WÓJT GMINY
RACIECHOWICE
woj. małopolskie

ZARZĄDZENIE NR 183/2019

WÓJTA GMINY RACIECHOWICE
z dnia 31 grudnia 2019 roku

w sprawie: wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Gminy Raciechowice.

Na podstawie art. 24 ust.1 i 2 Rozporządzenia Ogólnego 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 oraz rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla systemów teleinformatycznych (Dz. u. z 2017 r., poz. 2247 ze zm.) **zarządzam, co następuje:**

§ 1

W Urzędzie Gminy Raciechowice w celu utrzymania podstawowych atrybutów bezpieczeństwa Systemu Przetwarzania Informacji, w szczególności poufności, dostępności i integralności informacji, wprowadza się do użytku służbowego:

1. Politykę Bezpieczeństwa Informacji wraz z załącznikami stanowiąca załącznik nr 1 do niniejszego zarządzenia.

§ 2

Zobowiązuje się wszystkich pracowników do zapoznania się z treścią zarządzenia.

§ 3.

Wykonanie zarządzenia powierza się Sekretarzowi Gminy Raciechowice.

§ 4

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT GMINY
RACIECHOWICE
Wacław Żarski

Załącznik Nr 1 do Zarządzenia nr 183/2019
Wójta Gminy Raciechowice
z dnia 31 grudnia 2019 roku

POLITYKA BEZPIECZEŃSTWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH W URZĘDZIE GMINY RACIECHOWICE

Spis treści:

Spis treści

Wprowadzenie

Tworzy się niniejszy dokument o nazwie Polityka bezpieczeństwa celem realizacji obowiązków wynikających z ogólnego 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.)(dalej: Rozporządzenie RODO), a polegających na wdrożeniu przez administratora danych dokumentacji przetwarzania danych osobowych.
Celem opracowania i wdrożenia zapisów niniejszej dokumentacji jest zapewnienie należytej ochrony danych osobowych będących w zasobach administratora danych, w szczególności odpowiedniej do zagrożeń i kategorii danych osobowych objętych ochroną.
Bezpieczeństwo danych osobowych ma na celu zapewnienie ich poufności, dostępności, integralności oraz rozliczalności, poprzez wdrożenie niezbędnych do tego celu środków technicznych i organizacyjnych.
Zakres przedmiotowy stosowania niniejszej dokumentacji obejmuje wszystkie procesy i czynności przetwarzania danych zarówno w formie elektronicznej, jak i papierowej.
Zakres podmiotowy stosowania niniejszej dokumentacji obejmuje wszystkich pracowników oraz osoby przy pomocy, których administrator danych wykonuje swoje czynności, mające dostęp do danych osobowych. Szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych.
Administrator jest odpowiedzialny za przestrzeganie przepisów Rozporządzenia RODO i musi być w stanie wykazać ich przestrzeganie („rozliczalność").

Przetwarzanie danych

§ 1

Przetwarzanie danych osobowych przez organy publiczne jest zgodne z prawem wyłącznie w przypadkach, gdy:

1. Osoba której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2. Przetwarzanie jest konieczne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3. Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4. Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej;
5. Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

6. Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona:
   a. w prawie Unii; lub
   b. w prawie krajowym.

§ 2

Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać:

1. Za zgodą osoby, której dane dotyczą; lub
2. W celu ustalenia, dochodzenia lub obrony roszczeń; lub
3. W celu ochrony praw innej osoby fizycznej lub prawnej; lub
4. Z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała jego ograniczenia.

§ 3

Administrator danych osobowych powinien zapewnić, że przetwarzane dane są adekwatne, stosowne oraz ograniczone do celów, w których są przetwarzane. Administrator danych musi dbać, a by dane zawsze były prawidłowe, kompletne a w razie potrzeby – uaktualniane. Dane powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą. Dane powinny być przetwarzane przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

§ 4

Zgoda powinna być wyrażona dobrowolnie, świadomie i jednoznacznie.

Zaleca się odbieranie zgody w postaci możliwej do późniejszego udowodnienia.

Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tych samych celach.

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. W przypadku odwołania zgody na przetwarzanie danych osobowych Administrator zobowiązany jest usunąć wszystkie dane osobowe osoby, która cofnęła zgodę, chyba że istnieje inna podstawa prawna upoważniająca Administratora do dalszego przetwarzania tych danych dla innych celów niż wskazany w zgodzie.

W przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, Administrator może zgodnie z prawem przetwarzać dane osobowe dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

Zgoda osoby sprawującej władzę rodzicielską lub opiekę nie powinna być konieczna w przypadku usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku.

§ 5

W przypadku jakichkolwiek wątpliwości co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do IOD z wnioskiem o rozstrzygnięcie wątpliwości.

Przed udzieleniem przez IOD odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku posiadania już danych osobowych, których wątpliwość dotyczy należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości, czy są prawnie uzasadnione.

Określenie środków (zabezpieczeń) przetwarzanych danych

§ 1

1. Każdy kto przetwarza dane osobowe obowiązany jest zachować w tajemnicy dane osobowe, do których posiada dostęp, sposoby zabezpieczania danych jak również wszelkie informacje, które powziął w czasie przetwarzania danych, zarówno w sposób zamierzony jak i przypadkowy. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
2. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.
3. Hasła i loginy do systemu informatycznego nie mogą być ujawniane nawet po utracie ich ważności.
4. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
5. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać, w miarę możliwości innym środkiem komunikacji elektronicznej.

§ 2

1. Wszelkie dokumenty zawierające dane osobowe przechowywane są w szafach lub pomieszczeniach zamykanych na klucz.
2. Osoba będąca dysponentem kluczy jest zobowiązana nie przekazywać kluczy do budynków
   i pomieszczeń, w których przetwarzane są dane osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
3. Osoba która utraciła posiadane klucze do pomieszczeń Administratora, w których przetwarzane są dane, niezwłocznie zgłasza tą okoliczność IOD lub Administratorowi.
4. IOD lub Administrator podejmują wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.
5. Szczegółowy wykaz środków technicznych i organizacyjnych stosowanych przez Administratora celem zapewnienia poufności, integralności i rozliczalności przetwarzanych danych zawarty został w załączniku **zalacznik_1(zasoby)** do polityki bezpieczeństwa.

§ 3

1. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne zdanymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
2. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia (zaleca się, aby niszczarka spełniała wymogi normy DIN 66399, klasa bezpieczeństwa nie niższa niż 3) lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
3. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie.
4. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.
5. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej.
6. Szczegółowy opis środków bezpieczeństwa zastosowanych przez Administratora wskazany został w załączniku **zalacznik_5(obszary)** do polityki bezpieczeństwa.

Zasoby w formie tradycyjnej

§ 1

Administrator Danych Osobowych prowadzi bieżącą inwentaryzacje prowadzonych zasobów zawierających informacje mogące stanowić dane osobowe.

§ 2

Przeprowadzona inwentaryzacja wskazuje w sposób wyczerpujący informacje o zasobach w szczególności:

a. Kategorię danych osobowych,
b. Podstawę prawną przetwarzania danych osobowych,
c. Kategorię osób, których dane dotyczą,
d. Sposób pozyskania danych osobowych,
e. Planowany czas przetwarzania,
f. Odbiorców, którym ADO planuje udostępnić dane osobowe,
g. Planowane podpowierzenia danych osobowych,
h. Sposób zabezpieczenia danych osobowych,
i. Miejsce przechowywania danych osobowych,
j. Cel przetwarzania danych osobowych.

§ 3

Inwentaryzacja zasobów zapisywana jest w formie dokumentu, którego wzór stanowi **załącznik nr 1.**

§ 4

Na podstawie **załącznika nr 1** oraz po uwzględnieniu szacowania ryzyka, którego dokonuje się na podstawie arkusza, który stanowi **załącznik nr 2** ADO uzupełnia rejestr czynności

przetwarzania, który stanowi **załącznik nr 3**. Jeżeli przetwarzanie odbywa się zgodnie z art. 28 RODO, na zlecenie innego administratora, prowadzony jest rejestr wszystkich kategorii czynności przetwarzania ewidencjonowany na rzecz każdego z administratorów zgodnie z **załącznikiem nr 4.**

§ 5

W celu udokumentowania stosowanych fizycznych zabezpieczeń ADO prowadzi wykaz obszarów przetwarzania danych, który stanowi **załącznik nr 5**.

Urządzenia i oprogramowanie wykorzystywane do przetwarzania danych

§ 1

Administrator Danych Osobowych prowadzi bieżącą inwentaryzacje sprzętu wykorzystywanego do przetwarzania informacji mogących stanowić dane osobowe oraz oprogramowania.

