ZARZĄDZENIE Nr 45/2020
BURMISTRZA KARCZEWA
z dnia 15 maja 2020 r.

zmieniające Zarządzenie w sprawie ustalenia Polityki bezpieczeństwa danych osobowych w Urzędzie Miejskim w Karczewie, ustalenia Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń Urzędu Miejskiego w Karczewie, ustalenia Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych

Na podstawie art. 30 ust. 1, art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2020 r. poz. 713) oraz art. 24 ust. 1 i 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) zarządza się, co następuje:

§ 1. 1. Rozdział XXI Ogólna Instrukcja dla Informatyka w Załączniku Nr 1 do Zarządzenia Nr 29/2019 Burmistrza Karczewa z dnia 02 kwietnia 2019 r. Polityk Bezpieczeństwa Danych Osobowych w Urzędzie Miejskim w Karczewie otrzymuje nowe brzmienie:

„XXI. Ogólna instrukcja dla Informatyka

Obowiązki Informatyka:

1) wdrożenie i utrzymanie środków szyfrowania danych osobowych, przetwarzanych w ramach systemu informatycznego Urzędu Miejskiego w Karczewie;
2) właściwa konfiguracja systemu informatycznego służącego do przetwarzania danych osobowych w Urzędzie Miejskim w Karczewie, w celu zapewnienia jego zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
3) dbałość o utrzymanie i zabezpieczenie serwerów systemu informatycznego służącego do przetwarzania danych osobowych w Urzędzie Miejskim w Karczewie, niezależnie od tego czy serwer znajduje się w zasobach lokalnych Urzędu , czy poza nim, a w szczególności zapewnienie jego poufności, integralności, dostępności i odporności.
4) zapewnienie zdolności systemu informatycznego służącego do przetwarzania danych osobowych w Urzędzie Miejskim w Karczewie, do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
5) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych systemu informatycznego służącego do przetwarzania danych osobowych w Urzędzie, mających zapewnić bezpieczeństwo przetwarzania danych osobowych z jego użyciem.
6) instalacja, konfiguracja, usuwanie, zamawianie licencji i ich przedłużanie, w odniesieniu do oprogramowania używanego w urządzeniach teleinformatycznych stosowanych w systemie teleinformatycznym Urzędu.
7) nadzór na pracami podmiotów zewnętrznych, przeprowadzających prace przy naprawach, konserwacjach systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie, w celu zapewnienia zgodności tych czynności z zasadami przyjętymi w Urzędzie.
8) nadawanie, zmiana i wycofywanie identyfikatorów i haseł oraz uprawnień do korzystania z aplikacji i programów osobom upoważnionym do przetwarzania danych osobowych w Urzędzie;
9) nadzór nad prawidłowym wdrożeniem i funkcjonowaniem systemu sporządzania kopii bezpieczeństwa wszelkich nośników informacji, służących do przetwarzania danych osobowych w Urzędzie, zgodnie z przyjętą polityką tworzenia kopii zapasowych w Urzędzie.
10) podejmowanie działań w przypadku podejrzenia lub wykrycia naruszeń bezpieczeństwa w systemie zabezpieczeń systemu informatycznego służącego do przetwarzania danych osobowych w Urzędzie;

11) świadczenie pomocy technicznej w zakresie obsługi oprogramowania i urządzeń używanych w ramach systemu informatycznego służącego do przetwarzania danych osobowych w Urzędzie;
12) zabezpieczenie komputerów przenośnych służących do przetwarzania danych osobowych w Urzędzie.

XXI.I. Procedura ewidencjonowania urządzeń i nośników

1. Informatyk jest zobowiązany do ewidencjonowania wszelkich czynności wykonywanych w systemie informatycznym służącym do przetwarzania danych osobowych w Urzędzie, a także do ewidencjonowania urządzeń i nośników, służących do przetwarzania danych osobowych.
2. Ewidencjonowanie napraw, przeglądów i konserwacji systemu informatycznego oraz czynności w systemie informatycznym, następuje w dedykowanym programie komputerowym.
3. Ewidencjonowanie urządzeń i nośników, służących do przetwarzania danych osobowych następuje w rejestrze elektronicznym (**załącznik nr 12**).
4. Przed dopuszczeniem do użycia nowych urządzeń i nośników służących do przetwarzania danych osobowych w Urzędzie, należy je zewidencjować.
5. Po usunięciu urządzenia lub nośnika służącego do przetwarzania danych osobowych w Urzędzie, należy wykreślić go z Rejestru urządzeń i nośników, służących do przetwarzania danych osobowych.

XXI.II. Procedura wykonywania kontroli dostępu do systemu

1. W systemie informatycznym służącym do przetwarzania danych osobowych w Urzędzie stosuje się mechanizmy kontroli dostępu do tych danych. Osobą odpowiedzialną za ich funkcjonowanie jest informatyk.
2. Jeżeli dostęp do danych osobowych przetwarzanych w systemie informatycznym (w szczególności do urządzenia, aplikacji lub programu) posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

1) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
2) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

3. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

4. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, nie może być przydzielony innej osobie.
5. W przypadku, gdy do uwierzytelnienia użytkowników w systemie informatycznym służącym do przetwarzania danych osobowych używa się hasła, wdraża się środki wymuszające (jeżeli system informatyczny to umożliwia) stosowanie haseł składających się z co najmniej 8 znaków, w tym małych i wielkich liter oraz cyfr lub znaków specjalnych.

