Burmistrz Sośnicowic

ZARZĄDZENIE Nr 21/ 2019
Burmistrza Sośnicowic
z dnia 21.02.2019 r.

w sprawie wprowadzenia procedury powierzenia danych osobowych w Urzędzie Miejskim w Sośnicowicach

Na podstawie art. 33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2018 r. 994 z późn. zm.) w związku z art. 28 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) zarządzam, co następuje:

§ 1

Wprowadza się procedurę powierzenia przetwarzania danych osobowych w Urzędzie Miejskim w Sośnicowicach.

§ 2

Zobowiązuję wszystkich pracowników Urzędu Miejskiego w Sośnicowicach do zapoznania się z niniejszą instrukcją.

§ 3

Zarządzenie wchodzi w życie z dniem 22.02.2019 r.

BURMISTRZ SOŚNICOWICE

BURMISTRZ
Leszek Kołodziej

Procedura powierzenia przetwarzania danych osobowych w Urzędzie Miejskim w Sośnicowicach

Celem procedury jest określenie ogólnych zasad związanych z powierzeniem przetwarzania danych w Urzędzie Miejskim w Sośnicowicach. Procedura obowiązuje wszystkich pracowników Urzędu Miejskiego w Sośnicowicach.
Artykuł 28 Rozporządzenia Parlamentu Europejskiego (UE) 2016/679 z dnia 27 kwietnia 2016 roku, 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 – Rodo, dalej Rozporządzenie, zobowiązuje Urząd Miejski w Sośnicowicach czyli Administratora danych, do zawarcia Umowy powierzenia z podmiotem przetwarzającym (procesorem), któremu na potrzeby wykonania umowy, realizacji usługi, zlecenia przekazujemy dane osobowe.
Zgodnie z art. 28 ust. 9 Rozporządzenia, umowa powierzenia powinna mieć formę pisemną, w tym formę elektroniczną i może być elementem szerszej umowy. Zgodnie z artykułem 28 ust. 1 Rozporządzenia zadaniem Administratora danych jest wybór takiego usługodawcy, który gwarantuje wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność z Rozporządzeniem i ochronę praw osób, których dane dotyczą. Zawarcie umowy powierzenia przetwarzania danych przebiega zgodnie z opisanym poniżej schematem działania:

1. **Etap 1 - Potrzeba powierzenia danych** - dział / pracownik merytoryczny Administratora w porozumieniu z Inspektorem Ochrony Danych dokonuje sprawdzenia czy w trakcie wykonania umowy, realizacji usługi, zlecenia zachodzi konieczność powierzenia danych. Powierzenie może dotyczyć różnego rodzaju czynności przetwarzania danych, np. związanych z obsługą informatyczną, serwisem urządzeń, archiwizacją i brakowaniem dokumentacji, niszczeniem nośników danych, hostingu strony internetowej itp.
2. **Etap 2 - Weryfikacja podmiotu przetwarzającego** - każdorazowo przed powierzeniem przetwarzania danych, pracownik merytoryczny w porozumieniu z Inspektorem Ochrony Danych, zgodnie z art. 28 ust.1 Rozporządzenia, dokonuje sprawdzenia podmiotu przetwarzającego na podstawie ankiety (zgodnie z załącznikiem nr 1 do procedury), zapytania lub audytu. Dokonując wyboru procesora należy kierować się nie tylko ceną za świadczone usługi, ale przede wszystkim podstawowym kryterium oceny powinna być możliwość spełnienia przez podmiot przetwarzający wymogów związanych z przetwarzaniem i ochroną danych. Ocena w tym zakresie powinna opierać się na informacjach na temat podmiotu, któremu administrator zamierza powierzyć przetwarzanie danych, w szczególności na dokumentach wskazujących możliwości techniczne, umiejętności oraz doświadczenie w zakresie przetwarzania i ochrony danych. W przypadku gdy podmiot, któremu administrator zamierza powierzyć przetwarzanie danych, nie jest w stanie spełnić wymogów dotyczących ochrony danych określonych w Rozporządzeniu, powierzenie przetwarzanie danych takiemu podmiotowi jest niedopuszczalne.

3. **Etap 3 - Projekt umowy powierzenia** - zgodnie z art. 28 ust. 3 Rozporządzenia przetwarzanie danych przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które wiążą podmiot przetwarzający i Administratora. Przygotowanie projektu umowy powierzenia powinno być konsultowane z Inspektorem Ochrony Danych oraz Radcą Prawnym. Za nadanie numeracji umowie powierzenia odpowiada **dział/pracownik merytoryczny. Właściwy numer umowy pracownik merytoryczny uzyska u Inspektora Ochrony Danych .**
4. **Etap 4 - Podpisanie umowy powierzenia** - przedstawienie umowy powierzenia podmiotowi przetwarzającemu do podpisania jest realizowane przez dział / pracownika merytorycznego. Umowy muszą być zawarte w takim terminie, by ich realizacja rozpoczęła się po dopełnieniu obowiązków wynikających z przepisów dotyczących ochrony danych osobowych.
5. **Etap 5 - Obieg dokumentacji:**

   - podpisany przez podmiot przetwarzający oryginał Umowy powierzenia trafia jeden egzemplarz do Inspektora Ochrony Danych , drugi egzemplarz zostaje w dokumentach sprawy dział/pracownik merytoryczny.
6. **Etap 6 - Ewidencja zawartych umów powierzenia** - wprowadzenie umowy powierzenia do rejestru zawartych umów jest dokonywane przez Inspektora Ochrony Danych na podstawie otrzymanej umowy. Prowadzenie ewidencji umów powierzenia przetwarzania odbywa się zgodnie ze wzorem z załącznika nr 2. Ewidencja może być prowadzona w formie papierowej lub elektronicznej.
7. **Etap 7** -Aktualizacja rejestru czynności przetwarzania dokonywana jest przez Inspektora Ochrony Danych.