§ 2

Inwentaryzacja zasobów informatycznych polega na ustaleniu w stopniu wyczerpującym i kompletnym:

a. Nazwy zasobu,
b. Miejsca przechowywania,
c. Zastosowanych zabezpieczeń informatycznych i technicznych,
d. Zastosowanych zabezpieczeń fizycznych i organizacyjnych,
e. Używanego systemu operacyjnego,
f. Używanego oprogramowania służącego do przetwarzania danych osobowych z określeniem czy przechowywany jest lokalnie, na serwerze czy na serwerach procesora,
g. Zainstalowanego oprogramowania zabezpieczającego,
h. Zasobu osobowego, który korzysta z urządzenia.

§ 3

Inwentaryzacja IT dokumentowana jest zgodnie z **załącznikiem nr 6.**

Metoda szacowania ryzyka

§ 1

ADO przeprowadza szacowanie ryzyka, które polega na określeniu możliwego do wystąpienia ryzyka naruszeń ochrony danych w związku z prowadzonymi czynnościami przetwarzania oraz określa ich prawdopodobieństwo i skutek wystąpienia dla osób, których dane dotyczą.

§ 2

ADO zobowiązany jest do uwzględnienia możliwości nieuprawnionego lub przypadkowego:

a. zniszczenia,
b. utraty,
c. zmodyfikowania,

d. nieuprawnionego ujawnienia,
e. nieuprawnionego dostępu.

§ 3

Metoda szacowania ryzyka opisana jest w **załączniku nr 7.** Przeprowadzone szacowanie ryzyka dokumentowane jest zgodnie z **załącznikiem nr 2.**

§ 4

Szacowanie ryzyka przeprowadzane jest z uwzględnieniem potencjalnych skutków naruszenia praw lub wolności dla osób, których dane osobowe są przetwarzane w ramach prowadzonej działalności.

Obowiązek informacyjny wobec osób, których dane dotyczą

§ 1

ADO przekazuje każdej osobie, której dane przetwarza informacje zgodnie z art. 13 RODO w przypadku pozyskania danych od osób, których dane dotyczą lub zgodnie z art. 14 jeżeli zostały pozyskane w inny sposób, chyba że przepis ustawy przewiduje zwolnienie z tego obowiązku.

§ 2

Wzór stosowanych klauzul informacyjnych oraz zgody na przetwarzanie danych osobowych stanowią **załącznik 8a i załącznik 8b.**

Realizacja uprawnień osób, których dane dotyczą

§ 1

Osoba, której dane dotyczą ma prawo:

a. dostępu do treści swoich danych,
b. do ich sprostowania,
c. do usunięcia,
d. do ograniczenia przetwarzania,
e. do przenoszenia danych,
f. do wniesienia sprzeciwu,
g. do cofnięcia zgody (jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) w dowolnym momencie bez wpływu na zgodność z prawemprzetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem),
h. do uzyskania bezpłatnej kopii swoich danych osobowych, chyba że przepisy krajowe zwalniają ADO z tego obowiązku lub żądania osób, których dane dotyczą są **nieuzasadnione** lub **nadmierne,**
i. do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

§ 2

W przypadku uznania żądania za ewidentnie nieuzasadnione lub nadmierne należy uzasadnić odmowę realizacji żądania wskazując powody przemawiające za przyjęciem takiej kwalifikacji i w formie pisemnej przekazać uzasadnienie osobie wnoszącej żądanie

informując,
o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

§ 3

ADO zobowiązuje się do przechowywania danych, które pozyskał na podstawie zgody w formie umożliwiającej przekazanie jej w ogólnodostępnym formacie innemu administratorowi jeżeli osoba, której dane dotyczą tego zażąda (dotyczy tylko danych przetwarzanych elektronicznie).

Sposoby powierzania przetwarzania danych osobowych

§ 1

Przed jakimkolwiek powierzeniem przetwarzania danych osobowych ADO zawiera z podmiotem, któremu zamierza powierzyć przetwarzanie danych umowę powierzenia zgodnie z **załącznikiem nr 9.** Administrator dobiera podmioty, którym powierza dane osobowe, które zapewniają takie środki organizacyjne i techniczne, aby w sposób zgodny z prawem i bezpieczny przetwarzać dane osobowe. Podmioty przetwarzające dane są zobowiązane do informowania ADO o wszelkich incydentach związanych z naruszeniem bezpieczeństwa danych oraz wspierają ADO w realizacjach obowiązków na nim spoczywających.
Każde powierzenie lub udostępnienie przetwarzania danych osobowych zostaje odnotowane w rejestrze powierzeń i udostępnień zgodnie z **załącznikiem nr 9a**.

