ZARZĄDZENIE NR 715/2021
BURMISTRZA MIASTA I GMINY KĄTY WROCŁAWSKIE

z dnia 8 kwietnia 2021 r.

w sprawie wprowadzenia nowej Polityki Ochrony Danych Osobowych w Urzędzie Miasta i Gminy Kąty Wrocławskie

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2020 r. poz. 713 z późn. zm.) oraz na podstawie art. 24 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 rozporządzeni o ochronie danych), zarządzam co następuje:

1. Wprowadzam Politykę Ochrony Danych Osobowych w Urzędzie Miasta i Gminy Kąty Wrocławskie wraz z załącznikami.

2. Z dniem wejścia w życie niniejszego zarządzenia traci moc zarządzenie nr 965/2018 z dnia 25 maja 2018 roku w sprawie aktualizacji dokumentacji wchodzącej w skład Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta i Gminy Kąty Wrocławskie oraz zarządzenie nr 923/2018 z dnia 28 marca 2018 roku w sprawie powołania zespołu do przeprowadzenia w Urzędzie Miasta i Gminy Kąty Wrocławskie szacowania i analizy ryzyka w obszarze danych osobowych oraz oceny skutków dla osób których dane dotyczą.

3. Zarządzenie wchodzi w życie z dniem podpisania.

pełniący funkcję Burmistrza
Miasta i Gminy Kąty Wrocławskie
mgr Julian Zygadło

Zatwierdzono pod
względem prawnym
radca. Izabela Pierwoła - Pszczółka

Załącznik Nr 1 do zarządzenia Nr 715/2021
Burmistrza Miasta i Gminy Kąty Wrocławskie
z dnia 08 kwietnia 2021 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH

SPIS TREŚCI

I. SŁOWNIK POJĘĆ

1.Określenia użyte w niniejszej polityce i jej załącznikach oznaczają:
a.**Polityka** – czyli Polityka ochrony danych osobowych- nadrzędny dokument wprowadzający uregulowania dotyczące przetwarzania danych osobowych przez administratora;
b.**procedura** – dokument będący częścią Polityki, regulujący w danym obszarze zasady przetwarzania danych osobowych;
c.**rozporządzenie UE 2016/679** - 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);
d.**dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (między innymi dane identyfikacyjne, dane adresowe, dane umieszczane na portalach społecznościowych; wizerunek; dane finansowe; dane pracownicze; informacje o wyrokach i naruszeniach prawa; dane szczególne(...));
e.**przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
f.**administrator** – Burmistrz Miasta i Gminy Kąty Wrocławskie;
g.**IOD** – oznacza inspektora ochrony danych powołanego zgodnie z art. 37–39 rozporządzenia UE 2016/679;
h.**jednostka przetwarzająca** – Urząd Miasta i Gminy Kąty Wrocławskie;
i.**kierownik** – należy przez to rozumieć kierownika lub dyrektora komórki organizacyjnej lub innego pracownika, któremu w danym zakresie podlegają inni pracownicy jednostki;

j.**naruszenie** – należy przez to rozumieć naruszenie bezpieczeństwa czyli zdarzenie prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

k.**zespół bezpieczeństwa danych lub ZBD** - osoby posiadające odpowiednie kwalifikacje lub wiedzę fachową w dziedzinach bezpośrednio powiązanych z przetwarzaniem danych osobowych lub ich bezpieczeństwem;

l.**komórka organizacyjna** – wydział, referat, dział, oddział, samodzielne stanowisko, wyodrębniona komórka ze struktur organizacyjnych jednostki przetwarzającej, mająca przypisane własne zadania;

m.**podmiot przetwarzający** – każdy kto w imieniu administratora przetwarza dane osobowe, także jeżeli je zbiera na użytek administratora;

n.**powierzenie przetwarzania** – działanie polegająca na zleceniu innemu podmiotowi przetwarzania danych

osobowych na użytek administratora;

o.**pracownik** – osoba fizyczna zatrudniona w jednostce przetwarzającej lub wykonująca zlecenie, staż, praktyki, zastępstwo, współpracująca z jednostką przetwarzającą będąca pod stałą kontrolą administratora i wykonująca jego polecenia;

p.**obowiązek informacyjny** – należy przez to rozumieć obowiązek prawny administratora wynikający z art. 12-14 rozporządzenia 2016/679, związku z którym administrator musi przekazać określony zakres informacji o przetwarzaniu osobie fizycznej, której dane przetwarza;

q.**czynność przetwarzania** – operacja, czynność, reakcja, która wymaga przetwarzania danych osobowych osobiście lub pośrednio za pomocą np. systemów, aplikacji itp.

r.**kontrola ryzyka** – kontrola adekwatności zastosowanych rozwiązań technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych osobowych oraz zgodność przetwarzania danych osobowych z przepisami Unijnymi i krajowymi;

s.**rejestr czynności przetwarzania** – ewidencja wszystkich wykonywanych w imieniu własnym czynności przetwarzania, w zakresie określonym w rozporządzeniu UE 2016/679;

t.**rejestr kategorii czynności** – ewidencja wszystkich wykonywanych w imieniu innego administratora czynności przetwarzania, w zakresie określonym w rozporządzeniu UE 2016/679;

u.**organ uprawniony** – jednostka, organ, który w ramach swoich uprawnień wynikających z przepisów unijnych lub krajowych może mieć dostęp do danych w niezbędnym zakresie;

v.**inny podmiot** – należy przez to rozumieć osoby prawne, osoby fizyczne prowadzące działalność gospodarczą, spółkę komandytową, cywilną, jawną, partnerską oraz inne formy prowadzenia działalności nieposiadającej osobowości prawnej wnioskujące o udostępnienie danych osobowych w ramach prowadzonej działalności;

w.**współadministrator** – co najmniej dwa podmioty, które w jakimkolwiek zakresie wspólnie ustalają cele lub sposoby przetwarzania tych samy danych osobowych;

x.**odbiorca** – każdy kto otrzyma lub otrzymać może dane osobowe od administratora;

y.**usunięcie** – należy przez to rozumieć usunięcie danych osobowych, anonimizację danych osobowych lub uszkodzenie ich w taki sposób, że nie jest możliwe ich odczytanie;

z.**przechowywanie** – należy przez to rozumieć okres przez który dane osobowe muszą pozostać w komórce organizacyjnej;

aa.**wykaz** – załącznik „wykaz terminów i sposobów usuwania danych osobowych"

bb.**upublicznianie** – należy rozumieć ujawnienie danych osobowych poprzez zamieszczenie ich w miejscach dostępnych dla niezidentyfikowanych odbiorców; np. umieszczenie danych na BIP, na stronie własnej, na portalach społecznościowych (też wizerunki), w gazecie, w radiu, na tablicach ogłoszeń, w miejscach dostępnych publicznie;

cc.**rejestr upublicznionych danych osobowych** – zawiera informacje dotyczące upublicznienia, stanowi załącznik do niniejszej procedury;

dd.**praca zdalna** – praca wykonywana poza stałym miejscem wykonywania pracy, lub praca wykonywana bez stałego miejsca pracy;

II. WPROWADZENIE

1.Polityka jest nadrzędnym dokumentem wewnętrznym we wszystkich sprawach związanych z przetwarzaniem danych osobowych.
2.Polityka określa zasady zapewniające bezpieczeństwo danych osobowych oraz przestrzeganie przepisów unijnych i krajowych dotyczących danych osobowych.
3.Wprowadzenie Polityki jest niezbędne ze względu na:
a.zapewnienie realizacji zasad i warunków, o których mowa w rozdziale II art. 5-11 rozporządzenia UE 2016/679;
b.zapewnienie realizacji praw osób fizycznych, których dane osobowe dotyczą zgodnie

z rozdziałem III art. 12-22 rozporządzenia UE 2016/679;
c.zapewnienie realizacji obowiązków administratora i podmiotu przetwarzającego wynikających z rozdziału IV rozporządzenia UE 2016/679.
4.Polityka ma zastosowanie do wszystkich danych osobowych przetwarzanych:
a.przez administratora i w imieniu administratora i/lub wspólnie ze współadministratorami;
b.w jednostce przetwarzającej i poza nią;
c.na nośnikach danych papierowych i elektronicznych;
d.bez trwałych zapisów np. ustnie.
5.Jeżeli przepisy unijne lub krajowe w inny sposób regulują postanowienia niniejszej Polityki to niniejsza Polityka w zakresie w jakim regulują to przepisy nie obowiązuje.
6.Z Polityką musi zapoznać się:
a.każdy pełnomocnik administratora;
b.każdy kierownik;
c.każdy pracownik, również nowy;
7.Zmiany w Polityce wymagają zgody administratora oraz zespołu bezpieczeństwa danych, a w szczególności inspektora ochrony danych i są wprowadzane pod ich ścisłym nadzorem.

III. PROCEDURY

1.W celu realizacji rozległego zakresu obowiązków wynikających z przetwarzania danych osobowych oraz zapewnienia poufności co do zastosowanych rozwiązań technicznych i organizacyjnych, zapewniających bezpieczeństwo danych osobowych, wprowadza się procedury będące załącznikami do niniejszej Polityki.
2.Procedury muszą zapewnić:
a.przestrzeganie unijnych i krajowych przepisów dotyczących przetwarzania danych osobowych;
b.nadzorowanie przestrzegania przepisów unijnych i krajowych w zakresie przetwarzania danych osobowych;
c.możliwość wykazania przestrzegania przepisów unijnych i krajowych dotyczących przetwarzania danych osobowych.
3.Każda procedura tworzona jest w tym samym formacie co Polityka oraz zawierać musi co najmniej:
a.słownik pojęć zastosowanych w procedurze;
b.wykaz załączników do procedury;
c.z powodu jakich przepisów zastosowano procedurę;
d.w jakim zakresie obowiązuje procedura;
e.wyjątki od stosowania procedury;
f.zakres dostępu do procedury i załączników;
g.sposób archiwizacji dokumentów;
h.kto odpowiada za realizację procedury.
4.Administrator w porozumieniu z zespołem bezpieczeństwa danych, a w szczególności z inspektorem ochrony danych ustala i wprowadza bądź zleca do wprowadzenia niezbędne procedury zapewniające bezpieczeństwo przetwarzania danych osobowych.
5.Wszystkie nowe procedury bądź zmiany w procedurach wprowadzane są zarządzeniem administratora.
6.Poniższa tabela wskazuje obecnie wprowadzone procedury oraz ich ostatnie aktualizacje.

Numer procedury	Nazwa procedury	Data ostatniej aktualizacji	Zakres aktualizacji	Wprowadzający zmianę
02	PROCEDURA ZARZĄDZANIA UPRAWNIENIAMI			
03	PROCEDURA NADZOROWANIA CZYNNOŚCI PRZETWARZANIA			
04	PROCEDURA REALIZACJI OBOWIĄZKU INFORMACYJNEGO			
05	PROCEDURA REALIZACJI PRAW OSÓB FIZYCZNYCH			
06	PROCEDURA POWIERZENIA PRZETWARZANIA			
07	PROCEDURA UDOSTĘPNIANIA DANYCH OSOBOWYCH			

08	PROCEDURA USÓWANIA DANYCH OSOBOWYCH			
09	PROCEDURA UPUBLICZNIANIA DANYCH OSOBOWYCH			
10	PROCEDURA PRACY ZDALNEJ			
11	PROCEDURA POSTĘPOWANIA Z NARUSZENIEM			
12	REGULAMIN MONITORINGU			
13	PROCEDURA WSPÓŁADMINISTROWANIA			

IV. OBOWIĄZKI

1. Administrator ma obowiązek:
a.zapewnić przestrzeganie i rozliczalność zasad i warunków przetwarzania ochrony danych osobowych wynikających z art. 5-10 rozporządzenia UE 2016/679;
b.zapewnić realizację praw osób fizycznych zgodnie z art. 12-22 rozporządzenia UE 2016/679;
c.zapewnić odpowiedni poziom bezpieczeństwa danych osobowych zgodnie z art. 24-29 i 32 rozporządzenia UE 2016/679;
d.prowadzić działania wynikające z naruszenia ochrony danych osobowych zgodnie z art. 33-34 rozporządzenia 2016/679;
e.prowadzić rejestr czynności przetwarzania zgodnie z art. 30 rozporządzenia UE 2016/679;
f.w wymaganych przypadkach przeprowadzić ocenę skutków zgodnie z art. 35 rozporządzenia UE 2016/679;
g.w wymaganych przypadkach powołać inspektora ochrony danych zgodnie z art. 37-39 rozporządzenia UE 2016/679.
2.Jeżeli został powołany, to do obowiązków inspektora ochrony danych należy:
a.informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia UE 2016/679 oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
b.monitorowanie przestrzegania rozporządzenia UE 2016/679, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania danych oraz powiązane z tym audyty;
c.udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 rozporządzenia 2016/679;
d.współpraca z organem nadzorczym;
e.pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia UE 2016/679, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
3.Ponadto inspektor ochrony danych:
a.posiada odpowiednie kwalifikacje zawodowe w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności pozwalające mu wypełniać ustawowe zadania;
b.wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania;
c.jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.
4.Administrator może powołać pełnomocnika lub nadać upoważnienie do realizacji wszystkich bądź części swoich obowiązków zgodnie z prawem unijnym lub krajowym.
5.Każdy na stanowisku kierowniczym ma obowiązek:
a.zapewnić przestrzeganie zasad i warunków przetwarzania danych osobowych, o których mowa w art. 5-10 rozporządzenia UE 2016/679 w obrębie własnej komórki organizacyjnej;
b.realizować prawa osób fizycznych związku z przetwarzaniem danych osobowych przez swoją komórkę organizacyjną zgodnie ze stosowną procedurą i art. 12-22 rozporządzenia UE 2016/679;
c.w przypadku wystąpienia naruszenia ochrony danych osobowych w komórce organizacyjnej, prowadzić działania wynikające ze stosownej procedury i art. 33-34 rozporządzenia UE 2016/679;
d.kontrolować ryzyko naruszenia ochrony danych osobowych w komórce organizacyjnej;

e.informować administratora i inspektora ochrony danych o ryzyku naruszenia ochrony danych, jeżeli takie zostanie zauważone;
f.poinformować administratora i zespół bezpieczeństwa danych o awarii zabezpieczeń technicznych zapewniających bezpieczeństwo;
g.poinformować administratora i inspektora ochrony danych o niestosowaniu procedur organizacyjnych dotyczących przetwarzania danych osobowych;
h.kontrolować pracę podległych pracowników w zakresie stosowania się do Polityki i jej procedur.
6.Każdy przetwarzający dane osobowe w imieniu administratora ma obowiązek:
a.poinformować bezpośredniego przełożonego, jeżeli wydane mu polecenie narusza przepisy unijne lub krajowe dotyczące przetwarzania danych osobowych;
b.stosować się do Polityki i procedur dotyczących danych osobowych;
c.poinformować bezpośredniego przełożonego o ryzyku bądź wystąpieniu naruszenia ochrony danych osobowych;
d.poinformować bezpośredniego przełożonego o awarii zabezpieczeń technicznych zapewniających bezpieczeństwo;
e.poinformować bezpośredniego przełożonego o niestosowaniu procedur organizacyjnych dotyczących przetwarzania danych osobowych;
f.przestrzegać zasad i warunków przetwarzania danych osobowych, o których mowa w art. 5-10 rozporządzenia UE 2016/679;
g.realizować prawa osób fizycznych związku z przetwarzaniem danych osobowych zgodnie ze stosowną procedurą i art. 12-22 rozporządzenia UE 2016/679.

V. UPRAWNIENIA

1.Administrator jest uprawniony do:
a.podejmowania decyzji co do celu i sposobu przetwarzania danych osobowych w zakresie nieuregulowanym przepisami unijnymi i krajowymi;
b.podejmowania decyzji co do odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania i zgodność z prawem;
c.kontroli pracowników jednostki przetwarzającej oraz podmiotu przetwarzającego w zakresie przestrzegania Polityki oraz unijnych i krajowych przepisów dotyczących przetwarzania danych osobowych;
d.wystawiania upoważnień i pełnomocnictw w zakresie realizacji swoich obowiązków i uprawnień;
e.monitorowania i audytowania procesów przetwarzania danych osobowych w pełnym zakresie.
2.Inspektor ochrony danych osobowych uprawniony jest do:
a.kontroli pracowników jednostki przetwarzającej oraz podmiotu przetwarzającego w zakresie przestrzegania Polityki oraz unijnych i krajowych przepisów dotyczących przetwarzania danych osobowych;
b.podziału obowiązków wynikających z Polityki, procedur oraz przepisów unijnych i krajowych dotyczących przetwarzania danych osobowych;
c.monitorowania i audytowania procesów przetwarzania danych osobowych w pełnym zakresie;
d.zlecania wykonania analizy ryzyka i oceny skutków.
3.Zakres uprawnień pełnomocnika lub upoważnionego wynika z zakresu jego pełnomocnictwa lub upoważnienia.
4.Każdy kierownik uprawniony jest do:
a.kontroli pracowników komórki organizacyjnej w zakresie przestrzegania Polityki oraz unijnych i krajowych przepisów dotyczących przetwarzania danych osobowych;
b.monitorowania i audytowania procesów przetwarzania danych osobowych w obrębie komórki organizacyjnej lub w zakresie wynikającym z obowiązków pracowniczych.
5.Każdy przetwarzający dane osobowe w imieniu administratora uprawniony jest do:
a.konsultacji z zespołem bezpieczeństwa danych oraz inspektorem ochrony danych w sprawach dotyczących przetwarzania danych;
b.otrzymania informacji o wynikach przeprowadzonej kontroli w zakresie realizacji własnych obowiązków wynikających z Polityki, procedur i przepisów unijnych oraz krajowych dotyczących przetwarzania danych osobowych;
c.odbycia niezbędnych szkoleń adekwatnych do zajmowanego stanowiska bądź pełnionej funkcji w dziedzinie danych osobowych.

VI. ZESPÓŁ BEZPIECZEŃSTWA DANYCH

1.Administrator powołuje podstawowy skład zespołu bezpieczeństwa danych oraz ustala jego przewodniczącego.

2.Administrator wspólnie z zespołem bezpieczeństwa danych ustala indywidualny zakres zadań każdego członka zespołu, z uwzględnieniem terminów ich realizacji.
3.Dodatkowe zadania zlecone związku z pełnieniem funkcji członka zespołu nie mogą powodować konfliktu interesów w stosunku do zadań wynikających z przepisów.
4.Skład zespołu bezpieczeństwa danych może być czasowo rozszerzany adekwatnie do rodzaju realizowanej sprawy.
5.Zespół bezpieczeństwa danych powinien się składać z:
a.osób pełniących funkcje wynikające z przepisów unijnych i krajowych, gdzie ich zakres obowiązków wynikający z tych przepisów dotyczy między innymi przetwarzania danych osobowych lub zapewnienia ich bezpieczeństwa;
b.osób posiadających kwalifikacje lub wiedzę w zakresie regulacji prawnych dotyczących danych osobowych;
c.osób posiadających kwalifikacje lub wiedzę w zakresie niezbędnych środków technicznych gwarantujących bezpieczeństwo przetwarzania danych osobowych;
d.osób posiadających kwalifikacje lub wiedzę w zakresie niezbędnych środków organizacyjnych gwarantujących bezpieczeństwo przetwarzania danych osobowych.
6.Zespół bezpieczeństwa danych ma za zadanie:
a.doradzać, prowadzić konsultacje w sprawach związanych z danymi osobowymi lub ich bezpieczeństwem;
b.nadzorować, kontrolować, monitorować, testować, audytować procesy przetwarzania danych osobowych pod kątem bezpieczeństwa i zgodności z przepisami unijnymi i krajowymi;
c.przeprowadzać szkolenia z wszystkich niezbędnych zakresów dotyczących danych osobowych;
d.prowadzić działania zwiększające świadomość w dziedzinie danych osobowych;
e.informować wszystkich uczestników przetwarzania, także podmioty przetwarzające, o obowiązkach wynikających z przetwarzania danych osobowych.

VII. POSTANOWIENIA KOŃCOWE

1.Do Polityki może mieć dostęp każdy zainteresowany natomiast do załączników Polityki dostęp uzyskać może jedynie:
a.osoby uprawnione przez administratora;
b.osoby uprawnione na podstawie przepisów;
c.organy nadzorcze w zakresie adekwatnym do swoich uprawnień.
2.Każdy kto nie przestrzega niniejszej Polityki, a jest do tego zobowiązany na mocy przepisów unijnych lub krajowych lub na mocy oświadczenia woli, ponosi odpowiedzialność za wszelkie szkody powstałe z powodu zaniechania zgodnie z Kodeksem Cywilnym, Kodeksem Pracy, Rozporządzeniem UE 2016/679 bądź innymi przepisami adekwatnymi do zaistniałej sytuacji.
3.Niniejsza Polityki obowiązuje z dniem _____.

VIII. METRYKA

aktualna wersja:		numer zarządzenia:	

Zakres aktualizacji	Data aktualizacji	Wprowadził aktualizacje	Zatwierdził aktualizacje

Załącznik Nr 2 do zarządzenia Nr Nr 715/2021
Burmistrza Miasta i Gminy Kąty Wrocławskie
z dnia 08 kwietnia 2021 r.

PROCEDURA ZARZĄDZANIA UPRAWNIENIAMI

SPIS TREŚCI

I. WPROWADZENIE

1.Niniejsza procedura jest integralną częścią Polityki, jednakże Polityka jest nadrzędnym dokumentem w stosunku do procedury.
2.Niniejsza procedura określa zasady wydawania, modyfikowania i odbierania upoważnień do przetwarzania danych osobowych.
3.Wprowadzenie niniejszej procedury jest niezbędne ze względu na:
a.zapewnienie, że osoby upoważnione przetwarzają dane osobowe w zakresie wydanego polecenia zgodnie z art. 32 ust. 4 rozporządzenia UE 2016/679;
b.zapewnienie poufności, integralności, minimalizacji danych, o których mowa w art. 5 rozporządzenia UE 2016/679;
c.zapewnienie rozliczalności przestrzegania zasad przetwarzania danych osobowych, o których mowa w art. 5 rozporządzenia UE 2016/679.
4.Niniejsza procedura obowiązuję wszystkich pracowników jednostki przetwarzającej.
5.Jeżeli przepisy unijne lub krajowe w inny sposób regulują postanowienia niniejszej procedury to niniejsza procedura w zakresie w jakim regulują to przepisy nie obowiązuje.
6.Z niniejszą procedurą musi się zapoznać:
a.każdy pełnomocnik administratora;
b.każdy kierownik;
c.każdy członek zespołu bezpieczeństwa danych.
7.Zmiany niniejszej procedury lub jej załączników wymagają zgody administratora oraz inspektora ochrony danych i są wprowadzane pod ich ścisłym nadzorem.

II. NADANIE UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

1.Kierownik pracownika, któremu mają zostać nadane upoważnienia do przetwarzania danych osobowych składa wniosek o nadanie upoważnienia do inspektora ochrony danych a następnie wysyła pracownika na szkolenia z:
a.bezpieczeństwa i higieny pracy;
b.instrukcji archiwalnych i kancelaryjnych;
c.bezpieczeństwa pracy przy komputerze, jeżeli będzie taka praca wykonywana;
d.ochrony danych osobowych.
2.IOD, po otrzymaniu wniosku i potwierdzeniu odbycia obowiązkowych szkoleń, przeprowadza test z dziedziny danych osobowych.
3.Przed nadaniem upoważnienia do przetwarzania danych osobowych pracownik musi podpisać oświadczenie dotyczące:
a.zachowania poufności w stosunku do danych i stosowanych środków bezpieczeństwa;
b. zapewnienia przestrzegania rozporządzenia UE 2016/679 oraz innych przepisów dotyczących ochrony danych;
c.zapoznania się z panującymi politykami, procedurami, standardami ochrony danych.
4.Po uzyskaniu przez pracownika pozytywnego wyniku z testu i podpisaniu oświadczenia IOD przekazuje przygotowane upoważnienie administratorowi celem zaakceptowania.

