:

1) **Regulaminie** – należy przez to rozumieć Regulamin postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w Starostwie Powiatowym w Łowiczu;
2) **Administratorze Danych** – o ile odrębne przepisy nie stanowią inaczej, należy przez to rozumieć:
   a) **Starostę Łowickiego** – w sprawach z zakresu postępowania administracyjnego,
   b) **Przewodniczącą Powiatowego Zespołu ds. Orzekania o Niepełnosprawności** – w sprawach nałożonych przepisami ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (tj. Dz. U. 2018, poz. 511, z późn. zm.),
   c) **Starostwo Powiatowe w Łowiczu** – w sprawach pozostałych,
   dalej zwanych „Administratorem";
3) **Inspektorze Ochrony Danych (lub „IOD")** – należy przez to rozumieć osobę, która sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych i jest odpowiedzialna za nadzorowanie przypadków naruszeń;
4) **Administratorze Systemów Informatycznych (lub „ASI")** – należy przez to rozumieć osobę upoważnioną przez Administratora do administrowania i zarządzania systemami informatycznymi, która we współdziałaniu z IOD jest odpowiedzialna za nadzorowanie przypadków naruszeń;
5) **Starostwie** – należy przez to rozumieć Starostwo Powiatowe w Łowiczu;
6) **Użytkowniku** – należy przez to rozumieć pracownika, w tym upoważnionego przez Administratora wyznaczonego do przetwarzania danych osobowych lub współpracownika;
7) **Organie nadzorczym** – należy przez to rozumieć niezależny organ publiczny ustanowiony zgodnie z art. 51 rozporządzenia Parlamentu Europejskiego i Rady (UE) 679/2016 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 (Dz. Urz. UE L 119/1);
8) **Pracowniku** – należy przez to rozumieć osobę pozostającą z Administratorem w stosunku pracy, bez względu na rodzaj wykonywanej pracy, wymiar czasu pracy, zajmowane stanowisko oraz podstawę prawną zatrudnienia;
9) **Współpracowniku** – należy przez to rozumieć osobę, przy pomocy której Administrator realizuje swoje zadania, a w szczególności:
   a) osobę świadczącą pracę na podstawie umowy cywilnoprawnej,
   b) stażystę,
   c) praktykanta,
   d) wolontariusza,
   e) osobę działającą w imieniu podmiotu zewnętrznego świadczącego usługi na rzecz Administratora;
10) **Poufności danych** – należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
11) **Integralności danych** – należy przez to rozumieć właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
12) **Rozliczalności danych** – należy przez to rozumieć właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;

13) **Naruszenie bezpieczeństwa danych** – należy przez to rozumieć działania zewnętrzne lub wewnętrzne w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności;
14) **Zagrożeniu** – należy przez to rozumieć świadome lub nieświadome działania wskutek których doszło do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.

§2. Celem wprowadzenia Regulaminu jest aktywna kontrola nad przypadkami naruszeń i podejrzeniami naruszeń w celu zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzania danych osobowych. Przestrzeganie postanowień niniejszego Regulaminu służyć ma wykrywaniu i właściwemu reagowaniu na przypadki naruszenia ochrony danych osobowych oraz dokonaniu prawidłowego zgłoszenia naruszeń organowi nadzorczemu.

Identyfikacja naruszeń

§3. 1. Naruszenie ochrony bezpieczeństwa danych może być skutkiem:

1) szkodliwego wpływu środowiska na system przetwarzania danych osobowych;
2) zewnętrznych zdarzeń losowych;
3) zamierzonych lub niezamierzonych czynności użytkowników systemów przetwarzania danych osobowych;
4) nieuprawnionych działań osób nieupoważnionych do dostępu do danych osobowych.