Incydenty naruszenia ochrony danych osobowych

§ 1

Pracownicy i współpracownicy ADO niezwłocznie informują go o wszystkich potencjalnych zagrożeniach dla ochrony danych osobowych.

§2

W przypadku pozyskania informacji z jakiegokolwiek źródła o potencjalnym naruszeniu ochrony danych, ADO natychmiast podejmuje niezbędne środki w celu ustalenia, czy konkretne zdarzenie miało miejsce, a następnie, czy stanowiło ono naruszenie ochrony danych osobowych. Na tyle, na ile jest to możliwe należy podjąć działania, które ograniczą rozmiar i dotkliwość naruszenia dla osób, których danych ono dotyczyło.

§3

Z chwilą stwierdzenia naruszenia, ADO dokonuje klasyfikacji naruszenia zgodnie z instrukcją z **załącznika nr 10a.**
Fakt wystąpienia naruszenia odnotowywany jest w rejestrze naruszeń zgodnie z **załącznikiem nr 10b.**

§4

Każde naruszenie, które zgodnie z jego zakwalifikowaniem nie jest uznane za mało prawdopodobne, by naruszało prawa lub wolność osób, których dane dotyczą należy zgłosić w ciągu maksymalnie 72 godzin po uzyskaniu wiedzy o wystąpieniu incydentu.

§5

ADO upoważnia pracowników i współpracowników do przetwarzania danych osobowych tylko i wyłącznie w takim zakresie jaki jest niezbędny do realizacji celu przetwarzania danych kierując się zasadą minimalizmu. Osoba upoważniona oraz osoby pracujące w obszarach przetwarzania oświadczają zachowanie w tajemnicy wszystkich danych osobowych do jakich uzyskają dostęp wykonując swoje obowiązki oraz zobowiązują się przestrzegać zasad, procedur i polityk ochrony danych wprowadzonych przez ADO, a także przepisów ochrony danych osobowych. Upoważnienie do przetwarzania jest przygotowywane zgodnie z **załącznikiem nr 11a**, oświadczenie jest przygotowywane zgodnie z **załącznikiem nr 11b.**
Osoby upoważnione oraz zobowiązane do zachowania tajemnicy są ewidencjonowane zgodnie z **załącznikiem 11c.**

Monitorowanie ochrony danych osobowych

§ 1

ADO regularnie monitoruje przestrzeganie obowiązków wynikających z przepisów ochrony danych osobowych ze szczególnym uwzględnieniem celowości i zgodności z prawem przetwarzania danych, zasad minimalizmu oraz pseudonimizacji, a także stosowanych zabezpieczeń w tym szyfrowania, oraz przestrzegania obowiązku informacyjnego względem osób, których dane dotyczą.

§ 2

W przypadku rozpoczynania świadczenia nowych usług, czy przetwarzaniu danych osobowych w związku z nowymi celami ADO weryfikuje, czy posiadane zgody w sposób jednoznaczny i konkretny zezwalają na takie przetwarzanie oraz stosując zasady projektowania ochrony danych osobowych ustala zabezpieczenia, sposoby przetwarzania, podpowierzania, realizacji praw osób, których dane dotyczą i obowiązków informacyjnych, przed wdrożeniem nowych rozwiązań.

§ 3

Okresowo ADO, osoba przez niego wyznaczona lub firma, której zlecono wykonanie sprawdzenia, dokonuje okresowego i/lub doraźnego sprawdzenia przestrzegania przepisów ochrony danych osobowych zgodnie z planem sprawozdania **załącznik 12a**. Po wykonaniu sprawdzenia zostaje sporządzony raport zgodnie z **załącznikiem nr 12b**

Zarządzanie Systemem Informatycznym

§ 1

W celu prawidłowego, kontrolowanego oraz rozliczalnego sposobu zarządzania systemami informatycznymi ADO wprowadza Instrukcję Zarządzania Systemem Informatycznym.