5.Wystawiając upoważnienie należy posługiwać się wzorem załączonym do niniejszej procedury.
6.Upoważnienie wydane w inny sposób niż na podstawie wzoru załączonego do niniejszej procedury musi zawierać co najmniej:
a.oznaczenie administratora;
b.oznaczenie osoby upoważnianej;
c.zakres obowiązków z którego wynika upoważnienie;
d.czas trwania upoważnienia.

III. MODYFIKACJA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

1.W celu wprowadzenia modyfikacji w zakresie upoważnienia, kierownik wnioskuje do inspektora ochrony danych wskazując:
a.w jakim celu upoważnienie ma być zmodyfikowane;
b.jaki zakres upoważnienia ma być zmodyfikowany.
2.Wnioskując o modyfikację upoważnienia należy posługiwać się wzorem załączonym do niniejszej procedury.
3.Po zatwierdzeniu wniosku o modyfikację upoważnienia, IOD przekazuję administratorowi aktualne upoważnienie celem zaakceptowania.
4.Jeżeli modyfikacja upoważnienia wymaga dodatkowych szkoleń, to przed ich wprowadzeniem muszą być przeprowadzone wszystkie niezbędne szkolenia.

IV. ODEBRANIE UPOWAŻNIEŃ

1.W przypadku gdy upoważnienie przestaje obowiązywać kierownik zobowiązany jest zgłosić ten fakt do IOD.
2.Wnioskując o odebranie upoważnień należy posługiwać się wzorem do niniejszej procedury.

V. UPRAWNIENIA DO SYSTEMÓW

1.Jeżeli pracownikowi ma zostać nadane, zmodyfikowane lub odebrane uprawnienie do systemów to kierownik musi postępować zgodnie z instrukcją zarządzania systemami.
2.IOD przy nadaniu bądź modyfikacji uprawnienia do systemów sprawdza adekwatność zakresu tego uprawnienia do zakresu posiadanego upoważnienia, a w przypadku wykrycia niezgodności, do czasu ich uregulowania w tym zakresie, uprawnienie do systemów nie obowiązuje.

VI. WZORY I DOKUMENTY

1.Zastosowanie mają następujące wzory dokumentów będące załącznikami do niniejszej procedury:
a.„02. ewidencja upoważnień" – wzór ewidencji wszystkich wydanych upoważnień do przetwarzania danych osobowych;
b.„02. skrypt szkolenie" – materiały szkoleniowe z zakresu ochrony danych osobowych;
c.„02. wniosek dotyczący upoważnienia" – wzór wniosku służącego do wydawania upoważnień do przetwarzania;
d.„02. oświadczenie RODO" – wzór oświadczenia, dotyczącego między innymi poufności;
e.„02. upoważnienie" wzór stosowanych upoważnień do przetwarzania;
2.W wyniku stosowania niniejszej procedury powstanie dokumentacja zawierająca dane osobowe lub/oraz informacje poufne o jednostce przetwarzającej dlatego administrator wyznacza osoby odpowiedzialne za przechowywanie tej dokumentacji w następujących zakresach:
a.złożone wnioski dotyczące wydania upoważnienia do przetwarzania – przechowuje w oryginale IOD;
b.wydane upoważnienia do przetwarzania danych osobowych – przechowuje w oryginale _____;
c.wnioski dotyczące nadania uprawnienia do systemów – przechowuje w oryginale _____;
d.oświadczenia dotyczące poufności – przechowuje w oryginale _____;
e.ewidencje wydanych upoważnień do przetwarzania – przechowuje w formie elektronicznej IOD.
3.Przechowywanie, archiwizowanie, modyfikowanie, ujawnianie, udostępnianie, niszczenie lub usuwanie i innego rodzaju przetwarzanie załączników lub treści w nich zawartych odbywa się zgodnie ze stosowną procedurą, chyba, że nie zawierają danych osobowych to zgodnie z przepisami unijnymi lub krajowymi lub uregulowaniami wewnętrznymi.

VII. POSTANOWIENIA KOŃCOWE

1.Nadzór nad niniejszą procedurą sprawuję:
a.IOD w pełnym zakresie;
b.każdy kierownik w obrębie własnej komórki organizacyjnej;
c.każdy pełnomocnik administratora w zakresie udzielonego pełnomocnictwa:

d.każdy upoważniony w zakresie nadanego upoważnienia.
2.Każdy kto nie przestrzega niniejszej procedury a jest do tego zobowiązany, na mocy przepisów unijnych lub krajowych lub na mocy wyrażonego oświadczenia woli, ponosi odpowiedzialność za wszelkie szkody powstałe z powodu tego zaniechania zgodnie z Kodeksem Cywilnym, Kodeksem Pracy, Rozporządzeniem UE 2016/679 bądź innymi przepisami adekwatnymi do zaistniałej sytuacji.
3.Niniejsza procedura obowiązuję z dniem _____.

IIX. METRYKA

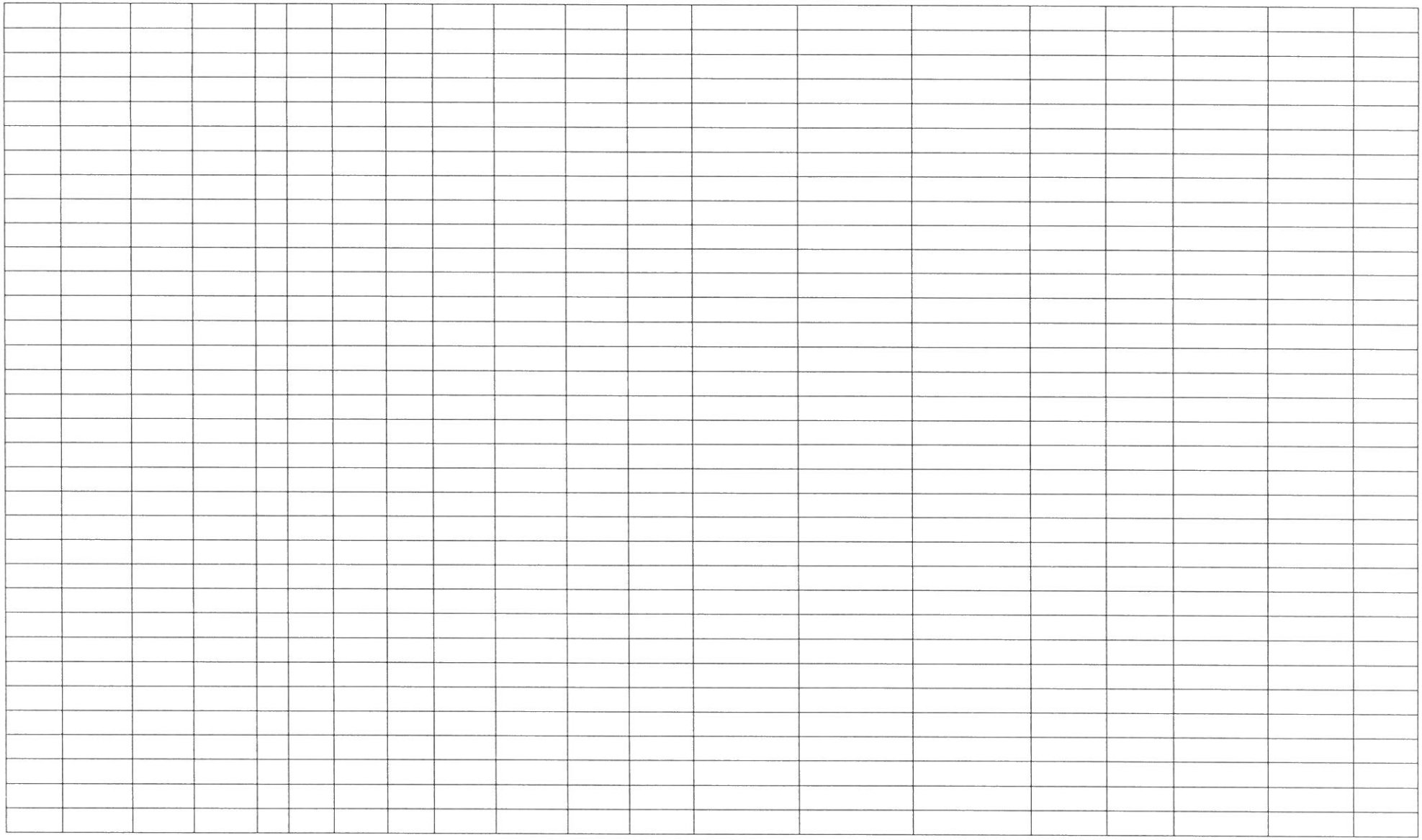
aktualna wersja:		numer zarządzenia:	

Zakres aktualizacji	Data aktualizacji	Wprowadził aktualizacje	Zatwierdził aktualizacje

Załącznik Nr 1 do Załącznika Nr 2

ewidencja upoważnień

Imię i nazwisko	Komórka organizacyjna	Stanowisko	Dane kontaktowe	LP	Numer UP	Status UP	Data nadania UP	Data ustania UP	Data szkolenia RODO	Data zdania testu	NOTATKI	Wniosek o nadanie uprawnień	Data otrzymania	Wniosek o nadanie uprawnień do systemów	Data otrzymania	Oświadczenie	Data otrzymania	Upoważnienie	Data wydania



skrypt szkolenie

PODSTAWOWE DEFNICJE

DANE OSOBOWE - oznaczają informacje o **zidentyfikowanej** lub możliwej do **zidentyfikowania** osobie fizycznej.	
informacje o osobie fizycznej	informacje, które możemy przyporządkować do konkretnej osoby fizycznej takie jak imię i nazwisko, numer identyfikacyjny(NIP, PESEL itp.), dane o lokalizacji (adres zamieszkania, pracy, korespondencyjny itp.), identyfikator internetowy (login, ID) lub jeden bądź kilka szczególnych czynników określających fizyczną (np. budowa ciała), fizjologiczną (np. praca narządów), genetyczną (np. kod DNA, cechy genetyczne), psychiczną (np. choroby psychiczne, skłonności psychiczne), ekonomiczną (np. posiadany majątek, zarobki), kulturową (np. podtrzymywane tradycje) lub społeczną tożsamość (np. identyfikacja z grupami społecznymi) osoby fizycznej
zidentyfikowana osoba fizyczna	zestaw informacji lub pojedyncza informacja, która jednoznacznie wskazuje na konkretną osobę fizyczną i jest to potwierdzone poprzez identyfikację (np. wylegitymowanie, przelew z indywidualnego konta, inny mechanizm organizacyjny lub techniczny jednoznacznie stwierdzający, że mamy do czynienia z konkretną osobą)
osoba fizyczna możliwa do zidentyfikowania	osoba fizyczna, która nie jest jeszcze zidentyfikowana ale pozyskane informacje jednoznacznie mogą wskazywać na konkretną osobę
szczególne kategorie danych	szczególne kategorie danych to dane osobowe dotyczące: opochodzenia rasowego lub etnicznego; opoglądów politycznych; oprzekonań religijnych lub światopoglądowych; oprzynależności do związków zawodowych; odanych genetycznych, biometrycznych, dotyczących zdrowia; oseksualności lub orientacji seksualnej.

PRZETWARZANIE - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak:	
oZbieranie, utrwalanie, pobieranie; oorganizowanie, porządkowanie; oprzechowywanie, przeglądanie, wykorzystywanie; oadaptowanie lub modyfikowanie;	oujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie; odopasowywanie lub łączenie; oograniczanie; ousuwanie lub niszczenie.

ADMINISTRATOR - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala **cele i sposoby** (*) przetwarzania danych osobowych.	
sektor prywatny	w działalnościach i ich pochodnych administratorem są osoby fizyczne prowadzące działalność gospodarczą, w przypadku spółek prawa handlowego (z o.o. i s. a.) to osoby realnie decydujące będą administratorami, spółka jako osobowość prawna może być administratorem tylko w przypadku gdy struktury organizacyjne nie pozwalają na decyzyjność osobową czyli cały zarząd, zgromadzenie podejmuje decyzję, a i w tych przypadkach w niektórych czynnościach to jednostki (osoby fizyczne) będą administratorem.
(*) Jeżeli **cele i sposoby** takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.	
sektor publiczny	w urzędach, szkołach, ośrodkach kultury, sportu i turystyki, w jednostkach rządowych i samorządowych administratora wyznaczają przepisy, jest to osoba fizyczna, która ze względu na pełnioną ustawowo funkcję, realizuje zadania publiczne lub wykonuje władzę publiczną, natomiast pracownicy zatrudnieni w placówce, którymi kieruje, realizują ich zadania w ich imieniu

NARUSZENIE OCHRONY DANYCH OSBOWYCH - oznacza **naruszenie bezpieczeństwa** prowadzące do **przypadkowego** lub **niezgodnego** z prawem:
o**zniszczenia** danych osobowych, o**utracenia** danych osobowych, o**zmodyfikowania** danych osobowych,

o**ujawnienia** danych osobowych, o**dostępu** do danych osobowych.

ORGAN NADZORCZY - oznacza niezależny organ publiczny tj. Prezes Urzędu Ochrony Danych Osobowych, właściwy w sprawach ochrony danych osobowych.
INFORMACJE TELEADRESOWE **Urząd Ochrony Danych Osobowych** ul. Stawki 2, 00-193 Warszawa tel. 22 531-03-00 godziny pracy urzędu: 8.00–16.00 kancelaria@uodo.gov.pl **Infolinia: 606-950-000** czynna w dni robocze: 10.00–14.00

ZAKRES OBOWIAZYWANIA

Rozporządzenie 2016/679 dotyczy każdego kto przetwarza dane osobowe:	o w imieniu własnym;
	o w imieniu administratora tych danych osobowych;
	o mając jednostkę organizacyjną zarejestrowaną w UE nawet jeżeli nie przetwarza danych w UE;
	o i nie ma jednostki organizacyjnej w UE ale przetwarza dane osobowe osób przebywających w UE.

Rozporządzenie 2016/679 nie dotyczy:	o nie objętych prawem Unii Europejskiej
	o państw członkowskich UE w zakresie działań zewnętrznych UE, wspólnej polityki zagranicznej i bezpieczeństwa (Rozdział 2 tytuł V TUE).
	o osób fizycznych w ramach czynności o czysto osobistym lub domowych charakterze.
	o danych osobowych przetwarzanych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

PODSTAWY PRAWNE

ZGODA – przetwarzanie jest zgodne z prawem jeżeli osoba fizyczna wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów.	
Warunki wyrażenia zgody	a. zgoda musi wyć wyrażona w określonym celu; b. zgoda musi być wyrażona dobrowolnie; c. należy być w stanie wykazać, że osoba, której dane dotyczą faktycznie wyraziła zgodę; d. zapytanie o zgodę musi być przedstawione w sposób wyraźniej odróżniający je od pozostałych kwestii; e. zapytanie o zgodę musi być w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem; f. osoba fizyczna musi mieć możliwość w dowolnym momencie wycofać zgodę; g. wycofanie zgody nie może wywoływać skutków prawnych; h. wycofanie zgody musi być co najmniej tak łatwe jak jej wyrażenie; i. w przypadku osoby niepełnoletniej zgodę wyrazić może tylko prawny opiekun dziecka.

UMOWA – przetwarzanie jest zgodne z prawem w przypadku gdy **jest niezbędne** do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.	
jest niezbędne do wykonania umowy	o musimy mieć faktyczną niezbędność przetwarzania konkretnych danych w celu realizacji umowy w innym przypadku musimy poszukać innej podstawy prawnej lub zaprzestać przetwarzania danych osobowych, które nie są niezbędne
jest niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy	o jak powyżej, musimy mieć faktyczną niezbędność; o wszystkie żądania osoby fizycznej muszą być niezbędne w celu zawarcia umowy

OBOWIĄZEK PRAWNY – przetwarzanie jest zgodne z prawem w przypadku gdy **jest niezbędne** do wypełnienia obowiązku prawnego ciążącego na administratorze.	
jest niezbędne do wykonania obowiązku prawnego	o przetwarzanie może odbywać się tylko wyłącznie w zakresie niezbędnym do realizacji obowiązku prawnego;

	○jeżeli jest możliwość realizacji obowiązku prawnego bez wykorzystania danych osobowych to nie wolno przetwarzać danych osobowych; ○jeżeli przepisy określają zakres danych jaki jest obowiązek przetwarzać to może być tylko wskazany zakres przetwarzany.

ŻYWOTNY INTERES – przetwarzanie jest zgodne z prawem w przypadku gdy **jest niezbędne** do w ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.	
jest niezbędne do wykonania obowiązku prawnego	○przetwarzanie może odbywać się tylko wyłącznie w zakresie niezbędnym do ochrony żywotnego interesu; ○jeżeli jest możliwość ochrony żywotnego interesu bez wykorzystania danych osobowych to nie wolno przetwarzać danych osobowych.

INTERES PUBLICZNY I WŁADZA PUBLICZNA – przetwarzanie jest zgodne z prawem w przypadku gdy **jest niezbędne** do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi	
jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach władzy publicznej	○przetwarzanie może odbywać się tylko wyłącznie w zakresie niezbędnym do wykonania zadania realizowanego w interesie publicznym lub w ramach władzy publicznej ○jeżeli jest możliwość wykonania zadania realizowanego w interesie publicznym lub w ramach władzy publicznej bez wykorzystania danych osobowych to nie wolno przetwarzać danych osobowych; ○przepisy mogą wskazywać dokładnie jakie dane osobowe należy przetwarzać.

PRAWNIE UZASADNIONY INTERES – przetwarzanie jest zgodne z prawem tylko w przypadku gdy **jest niezbędne** do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora	
jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora	○wyjątkiem są sytuacje, w których nadrzędny charakter mają interesy lub prawa i wolność osób fizycznych, których dane dotyczą; ○jeżeli jest możliwość wykonania prawnego interesu administratora bez wykorzystania danych osobowych to nie wolno przetwarzać danych osobowych; ○przepisy mogą wskazywać dokładnie jakie dane osobowe należy przetwarzać, w konkretnych przypadkach

SZCZEGÓLNE PRZYPADKI PRZETWARZANIA

Przetwarzanie **szczególnych kategorii** danych osobowych jest dozwolone tylko wyłącznie w następujących przypadkach:	a.osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
	b.przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
	c.przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
	d.przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
	e.przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
	f.przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
	g.przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
	h.przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;
	i.przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
	j.przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Przetwarzanie danych osobowych dotyczących **wyroków skazujących i naruszeń prawa**	Przetwarzanie danych osobowych dotyczących wyroków skazujących, naruszeń prawa lub środków bezpieczeństwa dotyczących przetwarzania tych danych jest dozwolone tylko:
	Ona podstawie zgody osoby fizycznej, której dane dotyczą i dokonywane jest wyłącznie pod nadzorem władzy publicznej;
	Ona podstawie przepisu krajowego z zastosowaniem odpowiednich zabezpieczeń, pod nadzorem władzy publicznej.

Przetwarzanie a **wolność wypowiedzi i informacji**	Opaństwa członkowskie UE we własnym zakresie określają przepisy dotyczące przetwarzania danych osobowych dla potrzeb dziennikarskich oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej, mogą one zawierać wyjątki od przepisów RODO; Ow zakresie nieuregulowanym zastosowanie mają przepisy rozporządzenia 2016/679 (RODO).

Przetwarzanie a **publiczny dostęp do dokumentów urzędowych**	Opaństwa członkowskie określają przepisy ale muszą one być spójne z RODO; Ow zakresie nieuregulowanym zastosowanie mają bezpośrednio przepisy rozporządzenia 2016/679 (RODO).

Przetwarzanie **krajowego numeru identyfikacyjnego**	Opaństwa członkowskie określają przepisy ale muszą one być spójne z RODO; Ow zakresie nieuregulowanym zastosowanie mają bezpośrednio przepisy rozporządzenia 2016/679 (RODO).

Przetwarzanie **w kontekście zatrudnienia**	Opaństwa członkowskie określają przepisy ale muszą one być spójne z RODO; Ow zakresie nieuregulowanym zastosowanie mają bezpośrednio przepisy rozporządzenia 2016/679 (RODO).

ZASADY PRZETWARZANIA

ZGODNOŚĆ Z PRAWEM, RZETELNOŚĆ I PRZEJRZYSTOŚĆ – dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.	Ozgodność z prawem, czyli jeżeli przepisy określają dokładnie sposób i zakres przetwarzania to stosujemy ten przepis, jeżeli natomiast nie mamy tego uregulowanego to przetwarzamy zgodnie z art. 6 RODO czyli przetwarzanie danych osobowych musi odbywać się na podstawie zgody lub musi być **niezbędne** do realizacji umowy, obowiązku prawnego, ochrony żywotnych interesów, realizacji zadań publicznych, wykonywania władzy publicznej lub realizacji prawnego interesu;
	Orzetelnie, czyli tak jak dokładnie chcielibyśmy aby ktoś inny przetwarzał nasze dane osobowe, z należytą powagą i dbałością;
	Oprzejrzyście, czyli przetwarzanie ma być zrozumiałe dla osoby fizycznej, ma wiedzieć dlaczego i w jakim zakresie przetwarzamy jej dane osobowe.

OGRANICZENIE CELU – dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami	Odane osobowe mogą być przetwarzane tylko w prawnie uzasadnionych celach;
	Oprzetwarzanie danych do innych celów niż te dla których zostały zebrane może się tylko odbyć jeżeli wynika to z przepisów bądź mamy na to zgodę osoby fizycznej, której dane dotyczą;

MINIMALIZACJA DANYCH – dane osobowe muszę być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów w których są przetwarzane	Onależy przetwarzać tylko tyle danych ile jest **niezbędnych** do realizacji celów, dla których te dane pobieraliśmy;
	Ojeżeli jesteśmy w stanie osiągnąć cel przetwarzania bez pobierania danych, bądź z minimalnym zakresem danych, to tylko tak należy osiągać ten cel;
	Onie pobieramy danych osobowych „na zaś" lub „na wszelki wypadek" lub „bo ktoś może nie zapłacić" itp.

PRAWIDŁOWOŚĆ – dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane	Onależytą staranność zachowujemy przy pobieraniu, przepisywaniu czy modyfikowaniu danych osobowych, tak aby mieć pewność, że dane osobowe są prawidłowe;
	Onależy sprostować dane osobowe, które są nieaktualne poprzez zastosowanie lub wprowadzenie środków technicznych i organizacyjnych pozwalających na dokonanie takiej aktualizacji;
	Ojeżeli dane osobowe nie są poprawne to należy je niezwłocznie usuną lub sprostować.

OGRANICZENIE PRZECHWYWANI – dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów	Odane osobowe możemy przetwarzać tylko do czasu zakończenia realizacji celu, dla którego je pobraliśmy;
	Opo zakończeniu realizacji celu przetwarzania należy usunąć dane osobowe albo zmodyfikować je tak aby na ich podstawie nie można było zidentyfikować osoby, której one dotyczą;
	Odane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane

w których dane te są przetwarzane;	wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą, A PRZEDE WSZYSTKIM MINIMALIZACJA DANYCH.

INTEGRALNOŚĆ I POUFNOŚĆ – dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych	oDane osobowe musza być zabezpieczone przed: §niedozwolonym lub niezgodnym z prawem przetwarzaniem; §przed przypadkową utratą danych; §przed przypadkowym zniszczeniem.
	oodpowiednie bezpieczeństwo danych osobowych należy osiągnąć poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, minimalizujących ryzyko powstania powyższych zagrożeń.

ROZLICZALNOŚĆ	oadministrator musi być wstanie wykazać, że przestrzega 6 zasad dotyczących przetwarzania danych osobowych.

PRAWA OSÓB FIZYCZNYCH

OBOWIĄZEK INFORACYJNY	oinformację wynikające z obowiązku informacyjnego przedstawiamy w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem;
	oJeżeli pozyskujemy dane od osoby fizycznej to obowiązek spełniamy najpóźniej przy pozyskaniu danych;
	oJeżeli administrator nie pozyskał danych od osoby fizycznej to obowiązek spełnia najpóźniej przy pierwszym ujawnieniu, przy pierwszej komunikacji z tą osobą ale nie później niż w ciągu 30 dni od pozyskania danych;
	oJeżeli administrator dalej będzie przetwarzał dane osobowe w innym celu, to spełnia on ponownie obowiązek informacyjny przed dalszym przetwarzaniem w tym celu.