XXI.III Procedura zabezpieczenia antywirusowego

1. Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych stosowane jest oprogramowanie antywirusowe.
2. Za zaplanowanie i zapewnienie ochrony antywirusowej, w tym za zapewnienie odpowiedniej ilości licencji odpowiada Informatyk.
3. Każdy plik wczytywany do urządzenia informatycznego, w tym także wiadomości e-mail, podlega przetestowaniu programem antywirusowym.
4. W każdym urządzeniu informatycznym wyposażonym w dostęp do Internetu, musi być zainstalowane oprogramowanie antywirusowe.
5. Aktualizacja definicji wirusów odbywa się automatycznie przez system.

XXI.IV. Procedura tworzenia kopii zapasowych

1. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych tych danych.
2. Za system sporządzania kopii zapasowych danych osobowych odpowiedzialny jest Informatyk.
3. Kopie zapasowe danych osobowych w systemie informatycznym wykonuje wyłącznie Informatyk.
4. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
5. Kopie zapasowe powinny być cyklicznie kontrolowane przez Informatyka, w szczególności pod kątem prawidłowości ich wykonania oraz możliwości odtworzenia, poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.
6. Nośniki zawierające kopie danych osobowych przetwarzanych w systemie informatycznym Urzędu są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieupoważnionych.
7. Kopie zapasowe przechowuje się w odrębnej lokalizacji względem oryginału zabezpieczonych danych.
8. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.

XXI.V. Procedura usuwania urządzeń i nośników

1. Nośniki informacji służące do przetwarzania danych osobowych w Urzędzie pozbawia się tych danych przed usunięciem, a następnie poddaje się je procedurze przynajmniej trzykrotnego całkowitego nadpisywania.
2. W przypadku braku możliwości, o której stanowi pkt wyżej (np. płyty CD, uszkodzone dyski twarde), nośniki informacji służące do przetwarzania danych osobowych w Urzędzie, przed usunięciem poddaje się innym czynnościom skutkującym ich trwałemu fizycznemu uszkodzeniu, uniemożliwiającemu odczytanie danych zgromadzonych na nośniku.
3. Po usunięciu urządzenia lub nośnika służącego do przetwarzania danych osobowych w Urzędzie, należy wykreślić go z Rejestru urządzeń i nośników, służących do przetwarzania danych osobowych.

XXI.VI. Procedura przeglądów i konserwacji

1. Przeglądy, naprawy i konserwacje urządzeń informatycznych służących do przetwarzania danych osobowych, przeprowadzane są w lokalizacji Urzędu przez Informatyka, z zastrzeżeniem poniższych punktów.
2. Naprawy i konserwacje urządzeń informatycznych służących do przetwarzania danych osobowych mogą być wykonywane przez przedsiębiorstwa lub wykonawców zewnętrznych wyłącznie na podstawie zawartych umów.
3. W przypadku przekazywania do naprawy urządzeń informatycznych służących do przetwarzania danych osobowych:

a) jeśli uszkodzenie nie dotyczy nośników pamięci, należy je wymontować i do naprawy przekazać urządzenie nie zawierające nośników, na których są dane osobowe,
b) jeśli uszkodzenie dotyczy nośników pamięci, należy zniszczyć je, przywracając pliki zawierające dane osobowe z kopii zapasowej,
c) jeśli uszkodzenie dotyczy nośników pamięci a jednocześnie brak jest plików zawierających dane osobowe, wówczas należy zrealizować naprawę pod bezpośrednim nadzorem osoby upoważnionej albo po zawarciu umowy powierzenia danych osobowych.

4. Informatyk jest zobowiązany wykonywać przynajmniej wyrywkowe przeglądy techniczne urządzeń służących do przetwarzania danych osobowych nie rzadziej niż raz w roku.
5. Informatyk prowadzi rejestr napraw, przeglądów i konserwacji systemu informatycznego.”.

2. Załącznik Nr 1 do Polityki Bezpieczeństwa Danych Osobowych dla Urzędu Miejskiego w Karczewie do Zarządzeniu Nr 29/2019 Burmistrza Karczewa z dnia 02 kwietnia 2019 r. w sprawie ustalenia Polityki bezpieczeństwa danych osobowych w Urzędzie Miejskim w Karczewie, ustalenia Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń

Urzędu Miejskiego w Karczewie, ustalenia Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych otrzymuje nowe brzmienie, jak w Załączniku Nr 1do niniejszego zarządzenia.

3. Załącznik Nr 11 do Polityki Bezpieczeństwa Danych Osobowych dla Urzędu Miejskiego w Karczewie do Zarządzeniu Nr 29/2019 Burmistrza Karczewa z dnia 02 kwietnia 2019 r. w sprawie ustalenia Polityki bezpieczeństwa danych osobowych w Urzędzie Miejskim w Karczewie, ustalenia Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń Urzędu Miejskiego w Karczewie, ustalenia Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych otrzymuje nowe brzmienie, jak w Załączniku Nr 2 do niniejszego zarządzenia.

§ 2. Nadzór nad przestrzeganiem postanowień dokumentacji ochrony danych osobowych oraz stosowaniem niniejszego zarządzenia sprawuje Inspektor Ochrony Danych.

§ 3. Załączniki do zarządzenia są przeznaczone do użytku wewnętrznego.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Karczewa
Michał Rudzki