Procedura zawiera:

Załącznik nr 1- Ankieta dla podmiotu przetwarzającego

Załącznik nr 2 - Rejestr zawartych umów powierzenia

Procedurę opracował

Inspektor Ochrony Danych 21.02.2018 r. .....

(data i podpis)

Procedurę zatwierdził

Administrator Danych 21.02.2018 r. BURMISTRZ Leszek Kołodziej

(data i podpis)

Załącznik nr 1 do Procedury powierzenia przetwarzania danych osobowych w Urzędzie Miejskim w Sośnicowicach

Ankieta dla podmiotu przetwarzającego (procesora) dotycząca wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych osobowych zgodnie z RODO*

.....

(nazwa podmiotu przetwarzającego)

L.p	Pytanie dotyczące zabezpieczenia	Tak, jest stosowane	Nie jest stosowane	Uwagi
1	Czy wdrożono procedurę nadawania uprawnień dla pracowników i współpracowników świadczących pracę na danych osobowych?			
2	Czy realizowane są szkolenia dla personelu zatrudnionego przy przetwarzaniu z zakresu ochrony danych osobowych?			
3	Czy jest prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych?			
4	Czy prowadzone są audyty z zakresu bezpieczeństwa informacji?			
5	Czy realizowane są testy penetracyjne?			
6	Czy wdrożono procedurę zachowania ciągłości działania firmy?			
7	Czy zastosowano procedurę ciągłości działania?			
8	Czy realizowana jest polityka kontroli dostępu do pomieszczeń/komputerów?			
9	Czy pomieszczenia, w których przetwarzane są dane osobowe, są zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym?			
10	Czy pomieszczenia, w których są przetwarzane dane osobowe są zabezpieczone przed pożarami za pomocą gaśnic/ czujki dymu?			
11	Czy dostęp do pomieszczeń, w których przetwarzane są dane osobowe jest kontrolowany przez system monitoringu/ alarm?			
12	Czy firma zabezpiecza dostęp do serwerowni/ archiwum?			
13	Czy dokumenty papierowe niszczone są w niszczarkach?			
14	Czy dokumentacja w pomieszczeniach jest przechowywana w szafach			

Ankieta dla podmiotu przetwarzającego (procesora) dotycząca wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych osobowych zgodnie z RODO*

	zamykanych na klucz? Czy szafy są metalowe?			
15	Czy wyznaczone są strefy dostępu? Czy został wdrożony system kontroli dostępu?			
16	Czy istnieje możliwość, aby osoby nieuprawnione miały dostęp do danych osobowych? (Dostęp do komputera/ dostęp do stojącej drukarki na korytarzu/ możliwość patrzenia na ekran komputera w czasie pracy/ możliwość przeczytania danych na aktach i dokumentach leżących na biurku, w otwartych szafach itp.)?			
17	Czy firma posiada wdrożone systemy antywirusowe i antyspamowe?			
18	Czy firma posiada systemy zasilania awaryjnego UPS?			
19	Czy firma szyfruje połączenia/pocztę/pendrivy?			
20	Czy firma posiada procedurę zarządzania aktualizacjami?			
21	Czy firma posiada procedurę tworzenia kopii zapasowych?			
22	Czy firma stosuje zasadę rozliczalności operacji?			
23	Czy firma czyści / niszczy nośniki z danymi przed ich utylizacją?			
24	Czy firma zarządza uprawnieniami np. stosowana jest zasada minimalizacji uprawnień, separacja obowiązków?			
25	Czy firma posiada procedurę napraw w serwisach?			
26	Czy firma korzysta z hostingu poczty elektronicznej / serwera			
27	Czy komputery, na których przetwarzane są dane osobowe połączone są siecią zarządzaną przez serwer czy połączone są ze sobą bez możliwości centralnej administracji?			
28	Czy dostęp do komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem			

Ankieta dla podmiotu przetwarzającego (procesora) dotycząca wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych osobowych zgodnie z RODO*

	identyfikatora użytkownika oraz hasła – wyłączenie możliwości logowania anonimowego?			
29	Czy hasło składa się z co najmniej 8 znaków i jest skonstruowane w sposób uniemożliwiający jego identyfikację (zawiera małe i wielkie litery oraz cyfry lub znaki specjalne)?			
30	Czy zastosowano okresową zmianę hasła dostępu do zbiorów danych dla każdego użytkownika – co 30 dni?			
31	Czy zastosowano automatyczne uruchamianie wygaszaczy ekranu po określonym czasie bezczynności?			
32	Czy zastosowano mechanizm umożliwiający rejestrację identyfikatora użytkownika wprowadzającego dane osobowe do systemu? Bez możliwości wspólnej pracy na jednym koncie użytkownika.			
33	Czy stosowana jest procedura postępowania z nośnikami danych oraz sprzętem poza organizacją?			
34	Czy stosowane są środki ochrony kryptograficznej w stosunku do danych osobowych przetwarzanych na komputerach przenośnych o ile są używane poza obszarem przetwarzania danych osobowych?			
35	Czy osoby użytkujące sprzęt w ten sposób są przeszkolone w zakresie bezpieczeństwa?			
36	Czy dane osobowe przetwarzane są na urządzeniach mobilnych (smartphony, tablety)? Jeśli tak to w jaki sposób urządzenia są zabezpieczone?			

**Rozporządzenie 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)*

Rejestr zawartych umów powierzenia

Lp.	Podmiot przetwarzający	Numer umowy powierzenia	Data powierzenia przetwarzania danych	Cel przetwarzania	Kategoria osób, których dane dotyczą	Kategoria / zakres danych
1						
2						
3						
4						
5						
6						