ZASADY REALIZACJI PRAW OSÓB FIZYCZNYCH	oNależy prowadzić wszelką niezbędną komunikację z osobą fizyczna, w zakresie realizacji jej praw;
	oodpowiedzi udziela się w formie w jakiej wysłane zostało żądanie, chyba że wskazana jest inna forma udzielania odpowiedzi to odpowiadamy we wskazany sposób;
	oodpowiedzi na żądanie udzielamy w ciągu 30, także odmownej;
	oprzed realizacją żądania należy zweryfikować tożsamość osoby fizycznej zgodnie z obowiązującymi przepisami lub metodami jednoznacznie identyfikującą osobę fizyczną jeżeli nie ma tego określonego w przepisach.
	oJeżeli administrator dokonał usunięcia, sprostowania lub ograniczenia przetwarzania związku z realizacją żądania osoby fizycznej, której dane dotyczą to: §informuje o tym wszystkich odbiorców, którym ujawnił dane osobowe chyba, że okażę się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku; §informuje o odbiorcach osobę fizyczną, jeżeli tego zażąda.

PRAWO DOSTEPU	oosoba fizyczna, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące
	oosoba fizyczna, której dane dotyczą, jest uprawniona do uzyskania od administratora kopii swoich danych osobowych, które przetwarza administrator;
	oosoba fizyczna, której dane dotyczą, jest uprawniona do uzyskania od administratora następujących informacji: §cele przetwarzania; §kategorie odnośnych danych osobowych; §informacje o odbiorcach lub kategoriach odbiorców; §w miarę możliwości planowany okres przechowywania danych osobowych; §informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania; §informacje o prawie wniesienia skargi do organu nadzorczego; §wszelkie dostępne informacje o ich źródle;

	§informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu; §informacji o zabezpieczeniach jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej.
	oKopia danych osobowych nie może zawierać danych poufnych i danych osobowych innych osób fizycznych, jeżeli nie przewidują tego przepisy.

PRAWO DO SPORSTOWANIA	oOsoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
	oZ uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

PRAWO DO USUNIĘCIA	oosoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności: §dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane; §osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania; §osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania; §dane osobowe były przetwarzane niezgodnie z prawem; §dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego; §dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.
	oJeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to (biorąc pod uwagę dostępną technologię i koszt realizacji) podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje;
	oprawo do usunięcia nie ma zastosowania w zakresie w jakim przetwarzanie jest niezbędne: §do korzystania z prawa do wolności wypowiedzi i informacji; §do wywiązania się z prawnego obowiązku wymagającego przetwarzania lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; §z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego; §do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych; §do ustalenia, dochodzenia lub obrony roszczeń.

PRAWO DO OGRANICZENIA PRZETWARZANIA	oosoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach: §osoba, której dane dotyczą kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych; §przetwarzanie jest niezgodne z prawem a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania; §administrator nie potrzebuje już danych osobowych do celów przetwarzania ale są one potrzebne osobie, której dane dotyczą do ustalenia, dochodzenia lub obrony roszczeń; §osoba, której dane dotyczą wniosła sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
	ojeżeli przetwarzanie zostało ograniczone to dalsze przetwarzanie może nastąpić tylko: §w celu przechowywania; §za zgodą osoby fizycznej, której dane dotyczą; §w celu ustalenia, obrony lub dochodzenia roszczeń; §w celu ochrony praw innej osoby fizycznej lub prawnej; ze względu na ważny interes publiczny.

PRAWO DO PRZENOSZENIA	ojeżeli administrator przetwarza w sposób zautomatyzowany dane osobowe na podstawie zgody lub umowy to: §osoba fizyczna ma prawo otrzymać dane jej dotyczące

	w powszechnej formie nadającej się do odczytu maszynowego; §osoba fizyczna ma prawo zażądać przesłania swoich danych innemu administratorowi, jeżeli jest to technicznie możliwe.
	oprawo do przenoszenia nie dotyczy przetwarzania niezbędnego do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowanej władzy powierzonej administratorowi.

PRAWO DO SPRZECIWU	oosoba, której dane dotyczą ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych jeżeli: §przetwarzanie odbywa się na podstawie interesu publicznego lub władzy publicznej; §przetwarzanie odbywa się na podstawie prawnego interesu administratora; §przetwarzanie odbywa się na potrzeby marketingu bezpośredniego i profilowania; §przetwarzanie odbywa się a potrzeby badań naukowych lub historycznych; §przetwarzanie odbywa się w celach statystycznych.
	ojeżeli osoba fizyczna wniesie sprzeciw nie wolno przetwarzać już tych danych chyba że: §istnieje ważny prawny interes, nadrzędny w stosunku do praw osoby fizycznej; §przetwarzanie jest niezbędne do ustalenia, dochodzenia i obrony roszczeń; §przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
	oprzy pierwszej komunikacji z osobą fizyczną informuje się o prawie do wniesienia sprzeciwu, informacja ma być jasna i wyraźnie odróżniona o pozostałej treści.

ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI	oosoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.
	oosoba, której dane dotyczą, nie ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, jeżeli ta decyzja: §jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą a administratorem; §jest dozwolona prawem; §opiera się na wyraźnej zgodzie osoby, której dane dotyczą.
	oprzypadkach, o których mowa powyżej administrator: §wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, §zapewnia realizację prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

KONTROLE I KARY

UPRAWNIENI DO KONTROLI	oWewnętrznie §Administrator; §Inspektor ochrony danych.
	oOrgan nadzorczy §Prezes UODO; §Upoważniony pracownik UODO; §Upoważniony specjalista w obecności pracownika UODO; §Inne organy nadzorcze (np. NIK) w zakresie swoich kompetencji.
	oZewnętrznie §Audytor jednostki nadrzędnej (musi posiadać kwalifikacje takie jak IOD); §Administrator w stosunku do podmiotu przetwarzającego.

KONTROLA UODO ZAKRES UPRAWNIEŃ	oKontrola UODO uprawniona jest do: a.wstępu w godzinach od 6:00 do 22: 00 na grunt oraz do budynków, lokali lub innych pomieszczeń; b.wglądu do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;

	c.przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych; d.żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego; e.zlecać sporządzanie ekspertyz i opinii.

OKOLICZNOŚCI NAKŁADANIA KAR PIENIĘŻNEJ - WYTYCZNE	oadministracyjne kary pieniężne nakłada się zależnie od okoliczności każdego indywidualnego przypadku. Decydując czy nałożyć administracyjną karę pieniężną oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na: a.charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą oraz rozmiaru poniesionej przez nie szkody; b.umyślny lub nieumyślny charakter naruszenia; c.działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą; d.stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich; e.wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego; f.stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków; g.kategorie danych osobowych, których dotyczyło naruszenie; h.sposób w jaki organ nadzorczy dowiedział się o naruszeniu w szczególności czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie; i.jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 – przestrzeganie tych środków (nakaz wykonania konkretnych działań wymaganych przepisami); j.stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji.

ZA JAKIE PRZEWINIENIA KARA	oKarę pieniężną otrzymać można za naruszenia przepisów dotyczących następujących kwestii: a.podstawowych zasad przetwarzania, w tym warunków zgody; b.praw osób, których dane dotyczą, o których mowa w art. 12–22 RODO; c.przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej; d.wszelkich obowiązków wynikających z prawa państwa członkowskiego; e.nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy lub niezapewnienia dostępu skutkującego naruszeniem.

WYSOKOŚĆ KARY PIENIĘŻNEJ	oWysokość kar dla podmiotów innych niż jednostka sektora finansów publicznych, instytut badawczy, Narodowy Bank Polski: §do 20 000 000 EUR lub do 4 % całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.
	oWysokość kar dla jednostek sektora finansów publicznych, instytutów badawczych, Narodowego Banku Polskiego: §do 100 000 złotych.

POSTĘPOWANIA KARNE	oKażdy kto przetwarza dane osobowe, choć ich przetwarzanie **nie jest dopuszczalne** albo do ich przetwarzania **nie jest uprawniony**, §podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
	oKażdy kto przetwarza **kategorie danych szczególnych** a nie jest do tego uprawniony: §podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
	oKażdy kto **udaremnia lub utrudnia** kontrolującemu **prowadzenie kontroli** przestrzegania przepisów o ochronie danych osobowych, §podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

INSPEKTOR OCHRONY DANYCH

STATUT IOD	oadministrator oraz wszystkie osoby uprawnione zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany **we wszystkie sprawy dotyczące przetwarzania danych**

	osobowych, także tych planowanych. (art. 38 ust 1 RODO)
	oAdministrator oraz wszyscy uprawnieni **wspierają** inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz **dostęp do danych osobowych i operacji przetwarzania**. (art. 38 ust 2 RODO)
	oadministrator oraz wszyscy uprawnieni zapewniają, by inspektor ochrony **danych nie otrzymywał instrukcji** dotyczących wykonywania własnych zadań. Nie jest on **odwoływany ani karany** przez administratora ani uprawnionych za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega **najwyższemu kierownictwu**. (art. 38 ust 3 RODO)
	oosoby, których dane dotyczą mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia. (art. 38 ust 4 RODO)
	oadministrator oraz wszystkie osoby uprawnione mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem.
	oinspektor ochrony danych jest zobowiązany do poufności co do wykonywania swoich zadań. (art. 38 ust 5 RODO)
	oinspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. (art. 38 ust 6 RODO)

ZADANIA IOD	oinformowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
	omonitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
	oudzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
	owspółpraca z organem nadzorczym;
	opełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

OBOWIĄZKI ADMINISTRATORA (DOTYCZY TYLKO KADRY KIEROWNICZEJ)

ZAWIADOMIENIE O NARUSZNEIU OCHRONY DANYCH OSOBOWYCH - OSOBA FIZYCZNA -	oJeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu.
	oZawiadomienie o naruszeniu ochrony danych: §jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych; §imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego od którego można uzyskać więcej informacji; §możliwe konsekwencje naruszenia ochrony danych osobowych; §środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych.

ZAWIADOMIENIE O NARUSZNEIU OCHRONY DANYCH OSOBOWYCH - URZĄD OCHRONY DANYCH -	onaruszenie ochrony danych osobowych należy zgłosić do UODO, jeżeli może skutkować naruszeniem praw i wolności osoby fizycznej;
	onaruszanie ochrony danych osobowych należy zgłaszać do UODO wciągu 72 godzin od stwierdzenia naruszenia;

REJSTR NARUSZEŃ OCHRONY DANYCH	oadministrator musi prowadzić rejestr wszystkich naruszeń, również tych niewymagających zgłoszenia zawierający co najmniej: §okoliczności naruszenia; §skutki naruszenia; §działania zaradcze.

ANALIZA RYZYKA	oUwzględniając wiedzę techniczną i koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania w wyniku analizy ryzyka w stosownych przypadkach należy zastosować następujące **środki techniczne i organizacyjnie**: §pseudonimizację i szyfrowanie danych osobowych; §zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; §zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; §regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania; §przepisy sektorowe wskazujące minimalne wymagania bezpieczeństwa (np. przepisy BHP, Krajowe Ramy Interoperacyjności, Instrukcje Kancelaryjne i Archiwalne).

OCENA SKUTKÓW	oocena skutków wymagana jest w następujących przypadkach: §w wyniku analizy ryzyka wyszło wysokie ryzyko naruszenia praw i wolności osób fizycznych i nie ma możliwości zastosować środków technicznych i organizacyjnych, które to ryzyko zminimalizują; §systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną; §przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; §systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie; §czynność wskazana jest w wykazie rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych wydany przez UODO.
	oocena skutków zawiera co najmniej: §systematyczny opis planowanych operacji przetwarzania; §cele przetwarzania; §ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów; §analizę ryzyka naruszenia praw lub wolności osób, których dane dotyczą; §środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą i innych osób, których sprawa dotyczy.

REJESTR CZYNNOŚCI	okażdy administrator ma obowiązek prowadzić rejestr czynności a podmiot przetwarzający rejestr kategorii czynności jeżeli zostanie spełniony jeden z poniższych warunków: §zatrudnia co najmniej 250 pracowników; §przetwarzanie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych; §przetwarzanie nie ma charakteru sporadycznego; §przetwarza szczególne kategorie danych osobowych; §przetwarza dane dotyczące wyroków skazujących i naruszeń prawa.

OCHRONA DANYCH OSOBOWYCH W FACIE PROJEKTOWANIA	oUwzględniając §wiedzę techniczną §koszt wdrożenia §oraz charakter, zakres, kontekst i cele przetwarzania **przed określaniem sposobów przetwarzania** należy zastosować następujące **środki techniczne i organizacyjnie**: §minimalizację danych osobowych; §pseudonimizację i szyfrowanie danych osobowych; §wdrożyć przepisy sektorowe wskazujące minimalne wymagania bezpieczeństwa (np. przepisy BHP, Krajowe Ramy Interoperacyjności, Instrukcje Kancelaryjne i Archiwalne); §inne niezbędne do zagwarantowania zgodności przetwarzania z RODO.

DOMYŚLNA OCHRONA	oDomyślna ochrona danych osobowych to wprowadzenie środków technicznych i organizacyjnych

DANYCH OSOBOWYCH	mających zapewnić, że: §przetwarzane są wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania; §zakres danych jest adekwatny do celu przetwarzania i niezbędny do jego realizacji; §dane są przetwarzane przez okres niezbędny do realizacji celu przetwarzania; §dane osobowe są udostępniane jedynie uprawnionym odbiorcom; §wprowadzone są mechanizmy zapewniające kontrolę ludzką dotyczącą udostępniania danych.

WSPÓŁADMINISTRATORZY	oWspóładministratorzy: §wspólnie ustalają cele i sposoby przetwarzania; §przepisy lub regulaminy wspólnie wyznacza ich do realizacji danych czynności.
	oJeżeli mamy do czynienia ze współadministratorstwem to musimy zawrzeć porozumienie zawierające co najmniej: §sposób realizacji praw osób fizycznych; §sposób realizacji obowiązku informacyjnego; §punkt kontaktowy dla osób fizycznych; §sposób uregulowania pozostałych obowiązków wynikających z RODO.

PODMIOT PRZETWARZAJACY	oJeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia 2016/679 i chroniło prawa osób, których dane dotyczą;
	oPodmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian;
	oPodmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian;
	oJeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia;
	oPrzetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.
	oInstrument prawny regulujący powierzenie przetwarzania zapewnia w szczególności, że podmiot przetwarzający: a.przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny; b.zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy; c.podejmuje wszelkie środki wymagane na mocy art. 32; d.przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4; e.biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;

	f.uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36; g.uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36; h.udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. i.korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym j.informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

PRZETWARZANIE NA POLECENIE ADMINISTRATORA	oadministrator oraz każdy podmiot przetwarzający musi zadbać aby każda czynność przetwarzania, przetwarzana w ich imieniu przez konkretne osoby fizyczne odbywała się na ich wyraźne polecenie;
	opolecenie administratora może być zawarte w: §zakresie obowiązków; §umowie o pracę / zlecenie / itp.

Załącznik Nr 3 do Załącznika Nr 2

wniosek dotyczący upoważnienia

WNIOSEK DOT. UPOWAŻNIEŃ DO PRZETWARZANIA

1. Wniosek wypełnia bezpośredni przełożony osoby upoważnianej.
2. Należy wypełnić wszystkie puste szare pola.
3. W przypadku pól wyboru ☐ należy wybrać tylko jedną pole i uzupełnić szare puste pole go dotyczące.
4. W punktach 4-6 wypełniamy tylko pola, które dotyczą wybranego działania.
5. Do wniosku należy dołączyć aktualny zakres obowiązków służbowych, zatwierdzony przez administratora bądź innego uprawnionego do tego przełożonego.
6. Wniosek musi zostać podpisany przez przełożonego oraz inspektora ochrony danych.
7. Wniosek sporządza się w dwóch egzemplarzach jeden dla IOD drugi dla składającego wniosek przełożonego.

1. DANE ADMINISTRATORA	
Nazwa administratora:	
Adres siedziby:	

2. DANE WNIOSKUJĄCEGO (PRZEŁOŻONEGO)	
Imię i nazwisko:	
Stanowisko/funkcja:	
Komórka organizacyjna:	

3. DANE OSOBY UPOWAŻNIONEJ	
Imię i nazwisko:	
Stanowisko/funkcja:	
Komorka organizacyjna:	

☐	**4. NADANIE UPOWAŻNIENIA (tylko nowy pracownik)**	
Proszę o nadanie nowego upoważnienia do przetwarzania w zakresie niezbędnym do realizacji następujących zadań służbowych wskazanej powyżej osobie:		
1. _____		
2. _____		
3. _____		
4.		
Upoważnienie obowiązywać będzie:		
☐	do zakończenia stosunku pracy.	
☐	do zakończenia obowiązywania obecnej umowy.	
☐	do	

☐	**5. MODYFIKACJA UPOWAŻNIENIA**	
Proszę o modyfikację upoważnienia w zakresie niezbędnym do realizacji aktualnych następujących zadań służbowych:		
1. _____		
2. _____		
3. _____		
4.		
Aktualne upoważnienie obowiązywać będzie:		
☐	do zakończenia stosunku pracy.	
☐	do zakończenia obowiązywania obecnej umowy.	
☐	do	
Poprzednie upoważnienia do przetwarzania danych osobowych:		
☐	zostaje wycofane;	
☐	pozostaje bez zmian;	
☐	nie dotyczy.	

☐	**6. WYCOFANIE UPOWAŻNIENIA**
Proszę o wycofanie upoważnienia do przetwarzania danych osobowych:	
☐	w pełnym zakresie.
☐	w następującym zakresie:
1. _____ 2. _____ 3. _____ 4.	
Upoważnienie przestaje obowiązywać:	
☐	z dniem złożenia wniosku.
☐	z dniem

miejscowość	*data*	*miejscowość*	*data*
Podpis IOD		*Podpis przełożonego*	

_____

(czytelny podpis administratora)

Załącznik Nr 4 do Załącznika Nr 2

oświadczenie RODO

Załącznik nr ____

do _____

obowiązującej w

_____

OŚWIADCZENIE

sygnatura:

miejscowość i data:

Pracownik
Imię i nazwisko:

Komórka organizacyjna:

Stanowisko:

Pracodawca
Nazwa jednostki:

Adres siedziby:

Administrator:

Oświadczam, że zostałem przeszkolony z następującego zakresu:
·zasady przetwarzania danych osobowych;
·prawa osób fizycznych, których dane są przetwarzane;
·zasady bezpieczeństwa przy przetwarzaniu danych osobowych;
·normy prawne regulujące przepisy dotyczące przetwarzania;
·obowiązki wynikające z przetwarzania danych osobowych;
·_____.

Ponadto zobowiązuję się do:
a.stosowania postanowień polityk bezpieczeństwa oraz zasad bezpieczeństwa i higieny pracy;
b.zachowania w poufności wszystkich informacji pozyskanych związku z wykonywaniem pracy, a w szczególności informacji dotyczących danych osobowych, danych poufnych, danych technicznych i organizacyjnych środków bezpieczeństwa;
c.przetwarzania danych osobowych tylko w zakresie adekwatnym, stosownym i ograniczonym do zakresu obowiązków służbowych zgodnie z zasadą minimalizacji danych osobowych;
d.zgłaszania każdego naruszenia bezpieczeństwa niezwłocznie po wykryciu;
e.zapewnienia największego możliwego bezpieczeństwa przetwarzanych danych osobowych i danych poufnych;
f.wspierania osób kontrolujących bezpieczeństwo przetwarzania i wykonywania ich poleceń.

Zostałem poinformowany, że złamanie zasad określonych w Politykach Ochrony Danych lub złamanie postanowień złożonego oświadczenia będzie stanowić naruszenie obowiązków pracowniczych.

podpis uprawnionego podpis oświadczającego (pracownik)			
sygnatura:		miejscowość i data:	

Pracownik Imię i nazwisko: Komórka organizacyjna: Stanowisko:	**Pracodawca** Nazwa jednostki: Adres siedziby: Administrator:

Oświadczam, że zostałem przeszkolony z następującego zakresu:

- zasady przetwarzania danych osobowych;
- prawa osób fizycznych, których dane są przetwarzane;
- zasady bezpieczeństwa przy przetwarzaniu danych osobowych;
- normy prawne regulujące przepisy dotyczące przetwarzania;
- obowiązki wynikające z przetwarzania danych osobowych;
- _____.

Ponadto zobowiązuję się do:

a. stosowania postanowień polityk bezpieczeństwa oraz zasad bezpieczeństwa i higieny pracy;

b. zachowania w poufności wszystkich informacji pozyskanych związku z wykonywaniem pracy, a w szczególności informacji dotyczących danych osobowych, danych poufnych, danych technicznych i organizacyjnych środków bezpieczeństwa;

c. przetwarzania danych osobowych tylko w zakresie adekwatnym, stosownym i ograniczonym do zakresu obowiązków służbowych zgodnie z zasadą minimalizacji danych osobowych;

d. zgłaszania każdego naruszenia bezpieczeństwa niezwłocznie po wykryciu;

e. zapewnienia największego możliwego bezpieczeństwa przetwarzanych danych osobowych i danych poufnych;

f. wspierania osób kontrolujących bezpieczeństwo przetwarzania i wykonywania ich poleceń.

Zostałem poinformowany, że złamanie zasad określonych w Politykach Ochrony Danych lub złamanie postanowień złożonego oświadczenia będzie stanowić naruszenie obowiązków pracowniczych.

podpis uprawnionego	podpis oświadczającego (pracownik)

Załącznik Nr 5 do Załącznika Nr 2

upoważnienie

_____, _____

(miejscowość) (data złożenia wniosku)

_____

(sygnatura sprawy)

UPOWAŻNIENIE

do przetwarzania danych osobowych

Oświadczam, że Pani/Pan:

imię i nazwisko	stanowisko
komórka organizacyjna	

jest upoważniona/y do przetwarzania danych osobowych w zakresie niezbędnym do realizacji następujących obowiązków służbowych:

1. ____
2. ____

Upoważnienie jest ważne do czasu zakończenia stosunku pracy lub do wycofania upoważnienia.

Poprzednie upoważnienia do przetwarzania danych osobowych:

☐ zostają wycofane;

☐ pozostają bez zmian;

☐ nie dotyczy.

_____

(czytelny podpis administratora)

Załącznik Nr 6 do Załącznika Nr 2

wniosek dot. uprawnień do systemów

Załącznik Nr 3 do zarządzenia Nr Nr 715/2021
Burmistrza Miasta i Gminy Kąty Wrocławskie
z dnia 08 kwietnia 2021 r.

PROCEDURA NADZOROWANIA CZYNNOŚCI

PROCEDURA NADZOROWANIA CZYNNOŚCI

SPIS TREŚCI

I. WPROWADZENIE

1.Niniejsza procedura jest integralną częścią Polityki, jednakże Polityka jest nadrzędnym dokumentem w stosunku do procedury.
2.Niniejsza procedura określa zasady:
a.wprowadzania nowych czynności przetwarzania;
b.nadzorowania obecnie wykonywanych czynności;
c.przeprowadzania kontroli wykonywanych czynności;
d.prowadzenia rejestru czynności przetwarzania i rejestru kategorii czynności.
3.Wprowadzenie niniejszej procedury jest niezbędne ze względu na:
a.zapewnienie odpowiednich środków technicznych i organizacyjnych wynikających z art. 24 rozporządzenia UE 2016/679;
b. zapewnienie uwzględnienia ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych, o której mowa w art. 25 rozporządzenia UE 2016/679;
c.zapewnienie prowadzenia rejestru czynności przetwarzania i kategorii czynności wynikającego z art. 30 rozporządzenia UE 2016/679;
d.zapewnienie bezpieczeństwa, o którym mowa w art. 33 rozporządzenia 2016/679;
e.zapewnienie realizacji oceny skutków, o której mowa w art. 35 rozporządzenia UE 2016/679;
f.zapewnienie rozliczalności przestrzegania zasad przetwarzania danych osobowych, o których mowa w art. 5 rozporządzenia UE 2016/679.
4.Niniejsza procedura dotyczy wszystkich wykonywanych i planowanych czynności przetwarzania.
5.Jeżeli przepisy unijne lub krajowe w inny sposób regulują postanowienia niniejszej procedury to niniejsza procedura w zakresie w jakim regulują to przepisy nie obowiązuję.
6.Z niniejszą procedurą musi się zapoznać:
a.każdy pełnomocnik administratora;
b.każdy kierownik;
c.każdy członek zespołu bezpieczeństwa danych;
7.Zmiany niniejszej procedury lub jej załączników wymagają zgody Administratora oraz inspektora ochrony danych i są wprowadzane pod ich ścisłym nadzorem.