2. Za naruszenie lub podejrzenie naruszenia bezpieczeństwa danych uważa się przede wszystkim:

1) losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.);
2) niewłaściwe parametry środowiska (nadmierna wilgotność, wysoka temperatura, oddziaływanie pola elektromagnetycznego, wibracje lub wstrząsy wywołane urządzeniami przemysłowymi);
3) awarię sprzętu lub oprogramowania, która wyraźnie wskazuje na umyślne działanie w kierunku naruszenia danych;
4) ujawnianie indywidualnych haseł dostępu do systemu;
5) naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa (np. niewylogowanie się z systemu przed opuszczeniem stanowiska pracy);
6) brak możliwości zalogowania się do systemu;
7) zmiany w wyglądzie aplikacji zawierających dane osobowe;
8) ograniczenie lub spowolnienie pracy systemu;
9) brak aktywnego programu antywirusowego;
10) brak dostępu do zawartości zbioru danych - zbiór istnieje, lecz nie można go otworzyć;
11) pojawienie się niestandardowych komunikatów generowanych przez system;
12) informacja o zainfekowaniu systemu wirusami;
13) fizyczne zniszczenie lub podejrzenie zniszczenia urządzeń systemu;
14) dopuszczenie do przetwarzania danych osób bez odpowiednich upoważnień;
15) stwierdzenie prób włamania do systemu lub nieautoryzowanej modyfikacji danych;
16) udostępnianie danych osobom/podmiotom nieuprawnionym;

17) utratę, kradzież lub zniszczenie nośników danych;
18) stosowanie nieodpowiednich technik usuwania danych;
19) brak możliwości fizycznego dostępu do danych (np. zagubiony klucz do pomieszczenia lub mebli biurowych);
20) zmienioną zawartość zbioru, niepoprawną treść/postać;
21) próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia, w którym jest przetwarzany, np. zmiana ułożenia kolejności dokumentów, otwarte drzwi lub meble biurowe, nietypowe ustawienia sprzętu;
22) zmianę lub utratę danych zapisanych na kopiach awaryjnych lub zapisach archiwalnych;
23) pozyskiwanie danych osobowych z nielegalnego źródeł,
24) inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa danych osobowych.

Procedury postępowania w przypadku naruszeń

§4. 1. Każdy użytkownik w przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony, o których mowa w §3 ust. 2 Regulaminu, zobowiązany jest do bezzwłocznego powiadomienia Inspektora Ochrony Danych, a w czasie jego nieobecności Administratora Systemów Informatycznych.

2. W razie braku możliwości zawiadomienia osób nadzorujących naruszenia, o których mowa w ust. 1, należy zawiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce osób nadzorujących naruszenia, użytkownik powinien:

1) o ile jest to możliwe, niezwłocznie podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony;
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia; na ile jest to możliwe należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia ochrony i udokumentowanie zdarzenia;
3) podjąć działania, które zapobiegną ewentualnej utracie danych osobowych;
4) podjąć działania w celu ustalenia przyczyny i sprawcy naruszenia ochrony oraz zapisać wszelkie informacje i okoliczności związane ze zdarzeniem;
5) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia;
6) zabezpieczyć dostęp do pomieszczenia lub urządzenia.

4. Dokonywanie zmian w miejscu naruszenia ochrony jest dopuszczalne tylko w wypadku konieczności ratowania osób, mienia albo zapobiegania powstania innego niebezpieczeństwa.

5. W przypadku stwierdzenia przez użytkownika naruszenia bezpieczeństwa danych w systemie informatycznym należy:

1) odłączyć system od sieci komputerowej;
2) o ile jest to możliwe, wykonać kopie bezpieczeństwa danych na oddzielnym nośniku informacji;
3) wyłączyć system, aby zapobiec działaniu złośliwego oprogramowania lub hakera.

§5. Po przybyciu na miejsce naruszenia bezpieczeństwa danych osobowych osoba odpowiedzialna za nadzór nad naruszeniami podejmuje następujące kroki:

1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy;

2) wysłuchuje relacji użytkownika, który dokonał zgłoszenia;
3) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia bezpieczeństwa danych (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów, itp.);
4) zabezpiecza i utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia;
5) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia;
6) może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym zdarzeniem;
7) nawiązuje kontakt ze specjalistami (jeśli zachodzi taka potrzeba);
8) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych;
9) proponuje działania naprawcze, w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych;
10) wskazuje osoby odpowiedzialne za naruszenie ochrony oraz formułuje wnioski co do ewentualnych działań proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości;
11) dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając ***Raport z naruszenia bezpieczeństwa danych osobowych***, którego wzór stanowi załącznik nr 1 do Regulaminu.

§6. 1. Raport, o którym mowa w §5 pkt 11, zostaje przedłożony do zatwierdzenia Administratorowi i podlega ewidencji w ***Rejestrze naruszeń***, prowadzonym przez Inspektora Ochrony Danych.

