Zarządzenie Nr 43/2018
Burmistrza Miasta i Gminy Prabuty
z dnia 22 maja 2018 roku

dotyczące uzyskania i utrzymania w Urzędzie Miasta i Gminy w Prabutach zgodności z wymaganiami 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).

Mając na uwadze obowiązek spełnienia przez Urząd Miasta i Gminy w Prabutach, Organizacją będącą Administratorem Danych Osobowych zw.d. ADO lub Organizacją) wymagań 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) (zw.d. RODO) oraz w związku z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, (zw.d. u.o.d.o.), zarządzam co następuje:

§ 1.

1. Z dniem 25 maja 2018 r. wyznaczam na Inspektora Ochrony Danych, w związku z art. 37-39 RODO Pana Dariusza Klimowskiego, zw.d. IOD.
2. Do zadań IOD w szczególności należą:
   1) koordynacja uzyskania i utrzymania systemu zarządzania spełniającego wymagania RODO na podstawie regulacji wewnętrznych, z uwzględnieniem:
      a) zarządzania ryzykiem,
      b) zarządzania incydentami,
      c) opracowania i prowadzenia rejestru czynności przetwarzania,
      d) przeprowadzenia szkoleń dla pracowników w zakresie wymagań RODO,
   2) nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych, bezpieczeństwa informacji oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, jak również przestrzegania zasad określonych w tej dokumentacji poprzez weryfikację:
      a) opracowania, kompletności oraz aktualności dokumentacji przetwarzania danych, w postaci Polityki Przetwarzania Danych Osobowych i Instrukcji Zarządzania Systemem Informatycznym,
      b) zgodności dokumentacji oraz zasad przetwarzania danych z obowiązującymi przepisami prawa oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
      c) stanu faktycznego w zakresie przetwarzania danych osobowych,
      d) zgodności ze stanem faktycznym zgodnie z dokumentacją przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych;
   3) przestrzeganie zasad i obowiązków określonych w dokumentacji przetwarzania danych,
   4) dokonywanie sprawdzeń zgodności przetwarzania danych osobowych z RODO,
   5) nadzorowanie zgodności rejestru zbiorów danych przetwarzanych przez administratora danych,
   6) prowadzenie szkoleń wewnętrznych w zakresie ochrony danych osobowych i bezpieczeństwa informacji na podstawie odrębnych regulacji,
   7) przygotowywanie oraz opiniowanie umów dotyczących powierzenia przetwarzania danych osobowych,
   8) nadzór nad zgodnym z RODO regulowaniem stosunków umownych z podmiotami przetwarzającymi dane osobowe należące do ADO,
   9) reprezentowanie ADO w kontaktach z organem nadzoru odpowiedzialnego za ochronę danych osobowych, z zakresie kontroli zdalnej oraz bezpośredniej,
   10) współpraca z Działem IT Organizacji w zakresie tych obszarów, które ściśle wiążą się z ochroną danych osobowych,
      a) opiniowanie innych dokumentów Organizacji pod kątem zgodności z przepisami ustawy o ochronie danych osobowych oraz z przepisami wykonawczymi;
      b) rozpatrywanie skarg osób fizycznych w związku z zarzutem naruszenie ich praw w zakresie zasad przetwarzania danych osobowych;
      c) przygotowanie poleceń i upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

d) bieżące monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz konsultacje w przedmiocie aktualizacji zabezpieczeń danych w razie istotnych zmian organizacyjnych;
e) opiniowanie wniosków o udostępnienie danych osobowych;
f) konsultacje w sprawach związanych z ochroną danych osobowych;
g) określenie zasad i procedur (we współpracy z Działem IT) zapewniających bezpieczeństwo systemu informatycznego przetwarzającego dane osobowe;
h) informowanie administratora o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii Europejskiej lub jej państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
i) monitorowanie przestrzegania RODO oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podziału obowiązków,
j) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
k) współpraca z organem nadzorczym;
l) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

3. Dane kontaktowe IOD:
   1) imię i nazwisko IOD – Dariusz Klimowski
   2) e-mail: IOD@fioi.org,
   3) tel. 552394874,
   4) adres Kancelarii IOD: 82-300 Elbląg, ul. Kosynierów Gdyńskich 25.
4. Zobowiązuję Pana Dariusza Pietkiewicza do zamieszczenia informacji, o których mowa w ust. 3 powyżej na stronie internetowej Organizacji pod adresem http://www.prabuty.pl oraz w Biuletynie Informacji Publicznej pod adresem http://bip.prabuty.pl.
5. W związku z art. 10 ust. 1 u.o.d.o. zobowiązuję Pana Jędrzeja Krasińskiego, Sekretarza Miasta i Gminy Prabuty do dokonania zgłoszenia IOD do organu nadzorczego w terminie 14 dni od dnia wejścia w życie niniejszego Zarządzenia.