II. KONTROLA RYZYKA

1.Kontrola ryzyka wykonywana jest każdorazowo zgodnie z załącznikiem „03. kontrola ryzyka".
2.Kontrola ryzyka wykonywana jest zawsze w następujących przypadkach:
a.wprowadzanie nowej czynności przetwarzania, przed jej wprowadzeniem;
b.zmiana organizacyjna bądź techniczna związana z danymi osobowymi;
c.raz na 3 w przypadku każdej czynności przetwarzania.
3.Za zgłoszenie konieczności wykonania kontroli ryzyka odpowiedzialny jest kierownik komórki organizacyjnej,

która odpowiedzialna jest za wprowadzenie nowej czynności przetwarzania lub wprowadzenie zmiany organizacyjnej bądź technicznej.
4.Wszystkie kontrole ryzyka wykonywane są przez zespół bezpieczeństwa danych zgodnie z częścią A załącznika „03. kontrola ryzyka".
5.Cześć B załącznika „ 03. kontrola ryzyka" wypełnia IOD.
6.Wprowadzenie nowej czynności przetwarzania oraz zmiany technicznej lub organizacyjnej wpływającej na czynność przetwarzania wymaga pozytywnego wyniku z przeprowadzonej kontroli ryzyka.

III. REJESTR CZYNNOSĆI PRZETWARZANIA

1.Rejestr czynności przetwarzania jest prowadzony w celu realizacji obowiązku prawnego ale pełni też funkcję ewidencji realizowanych czynności przetwarzania.
2.Każda czynność przetwarzania musi być wprowadzona do rejestru czynności przetwarzania w zakresie wskazanym we wzorze.
3.Jeżeli informacje dotyczące czynności przetwarzania wskazanej w rejestrze czynności przetwarzania ulegną zmianie, to należy je zaktualizować.
4.Czynności przetwarzania oraz zmiany w obecnie wykonywanych czynnościach przetwarzania wprowadzane są do rejestru czynności przetwarzania po przeprowadzeniu kontroli ryzyka i uzyskaniu pozytywnego wyniku kontroli.
5.Zakończone czynności przetwarzania pozostają w rejestrze czynności przetwarzania z oznaczeniem „zakończone".
6.Wpisy do rejestru czynności przetwarzania wprowadza inspektor ochrony danych.

IV. REJESTR KATEGORII CZYNNOŚCI

1.Do rejestru kategorii czynności wpisujemy wszystkie czynności przetwarzania, które wykonywane są w imieniu innego administratora.
2.Każda czynność przetwarzania musi być wprowadzona do rejestru kategorii czynności w zakresie wskazanym we wzorze.
3.Jeżeli informacje dotyczące czynności przetwarzania wskazanej w rejestrze kategorii czynności ulegną zmianie to należy je zaktualizować.
4.Zakończone czynności pozostają w rejestrze kategorii czynności z oznaczeniem „zakończone".
5.Wpisy do rejestru kategorii czynności wprowadza inspektor ochrony danych.

V. WZORY I DOKUMENTY

1.Zastosowanie mają następujące wzory dokumentów będące załącznikami do niniejszej procedury:
a.„03. Rejestr czynności przetwarzania i kategorii czynności."
b.„03. Kontrola ryzyka."
2.W wyniku stosowania niniejszej procedury powstanie dokumentacja zawierająca dane osobowe lub/oraz informacje poufne o jednostce przetwarzającej dlatego administrator wyznacza osoby odpowiedzialne za przechowywanie w następujących zakresach:
a.„03. Rejestr czynności przetwarzania i kategorii czynności." – przechowuję w oryginale IOD;
b.„03. Kontrola ryzyka." – przechowuję w oryginale IOD.
3.Przechowywanie, archiwizowanie, modyfikowanie, ujawnianie, udostępnianie, niszczenie lub usuwanie i innego rodzaju przetwarzanie załączników lub treści w nich zawartych odbywa się zgodnie ze stosowną procedurą, chyba, że nie zawierają danych osobowych to zgodnie z przepisami unijnymi lub krajowymi lub uregulowaniami wewnętrznymi.

VI. POSTANOWIENIA KOŃCOWE

1.Nadzór nad niniejszą procedurą sprawuję:
a.IOD w pełnym zakresie;
b.każdy kierownik w obrębie własnej komórki organizacyjnej;
c.każdy pełnomocnik administratora w zakresie udzielonego pełnomocnictwa:
d.każdy upoważniony w zakresie nadanego upoważnienia;
2.Każdy kto nie przestrzega niniejszej procedury a jest do tego zobowiązany, na mocy przepisów unijnych lub krajowych lub na mocy wyrażonego oświadczenia woli, ponosi odpowiedzialność za wszelkie szkody powstałe z powodu tego zaniechania zgodnie z Kodeksem Cywilnym, Kodeksem Pracy, Rozporządzeniem UE 2016/679 bądź innymi przepisami adekwatnymi do zaistniałej sytuacji.

3.Niniejsza procedura obowiązuję z dniem _____.

VII. METRYKA			
aktualna wersja:		numer zarządzenia:	

Zakres aktualizacji	Data aktualizacji	Wprowadził aktualizacje	Zatwierdził aktualizacje

Załącznik Nr 1 do Załącznika Nr 3

Rejestr czynności przetwarzania i kategorii czynności

Nazwa podmiotu przetwarzającego		**Dane kontaktowe podmiotu przetwarzającego**	
Imię i nazwisko IOD		Dane kontaktowe IOD	
Opis/nazwa czynności	Nazwa i adres siedziby administratora	Opis kategorii przetwarzania	Zastosowane techniczne i organizacyjne środki bezpieczeństwa

Kontrola ryzyka

AUDYT RYZYKA CZĘŚĆ A - OBSERWACJA	AUDYT RYZYKA CZĘŚĆ B - SPRAWOZDANIE
I. Audyt ryzyka związanego z przetwarzaniem danych osobowych ma zapewnić: a. przestrzeganie wymogów prawnych i formalnych; b. zapewnić wynikającą z rozporządzenia UE 2016/679 rozliczalność przestrzegania zasad przetwarzania danych osobowych. II. Część A wypełnia wspólnie zespół merytoryczny z pracownikiem nadzorującym przy wsparciu inspektora ochrony danych. III. Audyt ryzyka należy wypełnić w Excelu i przesłać do inspektora ochrony danych. IV. Jeżeli inspektor ochrony danych uzna, że "Audyt ryzyka" wymaga uzupełnienia, to pracownik nadzorujący w ustalonym terminie uzupełnia "Audytu ryzyka" samodzielnie bądź ze wskazanymi pracownikami.	I. Część B "kontroli ryzyka" wypełnia inspektor ochrony danych bądź jego zastępca. II. Oceny i zalecenia wskazywane są na podstawie obowiązujących przepisów a w szczególności na podstawie rozporządzenia 2016/679 oraz opinii, poradników i wytycznych organu nadzorczego tj. Urząd Ochrony Danych Osobowych. III. W przypadku wprowadzenia zaleceń bądź dokonania zmian w przetwarzaniu wykonuje się kolejną kontrolę ryzyka, nie można poprawiać już wykonanej kontroli. IV. Inspektor ochrony danych po przygotowaniu sprawozdania z kontroli ryzyka udostępnia je wydrukowane i podpisane: a. administratorowi; b. pracownikowi nadzorującemu.
Numer kontroli:	Data wykonania kontroli:	Data sporządzenia sprawozdania:	
Dane członków zespołu merytorycznego		Imię i nazwisko wypełniającego:	
Imię i nazwisko	Stanowisko / Komórka organizacyjna	Imiona, nazwiska i stanowiska lub komórki organizacyjne osób, którym dostarczono sprawozdanie:	
	Pracownik nadzorujący		
	Inspektor ochrony danych		
	Archiwista		
	Administrator systemów inf.		
Nazwa czynności przetwarzania:		1. Podsumowanie przeprowadzonej kontroli ryzyka:	
1. Opis czynności przetwarzania.			
a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości.			
Wypełnia pracownik nadzorujący. Opis musi być jak najbardziej szczegółowy.		SKALA OCEN DLA ZAGADNIEŃ 2-13 ocena **"pozytywna"** - prawidłowe działanie, nie wymaga żadnych uregulowań; ocena **"mała niezgodność"** - działanie wymaga poprawy w ustalonym terminie, nie jest to duża niezgodność; ocena **"duża niezgodność"** - działanie niezgodne z wymogami prawnymi, należy niezwłocznie wprowadzić zalecenia.	

2. Cel i podstawa prawna przetwarzania danych osobowych.			2. Cel i podstawa prawna przetwarzania danych osobowych.				
a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada ograniczenia celu.			a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada ograniczenia celu.				
LP.	Cel przetwarzania danych osobowych? Każdy wpisujemy osobno.	a. z czego wynika podstawa prawna do przetwarzania danych osobowych? (należy wpisać szczegółowo) - jeżeli podstawą prawną jest zgoda to czy jest dobrowolna, jasna, świadoma, konkretna, czy jest odrębną częścią w stosunku do reszty formalności?	LP.	Obserwacja	UZASADNIENIE	Zalecenia	Termin realizacji zaleceń
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			

3. Niezbędny zakres danych osobowych.	3. Niezbędny zakres danych osobowych.

a. analiza ryzyka; b. ocena skutków; c. zasada minimalizacji danych.			a. analiza ryzyka; b. ocena skutków; c. zasada minimalizacji danych.				
LP.	Wpisujemy każdą daną osobową osobno.	a. z czego wynika niezbędność przetwarzania wskazanej danej osobowej / do czego jest potrzebna/niezbędna?	LP.	Obserwacja	UZASADNIENIE	Zalecenia	Termin realizacji zaleceń
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			

4. Czas przetwarzania i archiwizacja.			**4. Czas przetwarzania i archiwizacja.**				
a. zasada ograniczenia przechowywania; b. zasada zgodności z prawem, rzetelności i przejrzystości.			a. zasada ograniczenia przechowywania; b. zasada zgodności z prawem, rzetelności i przejrzystości.				
LP.	Wpisujemy kategorie danych z uwzględnieniem kategorii archiwizacji.	a. Jak długo dane osobowe przechowywane są w komórce merytorycznej? b. Jak długo później są archiwizowane? c. Z czego wynika wskazany czas przechowywania i archiwizacji?	LP.	Obserwacja	UZASADNIENIE	Zalecenia	Termin realizacji zaleceń
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			

5. Systemy informatyczne i nośniki elektryczne.			**5. Systemy informatyczne i nośniki elektryczne.**				
a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada ograniczenia celu; e. zasada integralności i poufności.			a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada ograniczenia celu; e. zasada integralności i poufności.				
LP.	Zakres przetwarzanych danych osobowych przez wskazany system. Wyszczególniamy wszystkie.	a. jaki system? b. w jakim celu jest wykorzystywany? c. czy jest niezbędny do przetwarzania danych osobowych i dlaczego? d. czy wszystkie wymogi prawne są uregulowane, jakie i w jakim zakresie są i nie są?	LP.	Obserwacja	UZASADNIENIE	Zalecenia	Termin realizacji zaleceń
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			

6. Wymiana danych między systemami.			**6. Wymiana danych między systemami.**				
a. analiza ryzyka; b. ocena skutków; c. zasada integralności i poufności.			a. analiza ryzyka; b. ocena skutków; c. zasada integralności i poufności.				
LP.	Zakres danych każdej pojedynczej wymiany danych osobowych między systemami.	a. z jakiego systemu do jakiego przesyłane są dane osobowe? b. w jakim celu przesyłane są dane osobowe?	LP.	Obserwacja	UZASADNIENIE	Zalecenia	Termin realizacji zaleceń
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			

7. Przetwarzanie tradycyjne (papierowe).			7. Przetwarzanie tradycyjne (papierowe).				
a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada ograniczenia celu			a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada ograniczenia celu				
LP	Zakres danych osobowych wymagany w każdym dokumencie.	a. nazwa dokumentu; b. czy jest to dokument stworzony przez administratora czy wynikający z przepisów; jakich przepisów?; c. w jakich celach stosuje się dokument?	LP.	Obserwacja	UZASADNIENIE	Zalecenia	Termin realizacji zaleceń
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			

8. Pobieranie danych osobowych.			8. Pobieranie danych osobowych.				
a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada ograniczenia celu; e. zasada prawidłowości; f. zasada minimalizacji.			a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada ograniczenia celu; e. zasada prawidłowości; f. zasada minimalizacji.				
LP.	Zakres danych osobowych pobierany z każdego pojedynczego źródła.	a. nazwa źródła danych osobowych; b. na jakiej podstawie prawnej pobierane są dane? c. czy jest inny sposób na pobranie danych? d. w jaki sposób weryfikowana jest prawidłowość pobranych danych osobowych?	LP.	Obserwacja	UZASADNIENIE	Zalecenia	Termin realizacji zaleceń
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			

9. Odbiorcy danych osobowych.			9. Odbiorcy danych osobowych.				
a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada integralności i poufności; e. zasada minimalizacji danych.			a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada integralności i poufności; e. zasada minimalizacji danych.				
LP.	Zakres danych osobowych jednorazowo możliwy do udostępnienia.	a. nazwa odbiorcy / kategoria odbiorcy; b. z czego wynika uprawnienie odbiorcy; c. jak jest weryfikowany odbiorca?	LP.	Obserwacja	UZASADNIENIE	Zalecenia	Termin realizacji zaleceń
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			

10. Organy uprawnione do dostępu do danych osobowych.			10. Organy uprawnione do dostępu do danych osobowych.				
a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada integralności i poufności; e. zasada minimalizacji danych.			a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada integralności i poufności; e. zasada minimalizacji danych.				
LP.	Zakres danych osobowych jednorazowo możliwy do udostępnienia.	a. nazwa organu; b. z czego wynika uprawnienie organu? c. w jaki sposób dostarczane są dane osobowe?	LP.	Obserwacja	UZASADNIENIE	Zalecenia	Termin realizacji zaleceń
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			

			0	WYBIERZ			

11. Powierzenie przetwarzania danych osobowych.			11. Powierzenie przetwarzania danych osobowych.				
a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada ograniczenia celu; e. zasada integralności i poufności, f. zasada minimalizacji danych.			a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada ograniczenia celu; e. zasada integralności i poufności, f. zasada minimalizacji danych.				
LP.	Zakres danych osobowych powierzany każdemu pojedynczemu podmiotowi przetwarzającemu.	a. nazwa podmiotu, a w przypadku zamiaru zatrudnienia kategoria podmiotu przetwarzającego; b. w jakim celu będą powierzone dane osobowe? c. czy zostało uregulowane prawnie powierzenie przetwarzania danych osobowych? d. czy podmiot przetwarzający zapewnił wystarczające gwarancje bezpieczeństwa przetwarzania danych osobowych, w jaki sposób? e. w jaki sposób będą/są dostarczane dane osobowe?	LP.	Obserwacja	UZASADNIENIE	Zalecenia	Termin realizacji zaleceń
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			

12. Współadministratorzy.			12. Współadministratorzy.				
a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada ograniczenia celu; e. zasada minimalizacji danych.			a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada ograniczenia celu; e. zasada minimalizacji danych.				
LP.	Zakres danych osobowych współadministrowany przez każdego pojedynczego współadministratora.	a. nazwa współadministratora; b. w jakim celu będą współadministrowane dane osobowe? c. na jakiej podstawie prawnej będą współadministrowane dane osobowe? d. czy zawarto porozumienie między współadministratorami dot. przetwarzania danych osobowych i obowiązków prawnych?	LP.	Obserwacja	UZASADNIENIE	Zalecenia	Termin realizacji zaleceń
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			
			0	WYBIERZ			

13. Prawa osób fizycznych.			13. Prawa osób fizycznych.				
a. zasada zgodności z prawem, rzetelności i przejrzystości.			a. zasada zgodności z prawem, rzetelności i przejrzystości.				
LP.	Rodzaj prawa wynikającego z rozporządzenia 2016/679.	a. w jaki sposób realizowane są prawa osób fizycznych? b. z czego wynika ustalony sposób realizacji praw?	LP.	Obserwacja	UZASADNIENIE	Zalecenia	Termin realizacji zaleceń
	Obowiązek informacyjny		0	WYBIERZ			
	Prawo dostępu		0	WYBIERZ			
	Prawo do usunięcia		0	WYBIERZ			
	Prawo do sprzeciwu		0	WYBIERZ			
	Prawo do ograniczenia		0	WYBIERZ			
	Prawo do wycofania zgody		0	WYBIERZ			
			0	WYBIERZ			

14. Środki bezpieczeństwa (analiza ryzyka + ocena skutków)	14. Środki bezpieczeństwa (analiza ryzyka + ocena skutków)

a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada integralności i poufności.

Przy wszystkich kategoriach przetwarzania wskazujemy zastosowane techniczne i organizacyjne środki bezpieczeństwa z uwzględnieniem przetwarzania na nośnikach papierowych i elektronicznych.

a. analiza ryzyka; b. ocena skutków; c. zasada zgodności z prawem, rzetelności i przejrzystości; d. zasada integralności i poufności.

"nie dotyczy" - tylko wtedy gdy dana kategoria przetwarzania nie występuje; **"małe ryzyko"** - ryzyka naruszenia ochrony danych osobowych nie ma w ogóle albo jest znikome, poprawne zabezpieczenia organizacyjne i techniczne. **"średnie ryzyko"** - ryzyko naruszenia ochrony danych osobowych może wystąpić ale prawdopodobieństwo jest niewielkie, należy poprawić zabezpieczenia organizacyjne i techniczne; **"wysokie ryzyko"** - jest duże prawdopodobieństwo wystąpienia ryzyka naruszenia ochrony danych osobowych, należy niezwłocznie wprowadzić odpowiednie organizacyjne i techniczne środki bezpieczeństwa, nie można przetwarzać danych osobowych przed obniżeniem ryzyka.

Rodzaj ryzyka		Kategoria przetwarzania							SKALA RYZYKA	OBSERWACJA I UZASADNIENIE IOD	Zalecenia	Termin realizacji zaleceń
		* zbieranie; * pobieranie	* przechowywanie; * wykorzystywanie	* przeglądanie; * wykorzystywanie	* usuwanie; * rozpowszechnianie; * udostępnianie	* ulepszanie; * modyfikowanie; * organizowanie; * przeglądanie; * dostawanie się; * łączenie	* przechowywanie; * archiwizowanie	* usuwanie; * niszczenie				
niezgodne z prawem	zniszczenie								WYBIERZ			
	utracenie								WYBIERZ			
	zmodyfikowanie								WYBIERZ			
	ujawnienie								WYBIERZ			
	dostęp								WYBIERZ			
przypadkowe	zniszczenie								WYBIERZ			
	utracenie								WYBIERZ			
	zmodyfikowanie								WYBIERZ			
	ujawnienie								WYBIERZ			
	dostęp								WYBIERZ			

miejscowość i data	*czytelny podpis IOD*

Załącznik Nr 4 do zarządzenia Nr 715/2021
Burmistrza Miasta i Gminy Kąty Wrocławskie
z dnia 08 kwietnia 2021 r.

PROCEDURA REALIZACJI OBOWIĄZKU INFORMACYJNEGO

PROCEDURA REALIZACJI OBOWIĄZKU INFORMACYJNEGO

SIPIS TREŚCI

I. WPROWADZENIE

1.Niniejsza procedura jest integralną częścią Polityki, jednakże Polityka jest nadrzędnym dokumentem w stosunku do procedury.
2.Niniejsza procedura określa zasady realizacji obowiązku informacyjnego wynikającego z art. 12, 13 i 14 rozporządzenia UE 2016/679.
3.Wprowadzenie niniejszej procedury jest niezbędne ze względu na:
a.konieczność realizacji obowiązku informacyjnego zgodnie z art. 12 ust. 1 i 5 rozporządzenia UE 2016/679;
b.dostawanie się do wymaganych terminów realizacji obowiązku informacyjnego i poprawnych zakresów informacji zgodnie z art. 13 i 14 rozporządzenia UE 2016/679;
c.obowiązek wykazania rozliczalności przestrzegania zasad przetwarzania danych osobowych, o których mowa w art. 5 rozporządzenia UE 2016/679.
4.Niniejsza procedura ma zastosowanie zawsze kiedy:
a.pozyskano dane osobowe od osoby fizycznej, której dane dotyczą;
b.pozyskano dane osobowe z innego źródła niż osoba fizyczna, której dane dotyczą.
5.Jeżeli przepisy unijne lub krajowe w inny sposób regulują postanowienia niniejszej procedury, to niniejsza procedura w zakresie w jakim regulują to przepisy nie obowiązuje.
6.Z niniejszą procedurą musi się zapoznać:
a.każdy pełnomocnik administratora;
b.każdy kierownik;
c.każdy pracownik przetwarzający dane osobowe.
7.Zmiany niniejszej procedur lub jej załączników wymagają zgody administratora oraz IOD i są wprowadzane pod ich ścisłym nadzorem.

II. ZASADY

1.Jeżeli będą pobierane dane osobowe to należy zrealizować obowiązek informacyjny w stosunku do osoby fizycznej, której dane osobowe będą przetwarzane.
2.Jeżeli pozyskujemy dane osobowe bezpośrednio od osoby fizycznej, której dane dotyczą to obowiązek informacyjny należy zrealizować najpóźniej przy pobraniu danych osobowych.
3.Jeżeli pozyskujemy dane osobowe od innej osoby niż od osoby fizycznej, której dane dotyczą to obowiązek informacyjny należy wypełnić:
a) w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych;

b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub

c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu. Jeżeli przetwarzanie danych osobowych określone jest przepisami unijnymi lub krajowymi i pozyskujemy dane osobowe

z innego źródła niż osoba fizyczna, której dane dotyczą to realizacja obowiązku informacyjnego nie jest wymagana.

4.Jeżeli dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego lub związku z ustawowym obowiązkiem zachowania tajemnicy i dane osobowe zostały pozyskane z innego źródła niż osoba fizyczna, której dane osobowe dotyczą to nie można w tym zakresie realizować obowiązku informacyjnego.
5.Szykując klauzule informacyjną dla osoby fizycznej należy posługiwać się wzorem „04. wzór - obowiązek informacyjny" i przy wprowadzaniu informacji postępować zgodnie z jego instrukcją.
6.Jeżeli inspektor ochrony danych wyrazi zgodę na odstępstwo od korzystania ze wzoru „04. wzór - obowiązek informacyjny" to klauzula informacyjna ma być przygotowana w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, i musi być napisana jasnym i prostym językiem.
7.Jeżeli dane osobowe będą przetwarzanie w innym celu niż zostały zebrane, to należy ponownie spełnić obowiązek informacyjny, uzupełniając go o aktualne cele i pozostałe niezbędne informacje a przede wszystkim o te, które uległy zmianie.

