ZARZĄDZENIE Nr 92
Burmistrza Miasta Rawa Mazowiecka
z dnia 9 września 2020 r.

w sprawie wyznaczenia Administratora Systemów Informatycznych

Na podstawie 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) (Dz.U.UE.L.2016.119.1 z dnia 04.05.2016 r.) oraz wprowadzonej Zarządzeniem Nr 18/2020 Burmistrza Miasta Rawa Mazowiecka dnia 2 września 2019 r. Polityki Ochrony Danych Osobowych w Urzędzie Miasta Rawa Mazowiecka zarządzam co następuje:

§ 1.

Z dniem 9 września 2020 r. powołuję **Pana Roberta Fedorowicza na funkcję Administratora Systemów Informatycznych w Urzędzie Miasta Rawa Mazowiecka (ASI).**

§ 2.

Zakres czynności Administratora Systemów Informatycznych stanowi załącznik do niniejszego zarządzenia.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ MIASTA
mgr inż. Piotr Irla

Mariusz Marusiński
RADCA PRAWNY

Załącznik do Zarządzenia Nr 92 z dnia 9.09.2020 r.
Zakres czynności Administratora Systemu Informatycznego
w Urzędzie Miasta Rawa Mazowiecka

1. **Współpraca przy przygotowaniu, wdrażaniu oraz respektowaniu przez pracowników dokumentacji ochrony danych osobowych,** w szczególności instrukcji zarządzania systemem informatycznym. Nadzór nad zabezpieczeniami technicznymi i organizacyjnymi zgodnie z motywem 78 RODO w zakresie:
   - zarządzanie aktywami,
   - kontroli dostępu (rejestrowanie i wyrejestrowywanie użytkowników, zarządzanie hasłami, użycie uprzywilejowanych programów narzędziowych),
   - środków ochrony kryptograficznej (polityka stosowania zabezpieczeń, zarządzanie kluczami),
   - bezpieczeństwa fizycznego i środowiskowego oraz bezpieczeństwo eksploatacji (zarządzanie zmianami, zarządzanie pojemnością, zapewnienie ciągłości działania, rejestrowanie zdarzeń i monitorowanie),
   - bezpieczeństwa komunikacji (zabezpieczenie, rozdzielenie sieci),
   - pozyskiwania, rozwoju i utrzymywania systemów,
   - relacji z dostawcami (umowy, w tym umowy powierzenia przetwarzania),
   - zarządzania incydentami związanymi z bezpieczeństwem informacji,
   - zarządzania ciągłością działania,
   - zgodnością z wymaganiami prawnymi i umownymi.

2. **Współpraca przy przeprowadzaniu okresowych sprawdzeń**, czyli monitorowanie przestrzegania RODO, w tym działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.
3. **Współpraca podczas przeprowadzania procesu analizy ryzyka** wynikiem, której powinny być obszary lub też zasoby, które nie są zabezpieczone lub zastosowane wobec nich zabezpieczenia nie są wystarczające. Mowa o zasobach, które powodują największe prawdopodobieństwo zmaterializowania się przyjętych zagrożeń w organizacji.
4. **Zapewnienia ciągłości działania systemu,** w tym zabezpieczenie zbiorów danych oraz programów służących do przetwarzania danych osobowych poprzez systematyczne wykonywanie kopii zapasowych.
5. **Monitorowanie źródeł zasilania oraz zabezpieczenie przed zakłóceniami w sieci zasilającej** systemów informatycznych służących do przetwarzania danych osobowych, których nagła przerwa w pracy mogłaby spowodować utratę danych lub naruszenie ich integralności.
6. **Nadzór nad naprawą oraz likwidacją urządzeń komputerowych.**
7. **Kontrola przeglądu i konserwacji systemów informatycznych służących do przetwarzania danych osobowych,** w tym m.in. wykorzystywanie jedynie oprogramowania posiadającego wsparcie producenta oraz systematyczne, automatyczne lub zgodne z biuletynem bezpieczeństwa jego aktualizowanie

8. **Zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego,** którego celem może okazać się uzyskanie nieuprawnionego dostępu do danych.
9. **Dostosowywanie systemów informatycznych służących do przetwarzania danych osobowych** do wymogów RODO w tym m.in.:
    - zapewnienie możliwości realizacji prawa do przenoszenia danych,
    - zapewnienie możliwości realizacji prawa do ograniczenia przetwarzania,
    - zapewnienie możliwości realizacji prawa do bycia zapomnianym,
    - zapewnienie możliwości realizacji prawa do zgłoszenia sprzeciwu wobec realizowanych działań marketingowych, gdzie w ramach zasady rozliczalności warto pamiętać o zapewnieniu możliwości zweryfikowania dokładnej godziny i daty, kiedy zgoda została wyrażona lub wycofana.
10. **Dbanie o zabezpieczenie pomieszczeń, w których przetwarzane są dane osobowe**, w szczególności archiwów, szachtów sieciowych lub serwerowni przed dostępem osób nieuprawnionych lub innymi zdarzeniami losowymi, w tym m.in. zabezpieczenia:
    - fizyczne (drzwi, ściany, stropy itp.),
    - techniczne (elektroniczne systemy zabezpieczeń),
    - środowiskowe (zapewnienie optymalnych warunków pracy urządzeń i ochrona przeciwpożarowa),
    - personalne (pracownicy ochrony, świadomy personel przedsiębiorstwa),
    - organizacyjne (obowiązujące w przedsiębiorstwie regulaminy, polityki itp.)
11. **Ochrona przed zagrożeniami pochodzącymi z sieci publicznej** poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, w tym
    - firewalle,
    - filtry antyspamowe,
    - wydzielanie VLAN'ów
    - stosowanie filtracji urządzeń, które mogą uzyskać dostęp do sieci produkcyjnej,
    - stosowanie wielu innych rozwiązań z uwzględnieniem dostępnych technologii oraz dostępnych środków finansowych.

12. Śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych i wdrażanie takich narzędzi, metod pracy oraz sposobów zarządzania systemem informatycznym, które bezpieczeństwo to wzmocnią.