§ 2.

Powołuję Zespół ds. uzyskiwania i utrzymywania zgodności z wymaganiami RODO w składzie:
1) IOD – koordynator,
2) Przewodniczący/a Zespołu działający w imieniu ADO – Jędrzej Krasiński,
3) Koordynator systemów i zasobów informatycznych – Dariusz Pietkiewicz,

§ 3.

Zakres zadań Zespołu ds. uzyskiwania i utrzymywania zgodności z wymaganiami RODO obejmuje:
1) w zakresie obowiązkowych rejestrów:
   a) opracowanie rejestru czynności przetwarzania przez komórki organizacyjne, zgodnie z wzorem preferowanym przez organ nadzorczy,
   b) opracowanie rejestru kategorii czynności przetwarzania przez komórki organizacyjne, zgodnie z wzorem preferowanym przez organ nadzorczy, w przypadku pełnienia funkcji podmiotu przetwarzającego,
2) w zakresie analizy ryzyka i implementacji zabezpieczeń:
   a) identyfikację wymagań prawnych związanych z ochroną danych osobowych,
   b) określenie zasobów informacyjnych wymagających zastosowania mechanizmów zabezpieczających,
   c) klasyfikację ryzyk i oszacowanie prawdopodobieństwa lub częstości ich występowania,
   d) identyfikację podatności zasobów na ryzyko,
   e) oszacowanie ryzyka,
   f) ocenę możliwych zabezpieczeń pod względem bezpieczeństwa,
   g) pod kątem ekonomicznym i użytkowym,
   h) wybór i zapewnienie zabezpieczeń optymalnych,
3) w zakresie zarządzania incydentami:
   a) określenie metod identyfikacji incydentów,
   b) ustalenie sposobu postępowania z incydentami,
   c) ustalenie sposobu zgłaszania incydentów do organu nadzorczego,
4) w zakresie organizacji ochrony danych osobowych i bezpieczeństwa informacji:
   a) opracowanie systemowych mechanizmów klasyfikacji informacji (klauzul), zmierzających do zapewnienia bezpieczeństwa danych osobowych oraz kontroli nad dostępem i przepływem informacji,
   b) opracowanie systemowych mechanizmów zarządzania klauzulami,

c) opracowanie mechanizmów bezpieczeństwa osobowego,
d) opracowanie programu szkoleń dla pracowników oraz personelu wykonującego pracę z wykorzystaniem zasobów Organizacji na podstawie umów innych niż umowa o pracę,
e) opracowanie systemowych mechanizmów zarządzania zmianami.

5) w zakresie zabezpieczeń teleinformatycznych i technicznych:
a) opracowanie systemowych mechanizmów zarządzania oprogramowaniem,
b) opracowanie systemowych mechanizmów zarządzania kopiami zapasowymi,
c) opracowanie mechanizmów utrzymywania gotowości i reagowania na incydenty w środowisku elektronicznym,
d) opracowanie mechanizmów bezpieczeństwa sieci i okablowania,
e) opracowanie systemowych mechanizmów nadzoru nad konserwacją i serwisem sieci, sprzętu teleinformatycznego i okablowania,
f) określenie wymagań technicznych i procedur zarządzania mechanizmami kryptograficznymi,
g) ustanowienie i przeprowadzenie walidacji bezpieczeństwa informacji.

6) w zakresie dokumentacji do obsługi adekwatnych działań wynikających z RODO:
a) weryfikację Polityk Bezpieczeństwa,
b) opracowanie Planu ciągłości działania,
c) weryfikację wdrożonych i opracowanie nowych regulaminów i wytycznych w zakresie bezpieczeństwa informacji,
d) weryfikację procedur pod kątem zgodności z dokumentem odniesienia – RODO,
e) opracowanie procedur i instrukcji,
f) opracowanie systemowych mechanizmów ewidencjonowania i zapisu działań związanych z ochroną danych osobowych i informacji.

§ 4.