III. ZAKRES

1.Pozyskując dane osobowe bezpośrednio od osoby fizycznej, której dane dotyczą należy przekazać następujące informacje:
a.tożsamość i dane kontaktowe administratora;
b.dane kontaktowe inspektora ochrony danych jeżeli został powołany;
c.cele przetwarzania danych osobowych;
d.podstawę prawną przetwarzania, a w przypadku prawnie uzasadnionego interesu należy wskazać ten interes;
e.dane odbiorców danych osobowych lub ich kategorie jeżeli nie są znani;
f.gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi rozporządzenia UE 2016/679, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
g.okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
h.o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, prawie do wycofania zgody (jeżeli jest podstawą przetwarzania), prawnie wniesienia skargi do organu nadzorczego;
i.czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
j.jeżeli występuje to o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2.Pozyskując dane osobowe z innego źródła niż osoba fizyczna, której dane dotyczą należy przekazać następujące informacje:
a.tożsamość i dane kontaktowe administratora;
b.dane kontaktowe inspektora ochrony danych jeżeli został powołany;
c.cele przetwarzania danych osobowych;
d.podstawę prawną przetwarzania, a w przypadku prawnie uzasadnionego interesu należy wskazać ten interes;
e.kategorie przetwarzanych danych osobowych;
f.źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
g.dane odbiorców danych osobowych lub ich kategorie jeżeli nie są znani;
h.gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi rozporządzenia UE 2016/679, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
i.okres przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
j.o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich

sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, prawie do wycofania zgody (jeżeli jest podstawą przetwarzania), prawnie wniesienia skargi do organu nadzorczego;
k.jeżeli występuje to o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

IV. WZORY DOKUMENTÓW

1.Zastosowanie mają następujące wzory dokumentów będące załącznikami do niniejszej procedury:
a.„04. wzór – obowiązek informacyjny:
2.W wyniku stosowania niniejszej procedury powstanie dokumentacja zawierająca dane osobowe lub/oraz informacje poufne o jednostce przetwarzającej dlatego administrator wyznacza osoby odpowiedzialne za przechowywanie w następujących zakresach:
a.za każdy wypełniony
3.Przechowywanie, archiwizowanie, modyfikowanie, ujawnianie, udostępnianie, niszczenie lub usuwanie i innego rodzaju przetwarzanie załączników lub treści w nich zawartych odbywa się zgodnie ze stosowną procedurą, chyba, że nie zawierają danych osobowych to zgodnie z przepisami unijnymi lub krajowymi lub uregulowaniami wewnętrznymi.

V. POSTANOWIENIA KOŃCOWE

1.Nadzór nad niniejszą procedurą sprawuję:
a.IOD w pełnym zakresie;
b.każdy kierownik w obrębie własnej komórki organizacyjnej;
c.każdy pełnomocnik administratora w zakresie udzielonego pełnomocnictwa:
d.każdy upoważniony w zakresie nadanego upoważnienia.
2.Każdy kto nie przestrzega niniejszej procedury a jest do tego zobowiązany, na mocy przepisów unijnych lub krajowych lub na mocy wyrażonego oświadczenia woli, ponosi odpowiedzialność za wszelkie szkody powstałe z powodu tego zaniechania zgodnie z Kodeksem Cywilnym, Kodeksem Pracy, Rozporządzeniem UE 2016/679 bądź innymi przepisami adekwatnymi do zaistniałej sytuacji.
3.Niniejsza procedura obowiązuję z dniem jej wprowadzenia zarządzeniem.

VI. METRYKA

aktualna wersja:		numer zarządzenia:	

Zakres aktualizacji	Data aktualizacji	Wprowadził aktualizacje	Zatwierdził aktualizacje

Załącznik Nr 1 do Załącznika Nr 4

wzór – obowiązek informacyjny

INFORMACJE DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

INSTRUKCJA DLA WYPEŁNIAJĄCEGO

1. W przypadku pozyskiwania informacji bezpośrednio od osoby fizycznej, poniższe informacje musimy przekazać **najpóźniej przy pobieraniu** danych osobowych.
2. W przypadku pozyskiwania informacji z innych źródeł niż osoba fizyczna, której dane dotyczą to poniższe informacje musimy przekazać w ciągu 30 dni od pozyskania danych osobowych.
3. Każdy opracowujący informacje dotyczące przetwarzania musi podjąć odpowiednie środki aby poniższe informacje przekazywane były w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
4. Cały szablon można edytować do własnych potrzeb, jednak treść musi zostać ta sama, chyba że inspektor ochrony danych wyrazi zgodę na wskazaną zmianę.
5. Po zakończeniu edycji treści należy zmodyfikować szablon i usunąć wszystkie zbędne komórki, także tą.
6. W przypadku realizacji obowiązku informacyjnego trzeba pamiętać, że należy być w stanie wykazać, że został on zrealizowany.
7. W przypadku 6 ust. 1 lit. e) lub f) rozporządzenia UE 2016/679 prawo do sprzeciwu należy wytłuścić i powiększyć czcionkę.

TOŻSAMOŚĆ I DANE KONTAKTOWE ADMINISTRATORA

Administratorem przetwarzającym dane osobowe jest _____. Z administratorem można skontaktować się:

·telefonicznie - _____; (telefon stacjonarny bądź komórka)

·pisemnie - _____; (adres e-mail)

·osobiście lub pisemnie - _____. (adres siedziby, korespondencyjny).

1. Dotyczy przypadków kiedy zbieramy dane bezpośrednio od osoby fizycznej, której dane dotyczą oraz kiedy zbieramy dane z innego źródła (art. **13 i 14** rozporządzenia (UE) 2016/679).
2. Puste miejsca uzupełniamy, a podpowiedzi w nawiasach usuwamy.
3. Poniższe pole „NOTATKI" służy do wprowadzania przydatnych informacji ale po zakończeniu edycji pola usuwamy wszystkie notatki, łącznie z komórką.
4. Po zakończeniu edycji pola usuwamy tą komórkę.

NOTATKA

DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH

Z inspektorem ochrony danych można skontaktować się:

·telefonicznie - _____; (telefon stacjonarny bądź komórka)

·pisemnie - _____; (adres e-mail)

·osobiście lub pisemnie - _____; (adres siedziby, korespondencyjny).

1. Dotyczy przypadków kiedy zbieramy dane bezpośrednio od osoby fizycznej, której dane dotyczą oraz kiedy zbieramy dane z innego źródła (art. **13 i 14** rozporządzenia (UE) 2016/679).
2. Puste miejsca uzupełniamy, a podpowiedzi w nawiasach usuwamy.
3. Poniższe pole „NOTATKI" służy do wprowadzania przydatnych informacji ale po zakończeniu edycji pola usuwamy wszystkie notatki, łącznie z komórką.
4. Po zakończeniu edycji pola usuwamy tą komórkę.

NOTATKA

CEL I PODSTAWA PRAWNA PRZETWARZANIA ORAZ KATEGORIE DANYCH OSOBOWYCH

Dane osobowe przetwarzane są lub będą:

·w celu _____ na podstawie _____, w zakresie _____;

·w celu _____ na podstawie _____,w zakresie _____.

1. Dotyczy przypadków kiedy zbieramy dane bezpośrednio od osoby fizycznej, której dane dotyczą oraz kiedy zbieramy dane z innego źródła (art. **13 i 14** rozporządzenia (UE) 2016/679).
2. Puste miejsca uzupełniamy, a podpowiedzi w nawiasach usuwamy.
3. Poniższe pole „NOTATKI" służy do wprowadzania przydatnych informacji ale po zakończeniu edycji pola usuwamy wszystkie notatki, łącznie z komórką.
4. Po zakończeniu edycji pola usuwamy tą komórkę.

NOTATKA

WYMOGI I KONSEKWENCJE

1.Podanie/udostępnienie danych osobowych w zakresie _____ jest wymagane na podstawie _____.
Osoba fizyczna, której dane dotyczą nie jest/jest zobowiązana do ich podania.
W przypadku odmowy podania/udostępnienia danych osobowych _____.
2.Podanie/udostępnienie danych osobowych w zakresie_____ jest warunkiem _____, (warunek podania danych osobowych).
Osoba fizyczna, której dane dotyczą nie jest/jest zobowiązana do ich podania (obowiązek podania/udostępnienia danych osobowych).
W przypadku odmowy podania/udostępnienia danych osobowych _____ (konsekwencje nie podania/udostępnienia danych osobowych).
3.Podanie/udostępnienie danych osobowych nie jest wymagane i osoba fizyczna, której dane dotyczą nie jest zobowiązana do ich podania.
W przypadku odmowy podania/udostępnienia danych osobowych _____ (konsekwencje nie podania/udostępnienia danych osobowych).

1.Dotyczy tylko przypadków kiedy pobieramy dane osobowe bezpośrednio od osoby fizycznej, którą dane dotyczą. (art. **13** rozporządzenia (UE) 2016/679
2.Puste miejsca uzupełniamy, a podpowiedzi w nawiasach usuwamy.
3.Jeżeli dana pozycja nie dotyczy danego przetwarzania to ją usuwamy.
4.Poniższe pole „NOTATKI" służy do wprowadzania przydatnych informacji ale po zakończeniu edycji pola usuwamy wszystkie notatki, łącznie z komórką.
5.Po zakończeniu edycji pola usuwamy tą komórkę.

NOTATKA

ŹRÓDŁO POCHODZENIA DANYCH OSOBOWYCH

1.Dane osobowe w zakresie _____, zostały pobrane _____.
2.Dane osobowe w zakresie _____, zostały pobrane _____.
3.Dane osobowe w zakresie _____, zostały pobrane _____.
4.Dane osobowe w zakresie _____, zostały pobrane _____.

1.Dotyczy tylko przypadków kiedy pobieramy dane osobowe z innego źródła niż osoba fizyczna, którą dane dotyczą (art. **14** rozporządzenia (UE) 2016/679).
2.Jeżeli dane pochodzą ze źródła publicznie dostępnego, to należy to wskazać.
3.Puste miejsca uzupełniamy, a podpowiedzi w nawiasach usuwamy.
4.Jeżeli dana pozycja nie dotyczy danego przetwarzania to ją usuwamy.
5.Poniższe pole „NOTATKI" służy do wprowadzania przydatnych informacji ale po zakończeniu edycji pola usuwamy wszystkie notatki, łącznie z komórką.
6.Po zakończeniu edycji pola usuwamy tą komórkę.

NOTATKA

INFORMACJE O ODBIORCACH DANYCH OSOBOWYCH

Następujące podmioty będą miały dostęp do danych osobowych we wskazanych zakresach:
a._____, z siedzibą _____ - zakres danych osobowych _____;
b._____, z siedzibą _____ - zakres danych osobowych _____;
c._____, z siedzibą _____ - zakres danych osobowych _____;
d._____, z siedzibą _____ - zakres danych osobowych _____.

1.Dotyczy przypadków kiedy zbieramy dane bezpośrednio od osoby fizycznej, której dane dotyczą oraz kiedy zbieramy dane z innego źródła (art. **13 i 14** rozporządzenia (UE) 2016/679).
2.Puste miejsca uzupełniamy, a podpowiedzi w nawiasach usuwamy.
3.Poniższe pole „NOTATKI" służy do wprowadzania przydatnych informacji ale po zakończeniu edycji pola usuwamy wszystkie notatki, łącznie z komórką.
4.Po zakończeniu edycji pola usuwamy tą komórkę.

NOTATKA

CZAS PRZETWARZANIA DANYCH OSOBOWYCH

Następujące dane osobowe będą przetwarzane we wskazanym czasie:
a._____ będą przetwarzane _____, a później będą archiwizowane przez _____ zgodnie z

instrukcją archiwalną;

b._____ będą przetwarzane _____, a później będą archiwizowane przez _____ zgodnie z instrukcją archiwalną;

c._____ będą przetwarzane _____, a później będą archiwizowane przez _____ zgodnie z instrukcją archiwalną.

1.Dotyczy przypadków kiedy zbieramy dane bezpośrednio od osoby fizycznej, której dane dotyczą oraz kiedy zbieramy dane z innego źródła (art. **13 i 14** rozporządzenia (UE) 2016/679).

2.Puste miejsca uzupełniamy, a podpowiedzi w nawiasach usuwamy.

3.Poniższe pole „NOTATKI" służy do wprowadzania przydatnych informacji ale po zakończeniu edycji pola usuwamy wszystkie notatki, łącznie z komórką.

4.Po zakończeniu edycji pola usuwamy tą komórkę.

NOTATKA

PRAWA OSÓB FIZYCZNYCH

1.Każda osoba fizyczna, której administrator przetwarza dane osobowe ma prawo:

a.jeżeli przetwarzanie danych osobowych odbywa się na podstawie zgody, to wycofać tę zgodę w dowolnym momencie;

b.otrzymać od administratora kopię swoich danych osobowych oraz szczegółowe informacje dotyczące przetwarzania tych danych osobowych;

c.zażądać zmiany lub uzupełnienia swoich danych osobowych, które są niepoprawne, niekompletne lub nieaktualne;

d.zażądać usunięcia swoich danych osobowych, jeżeli zachodzą uzasadnione prawnie okoliczności;

e.zażądać we wskazanym zakresie ograniczenia przetwarzania swoich danych osobowych, jeżeli zachodzą uzasadnione prawnie okoliczności;

f.zażądać przesłania swoich danych osobowych przez administratora do innego wskazanego administratora, jeżeli jest to technicznie możliwe i jeżeli zachodzą uzasadnione prawnie okoliczności;

g.wnieść sprzeciw w stosunku do przetwarzania jej danych, jeżeli zachodzą uzasadnione prawnie okoliczności; **(W przypadku 6 ust. 1 lit. e) lub f) rozporządzenia UE 2016/679 prawo do sprzeciwu należy wytłuścić i powiększyć czcionkę.)**

h.nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu i wywołuje wobec niej skutki prawne lub w inny sposób na nią wpływa;

i.wnieść skargę do Urzędu Ochrony Danych Osobowych jeżeli uważa, że realizacja prawa lub procesy przetwarzania nie są zgodne z obowiązującymi przepisami.

2.Realizacja każdego żądania wymaga wcześniejszej weryfikacji tożsamości, zbadania zasadności i możliwości prawnych realizacji żądanego prawa.

3.W ciągu 30 dni od złożenia żądania administrator zobowiązany jest zrealizować żądanie lub odmówić realizacji żądania.

4.Odmowa realizacji żądania zawsze musi zawierać uzasadnienie.

1.Dotyczy przypadków kiedy zbieramy dane bezpośrednio od osoby fizycznej, której dane dotyczą oraz kiedy zbieramy dane z innego źródła (art. **13 i 14** rozporządzenia (UE) 2016/679).

2.Puste miejsca uzupełniamy, a podpowiedzi w nawiasach usuwamy.

3.Poniższe pole „NOTATKI" służy do wprowadzania przydatnych informacji ale po zakończeniu edycji pola usuwamy wszystkie notatki, łącznie z komórką.

4.Po zakończeniu edycji pola usuwamy tą komórkę.

NOTATKA

ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI

1.W stosunku do danych osobowych _____ podejmowana jest decyzja polegająca na zautomatyzowanym przetwarzaniu. W tym przypadku zautomatyzowane przetwarzanie polega na _____. Zautomatyzowane przetwarzanie ma znaczenia dla _____ i może powodować następujące konsekwencje _____.

2.W stosunku do danych osobowych _____ podejmowana jest decyzja polegająca na zautomatyzowanym przetwarzaniu. W tym przypadku zautomatyzowane przetwarzanie polega na _____. Zautomatyzowane przetwarzanie ma znaczenia dla _____ i może powodować następujące konsekwencje _____.

1.Dotyczy przypadków kiedy zbieramy dane bezpośrednio od osoby fizycznej, której dane dotyczą oraz kiedy zbieramy dane z innego źródła (art. **13 i 14** rozporządzenia (UE) 2016/679).

2.Dotyczy tylko przypadków kiedy faktycznie występuję podejmowanie decyzji w sposób całkowicie zautomatyzowany.

3.Puste miejsca uzupełniamy, a podpowiedzi w nawiasach usuwamy.

4.Poniższe pole „NOTATKI" służy do wprowadzania przydatnych informacji ale po zakończeniu edycji pola usuwamy wszystkie notatki, łącznie z komórką.

5.Po zakończeniu edycji pola usuwamy tą komórkę.

NOTATKA

PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH / ORGANIZACJI MIĘDZYNARODOWYCH

Następujące dane osobowe _____, będą przekazywane do _____ (nazwa państwa trzeciego lub organizacji międzynarodowej). Związku z przekazywaniem wskazanych danych zostały wprowadzone następujące środki bezpieczeństwa: _____. Kopie przekazywanych danych wraz z dodatkowymi informacjami dotyczącymi przetwarzania można uzyskać _____.

1. Dotyczy przypadków kiedy zbieramy dane bezpośrednio od osoby fizycznej, której dane dotyczą oraz kiedy zbieramy dane z innego źródła (art. **13 i 14** rozporządzenia (UE) 2016/679).
2. Dotyczy tylko przypadków kiedy faktycznie występuje przekazywanie danych do państw trzecich lub organizacji międzynarodowych.
3. Puste miejsca uzupełniamy, a podpowiedzi w nawiasach usuwamy.
4. Poniższe pole „NOTATKI" służy do wprowadzania przydatnych informacji ale po zakończeniu edycji pola usuwamy wszystkie notatki, łącznie z komórką.
5. Po zakończeniu edycji pola usuwamy tą komórkę.

NOTATKA

miejscowość, data	*podpis osoby fizycznej, której dane dotyczą*

miejscowość, data	*podpis opiekuna prawnego osoby fizycznej, której dane dotyczą*

Załącznik Nr 5 do zarządzenia Nr 715/2021
Burmistrza Miasta i Gminy Kąty Wrocławskie
z dnia 08 kwietnia 2021 r.

PROCEDURA REALIZACJI PRAW OSÓB FIZYCZNYCH

SIPIS TREŚCI

I. WPROWADZENIE

1.Niniejsza procedura jest integralną częścią Polityki, jednakże Polityka jest nadrzędnym dokumentem w stosunku do procedury.
2.Niniejsza procedura określa sposoby realizacji praw osób fizycznych, których dane są lub będą przetwarzane, o których mowa w rozdziale III rozporządzenia UE 2016/679.
3.Wprowadzenie niniejszej procedury jest niezbędne ze względu na zapewnienie:
a.poprawnej realizacji praw osób fizycznych wynikających z rozdziałem III rozporządzenia UE 2016/679;
b.zgodności z prawem, rzetelności i przejrzystości, o której mowa w art. 5 rozporządzenia UE 2016/679;
c.integralności i poufności, o której mowa w art. 5 rozporządzenia UE 2016/679;
d.rozliczalności przestrzegania zasad przetwarzania danych osobowych, o których mowa w art. 5 rozporządzenia UE 2016/679.
4.Niniejsza procedura ma zastosowanie do wszystkich przypadków związanych z prawami osób fizycznych, wnikających z przetwarzania danych osobowych.
5.Jeżeli przepisy unijne lub krajowe w inny sposób regulują postanowienia niniejszej procedury, to niniejsza procedura w zakresie w jakim regulują to przepisy, nie obowiązuje.
6.Z niniejszą procedurą musi zapoznać się:
a.każdy pełnomocnik administratora;
b.każdy kierownik;
c.każdy pracownik.
7.Zmiany niniejszej procedury lub jej załączników wymagają zgody administratora oraz inspektora ochrony danych i są wprowadzane pod ich ścisłym nadzorem.

II. PODSTAWOWE ZASADY REALIZACJI PRAW OSÓB FIZYCZNYCH

1.Jeżeli osoba fizyczna żąda realizacji jej praw przysługujących jej na podstawie rozporządzenia UE 2016/679 to w pierwszej kolejności należy jednoznacznie zweryfikować jej tożsamość.
2.Weryfikowanie tożsamości odbywa się na podstawie posiadanych danych osobowych, chyba że nie pozwala to zweryfikować tej osoby, to należy zażądać dodatkowych takich danych, które to umożliwią.
3.Osoba fizyczna, której dane osobowe przetwarza administrator, może złożyć żądanie dotyczące jej praw wynikających z rozdziału III rozporządzenia UE 2016/679 za pomocą wzoru załączonego do procedury lub w inny sposób.
4.W przypadku jakichkolwiek braków formalnych, należy wezwać osobę fizyczną do ich uzupełnienia.

5.Wszelka komunikacja, dotycząca realizacji praw wynikających z rozdziału III rozporządzenia UE 2016/679, jest prowadzona:
a.przez adres e-mail (jeżeli wcześniej został zweryfikowany);
b.przez skrytkę ePUAP;
c.przez adres do korespondencji tradycyjnej;
d.osobiście lub przez pełnomocnika.
6.Odpowiedzi dotyczące złożonego żądania udziela się sposobem wskazanym we wniosku.
7.Jeżeli nie został wskazany sposób odpowiedzi, to udziela się jej w takiej formie w jakiej zostało złożone żądnie.
8.Odpowiedzi udziela pracownik do tego upoważniony po wcześniejszym zaopiniowaniu przez IOD.
9.Rozpatrywanie żądań odbywa się niezwłocznie.
10.Udzielanie odpowiedzi musi nastąpić w ciągu 30 dni od złożenia żądania.
11.Jeżeli żądanie nie będzie realizowane, to należy w ciągu 30 dni od złożenia żądania poinformować osobę składającą żądanie o:
a.powodach odmowy;
b.możliwości złożenia skargi do Urzędu Ochrony Danych Osobowych;
c.możliwości obrony swoich praw przed Sądem.
12.Wszystkie sprawy związane z realizacją praw osób fizycznych są wolne od opłat.

III. PRAWO DO WYCOFANIA ZGODY

1.Każda osoba, której dane osobowe są przetwarzane przez administratora na podstawie wyrażonej zgody, w dowolnym momencie ma prawo wycofać tę zgodę.
2.Jeżeli osoba fizyczna wycofa swoją zgodę na przetwarzanie danych osobowych to należy usunąć wszystkie dane osobowe dotyczące tej zgody, także te, które zostały przekazane odbiorcom.
3.Zgodę można wycofać co najmniej tak łatwo jak ją wyrażono.

IV. PRAWO DOSTĘPU DO INFORMACJI I KOPII DANYCH

1.Każda osoba fizyczna, której dane osobowe są przetwarzane, ma prawo uzyskać informację czy przetwarzane są jego dane osobowe a jeżeli tak, to ma prawo:
a.otrzymać kopię tych danych;
b.otrzymać pełne informacje dotyczące przetwarzania jego danych.
2.Informacje dotyczące przetwarzania zawierają:
a.cele przetwarzania;
b.kategorie przetwarzanych danych osobowych;
c.nazwy i siedziby odbiorców;
d.czas przechowywania danych osobowych;
e.informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
f.informacje o prawie wniesienia skargi do organu nadzorczego;
g.jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
h.informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą oraz o odpowiednich zabezpieczeniach, związanych z przekazaniem.
3.Kopia danych osobowych nie może zawierać danych osobowych innych osób fizycznych, chyba, że wynika to z przepisów unijnych lub krajowych.
4.Za pierwszą kopię danych nie pobiera się opłat, za kolejne opłata wynosi _____.
5.Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 rozporządzenia UE 2016/679.
6.Prawo do uzyskania kopii nie może niekorzystnie wpływać na prawa i wolności innych.

V. PRAWO DO SPROSTOWANIA

1.Każda osoba fizyczna, której dane osobowe są przetwarzane, ma prawo żądać:
a.sprostowania niepoprawnych danych osobowych;
b.uzupełnienia niekompletnych danych.

2.O sprostowaniu danych należy poinformować każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
3.Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli ta osoba tego zażąda.

VI. PRAWO DO USUNIĘCIA

1.Każda osoba fizyczna, której dane osobowe są przetwarzane, ma prawo żądać niezwłocznego usunięcia dotyczących jej danych osobowych. Należy je bez zbędnej zwłoki usunąć, jeżeli zachodzi jedna z następujących okoliczności:
a.dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b.osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej do dalszego przetwarzania;
c.osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 rozporządzenia UE 2016/679 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 rozporządzenia UE 2016/679 wobec przetwarzania;
d.dane osobowe były przetwarzane niezgodnie z prawem;
e.dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
f.dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 rozporządzenia UE 2016/679.
2.Ust. 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:
a.do korzystania z prawa do wolności wypowiedzi i informacji;
b.do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator;
c.do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
d.z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 rozporządzenia UE 2016/679;
e.do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 rozporządzenia UE 2016/679, o ile prawdopodobne jest, że realizacja prawa do usunięcia uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
f.do ustalenia, dochodzenia lub obrony roszczeń.
3.Jeżeli dane osobowe zostaną lub zostały usunięte w związku z realizacją prawa do usunięcia danych osobowych to należy poinformować każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
4.Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

VII. PRAWO DO OGRANICZENIA PRZETWARZANIA

1.Każda osoba fizyczna, której dane osobowe są przetwarzane, ma prawo żądać ograniczenia przetwarzania w następujących przypadkach:
a.osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
b.przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
c.administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
d.osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 rozporządzenia UE 2016/679 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
2. Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać – także usuwać - z wyjątkiem przechowywania, wyłącznie:
a.za zgodą osoby, której dane dotyczą, lub
b.w celu ustalenia, dochodzenia lub obrony roszczeń, lub
c.w celu ochrony praw innej osoby fizycznej lub prawnej, lub
d.z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.
3. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która

żądała ograniczenia na mocy ust. 1.
4. Jeżeli przetwarzanie będzie ograniczone na mocy ust. 1 to należy poinformować każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
4.Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą tego zażąda.