2. Wzór rejestru, o którym mowa w ust. 1, stanowi załącznik nr 2 do Regulaminu.

3. Rejestr może obejmować okres dłuższy niż jeden rok.

4. Numerację rozpoczyna się w każdym roku kalendarzowym od numeru 1. Numer z rejestru łamany jest przez rok, w którym zaistniało naruszenie.

§7. W przypadku naruszenia danych w systemie informatycznym osoba nadzorująca przetwarzanie danych w systemie informatycznym:

1) sprawdza stan urządzeń wykorzystanych do przetwarzania danych osobowych;
2) w celu powstrzymania lub ograniczenia dostępu do danych osoby nieupoważnionej podejmuje odpowiednie koki zmierzające do fizycznego odłączenia urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do danych osobie nieupoważnionej, wylogowania użytkownika systemu podejrzanego o naruszenie zabezpieczenia ochrony danych, zmiany hasła poprzez które uzyskano nielegalny dostęp, aby uniknąć ponownej próby działania systemu;
3) przywraca prawidłowy stan działania systemu;
4) sprawdza sposób działania programów, w tym obecność wirusów komputerowych;
5) sprawdza jakość komunikacji w sieci telekomunikacyjnej;
6) wyraża zgodę na ponowne uruchomienie komputera lub innych urządzeń.

§8. Osoba nadzorująca naruszenia podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

1) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub inny atak sieciowy, jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie zleca przeprowadzenie przeglądów oraz konserwacji urządzeń i programów, ustalenie źródła pochodzenia wirusa komputerowego lub innego ataku sieciowego oraz wdrożenie skuteczniejszego zabezpieczenia antywirusowego, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych w celu usprawnienia systemu zabezpieczeń;
2) jeżeli przyczyna zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza dodatkowe kursy i szkolenia osób upoważnionych do przetwarzania danych osobowych, a wobec osób winnych zaniedbań wnioskuje o wyciągnięcie konsekwencji przewidzianych prawem;
3) jeżeli przyczyną zdarzenia było włamanie w celu nielegalnego pozyskania danych dokonuje szczegółowej analizy wdrożonych środków zabezpieczenia i proponuje wdrożenie skuteczniejszej ochrony fizycznej;
4) jeżeli przyczyną zdarzenia był czyn zabroniony lub zachodzi uzasadnione podejrzenie popełnienia takiego czynu, zawiadamia organy ścigania;
5) jeżeli istotność naruszenia danych w systemie informatycznym jest wysoka może zawiadomić Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL pełniący rolę głównego zespołu CERT w obszarze administracji rządowej, poprzez wypełnienie formularza zgłoszeń, który jest dostępny na stronie www.cert.gov.pl oraz wysłanie go do CERT dwutorowo, tj. faksem na numer +48 22 58 58 833 oraz pocztą elektroniczną na adres incydent@cert.gov.pl; dalsza korespondencja z CERT w sprawie tego naruszenia odbywa się za pomocą szyfrowanej poczty elektronicznej.

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

§9. 1. W przypadku wystąpienia naruszenia ochrony danych osobowych, które mogłoby skutkować naruszeniem praw i wolności osób fizycznych, Administrator zgłasza ten fakt organowi nadzorczemu bez zbędnej zwłoki, nie później jednak niż w terminie 72 godzin od stwierdzenia naruszenia bezpieczeństwa danych osobowych.

2. Zgłoszenie, o którym mowa w ust. 1, musi zawierać co najmniej:
1) opis charakteru naruszenia;
2) kategorie i przybliżoną ilość osób, których dane zostały narażone na naruszenie;
3) kategorie i przybliżoną ilość wpisów danych osobowych, których dotyczy naruszenie;
4) imię i nazwisko oraz dane kontaktowe inspektora danych osobowych;
5) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
6) opis podjętych rozwiązań w celu zaradzenia naruszeniu ochrony danych osobowych, w tym rozwiązań podjętych w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. W razie wystąpienia trudności w udzieleniu informacji, o których mowa w ust. 2, w tym samym czasie, należy ich udzielać sukcesywnie bez zbędnej zwłoki.