§ 2

Instrukcja ma na celu dokumentowanie nadawanych uprawnień do systemów informatycznych, rejestrowania tworzenia kopii zapasowych oraz sposobów postępowania w celu zabezpieczenia działania urządzeń teleinformatycznych używanych przez ADO i jego pracowników.

Zarządzanie dostępem do Obszarów Przetwarzania

§ 1

ADO w celu wyeliminowania dostępu do danych osobowych osób nieupoważnionych do ich przetwarzania wprowadza zasady dotyczące przebywania osób nieupoważnionych w pomieszczeniach, w których znajdują się dane osobowe.

§ 2

W obszarze przetwarzania danych osobowych bez nadzoru osoby upoważnionej mogą przebywać tylko osoby, które zostały pouczone o odpowiedzialności, zapoznały sięz procedurami funkcjonującymi u ADO, oraz podpisały oświadczenie o zachowaniu poufności zgodnie z **załącznikiem nr 11b.**Inne osoby niż wymienione wyżej przebywać mogą w pomieszczeniach, gdzie przetwarzane są dane osobowe tylko i wyłącznie pod nadzorem osób upoważnionych lub ADO.W celu zapewnienia pełnego bezpieczeństwa danych osobowych przed ich nieuprawnionym ujawnieniem dokumenty zawierające informacje
o charakterze danych osobowych są zamykane na klucz, a klucz do szafek, biurek lub szaf, w których zamknięte są dokumenty posiadają tylko osoby upoważnione oraz ADO (klucz zapasowy). Dzięki zastosowaniu tej zasady, osoby nieupoważnione do przetwarzania danych, lecz pracujące w obszarach przetwarzania danych bez nadzoru nie posiadają dostępu do danych osobowych.

Prawa osób których dane dotyczą

§ 1

W **załączniku nr 13** ADO reguluje sposób realizacji uprawnień osób, których dane są przetwarzane przez administratora oraz ma na celu usprawnienie tego procesu.
Prawa te są określone w art. 15 RODO.

Procedura rekrutacji do pracy

§ 1

Załącznik nr 14 reguluje sposób przeprowadzania rekrutacji oraz wypełniania obowiązku informacyjnego wymaganego przez RODO, wobec kandydatów do pracy.

Inspektor Ochrony Danych (IOD)

§ 1

Administrator powołuje Zarządzeniem Kierownika jednostki zgodnie z art. 37 ogólnego rozporządzenia o ochronie danych (RODO) funkcję Inspektora Ochrony Danych (IOD), który realizuje zadania określone w art. 39. Administrator zapewnia niezbędne warunki do pełnienia funkcji zgodnie z wymogami opisanymi w art. 38 RODO. Wybór IOD został

dokonany na podstawie kwalifikacji zawodowych, w tym wiedzy fachowej na temat prawa i praktyk w ochronie danych i przepisów dotyczących funkcjonowania jednostki oraz posiadanych umiejętności do wypełnienia zadań określonych w art. 39.

§ 2

O powołaniu IOD, o którym mowa w par. 1 Administrator informuje w ciągu 14 dni Prezesa Urzędu Ochrony Danych Osobowych zgodnie z art. 10 Ustawy o Ochronie Danych Osobowych z dnia 10 maja 2018 roku w formie elektronicznej, a zawiadomienie takie opatruje bezpiecznym podpisem kwalifikowanym lub za pomocą profilu zaufanego ePUAP. Administrator przekazuje informacje o wyznaczeniu IOD na swojej stronie internetowej lub na stronie BIP oraz podaje do publicznej wiadomości adres e-mail za pomocą, którego osoby, których dane dotyczą mogą się z nim skontaktować.

Informacje końcowe

§ 1

W sprawach nieuregulowanych niniejszym dokumentem znajdują zastosowanie odpowiadające w konkretnej sprawie postanowienia zawarte w wytycznych, opiniach oraz decyzjach grupy roboczej art. 29, Europejskiej Rady Ochrony Danych, Urzędu Ochrony Danych Osobowych, Komisji Europejskiej oraz zatwierdzonych przez Urząd Ochrony Danych mechanizmach certyfikacyjnych lub kodeksach postępowania oraz akty prawne Ogólne Rozporządzenie o Ochronie Danych Osobowych, Ustawa Ochrony Danych Osobowych, Ustawa wprowadzająca Ochronę Danych Osobowych.

WÓJT GMINY RACIBÓRZ CHOWICE
Wiesław Gorski

.....

Podpis Administratora Danych Osobowych