IIX. PRAWO DO PRZENOSZENIA DANYCH

1.Każda osoba, której dane osobowe są przetwarzane, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie, nadającym się do odczytu maszynowego, dane osobowe jej dotyczące, które dostarczyła administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi. Może też zażądać by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.
2.Ust. 1 ma zastosowanie tylko w przypadku kiedy dane osobowe są przetwarzane w sposób zautomatyzowany i na podstawie umowy lub zgody.
3.Realizacja prawa, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.

IX. PRAWO DO SPRZECIWU

1.Każda osoba fizyczna, której dane osobowe są przetwarzane, ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania dotyczących jej danych osobowych:
a.opartego na art. 6 ust. 1 lit. e) lub f) rozporządzenia UE 2016/679;
b.jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego.
2.Jeżeli wniesiono sprzeciw na mocy ust. 1 nie wolno już przetwarzać tych danych osobowych, chyba że:
a.istnieje ważna prawnie uzasadniona podstawa do przetwarzania, nadrzędna wobec interesów, praw i wolności osoby, której dane dotyczą;
b.są podstawą do ustalenia, dochodzenia i obrony roszczeń.
3.Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 rozporządzenia UE 2016/679, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym

X. PRAWO DO NIEPODLEGANIA ZAUTOMATYZOWANEMU PODEJMOWANIU DECYZJI

1.Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.
2.Ust. 1 nie ma zastosowania, jeżeli ta decyzja:
a.jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą a administratorem;
b.jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
c.opiera się na wyraźnej zgodzie osoby, której dane dotyczą.
3.W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.
4.Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia UE 2016/679, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) rozporządzenia UE 2016/679 i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

XI. WZORY I DOKUMENTY

1.Zastosowanie mają następujące wzory dokumentów będące załącznikami do niniejszej procedury:
a.„05. WNIOSEK - żądania RODO".
2.W wyniku stosowania niniejszej procedury powstanie dokumentacja zawierająca dane osobowe lub/oraz informacje poufne o jednostce przetwarzającej dlatego administrator wyznacza osoby odpowiedzialne za przechowywanie w następujących zakresach:

a.osoby merytorycznie odpowiedzialne za sprawę przechowują do zakończenia sprawy oryginały złożonych wniosków dotyczących żądań.
3.Przechowywanie, archiwizowanie, modyfikowanie, ujawnianie, udostępnianie, niszczenie lub usuwanie i innego rodzaju przetwarzanie załączników lub treści w nich zawartych odbywa się zgodnie ze stosowną procedurą, chyba, że nie zawierają danych osobowych to zgodnie z przepisami unijnymi lub krajowymi lub uregulowaniami wewnętrznymi.

XII. POSTANOWIENIA KOŃCOWE

1.Nadzór nad niniejszą procedurą sprawuję:
a.IOD w pełnym zakresie;
b.każdy kierownik w obrębie własnej komórki organizacyjnej;
c.każdy pełnomocnik administratora w zakresie udzielonego pełnomocnictwa:
d.każdy upoważniony w zakresie nadanego upoważnienia;
2.Każdy kto nie przestrzega niniejszej procedury a jest do tego zobowiązany, na mocy przepisów unijnych lub krajowych lub na mocy wyrażonego oświadczenia woli, ponosi odpowiedzialność za wszelkie szkody powstałe z powodu tego zaniechania zgodnie z Kodeksem Cywilnym, Kodeksem Pracy, Rozporządzeniem UE 2016/679 bądź innymi przepisami adekwatnymi do zaistniałej sytuacji.
3.Niniejsza procedura obowiązuję z dniem _____.

XIII. METRYKA

aktualna wersja:		numer zarządzenia:	

Zakres aktualizacji	Data aktualizacji	Wprowadził aktualizacje	Zatwierdził aktualizacje

Załącznik Nr 1 do Załącznika Nr 5

WNIOSEK - żądania RODO

WNIOSEK

1. Z wniosku może korzystać osoba fizyczna, chce skorzystać z prawa przysługującego jej związku z przetwarzaniem jej danych osobowych.
2. Wniosek wypełnia osoba, która go składa.
3. Wniosek należy wypełnić drukowanymi literami.
4. Wniosek należy wypełnić zgodnie z wytycznymi, pod rygorem nierozpatrzenia wniosku zgodnie z art. 64 § 2 Kodeksu postępowania administracyjnego.
5. Jeżeli wniosek nie jest składany w imieniu własnym należy dołączyć do wniosku dokument potwierdzający umocowanie prawne do reprezentowania zgodnie z Kodeksem postępowania administracyjnego.
6. Do wniosku należy dołączyć wszystkie niezbędne dokumenty potwierdzające uprawnienie do żądania.

1. **DANE ADMINISTRATORA**	
Nazwa administratora:	
Adres administratora:	

2. **DANE SKŁADAJĄCEGO WNIOSEK**	
Imię i nazwisko:	
Adres zamieszkania:	
Numer PESEL:	
Wniosek składany jest w imieniu:	
☐	własnym;
☐	innej osoby fizycznej.
Moje uprawnienie do reprezentowania wnioskującego wynika z załączonego do wniosku:	
☐	upoważnienia[1];
☐	pełnomocnictwa[2];
☐	orzeczenia sądu [3];
☐	

[1] – upoważnienie musi być dostarczone bezpośrednio przez osobę, której dane dotyczą;
[2] – pełnomocnictwo musi być dostarczone przez osobę, której dane dotyczą lub przez inną osobę jeżeli będzie to pełnomocnictwo notarialne lub osoba dostarczająca ma prawo zgodnie z przepisami Unijnymi lub krajowymi poświadczyć autentyczność pełnomocnictwa;
[3] – orzeczenie sądu musi być dołączone do wniosku.

3. **DANE WNIOSKUJĄCEGO[4]**	
Imię i nazwisko:	
Adres zamieszkania:	
Numer PESEL :	

[4] – uzupełniamy tylko jeżeli wniosek składany jest w imieniu innej osoby

4. **TREŚĆ ŻĄDANIA**	
Proszę o realizację mojego żądania w następującym zakresie:	
zakres żądania:	
podstawa prawna żądania:	

5. **LISTA ZAŁĄCZNIKÓW DO WNIOSKU**	
NAZWA ZAŁĄCZNIKA	CZEGO DOTYCZY

6. **FORMA UDZIELENIA ODPOWIEDZI**	
Proszę o kontakt ze mną poprzez udzielenie mi odpowiedzi:	
☐	adres e-mail;
Proszę wpisać adres skrzynki e-mail. Wpisujemy drukowanymi literami.	
☐	adres korespondencyjny;
Proszę wpisać adres korespondencyjny.	

Wpisujemy drukowanymi literami.	
☐ odbiór osobisty;	
Proszę napisać w jaki sposób poinformować o przygotowaniu odpowiedzi.	
☐ profil zaufany;	
Proszę podać nazwę użytkownika.	
☐ w inny sposób;	
Proszę napisać jakim sposobem dostarczyć odpowiedź.	

miejscowość, data	*podpis osoby fizycznej, której dane dotyczą*

INFORMACJE DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH ZAMIESZCZONYCH WE WNIOSKU

TOŻSAMOŚĆ I DANE KONTAKTOWE ADMINISTRATORA

Administratorem przetwarzającym dane osobowe jest _____.
Z administratorem można skontaktować się:
·telefonicznie - _____; (telefon stacjonarny bądź komórka)
·pisemnie - _____; (adres e-mail)
·osobiście lub pisemnie - _____. (adres siedziby, korespondencyjny)

DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH

Z inspektorem ochrony danych można skontaktować się:
·telefonicznie - _____; (telefon stacjonarny bądź komórka)
·pisemnie - _____; (adres e-mail)
·osobiście lub pisemnie - _____; (adres siedziby, korespondencyjny)

CEL I PODSTAWA PRAWNA PRZETWARZANIA ORAZ KATEGORIE DANYCH OSOBOWYCH

Dane osobowe przetwarzane są lub będą:
·w celu weryfikacji tożsamości i umocowań prawnych do reprezentowania na podstawie kodeksu postępowania administracyjnego w zakresie imienia, nazwiska, adresu zamieszkania, numeru PESEL składającego wniosek i osoby w imieniu, której składamy wniosek.
·w celu udzielenia odpowiedzi na wniosek na podstawie udzielonej zgody w zakresie adres email, korespondencyjny, telefon kontaktowy.

WYMOGI I KONSEKWENCJE

1. Podanie/udostępnienie danych osobowych w zakresie imienia, nazwiska i adresu zamieszkania jest wymagane na podstawie Kodeksu postępowania administracyjnego.
Osoba fizyczna, której dane dotyczą jest zobowiązana do ich podania.
W przypadku odmowy podania/udostępnienia danych osobowych wniosek zostanie nierozpatrzony.
2. Podanie/udostępnienie danych osobowych w zakresie numeru PESEL jest wymagane na podstawie prawnie uzasadnionego interesu realizowanego przez administratora.
Osoba fizyczna, której dane dotyczą nie jest zobowiązana do ich podania.
W przypadku odmowy podania/udostępnienia danych osobowych wniosek zostanie nierozpatrzony.
3. Podanie/udostępnienie danych osobowych w zakresie adresu e-mail lub korespondencyjnego lub telefonu kontaktowego nie jest wymagane ale konieczne do udzielenia odpowiedzi na wniosek.
W przypadku odmowy podania/udostępnienia danych osobowych odpowiedź na wniosek zostanie wysłana na adres zamieszkania.

ŹRÓDŁO POCHODZENIA DANYCH OSOBOWYCH

Wszystkie dane osobowe zostały pobrane od osoby składającej wniosek.

INFORMACJE O ODBIORCACH DANYCH OSOBOWYCH

Następujące podmioty będą miały dostęp do danych osobowych we wskazanych zakresach:
a. _____, z siedzibą _____ - zakres danych osobowych _____;
b. _____, z siedzibą _____ - zakres danych osobowych _____;
c. _____, z siedzibą _____ - zakres danych osobowych _____;
d. _____, z siedzibą _____ - zakres danych osobowych _____.

CZAS PRZETWARZANIA DANYCH OSOBOWYCH

Następujące dane osobowe będą przetwarzane we wskazanym czasie:

a._____ będą przetwarzane _____, a później będą archiwizowane przez _____ zgodnie z instrukcją archiwalną;

b._____ będą przetwarzane _____, a później będą archiwizowane przez _____ zgodnie z instrukcją archiwalną;

c._____ będą przetwarzane _____, a później będą archiwizowane przez _____ zgodnie z instrukcją archiwalną;

PRAWA OSÓB FIZYCZNYCH

1. Każda osoba fizyczna, której administrator przetwarza dane osobowe ma prawo:

a. jeżeli przetwarzanie danych osobowych odbywa się na podstawie zgody, to wycofać tę zgodę w dowolnym momencie;

b. otrzymać od administratora kopię swoich danych osobowych oraz szczegółowe informacje dotyczące przetwarzania tych danych osobowych;

c. zażądać zmiany lub uzupełnienia swoich danych osobowych, które są niepoprawne, niekompletne lub nieaktualne;

d. zażądać usunięcia swoich danych osobowych, jeżeli zachodzą uzasadnione prawnie okoliczności;

e. zażądać we wskazanym zakresie ograniczenia przetwarzania swoich danych osobowych, jeżeli zachodzą uzasadnione prawnie okoliczności;

f. zażądać przesłania swoich danych osobowych przez administratora do innego wskazanego administratora, jeżeli jest to technicznie możliwe i jeżeli zachodzą uzasadnione prawnie okoliczności;

g. wnieść sprzeciw w stosunku do przetwarzania jej danych, jeżeli zachodzą uzasadnione prawnie okoliczności;

h. nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu i wywołuje wobec niej skutki prawne lub w inny sposób na nią wpływa;

i. wnieść skargę do Urzędu Ochrony Danych Osobowych jeżeli uważa, że realizacja prawa lub procesy przetwarzania są zgodne z obowiązującymi przepisami.

2. Realizacja każdego żądania wymaga wcześniejszej weryfikacji tożsamości, zbadania zasadności i możliwości prawnych realizacji żądanego prawa.

3. W ciągu 30 dni od złożenia żądania administrator zobowiązany jest zrealizować żądanie lub odmówić realizacji żądania.

4. Odmowa realizacji żądania zawsze musi zawierać uzasadnienie.

miejscowość, data	*podpis osoby fizycznej, której dane dotyczą*

Załącznik Nr 2 do Załącznika Nr 5

Wezwanie do usunięcia braków formalnych

_____, dn. _____ r.

_____

_____

Wezwanie do usunięcia braków formalnych

W odpowiedzi na wniosek z dnia _____. dot. _____, wzywa do usunięcia braków formalnych poprzez:

1. _____;
2. _____.

Uzasadnienie

_____

_____

_____.

Tutejszy organ informuje, że nieusunięcie braków spowoduje pozostawienie wniosku bez rozpoznania, zgodnie z art. 64 § 2 Kodeksu postepowania administracyjnego (tj. Dz. U. z 2020 r. poz. 256 ze zm.).

_____

Załącznik Nr 3 do Załącznika Nr 5

DECYZJA DOTYCZĄCA REALIZACJI WNIOSKU

_____, dn. _____ r.

_____

_____

DECYZJA DOTYCZĄCA REALIZACJI WNIOSKU

Zgodnie z wewnętrznymi procedurami informuję Panią/Pana, że wniosek z dnia _____. dot. _____, został w całości odrzucony/w części odrzucony/w całości zrealizowany.

Uzasadnienie

_____

_____

_____

Ma Pani/Pan prawo do złożenia skargi do Urzędu Ochrony Danych Osobowych oraz obrony swoich praw przed Sądem.

_____

Załącznik Nr 6 do zarządzenia Nr 715/2021
Burmistrza Miasta i Gminy Kąty Wrocławskie
z dnia 08 kwietnia 2021 r.

PROCEDURA POWIERZENIA PRZETWARZANIA

SPIS TREŚCI

I. WPROWADZENIE

1.Niniejsza procedura jest integralną częścią Polityki, jednakże Polityka jest nadrzędnym dokumentem w stosunku do procedury.
2.Niniejsza procedura określa zasady powierzenia przetwarzania danych osobowych.
3.Wprowadzenie niniejszej procedury jest niezbędne ze względu na:
a.zapewnienie realizacji wszystkich obowiązków administratora wynikających z art. 28 rozporządzenia UE 2016/679;
b.zapewnienia realizacji zasad przetwarzania danych osobowych, w tym powierzenia, o których mowa w art. 5 rozporządzenia UE 2016/679;
c.zapewnienie rozliczalności przestrzegania zasad przetwarzania danych osobowych, o których mowa w art. 5 rozporządzenia UE 2016/679.
4.Niniejsza procedura ma zastosowanie do wszystkich sytuacji, w których administrator powierza przetwarzanie danych osobowych.
5.Jeżeli przepisy unijne lub krajowe w inny sposób regulują postanowienia niniejszej procedury, to niniejsza procedura w zakresie w jakim regulują to przepisy nie obowiązuje.
6.Z niniejszą procedurą musi się zapoznać:
a.każdy pełnomocnik administratora;
b.każdy kierownik;
c.każdy pracownik odpowiedzialny za wyszukiwanie i wybór kontrahentów oraz zawieranie z nimi umów.
7.Zmiany niniejszej procedury lub jej załączników wymagają zgody administratora oraz inspektora ochrony danych i są wprowadzane pod ich ścisłym nadzorem.

II. WARUNKI POWIERZENIA

1.Jeżeli niezbędne jest powierzenie przetwarzania danych osobowych zewnętrznemu podmiotowi lub ten podmiot będzie sam zbierał dane osobowe na użytek administratora to musi on spełniać następujące warunki:
a.wypełnić formatkę kontrolną według wzoru „06. Formatka kontrolna dla PPDO" i dostarczyć ją na adres e-mail: rodo@katywroclawskie.pl.
b.uzyskać pozytywną rekomendację IOD wydaną na podstawie wypełnionej formatki kontrolnej dla PPDO;
c.wypełnić wszystkie zasady powierzenia przetwarzania.
2.Jeżeli IOD nie wydał rekomendacji PPDO to ich wydanie jest możliwe jeżeli zostaną wprowadzone zalecenia wskazane w uzasadnieniu odmowy wydania rekomendacji.

III. ZASADY POWIERZENIA

1.Przetwarzanie przez PPDO danych osobowych w imieniu lub na użytek administratora obywać się może tylko wyłącznie na podstawie:
a.umowy powierzenia przetwarzania – załącznik do procedury „06. umowa powierzenia przetwarzania";
b.dodatkowego zapisu do zawieranej umowy – załącznik do procedury „06. Klauzula powierzenia."
c.zapisów zaproponowanych przez PPDO i zaakceptowanych przez IOD.

2.Zapisy dotyczące powierzenia przetwarzania muszą stanowić co najmniej, że podmiot przetwarzający:
a.przetwarza dane osobowe wyłącznie na wyraźne polecenie administratora;
b.zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c.posiada wdrożone stosowne środki organizacyjne i techniczne adekwatne do ryzyka naruszenia ochrony danych osobowych, gwarantujące odpowiedni poziom bezpieczeństwa;
d.przekazał listę swoich podmiotów przetwarzających, którym będzie powierzał dane administratora i uzyskał na to zgodę administratora;
e.będzie informował o każdej zmianie swoich podmiotów przetwarzających i umożliwi administratorowi złożenie sprzeciwu lub nie wyrażaniu zgody na taką zmianę;
f.każdy jego podmiot przetwarzający będzie miał co najmniej takie same warunki powierzenia przetwarzania jakie ma z administratorem;
g.pomaga realizować prawa osób fizycznych wynikające z przetwarzania ich danych osobowych;
h.pomaga realizować wymogi związane z naruszeniem ochrony danych osobowych;
i.pomaga administratorowi przeprowadzić ocenę skutków oraz wprowadzić zalecenia wynikające z jej wyników;
j.zwraca lub usuwa wszystkie dane osobowe po zakończeniu powierzenia przetwarzania, w zależności od wytycznych administratora;
k.udostępni wszelkie informacje związane z przetwarzaniem powierzonych danych osobowych;
l.umożliwi przeprowadzenie audytu z zakresu ochrony danych osobowych.
3.Każdy PPDO musi zostać wpisany do ewidencji PPDO prowadzonej przez IOD.
4.Każda umowa z PPDO dotycząca danych osobowych musi być sprawdzona i zaakceptowana przez IOD.

IV. WZORY I DOKUMENTY

1.Zastosowanie mają następujące wzory dokumentów będące załącznikami do niniejszej procedury:
a.„06. Formatka kontrolna dla PPDO.";
b.„06. ewidencja podmiotów przetwarzających";
c.„06. Klauzula powierzenia";
d.„06. umowa powierzenia przetwarzania".
2.W wyniku stosowania niniejszej procedury powstanie dokumentacja zawierająca dane osobowe lub/oraz informacje poufne o jednostce przetwarzającej dlatego administrator wyznacza osoby odpowiedzialne za przechowywanie w następujących zakresach:
a.Formatka kontrolna dla PPDO i ewidencja podmiotów przetwarzających uzupełnione w oryginale przechowuję IOD;
b.podpisane umowy powierzenia i klauzule powierzenia w oryginale przechowywane są z umowami głównymi.
3.Przechowywanie, archiwizowanie, modyfikowanie, ujawnianie, udostępnianie, niszczenie lub usuwanie i innego rodzaju przetwarzanie załączników lub treści w nich zawartych odbywa się zgodnie ze stosowną procedurą, chyba, że nie zawierają danych osobowych to zgodnie z przepisami unijnymi lub krajowymi lub uregulowaniami wewnętrznymi.

V. POSTANOWIENIA KOŃCOWE

1.Nadzór nad niniejszą procedurą sprawuję:
a.IOD w pełnym zakresie;
b.każdy kierownik w obrębie własnej komórki organizacyjnej;
c.każdy pełnomocnik administratora w zakresie udzielonego pełnomocnictwa:
d.każdy upoważniony w zakresie nadanego upoważnienia;
2.Każdy kto nie przestrzega niniejszej procedury a jest do tego zobowiązany, na mocy przepisów unijnych lub krajowych lub na mocy wyrażonego oświadczenia woli, ponosi odpowiedzialność za wszelkie szkody powstałe z powodu tego zaniechania zgodnie z Kodeksem Cywilnym, Kodeksem Pracy, Rozporządzeniem UE 2016/679 bądź innymi przepisami adekwatnymi do zaistniałej sytuacji.
3.Niniejsza procedura obowiązuję z dniem _____.

