Zarządzenie Nr 17/2019
Starosty Powiatu Ropczycko – Sędziszowskiego
z dnia 11 lutego 2019 r.

w sprawie wyznaczenia Inspektora Ochrony Danych oraz Administratora Systemu Informatycznego w Starostwie Powiatowym w Ropczycach.

Na podstawie art. 34 ust. 1 i art. 35 ust. 2 ustawy z dnia 5 czerwca 1998r. o samorządzie powiatowym (t.j. Dz. U. z 2018r., poz. 995 z późn. zm.), ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018r., poz. 1000) oraz art. 37 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 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(RODO), w związku z Uchwałą nr VI/43/2018 Zarządu Powiatu Ropczycko – Sędziszowskiego z dnia 18 grudnia 2018r. w sprawie uchwalenia Regulaminu Organizacyjnego Starostwa Powiatowego w Ropczycach

zarządzam co następuje:

§ 1. Mając na uwadze prawidłowość realizacji obowiązków wynikających ze wskazanego powyżej RODO, w celu maksymalizacji poziomu bezpieczeństwa danych osobowych administrowanych przez Starostę Powiatu Ropczycko -Sędziszowskiego wyznacza się:

1).Panią Dorotę Siorek do pełnienia funkcji Inspektora Ochrony Danych (IOD).

2) Pana Adama Kulig do pełnienia funkcji Administratora Systemu Informatycznego

§ 2. Do zadań Inspektora Ochrony Danych należy:

1) informowanie Administratora Danych Osobowych oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy aktualnie obowiązujących przepisów o ochronie danych osobowych i doradzanie im w tej sprawie;

2) monitorowanie przestrzegania RODO, innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych oraz polityk wewnętrznych administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;

4) współpraca z organem nadzorczym;

5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz w stosownych przypadkach we wszystkich innych sprawach związanych z przetwarzaniem danych;

6) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy ogólnego rozporządzenia o ochronie danych.

§ 3. Inspektor Ochrony Danych działa w ramach posiadanych upoważnień i pełnomocnictw, w szczególności jest uprawniony do:

1) nadzorowania wykonywanych zadań przez osoby upoważnione do przetwarzania danych osobowych oraz pozostałych pracowników w zakresie przestrzegania zasad, instrukcji i procedur zawartych w politykach wewnętrznych oraz aktualnie obowiązujących aktów prawnych w zakresie ochrony danych osobowych;

2) wstępu do wszystkich pomieszczeń w obszarze przetwarzania, a także wglądu do danych osobowych przetwarzanych przez Administratora Danych Osobowych w trakcie prowadzonych sprawdzeń wewnętrznych ;

3) występowania do wszystkich pracowników i współpracowników Administratora Danych Osobowych o złożenie wyjaśnień w procesie przetwarzania danych osobowych oraz udostępnienia informacji i dokumentów stanowiących dowód w sprawie;

4) wydawania poleceń wszystkim pracownikom i współpracownikom Administratora Danych Osobowych w zakresie zgodnego z prawem przetwarzania danych osobowych.

§ 4. Administrator danych osobowych zapewnia niezależność pełnienia funkcji Inspektora Ochrony Danych (IOD) poprzez:

1) zagwarantowanie bezpośredniej podległości w zakresie wykonywania zadań IOD oraz raportowania wyłącznie do Starosty Powiatu Ropczycko – Sędziszowskiego;

2) zapewnienie IOD odpowiednich środków organizacyjnych i technicznych w celu wykonywania zadań nałożonych przepisami prawa, w tym dostęp do danych i informacji o procesach przetwarzania;

3) niezwłoczne włączanie IOD we wszystkie zagadnienia dotyczące ochrony danych osobowych, które będą toczyły się u Administratora Danych Osobowych,

4) nienakładanie na IOD zadań, które powodowałyby konflikt interesów i uniemożliwiały zachowanie przez niego całkowitej niezależności.

§ 5. Administrator Systemu Informatycznego odpowiada za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych i teleinformatycznych u Administratora Danych Osobowych.

§ 6. Do zadań Administratora Systemu Informatycznego należy w szczególności:

1) monitorowanie:

a)zbierania, przechowywania, przekazywania i udostępniania danych osobowych przetwarzanych w systemach informatycznych,

b) zabezpieczeń systemów informatycznych w zakresie stosowania:

- IPS/Firewall/VPN oraz programów antywirusowych,
- szyfrowania dysków i środków ochrony kryptograficznej,
- mechanizmów autoryzacji i kontroli dostępu do danych (uwierzytelnianie użytkowników, hasła),
-zabezpieczenia przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do baz danych osobowych,

2) nadzorowanie:

a) zakładania, blokowania, zawieszania i uaktywniania kont w systemie informatycznym,
b) logicznych i informatycznych zabezpieczeń systemów w zakresie:
- przepływu informacji pomiędzy systemami informatycznymi a siecią publiczną,
- działań inicjowanych z sieci i z systemów informatycznych,
c) umów i procedur przekazywania podmiotowi zewnętrznemu dostępu do systemów informatycznych oraz elektronicznych nośników informacji zawierających dane osobowe,
d) tworzenia kopii zapasowych zbiorów danych osobowych,
e) zasad ochrony, przekazywania i niszczenia kopii zapasowych zbiorów danych osobowych oraz programów zastosowanych do ich przetwarzania,
3) realizowanie przedsięwzięć w zakresie:
a) wyjaśniania i dokumentowania, wspólnie z IOD, przypadków naruszenia zasad bezpieczeństwa systemów informatycznych,
b) dokonywania oceny zgodności programów z przepisami bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych,
d) kontrolowania, wspólnie z IOD, pracowników w zakresie przestrzegania zasad bezpieczeństwa i ochrony danych osobowych poprzez prowadzone sprawdzenia (kontrole lub audyty).

§ 7. Administrator Systemu Informatycznego wykonując czynności służbowe posiada uprawnienie do:

1) wstępu do wszystkich pomieszczeń w obszarze przetwarzania;
2) wglądu do danych osobowych przetwarzanych przez Administratora Danych Osobowych w systemach informatycznych, w zakresie prowadzonych sprawdzeń;
3) występowania do wszystkich pracowników i współpracowników Administratora Danych Osobowych o złożenie wyjaśnień w procesie przetwarzania danych osobowych w systemach informatycznych;
4) wydawania poleceń wszystkim pracownikom i współpracownikom Administratora Danych Osobowych w zakresie zgodnego z prawem przetwarzania danych osobowych w systemach informatycznych.

§ 8. Administrator Systemu Informatycznego w zakresie wykonywania swej funkcji podlega bezpośrednio Staroście Powiatu Ropczycko – Sędziszowskiego;

§ 9. Mając na względzie wsparcie IOD oraz ASI Administrator Danych Osobowych zobowiązuje wszystkich pracowników Starostwa Powiatowego, w szczególności osoby pełniące funkcje kierownicze, do pełnej współpracy z IOD i ASI w zakresie realizowanych przez nich zadań.

§ 10. Traci moc Zarządzenie numer 42/2015 Starosty Powiatu Ropczycko – Sędziszowskiego z dnia 26 czerwca 2015 r.

§ 11. Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązująca od dnia 1 stycznia 2019 r.

ADWOKAT
mgr Józef Gudyka

STAROSTA
Witold Darłak