1. Zobowiązuję wszystkich pracowników Organizacji do aktywnego uczestnictwa w pracach nad uzyskiwaniem i utrzymywaniem zgodności z wymaganiami RODO. Uczestnictwo to powinno obejmować w szczególności następujące działania:
1) przygotowywanie danych wejściowych niezbędnych do opracowania dokumentacji systemowej, w zakresie:
a) czynności przetwarzania i kategorii czynności przetwarzania w ramach zakresu czynności/obowiązków/uprawnień,
b) celów przetwarzania danych osobowych wraz z podaniem prawnego uzasadnienia przetwarzania poprzez:
- wskazanie przepisu prawa – akt prawny oraz właściwy art. i/lub paragraf,
- wskazanie innych podstaw do przetwarzania,
c) wpisania aktywów[1] związanych z ochroną danych osobowych do stosownego zestawienia (formularz – arkusz kalkulacyjny), zgodnie z Procedurą inwentaryzacji aktywów i postępowania z ryzykiem, w tym:
- aktywa sprzętowe i infrastrukturalne,
- oprogramowanie,
- dokumentacja i zapisy,
- określenia czy dane aktywa należą do lub są częścią systemów krytycznych[2] lub niekrytycznych,
- określenia kategorii informacji,
- określenia własności aktywów i ryzyka,
- wskazania miejsca przetwarzania danych osobowych – lokalizacji aktywów,
d) zabezpieczeń technicznych i teleinformatycznych:
- wskazanie zabezpieczeń w budynkach, wokół budynków czy terenu Organizacji,
- wskazanie zabezpieczeń technicznych i organizacyjnych dla infrastruktury teleinformatycznej i jej towarzyszącej,
- zabezpieczeń dla urządzeń mobilnych i pracowników realizujących pracę zdalnie lub uprawnionych do wynoszenia danych osobowych w celach służbowych poza Organizację,

2) aktywny udział w uzyskiwaniu i utrzymywaniu zgodności z RODO, w tym:
a) niezwłoczne wnoszenie do IOD informacji o nowych lub zmodyfikowanych zbiorach danych osobowych na własnych stanowiskach pracy lub w komórkach organizacyjnych,

---

[1] Aktywa – zasoby służące do przetwarzania danych osobowych i informacji oraz dane osobowe i informacje jako zbiory dokumentów i zapisów.

[2] Systemy krytyczne – systemy obejmujące procesy lub składniki majątku o istotnym znaczeniu dla Organizacji, których utrata, uszkodzenie lub modyfikacja mogłaby spowodować utratę ciągłości działania oraz bezpowrotną utratę fizyczną. Przykładami systemów krytycznych są: serwer, dyski z kopiami zapasowymi, archiwum dokumentacji papierowej, stanowiska przetwarzające dane osobowe bez dostępu do automatycznych kopii zapasowych w ramach sieci łączącej stanowiska z serwerem. Katalog systemów krytycznych jest adekwatny do rejestrów czynności przetwarzania oraz rejestrów kategorii czynności przetwarzania (jeśli dotyczy) w Organizacji.

b) niezwłoczne wnoszenie do IOD informacji o podmiotach przetwarzających, o których mowa w art. 28 RODO,
c) niezwłoczne informowanie o zagrożeniach dla ochrony danych osobowych,
d) uczestnictwo w zarządzaniu ryzykiem wg Procedury inwentaryzacji aktywów i postępowania z ryzykiem,
e) formułowanie i wspólna z IOD analiza kazusów związanych ze stanowiskiem pracy, w celu dokładnego zweryfikowania czynności przetwarzania bądź kategorii czynności przetwarzania,

3) wykonanie czynności związanych ze skutecznym funkcjonowaniem systemu zgodności z RODO na swoich stanowiskach pracy.

2. Powyższe czynności odbywać się powinny w stałym kontakcie z IOD, w celu uzyskania gotowego zbioru udokumentowanej informacji odpowiadającej wymaganiom RODO.

§ 5.

Zobowiązuję wszystkich pracowników Organizacji do stosowania zasad zapewniających zgodność z RODO poprzez:

1) przetwarzanie danych osobowych na stanowiskach pracy wyłącznie w przypadkach określonych w RODO z zastrzeżeniem:
   a) spełnienia zasad dotyczących przetwarzania,
   b) uzyskania zgodności przetwarzania z prawem,
   c) spełnienia warunków uzyskania zgody osób fizycznych lub przetwarzania w warunkach niewymagających zgody,
2) przetwarzanie danych osobowych przez wszystkich pracowników powinno odbywać się:
   a) w sposób zapewniający wywiązanie się ADO z obowiązków prawnych,
   b) w sposób zapewniający skuteczny nadzór nad danymi osobowymi przekazanymi podmiotom przetwarzającym lub współadministratorom.
3) stosowanie się do postanowień określonych w dokumentacji systemu przetwarzania danych osobowych zgodne z RODO, to jest do:
   a) Systemu zarządzania ochroną danych osobowych i bezpieczeństwem informacji (Wewnętrzny kodeks postępowania),
   b) Deklaracji stosowania zabezpieczeń w systemie zarzadzania ochroną danych osobowych i bezpieczeństwem informacji,
   c) Procedur systemu zarzadzania ochroną danych osobowych i bezpieczeństwem informacji.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta i Gminy Prabuty