VI. METRYKA

aktualna wersja:		numer zarządzenia:	

Zakres aktualizacji	Data aktualizacji	Wprowadził aktualizacje	Zatwierdził aktualizacje

Formatka kontrolna dla PPDO

Wypełnia wykwalifikowany pracownik podmiotu przetwarzającego. Należy uzupełnić jedynie wszystkie pola zaznaczone na biało. Uzupełnioną ankietę należy wysłać na adres e-mail: _____. W przypadku pytań proszę o kontakt z _____, tel.: _____, e-mail: _____.				**Tą cześć wypełnia pracownik administratora (inspektor ochrony danych lub ktoś wykwalifikowany w zakresie ochrony danych osobowych). Wypełnić należy jedynie pola zaznaczone na biało.**			
Data wypełnienia:		PODMIOT PRZETWARZAJĄCY:		Data sprawdzenia:		Imię i nazwisko wypełniającego:	
Imię i nazwisko wypełniającego:		Stanowisko wypełniającego:		skala ocen	**pozytywna** - współpraca możliwa do nawiązania	**mała niezgodność** - współpraca możliwa do nawiązania ale z deklaracją uregulowania niezgodności	**krytyczna niezgodność** - współpraca możliwa do nawiązania tylko po usunięciu niezgodności
Zakres usługi świadczonej dla Administratora:				Pozytywna ocena - suma -	Mała niezgodność - suma -	Krytyczna niezgodność - suma	REKOMENDACJA SPRAWDZAJĄCEGO

LP.	PYTANIE	ODPOWIEDŹ	PYTANIE	ODPOWIEDŹ	LP.	Ocena	Uwagi i zalecenia
I. Specjaliści zaangażowani w czynności przetwarzania					**I. Specjaliści zaangażowani w czynności przetwarzania**		
1.1	Czy został powołany inspektor ochrony danych?	WYBIERZ			1.1	WYBIERZ	
1.2	Czy został wyznaczony Administrator Systemów Informatycznych?	WYBIERZ			1.2	WYBIERZ	
1.3	Czy został wyznaczony Archiwista?	WYBIERZ			1.3	WYBIERZ	
II. Stosowane środki bezpieczeństwa					**II. Stosowane środki bezpieczeństwa**		
2.1	Czy została opracowana i jest stosowana Polityka Ochrony Danych Osobowych?	WYBIERZ			2.1	WYBIERZ	
2.2	Czy została opracowana i jest stosowana Instrukcja Zarządzania Systemami Informatycznymi?	WYBIERZ			2.2	WYBIERZ	
2.3	Czy są stosowane jakieś inne procedury, standardy dotyczące bezpieczeństwa?	WYBIERZ			2.3	WYBIERZ	
2.4	Czy podmiot przetwarzający przeprowadził analizę ryzyka wynikającą z przetwarzania danych osobowych?	WYBIERZ			2.4	WYBIERZ	
2.5	Czy podmiot przetwarzający stosuje pseudonimizację i szyfrowanie danych?	WYBIERZ			2.5	WYBIERZ	
2.6	Czy podmiot przetwarzający jest w stanie zapewnić poufność systemów i usług przetwarzania?	WYBIERZ			2.6	WYBIERZ	
2.7	Czy podmiot przetwarzający jest w stanie zapewnić ciągłą dostępność systemów i usług przetwarzania, także w przypadku wszelkich incydentów?	WYBIERZ			2.7	WYBIERZ	
2.8	Czy podmiot przetwarzający jest w stanie zapewnić integralność systemów i usług przetwarzania?	WYBIERZ			2.8	WYBIERZ	
2.9	Czy podmiot przetwarzający zabezpiecza dane osobowe i inne informacje w sposób uniemożliwiający nieuprawnionemu ich ujawnienie, modyfikację, usunięcie lub zniszczenie?	WYBIERZ			2.9	WYBIERZ	

2.10	Czy podmiot przetwarzający zachowuje szczególną dbałość o aktualizację oprogramowania?	WYBIERZ			2.10	WYBIERZ	
2.11	Czy podmiot przetwarzający wdrożył procedury minimalizujące ryzyko utraty informacji w wyniku awarii?	WYBIERZ			2.11	WYBIERZ	
2.12	Czy podmiot przetwarzający wdrożył ochronę przed błędami, przypadkową utratą lub modyfikacją.	WYBIERZ			2.12	WYBIERZ	
2.13	Czy podmiot przetwarzający monitoruje podatność systemów informatycznych na możliwość naruszenia bezpieczeństwa?	WYBIERZ			2.13	WYBIERZ	
2.14	Czy podmiot przetwarzający prowadzi kontrolę systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa?	WYBIERZ			2.14	WYBIERZ	
2.15	Czy podmiot przetwarzający zapewnił utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację?	WYBIERZ			2.15	WYBIERZ	
2.16	Czy informacje będące własnością Administratora przechowywane są lub przenoszone w dowolnym momencie na urządzeniach przenośnych (laptopach, PDA, telefonach, dyskach USB)?	WYBIERZ			2.16	WYBIERZ	
2.17	Czy pracownicy i goście noszą identyfikatory?	WYBIERZ			2.17	WYBIERZ	
2.18	Czy prowadzony jest rejestr wejść i wyjść?	WYBIERZ			2.18	WYBIERZ	
2.19	Czy dostęp do wszystkich pomieszczeń jest ograniczany przez urządzenia elektroniczne, strażników lub recepcjonistów?	WYBIERZ			2.19	WYBIERZ	
2.20	Czy na wszystkich komputerach z systemem Windows jest zainstalowane oprogramowanie antywirusowe?	WYBIERZ			2.20	WYBIERZ	
2.21	Czy dostęp do komputerów chroniony jest hasłem?	WYBIERZ			2.21	WYBIERZ	
2.22	Czy każdy upoważniony dysponuje własnym loginem i hasłem do systemów, w których przetwarza dane osobowe?	WYBIERZ			2.22	WYBIERZ	
2.23	Czy hasła zmieniane są okresowo?	WYBIERZ			2.23	WYBIERZ	
2.24	Czy papierowe nośniki danych są zamykane w pomieszczeniach/szafach niedostępnych dla nieuprawnionych?	WYBIERZ			2.24	WYBIERZ	
2.25	Czy na wszystkich komputerach ustawiony jest wygaszacz ekranu z automatycznym włączeniem się i zablokowaniem komputera po zidentyfikowanym czasie bezczynności?	WYBIERZ			2.25	WYBIERZ	

III. Audyty i kontrole					**III. Audyty i kontrole**		
3.1	Czy był przeprowadzany audyt z ochrony danych osobowych?'	WYBIERZ			3.1	WYBIERZ	

3.2	Czy podmiot przetwarzający prowadzi regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełniania wymogów polityki ochrony danych lub innej wewnętrznej procedury, w tym ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?	WYBIERZ			3.2	WYBIERZ	
3.3	Czy podmiot przetwarzający jest przygotowany do poddania się audytowi przeprowadzonemu przez administratora danych lub audytora upoważnionego przez przez niego?	WYBIERZ			3.3	WYBIERZ	
3.4	Czy podmiot przetwarzający kontroluje zgodność z RODO swoich zleceniobiorców (podmiotów podprzetwarzających), którzy mają dostęp do danych osobowych?	WYBIERZ			3.4	WYBIERZ	
3.5	Czy w odniesieniu do systemów informatycznych prowadzone są okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz czy są podejmowane działania minimalizujące to ryzyko, stosownie do wyników przeprowadzonej analizy?	WYBIERZ			3.5	WYBIERZ	

IV. Naruszenie bezpieczeństwa					**IV. Naruszenie bezpieczeństwa**		
4.1	Czy w ciągu ostatnich 24 miesięcy wystąpiły naruszenia ochrony danych lub incydenty w systemach informatycznych?	WYBIERZ			4.1	WYBIERZ	
4.2	Czy została opracowana procedura zgłaszania incydentów i naruszeń ochrony danych?	WYBIERZ			4.2	WYBIERZ	
4.3	Czy została opracowana analiza pozwalająca określić czy mamy do czynienia z wysokim ryzykiem naruszenia praw i wolności w przypadku naruszenia ochrony danych osobowych?	WYBIERZ			4.3	WYBIERZ	

V. Szkolenia					**V. Szkolenia**		
5.1	Czy są prowadzone cykliczne szkolenia pracowników w zakresie bezpieczeństwa?	WYBIERZ			5.1	WYBIERZ	
5.2	Czy każdy nowy pracownik szkolony jest z BHP?	WYBIERZ			5.2	WYBIERZ	
5.3	Czy każdy nowy pracownik szkolony jest z ochrony danych osobowych?	WYBIERZ			5.3	WYBIERZ	
5.4	Czy każdy nowy pracownik szkolony jest z bezpieczeństwa w systemach informatycznych?	WYBIERZ			5.4	WYBIERZ	
5.5	Czy każdy nowy pracownik szkolony jest z archiwizacji dokumentacji?	WYBIERZ			5.5	WYBIERZ	
5.6	Czy każdy nowy pracownik szkolony jest z obiegu dokumentów?	WYBIERZ			5.6	WYBIERZ	
5.7	Czy prowadzona jest ewidencja przeprowadzonych szkoleń?	WYBIERZ			5.7	WYBIERZ	

VI. Wymiana danych osobowych i informacji					VI. Wymiana danych osobowych i informacji		
6.1	Czy realizowana jest wymiana danych w formie elektronicznej?	WYBIERZ			6.1	WYBIERZ	
6.2	Czy dane osobowe lub inne informacje przesyłane w formie elektronicznej są zabezpieczane?	WYBIERZ			6.2	WYBIERZ	
6.3	Czy istnieją inne niż siedziba lokalizacje przetwarzania?	WYBIERZ			6.3	WYBIERZ	

VII. Zmiany					VII. Zmiany		
7.1	Czy administrator informowany jest o wszelkich zmianach, które mogą wpłynąć na przetwarzanie danych osobowych Administratora?	WYBIERZ			7.1	WYBIERZ	
7.2	Czy przed wprowadzeniem zmiany w systemach wykonywana jest analiza ryzyka?	WYBIERZ			7.2	WYBIERZ	
7.3	Czy wszelkie zmiany w systemach wprowadzane są w oparci o przeprowadzone testy?	WYBIERZ			7.3	WYBIERZ	

VIII. Kopie zapasowe					VIII. Kopie zapasowe		
8.1	Czy wykonywane są kopie zapasowe(awaryjne, bezpieczeństwa)?	WYBIERZ			8.1	WYBIERZ	
8.2	Czy jest opracowana i stosowana procedura kopii zapasowych?	WYBIERZ			8.2	WYBIERZ	

IX. Usuwanie					IX. Usuwanie		
9.1	Czy opisany został proces bezpiecznego pozbywania się danych i nośników danych (elektronicznych i papierowych) kiedy nie są już używane, w celu ochrony przed ujawnieniem poufnych informacji?	WYBIERZ			9.1	WYBIERZ	
9.2	Czy używane są niszczarki do dokumentów?	WYBIERZ			9.2	WYBIERZ	
9.3	Czy wszystkie dane Administratora są usuwane po zakończeniu współpracy z administratorem?	WYBIERZ			9.3	WYBIERZ	

X. Podpowierzenie					X. Podpowierzenie		
10.1	Czy dane osobowe przekazywane są innym podmiotom (podmiotom podprzetwarzającym)? / chmurka, domeny, operator poczty e-mail, systemy, portale społecznościowe, księgowość itp. /	WYBIERZ			10.1	WYBIERZ	
10.2	Czy administrator informowany jest o zmianach podmiotów podprzetwarzających?	WYBIERZ			10.2	WYBIERZ	

XI. Upoważnienia i poufność					XI. Upoważnienia i poufność		
11.1	Czy została wprowadzona procedura nadawania upoważnień do przetwarzania, uprawnień do systemów oraz odbierania upoważnień i uprawnień?	WYBIERZ			11.1	WYBIERZ	
11.2	Czy od wszystkich pracowników wymaga się podpisania oświadczenia o zachowaniu poufności danych, do których mają dostęp?	WYBIERZ			11.2	WYBIERZ	

11.3	Czy uprawnienia nadawane użytkownikom przyznawane są zgodnie z zasadą minimalnych uprawnień czyli tylko osoby pracujące nad projektem Administratora mają dostęp do danych i systemów Administratora?	WYBIERZ			11.3	WYBIERZ	
11.4	Czy w przypadku zmiany stanowiska bądź zakresów obowiązków następuje bezzwłoczna zmiana uprawnień i upoważnień?	WYBIERZ			11.4	WYBIERZ	

XII. Monitoring					**XII. Monitoring**		
12.1	Czy na terenie podmiotu przetwarzającego jest zainstalowany monitoring?	WYBIERZ			12.1	WYBIERZ	
12.2	Czy dostęp do nagrań jest zabezpieczony?	WYBIERZ			12.2	WYBIERZ	
12.3	Czy nagrania z monitoringu są udostępniane?	WYBIERZ			12.3	WYBIERZ	
12.4	Czy jest opracowana i stosowana procedura monitoringu?	WYBIERZ			12.4	WYBIERZ	
12.5	Czy prowadzony jest monitoring pracy (obszar pracy, poczta, systemy, odwiedzane strony, itp..) pracownika?	WYBIERZ			12.5	WYBIERZ	
12.6	Czy pracownicy zostali zapoznani z regulaminem monitoringu pracy?	WYBIERZ			12.6	WYBIERZ	

XIII. Prawa osób fizycznych					**XIII. Prawa osób fizycznych**		
13.1	Czy podmiot przetwarzający posiada procedurę realizacji praw osób fizycznych?	WYBIERZ			13.1	WYBIERZ	
13.2	Czy osoby fizyczne w ciągu ostatniego roku składały żądania dotyczące RODO?	WYBIERZ			13.2	WYBIERZ	
13.3	Czy za udostępnienie kopii danych osobie fizycznej pobierane są opłaty?	WYBIERZ			13.3	WYBIERZ	
13.4	Czy wdrożono procedurę weryfikacji tożsamości składającego żądanie?	WYBIERZ			13.4	WYBIERZ	
13.5	Czy realizowany jest obowiązek informacyjny w stosunku do pracowników?	WYBIERZ			13.5	WYBIERZ	

XIV. Praca zdalna					**XIV. Praca zdalna**		
14.1	Czy pracownicy mają możliwość wykonywania pracy zdalnie?	WYBIERZ			14.1	WYBIERZ	
14.2	Czy jest stworzona i stosowana procedura pracy zdalnej?	WYBIERZ			14.2	WYBIERZ	
14.3	Czy pracownik pracujący zdalnie może posiadać przy sobie oryginały dokumentów?	WYBIERZ			14.3	WYBIERZ	
14.4	Czy praca zdalna może być wykonywana na prywatnych urządzeniach?	WYBIERZ			14.4	WYBIERZ	

XV. Rejestry i ewidencje					**XV. Rejestry i ewidencje**		
15.1	Czy jest prowadzony rejestr naruszeń ochrony danych?	WYBIERZ			15.1	WYBIERZ	
15.2	Czy podmiot przetwarzający prowadzi rejestr czynności przetwarzania?	WYBIERZ			15.2	WYBIERZ	
15.3	Czy podmiot przetwarzający prowadzi rejestr kategorii czynności?	WYBIERZ			15.3	WYBIERZ	
15.4	Czy prowadzona jest ewidencja wydanych upoważnień i uprawnień?	WYBIERZ			15.4	WYBIERZ	
15.6	Czy jest prowadzona ewidencja systemów informatycznych?	WYBIERZ			15.6	WYBIERZ	
15.7	Czy jest prowadzona ewidencja podmiotów przetwarzających?	WYBIERZ			15.7	WYBIERZ	

Załącznik Nr 2 do Załącznika Nr 6

ewidencja podmiotów przetwarzających

Lista podmiotów podprzetwarzających	Data rozpoczęcia współpracy	Data zakończenia współpracy	Dane inspektora ochrony danych podmiotu	Dane naszego pracownika odpowiedzialnego za umowę	Notatka z przeprowadzonej kontroli bezpieczeństwa

Załącznik Nr 3 do Załącznika Nr 6

Klauzula powierzenia

1. W trybie art. 28 rozporządzenia (UE) 2016/679 _____ jest podmiotem przetwarzającym, a _____ administratorem.

2. Administrator powierza do przetwarzania dane osobowe podmiotowi przetwarzającemu tylko w ustalonym zakresie
i wskazanym celu.

3. Każda zmiana zakresu danych lub celu przetwarzania wymaga zgody administratora i rekomendacji inspektora ochrony danych.

4. Podmiot przetwarzający przetwarzać będzie następujące dane we wskazanych celach:

Kategoria osób fizycznych	Dane osobowe	Cel powierzenia przetwarzania

5. Podmiot przetwarzający:

a.zobowiązuje się zachować w tajemnicy wszystkie przetwarzane dane osobowe oraz informacje dotyczące ich zabezpieczeń i sposobów przetwarzania;

b.zapewnia, że wszyscy pracownicy upoważnieni do przetwarzania danych osobowych zachowają w tajemnicy wszystkie przetwarzane dane osobowe oraz informacje dotyczące ich zabezpieczeń i sposobów przetwarzania.

6. Podmiot przetwarzający uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownych przypadkach:

a.pseudonimizację i szyfrowanie danych osobowych;

b.zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

c.zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

d.regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych nie powodującego wysokiego ryzyka naruszenia praw i wolności osób fizycznych, których dane dotyczą:

a.informuje administratora o przyczynach i skutkach powstałego naruszenia;

b.ocenia kto jest administratorem naruszenia ochrony danych osobowych w rozumieniu art. 28, ust. 10 rozporządzenia (UE) 2016/679;

c.jeżeli podmiot przetwarzający jest administratorem naruszenia to wprowadza działania zapobiegawcze i zaradcze i przekazuje ich wyniki administratorowi danych;

d.jeżeli podmiot przetwarzający nie jest administratorem naruszenia ochrony danych osobowych to ogranicza przetwarzanie danych do samej archiwizacji i czeka na dalsze wytyczne administratora danych.

8. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych powodującego wysokie ryzyko naruszenia praw i wolności osób fizycznych, których dane dotyczą:

e.informuje administratora o przyczynach i skutkach powstałego naruszenia, najpóźniej w ciągu 24 godzin po stwierdzeniu naruszenia;

f.ocenia kto jest administratorem naruszenia ochrony danych osobowych w rozumieniu art. 28, ust. 10 rozporządzenia (UE) 2016/679;

g.jeżeli podmiot przetwarzający jest administratorem naruszenia to wprowadza działania zapobiegawcze i zaradcze i przekazuje ich wyniki administratorowi danych a następnie działa godnie z art. 32 i 33 rozporządzenia (UE) 2016/679;

h.jeżeli podmiot przetwarzający nie jest administratorem naruszenia ochrony danych osobowych to ogranicza przetwarzanie danych do samej archiwizacji i czeka na dalsze wytyczne administratora danych.

9. Podmiot przetwarzający zobowiązuje się udzielić wszelkich informacji administratorowi dotyczących zabezpieczeń technicznych i organizacyjnych zastosowanych przy przetwarzaniu powierzonych danych osobowych niezbędnych do przeprowadzenia przez administratora analizy ryzyka i oceny skutków.

10. Administrator wyraża zgodę aby podmiot przetwarzający powierzył swojemu podmiotowi przetwarzającemu przetwarzanie danych osobowych administratora w następującym zakresie:

Nazwa podmiotu	Adres siedziby podmiotu	Zakres powierzonych danych	Cel powierzenia przetwarzania

11. Podmiot przetwarzający zapewnia, że w przypadku każdego swojego podmiotu przetwarzającego warunki powierzenia przetwarzania danych osobowych ma co najmniej na takim poziomie jakie wynikają z niniejszej _____.

12. Podmiot przetwarzający zobowiązuje się pobierać każdorazowo pisemną zgodę administratora na zmianę swojego podmiotu przetwarzającego lub zatrudnieniem jeżeli będzie mieć dostęp do danych administratora.

13. Podmiot przetwarzający zobowiązuje się wpierać administratora w rozpatrywaniu żądań osób fizycznych oraz realizacji ich praw wynikających z rozporządzenia (UE) 2016/679.

14. Podmiot przetwarzający po zakończeniu obowiązywania niniejszej _____ zobowiązuje się usunąć / zwrócić wszystkie dane osobowe w terminie _____.

15. Podmiot przetwarzający zobowiązuje się poddać kontroli związanej z przetwarzaniem powierzonych danych osobowych przeprowadzanej przez inspektora ochrony danych lub innego przez niego upoważnionego pracownika.

16. Podmiot przetwarzający zobowiązuje się niezwłocznie powiadomić administratora jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie prawa.

Załącznik Nr 4 do Załącznika Nr 6

Umowa powierzenia przetwarzania danych osobowych

zawarta w dniu pomiędzy:

nazwa podmiotu: _____
adres siedziby: _____
reprezentowany przez: _____

zwaną dalej **„Administratorem"**

a

nazwa podmiotu: _____
adres siedziby: _____
reprezentowany przez: _____

zwaną dalej **„Podmiotem przetwarzającym"**.

Łącznie zwanych **„Stronami"**

Mając na uwadze, że:

·Podmiot przetwarzający zapewnia na rzecz administratora usługę _____.

·Administrator jest zobowiązany zapewnić, iż przetwarzanie przez podmiot przetwarzający danych osobowych w jego imieniu będzie odbywało się zgodnie z art. 28 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679.

Strony postanowiły zawrzeć umowę o następującej treści:

§ 1. Definicje

Użyte w umowie określenia będą miały następujące znaczenie:

1. **Rozporządzenie (UE) 2016/679** – oznacza 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).

2. **Dane Osobowe** – oznacza dane w rozumieniu art. 4 pkt 1) Rozporządzenia (UE) 2016/679, tj. wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

3. **Naruszenie ochrony danych osobowych** – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

4. **Przetwarzanie** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

5. **Państwo trzecie** – oznacza państwo nienależące do Europejskiego Obszaru Gospodarczego.

§ 2. Przedmiot umowy

1. Przedmiotem niniejszej umowy jest określenie zasad przetwarzania oraz zabezpieczania danych osobowych, które podmiot przetwarzający przetwarza w imieniu administratora.

2. Podmiot przetwarzający będzie odpowiednio wykonywał obowiązki określone w niniejszej umowie również w przypadku uznania, że jest on administratorem lub współadministratorem danych osobowych.

§ 3. Przetwarzane dane osobowe

1. Administrator, działając na podstawie art. 28 ust. 3 Rozporządzenia (UE) 2016/679, powierza podmiotowi przetwarzającemu przetwarzanie następujących kategorii danych osobowych we wskazanych celach:

Kategoria osób fizycznych	Dane osobowe	Cel powierzenia przetwarzania

2. Administrator oświadcza, że spełnił wszelkie warunki legalności przetwarzania danych osobowych.

3. Administrator powierza podmiotowi przetwarzającemu przetwarzanie danych osobowych w jego imieniu przez okres _____.

§ 4. Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający jest uprawniony do przetwarzania danych osobowych wyłącznie na potrzeby realizacji wskazanych celów przetwarzania.

2. Osoby upoważnione przez podmiot przetwarzający do przetwarzania danych osobowych będą zobowiązane do zachowania ich w tajemnicy.

3. Podmiot przetwarzający podejmuje wszelkie środki wymagane na mocy art. 32 Rozporządzenia (UE) 2016/679 w celu zapewnienia bezpieczeństwa danych osobowych.

4. Podmiot przetwarzający, biorąc pod uwagę charakter przetwarzania, jest zobowiązany pomagać administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia (UE) 2016/679, co oznacza, że podmiot przetwarzający będzie realizował te obowiązki w imieniu administratora w zakresie w jakim przetwarza dane osobowe w ramach niniejszej umowy.

5. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 Rozporządzenia (UE) 2016/679.

6. Podmiot przetwarzający jest zobowiązany udostępnić administratorowi wszelkie informacje niezbędne do wykazania, iż spełnia obowiązki określone w niniejszym paragrafie umowy oraz umożliwi administratorowi lub upoważnionemu przez niego audytorowi przeprowadzanie audytów w terminach i sposobach uzgodnionych przez Strony.

7. Podmiot przetwarzający niezwłocznie poinformuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie Rozporządzenia (UE) 2016/679, innych przepisów unijnych lub krajowych z zakresu ochrony danych osobowych.

8. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych jest zobowiązany bez zbędnej zwłoki zgłosić je administratorowi wskazując w zgłoszeniu:
a) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
c) opis środków zastosowanych lub proponowanych przez podmiot przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym opis działań podjętych w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

§ 5. Dalsze powierzenie przetwarzania danych osobowych

1. Podmiot przetwarzający jest uprawniony do korzystania z usług innego podmiotu przetwarzającego tylko za wcześniejszą zgodą administratora.

2. Podmiot przetwarzający korzysta z usług następujących podmiotów przetwarzających, na co administrator wyraża zgodę:

Nazwa podmiotu	Adres siedziby podmiotu	Zakres powierzonych danych	Cel powierzenia przetwarzania

3. Podmiot przetwarzający jest zobowiązany zapewnić, iż inny podmiot przetwarzający, z którego usług zamierza korzystać przy przetwarzaniu danych osobowych, daje wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia (UE) 2016/679 i chroniło prawa osób, których dane dotyczą i wymogi te nie były mniejsze niż wskazane w niniejszej umowie.

§ 6. Postanowienia końcowe

1. Niniejsza umowa zostaje zawarta na czas _____.

2. Niniejsza umowa została sporządzona w ____ egzemplarzach.

3. Wszelkie zmiany lub uzupełnienia niniejszej umowy wymagają zachowania formy pisemnej pod rygorem nieważności.

Załącznik Nr 7 do zarządzenia Nr 715/2021
Burmistrza Miasta i Gminy Kąty Wrocławskie
z dnia 08 kwietnia 2021 r.

PROCEDURA UDOSTĘPNIANIA DANYCH OSOBOWYCH INNYM PODMIOTOM ORAZ ORGANOM UPRAWNIONYM

PROCEDURA UDOSTĘPNIANIA DANYCH OSOBOWYCH INNYM PODMIOTOM ORAZ ORGANOM UPRAWNIONYM

SIPIS TREŚCI

I. WPROWADZENIE

1.Niniejsza procedura jest integralną częścią Polityki, jednakże Polityka jest nadrzędnym dokumentem w stosunku do procedury.
2.Niniejsza procedura określa zasady udostępniania danych osobowych odbiorcom oraz organom uprawnionym.
3.Wprowadzenie niniejszej procedury jest niezbędne ze względu na:
a.zapewnienie przestrzegania 6 zasad przetwarzania danych osobowych, w tym udostępniania, o których mowa w art. 5 rozporządzenia UE 2016/679;
b.zapewnienie spełnienia co najmniej jednego z sześciu warunków przetwarzania danych osobowych, w tym udostępnienia, o których mowa w art. 6 rozporządzenia UE 2016/679;
c.zapewnienie rozliczalności przestrzegania zasad przetwarzania danych osobowych, o których mowa w art. 5 rozporządzenia UE 2016/679.
4.Niniejsza procedura ma zastosowanie do wszystkich czynności związanych z udostępnianiem danych osobowych.
5.Jeżeli przepisy unijne lub krajowe w inny sposób regulują postanowienia niniejszej procedury, to niniejsza procedura, w zakresie w jakim regulują to przepisy, nie obowiązuje.
6.Z niniejszą procedurą musi zapoznać się:
a.każdy pełnomocnik administratora;
b.każdy kierownik;
c.każdy pracownik udostępniający dane osobowe;
d.zespół bezpieczeństwa danych.
7.Zmiany niniejszej procedury lub jej załączników wymagają zgody administratora oraz inspektora ochrony danych i są wprowadzane pod ich ścisłym nadzorem.