§10. 1. W przypadku gdy naruszenie, o którym mowa w §9 ust. 1, powoduje wysokie ryzyko naruszenia praw i wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia o nim osoby, których dane dotyczą.

2. Zawiadomienie, o którym mowa w ust. 1, powinno zawierać informacje o których mowa w §9 ust. 2 pkt 4-6.

3. Jeżeli bezpośrednie zawiadomienie osób, których prawa i wolności zostały naruszone, wymagałoby niewspółmiernie dużego wysiłku, Administrator zamieszcza komunikat z informacją o naruszeniu na tablicy informacyjnej w budynkach Starostwa oraz w Biuletynie Informacji Publicznej.

Postanowienia końcowe

§11. 1.Każdy użytkownik obowiązany jest zapoznać się z Regulaminem oraz złożyć stosowne oświadczenie dotyczące znajomości wymienionych regulacji.

2. Wzór oświadczenia, o którym mowa w ust.1, stanowi załącznik nr 3 do Regulaminu.

§12. Za naruszenie obowiązków wynikających z Regulaminu ponoszona jest odpowiedzialność:

1) przewidziana w Kodeksie Pracy za ciężkie naruszenie podstawowych obowiązków pracowniczych, gdy naruszenia dopuścił się pracownik;
2) przewidziana za istotne naruszenie innego stosunku prawnego łączącego Administratora z osobą inną niż pracownik.

STAROSTA ŁOWICKI

Krzysztof Figat

Załącznik nr 1 do Regulaminu
postępowania w sytuacji naruszenia
bezpieczeństwa danych osobowych
w Starostwie Powiatowym w Łowiczu
wprowadzonego Zarządzeniem Nr 38/2018
Starosty Łowickiego z dnia 23 maja 2018 r.
w sprawie wprowadzenia
Regulaminu postępowania w sytuacji
naruszenia bezpieczeństwa danych
osobowych w Starostwie Powiatowym
w Łowiczu

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Nr raportu	...../.....
Data i godzina wystąpienia zdarzenia	
Miejsce wystąpienia zdarzenia	

1. Opis zdarzenia i rodzaj naruszenia
2. Przyczyny powstania zdarzenia
3. Zaistniałe skutki zagrożenia
4. Podjęte czynności naprawczo-zapobiegawcze
5. Osoby udzielające wyjaśnień w sprawie zdarzenia

Podpis osoby zgłaszającej	
Podpis osoby nadzorującej	

STAROSTA ŁOWICKI
Krzysztof Figat

Załącznik nr 2 do Regulaminu
postępowania w sytuacji naruszenia bezpieczeństwa
danych osobowych
w Starostwie Powiatowym w Łowiczu
wprowadzonego Zarządzeniem Nr 38/2018
Starosty Łowickiego z dnia 23 maja 2018 r.
w sprawie wprowadzenia
Regulaminu postępowania w sytuacji
naruszenia bezpieczeństwa danych osobowych
w Starostwie Powiatowym w Łowiczu

REJESTR NARUSZEŃ

Lp.	Nr raportu	Data i miejsce naruszenia	Opis naruszenia	Wyniki podjętych działań	Data zamknięcia sprawy	Podpisy osób nadzorujących

STAROSTA ŁOWICKI
Krzysztof Figat

Załącznik nr 3 do Regulaminu
postępowania w sytuacji naruszenia
bezpieczeństwa danych osobowych
w Starostwie Powiatowym w Łowiczu
wprowadzonego Zarządzeniem Nr 38/2018
Starosty Łowickiego z dnia 23 maja 2018 r.
w sprawie wprowadzenia Regulaminu
postępowania w sytuacji naruszenia
bezpieczeństwa danych osobowych
w Starostwie Powiatowym w Łowiczu

Łowicz, dnia .....

.....
(imię i nazwisko użytkownika)

.....
(stanowisko użytkownika)

OŚWIADCZENIE

Oświadczam, że zapoznałem/-am się z regulacjami zawartymi w Regulaminie postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w Starostwie Powiatowym w Łowiczu i przyjąłem/-am je do stosowania.

.....
(podpis użytkownika)

*użytkownik - należy przez to rozumieć pracownika, w tym upoważnionego przez Administratora wyznaczonego do przetwarzania danych osobowych lub współpracownika;

STAROSTA ŁOWICKI
Krzysztof Figat