II. ZASADY

1.Dane osobowe mogą być udostępniane:
a.podmiotom przetwarzającym w zakresie niezbędnym do realizacji powierzonych zadań;
b.współadministratorom w zakresie niezbędnym do realizacji wspólnych celów przetwarzania danych osobowych;
c.organom uprawnionym w zakresie ich kompetencji wynikających z przepisów i w stopniu adekwatnym do wskazanego celu przetwarzania;
d.osobom fizycznym i podmiotom upoważnionym w zakresie nadanego upoważnienia;
e.uprawnionym odbiorcom w zakresie i w celu wynikającym z przepisów unijnych lub krajowych.
2.Przed udostępnieniem żądanych danych osobowych, pracownik odpowiedzialny za realizację wniosku zobowiązany jest kolejno:
a.zweryfikować jednoznacznie tożsamość osoby fizycznej, która żąda udostępnienia;
b.w przypadku organu uprawnionego, jednoznacznie ustalić, czy osoba wnioskująca

o udostępnienie danych osobowych faktycznie reprezentuje wskazany organ;
c.w przypadku pełnomocnika lub osoby upoważnionej, sprawdzić autentyczność upoważnienia/pełnomocnictwa zgodnie z obowiązującymi przepisami;
d.w przypadku podmiotu przetwarzającego lub współadministratora sprawdzić, czy osoba żądająca udostępnienia, faktycznie reprezentuje wskazany podmiot i czy posiada ku temu odpowiednie uprawnienia;
e.sprawdzić możliwość udostępnienia wskazanego zakresu danych osobowych i jego adekwatność do podstawy prawnej i celu udostępnienia;
f.sprawdzić kompletność dostarczonych niezbędnych załączników;
g.ustalić formę udostępnienia danych osobowych i sposób ewentualnego kontaktu związanego z udostępnieniem.
3.Jeżeli złożony wniosek nie zawiera wszystkich koniecznych powyższych informacji, to wzywa się do uzupełnienia braków formalnych w wyznaczonym terminie pod rygorem pozostawienia wniosku bez rozpatrzenia.
4.Wnioski o udostępnienie danych osobowych należy składać:
a.na wzorze załączonym do niniejszej procedury;
b.lub w inny sposób, jeżeli zawierać będzie wszystkie niezbędne informacje wskazane w niniejszej procedurze.
5.Tryb udzielenie odpowiedzi na wiosek będzie zależał od rodzaju danej sprawy.

III. WNIOSKI – OSOBY FIZYCZNE

1.W przypadku gdy osoba fizyczna żąda udostępnienia danych osobowych innej osoby fizycznej, zobowiązana jest:
a.podać swoją tożsamość;
b.podać swój adres zamieszkania i numer PESEL;
c.jeżeli składa wniosek w imieniu innej osoby fizycznej, to podać tożsamość, adres zamieszkania i PESEL tej osoby fizycznej oraz;
d.jeżeli składa wniosek w imieniu innej osoby fizycznej to zgodnie z przepisami wskazać i udokumentować z czego wynika jej uprawnienie do reprezentowania;
e.wskazać żądany zakres danych;
f.wskazać podstawę prawną udostępnienia danych osobowych i ją udokumentować;
g.wskazać cel udostępnienia danych osobowych;
h.wskazać formę udostępnienia oraz sposób ewentualnego kontaktu.
2.Wnioski mogą być składane:
a.osobiście w _____, pod adresem _____, pokój _____ w godzinach _____;
b.korespondencyjnie na adres _____;
c.przez Elektroniczną Skrzynkę Podawczą.

IV. WNIOSKI – INNE PODMIOTY I ORGANY UPRAWNIONE

1.W przypadku gdy osoba żądająca udostępnienia reprezentuje organ uprawniony lub inny podmiot, zobowiązana jest:
a.podać swoją tożsamość;
b.podać swoje stanowisko służbowe oraz komórkę merytoryczną, którą reprezentuje;
c.wskazać z czego wynika jej uprawnienie do reprezentowania;
d.wskazać nazwę, siedzibę i numer NIP lub KRS organu uprawnionego lub podmiotu trzeciego, który reprezentuje;
e.wskazać żądany zakres danych;
f.wskazać podstawę prawną udostępnienia danych osobowych i ją udokumentować;
g.wskazać cel udostępnienia danych osobowych;
h.wskazać formę udostępnienia oraz sposób ewentualnego kontaktu.
2.Wnioski mogą być składane:
a.osobiście w _____, pod adresem _____, pokój _____ w godzinach _____;
b.korespondencyjnie na adres _____;
c.przez Elektroniczną Skrzynkę Podawczą.

V. WZORY I DOKUMENTY

1.Zastosowanie mają następujące wzory dokumentów będące załącznikami do niniejszej procedury:
a.„07. Wniosek o udostępnienie danych – podmioty";

b.„07. Wniosek o udostępnienie danych - osoba fizyczna".
2.W wyniku stosowania niniejszej procedury powstanie dokumentacja zawierająca dane osobowe lub/oraz informacje poufne o jednostce przetwarzającej dlatego administrator wyznacza osoby odpowiedzialne za przechowywanie w następujących zakresach:
a.wypełnione wnioski przechowują osoby merytorycznie odpowiedzialne za sprawę zgodnie z obowiązującymi zasadami archiwizacji.
3.Przechowywanie, archiwizowanie, modyfikowanie, ujawnianie, udostępnianie, niszczenie lub usuwanie i innego rodzaju przetwarzanie załączników lub treści w nich zawartych odbywa się zgodnie ze stosowną procedurą, chyba, że nie zawierają danych osobowych to zgodnie z przepisami unijnymi lub krajowymi lub uregulowaniami wewnętrznymi.

VI. POSTANOWIENIA KOŃCOWE

1.Nadzór nad niniejszą procedurą sprawuję:
a.IOD w pełnym zakresie;
b.każdy kierownik w obrębie własnej komórki organizacyjnej;
c.każdy pełnomocnik administratora w zakresie udzielonego pełnomocnictwa:
d.każdy upoważniony w zakresie nadanego upoważnienia;
2.Każdy kto nie przestrzega niniejszej procedury a jest do tego zobowiązany, na mocy przepisów unijnych lub krajowych lub na mocy wyrażonego oświadczenia woli, ponosi odpowiedzialność za wszelkie szkody powstałe z powodu tego zaniechania zgodnie z Kodeksem Cywilnym, Kodeksem Pracy, Rozporządzeniem UE 2016/679 bądź innymi przepisami adekwatnymi do zaistniałej sytuacji.
3.Niniejsza procedura obowiązuję z dniem _____.

VII. METRYKA

aktualna wersja:		numer zarządzenia:	

Zakres aktualizacji	Data aktualizacji	Wprowadził aktualizacje	Zatwierdził aktualizacje

Załącznik Nr 1 do Załącznika Nr 7

Wniosek o udostępnienie danych – podmioty

WNIOSEK
1. Wniosek wypełnia osoba, która go składa. 2. Wniosek należy wypełnić drukowanymi literami. 3. Wniosek należy wypełnić zgodnie z wytycznymi, pod rygorem nierozpatrzenia wniosku zgodnie z art. 64 § 2 Kodeksu postępowania administracyjnego. 4. Jeżeli wniosek nie jest składany w imieniu własnym należy dołączyć do wniosku dokument potwierdzający umocowanie prawne do reprezentowania zgodnie z Kodeksem postępowania administracyjnego. 5. Do wniosku należy dołączyć wszystkie niezbędne .

1. **DANE ADMINISTRATORA**	
Nazwa administratora:	
Adres administratora:	

2. **DANE SKŁADAJĄCEGO WNIOSEK**	
Imię i nazwisko:	
Stanowisko:	
Komórka organizacyjna:	
Moje uprawnienie do reprezentowania wnioskującego wynika z załączonego do wniosku:	
☐	upoważnienia[1];
☐	pełnomocnictwa[2];
☐	orzeczenia sądu [3];
☐	innego dokumentu [4];
[1] – upoważnienie musi być dostarczone bezpośrednio przez osobę, której dane dotyczą; [2] – pełnomocnictwo musi być dostarczone przez osobę, której dane dotyczą lub przez inną osobę jeżeli będzie to pełnomocnictwo notarialne lub osoba dostarczająca ma prawo zgodnie z przepisami Unijnymi lub krajowymi poświadczyć autentyczność pełnomocnictwa; [3] – orzeczenie sądu musi być dołączone do wniosku; [4] – np. zarządzenie, uchwała, przepisy prawa itp.	

3. **DANE WNIOSKUJĄCEGO[5]**	
Nazwa podmiotu:	
Adres siedziby:	
Numer NIP :	
[5] – dane podmiotu który reprezentuję składający wniosek	

4. **INFORMACJĘ DOTYCZĄCE UDOSTĘPNIENIA**	
zakres danych[5]:	
podstawa prawna[6]:	
cel przetwarzania[7]:	
[6] – należy napisać jaki zakres danych osobowych ma podlegać udostępnieniu; [7] – należy napisać na jakiej podstawie prawnej odbyć miałby się udostępnienie; [8] – należy napisać w jakim celu przetwarzane będą dane osobowe / do czego mają być wykorzystane.	

5. **LISTA ZAŁĄCZNIKÓW DO WNIOSKU**	
NAZWA ZAŁĄCZNIKA	CZEGO DOTYCZY

6. **FORMA UDZIELENIA ODPOWIEDZI**	
Proszę o udzielenie odpowiedzi przez:	
☐	adres e-mail;
Proszę wpisać adres skrzynki e-mail. Wpisujemy drukowanymi literami.	

☐	adres korespondencyjny;
Proszę wpisać adres korespondencyjny. Wpisujemy drukowanymi literami.	
☐	odbiór osobisty;
Proszę napisać w jaki sposób poinformować o przygotowaniu odpowiedzi.	
☐	profil zaufany;
Proszę podać nazwę użytkownika.	
☐	W inny sposób;
Proszę napisać jakim sposobem dostarczyć odpowiedź.	

miejscowość, data	*podpis osoby fizycznej, której dane dotyczą*

INFORMACJE DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH ZAMIESZCZONYCH WE WNIOSKU

TOŻSAMOŚĆ I DANE KONTAKTOWE ADMINISTRATORA

Administratorem przetwarzającym dane osobowe jest _____.
Z administratorem można skontaktować się:
·telefonicznie - _____; (telefon stacjonarny bądź komórka)
·pisemnie - _____; (adres e-mail)
·osobiście lub pisemnie - _____. (adres siedziby, korespondencyjny)

DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH

Z inspektorem ochrony danych można skontaktować się:
·telefonicznie - _____; (telefon stacjonarny bądź komórka)
·pisemnie - _____; (adres e-mail)
·osobiście lub pisemnie - _____; (adres siedziby, korespondencyjny)

CEL I PODSTAWA PRAWNA PRZETWARZANIA ORAZ KATEGORIE DANYCH OSOBOWYCH

Dane osobowe przetwarzane są lub będą:
·w celu weryfikacji tożsamości i umocowań prawnych do reprezentowania na podstawie kodeksu postępowania administracyjnego w zakresie imienia, nazwiska, adresu zamieszkania, numeru PESEL składającego wniosek i osoby w imieniu, której składamy wniosek.
·w celu udzielenia odpowiedzi na wniosek na podstawie udzielonej zgody w zakresie adres email, korespondencyjny, telefon kontaktowy.

WYMOGI I KONSEKWENCJE

1.Podanie/udostępnienie danych osobowych w zakresie imienia, nazwiska i adresu zamieszkania jest wymagane na podstawie Kodeksu postępowania administracyjnego.
Osoba fizyczna, której dane dotyczą jest zobowiązana do ich podania.
W przypadku odmowy podania/udostępnienia danych osobowych wniosek zostanie nierozpatrzony.
2.Podanie/udostępnienie danych osobowych w zakresie numeru PESEL jest wymagane na podstawie prawnie uzasadnionego interesu realizowanego przez administratora.
Osoba fizyczna, której dane dotyczą nie jest zobowiązana do ich podania.
W przypadku odmowy podania/udostępnienia danych osobowych wniosek zostanie nierozpatrzony.
3.Podanie/udostępnienie danych osobowych w zakresie adresu e-mail lub korespondencyjnego lub telefonu kontaktowego nie jest wymagane ale konieczne do udzielenia odpowiedzi na wniosek.
W przypadku odmowy podania/udostępnienia danych osobowych odpowiedź na wniosek zostanie wysłana na adres zamieszkania.

ŹRÓDŁO POCHODZENIA DANYCH OSOBOWYCH

Wszystkie dane osobowe zostały pobrane od osoby składającej wniosek.

INFORMACJE O ODBIORCACH DANYCH OSOBOWYCH

Następujące podmioty będą miały dostęp do danych osobowych we wskazanych zakresach:
a._____, z siedzibą _____ - zakres danych osobowych _____;
b._____, z siedzibą _____ - zakres danych osobowych _____;
c._____, z siedzibą _____ - zakres danych osobowych _____;

d._____, z siedzibą _____ - zakres danych osobowych _____.

CZAS PRZETWARZANIA DANYCH OSOBOWYCH

Następujące dane osobowe będą przetwarzane we wskazanym czasie:

a._____ będą przetwarzane _____, a później będą archiwizowane przez _____ zgodnie z instrukcją archiwalną;

b._____ będą przetwarzane _____, a później będą archiwizowane przez _____ zgodnie z instrukcją archiwalną;

c._____ będą przetwarzane _____, a później będą archiwizowane przez _____ zgodnie z instrukcją archiwalną;

PRAWA OSÓB FIZYCZNYCH

1. Każda osoba fizyczna, której administrator przetwarza dane osobowe ma prawo:

a. jeżeli przetwarzanie danych osobowych odbywa się na podstawie zgody, to wycofać tę zgodę w dowolnym momencie;

b. otrzymać od administratora kopię swoich danych osobowych oraz szczegółowe informacje dotyczące przetwarzania tych danych osobowych;

c. zażądać zmiany lub uzupełnienia swoich danych osobowych, które są niepoprawne, niekompletne lub nieaktualne;

d. zażądać usunięcia swoich danych osobowych, jeżeli zachodzą uzasadnione prawnie okoliczności;

e. zażądać we wskazanym zakresie ograniczenia przetwarzania swoich danych osobowych, jeżeli zachodzą uzasadnione prawnie okoliczności;

f. zażądać przesłania swoich danych osobowych przez administratora do innego wskazanego administratora, jeżeli jest to technicznie możliwe i jeżeli zachodzą uzasadnione prawnie okoliczności;

g. wnieść sprzeciw w stosunku do przetwarzania jej danych, jeżeli zachodzą uzasadnione prawnie okoliczności;

h. nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu i wywołuje wobec niej skutki prawne lub w inny sposób na nią wpływa;

i. wnieść skargę do Urzędu Ochrony Danych Osobowych jeżeli uważa, że realizacja prawa lub procesy przetwarzania są zgodne z obowiązującymi przepisami.

2. Realizacja każdego żądania wymaga wcześniejszej weryfikacji tożsamości, zbadania zasadności i możliwości prawnych realizacji żądanego prawa.

3. W ciągu 30 dni od złożenia żądania administrator zobowiązany jest zrealizować żądanie lub odmówić realizacji żądania.

4. Odmowa realizacji żądania zawsze musi zawierać uzasadnienie.

miejscowość, data	*podpis osoby fizycznej, której dane dotyczą*

Załącznik Nr 2 do Załącznika Nr 7

Wniosek o udostępnienie danych - osoba fizyczna

WNIOSEK
1. Wniosek wypełnia osoba, która go składa. 2. Wniosek należy wypełnić drukowanymi literami. 3. Wniosek należy wypełnić zgodnie z wytycznymi, pod rygorem nierozpatrzenia wniosku zgodnie z art. 64 § 2 Kodeksu postępowania administracyjnego. 4. Jeżeli wniosek nie jest składany w imieniu własnym należy dołączyć do wniosku dokument potwierdzający umocowanie prawne do reprezentowania zgodnie z Kodeksem postępowania administracyjnego. 5. Do wniosku należy dołączyć wszystkie niezbędne _____.

1. **DANE ADMINISTRATORA**	
Nazwa administratora:	
Adres administratora:	

2. **DANE SKŁADAJĄCEGO WNIOSEK**	
Imię i nazwisko:	
Adres zamieszkania:	
Numer PESEL:	
Wniosek składany jest w imieniu:	
☐	własnym;
☐	innej osoby fizycznej.
Moje uprawnienie do reprezentowania wnioskującego wynika z załączonego do wniosku:	
☐	upoważnienia[1];
☐	pełnomocnictwa[2];
☐	orzeczenia sądu [x];
☐	
[1] – upoważnienie musi być dostarczone bezpośrednio przez osobę, której dane dotyczą; [2] – pełnomocnictwo musi być dostarczone przez osobę, której dane dotyczą lub przez inną osobę jeżeli będzie to pełnomocnictwo notarialne lub osoba dostarczająca ma prawo zgodnie z przepisami Unijnymi lub krajowymi poświadczyć autentyczność pełnomocnictwa; [x] – orzeczenie sądu musi być dołączone do wniosku.	

3. **DANE WNIOSKUJĄCEGO[3]**	
Imię i nazwisko:	
Adres zamieszkania:	
Numer PESEL :	
[3] – uzupełniamy tylko jeżeli wniosek składany jest w imieniu innej osoby	

4. **INFORMACJĘ DOTYCZĄCE UDOSTĘPNIENIA**	
zakres danych[4]:	
podstawa prawna[5]:	
cel przetwarzania[6]:	
[4] – należy napisać jaki zakres danych osobowych ma podlegać udostępnieniu; [5] – należy napisać na jakiej podstawie prawnej odbyć miałby się udostępnienie; [6] – należy napisać w jakim celu przetwarzane będą dane osobowe / do czego mają być wykorzystane.	

5. **LISTA ZAŁĄCZNIKÓW DO WNIOSKU**	
NAZWA ZAŁĄCZNIKA	CZEGO DOTYCZY

6. **FORMA UDZIELENIA ODPOWIEDZI**	
Proszę o komunikować się ze mną przez:	
☐	adres e-mail;

Proszę wpisać adres skrzynki e-mail. Wpisujemy drukowanymi literami.	
☐ adres korespondencyjny;	
Proszę wpisać adres korespondencyjny. Wpisujemy drukowanymi literami.	
☐ odbiór osobisty;	
Proszę napisać w jaki sposób poinformować o przygotowaniu odpowiedzi.	
☐ profil zaufany;	
Proszę podać nazwę użytkownika.	
☐ W inny sposób;	
Proszę napisać jakim sposobem dostarczyć odpowiedź.	

miejscowość, data	*podpis osoby fizycznej, której dane dotyczą*

INFORMACJE DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH ZAMIESZCZONYCH WE WNIOSKU

TOŻSAMOŚĆ I DANE KONTAKTOWE ADMINISTRATORA

Administratorem przetwarzającym dane osobowe jest _____.
Z administratorem można skontaktować się:
·telefonicznie - _____; (telefon stacjonarny bądź komórka)
·pisemnie - _____; (adres e-mail)
·osobiście lub pisemnie - _____. (adres siedziby, korespondencyjny)

DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH

Z inspektorem ochrony danych można skontaktować się:
·telefonicznie - _____; (telefon stacjonarny bądź komórka)
·pisemnie - _____; (adres e-mail)
·osobiście lub pisemnie - _____; (adres siedziby, korespondencyjny)

CEL I PODSTAWA PRAWNA PRZETWARZANIA ORAZ KATEGORIE DANYCH OSOBOWYCH

Dane osobowe przetwarzane są lub będą:
·w celu weryfikacji tożsamości i umocowań prawnych do reprezentowania na podstawie kodeksu postępowania administracyjnego w zakresie imienia, nazwiska, adresu zamieszkania, numeru PESEL składającego wniosek i osoby w imieniu, której składamy wniosek.
·w celu udzielenia odpowiedzi na wniosek na podstawie udzielonej zgody w zakresie adres email, korespondencyjny, telefon kontaktowy.

WYMOGI I KONSEKWENCJE

1.Podanie/udostępnienie danych osobowych w zakresie imienia, nazwiska i adresu zamieszkania jest wymagane na podstawie Kodeksu postępowania administracyjnego.
Osoba fizyczna, której dane dotyczą jest zobowiązana do ich podania.
W przypadku odmowy podania/udostępnienia danych osobowych wniosek zostanie nierozpatrzony.
2.Podanie/udostępnienie danych osobowych w zakresie numeru PESEL jest wymagane na podstawie prawnie uzasadnionego interesu realizowanego przez administratora.
Osoba fizyczna, której dane dotyczą nie jest zobowiązana do ich podania.
W przypadku odmowy podania/udostępnienia danych osobowych wniosek zostanie nierozpatrzony.
3.Podanie/udostępnienie danych osobowych w zakresie adresu e-mail lub korespondencyjnego lub telefonu kontaktowego nie jest wymagane ale konieczne do udzielenia odpowiedzi na wniosek.
W przypadku odmowy podania/udostępnienia danych osobowych odpowiedź na wniosek zostanie wysłana na adres zamieszkania.

ŹRÓDŁO POCHODZENIA DANYCH OSOBOWYCH

Wszystkie dane osobowe zostały pobrane od osoby składającej wniosek.

INFORMACJE O ODBIORCACH DANYCH OSOBOWYCH

Następujące podmioty będą miały dostęp do danych osobowych we wskazanych zakresach:
a._____, z siedzibą _____ - zakres danych osobowych _____;

b._____, z siedzibą _____ - zakres danych osobowych _____;
c._____, z siedzibą _____ - zakres danych osobowych _____;
d._____, z siedzibą _____ - zakres danych osobowych _____.

CZAS PRZETWARZANIA DANYCH OSOBOWYCH

Następujące dane osobowe będą przetwarzane we wskazanym czasie:

a._____ będą przetwarzane _____, a później będą archiwizowane przez _____ zgodnie z instrukcją archiwalną;

b._____ będą przetwarzane _____, a później będą archiwizowane przez _____ zgodnie z instrukcją archiwalną;

c._____ będą przetwarzane _____, a później będą archiwizowane przez _____ zgodnie z instrukcją archiwalną;

PRAWA OSÓB FIZYCZNYCH

1. Każda osoba fizyczna, której administrator przetwarza dane osobowe ma prawo:

a. jeżeli przetwarzanie danych osobowych odbywa się na podstawie zgody, to wycofać tę zgodę w dowolnym momencie;

b. otrzymać od administratora kopię swoich danych osobowych oraz szczegółowe informacje dotyczące przetwarzania tych danych osobowych;

c. zażądać zmiany lub uzupełnienia swoich danych osobowych, które są niepoprawne, niekompletne lub nieaktualne;

d. zażądać usunięcia swoich danych osobowych, jeżeli zachodzą uzasadnione prawnie okoliczności;

e. zażądać we wskazanym zakresie ograniczenia przetwarzania swoich danych osobowych, jeżeli zachodzą uzasadnione prawnie okoliczności;

f. zażądać przesłania swoich danych osobowych przez administratora do innego wskazanego administratora, jeżeli jest to technicznie możliwe i jeżeli zachodzą uzasadnione prawnie okoliczności;

g. wnieść sprzeciw w stosunku do przetwarzania jej danych, jeżeli zachodzą uzasadnione prawnie okoliczności;

h. nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu i wywołuje wobec niej skutki prawne lub w inny sposób na nią wpływa;

i. wnieść skargę do Urzędu Ochrony Danych Osobowych jeżeli uważa, że realizacja prawa lub procesy przetwarzania są zgodne z obowiązującymi przepisami.

2. Realizacja każdego żądania wymaga wcześniejszej weryfikacji tożsamości, zbadania zasadności i możliwości prawnych realizacji żądanego prawa.

3. W ciągu 30 dni od złożenia żądania administrator zobowiązany jest zrealizować żądanie lub odmówić realizacji żądania.

4. Odmowa realizacji żądania zawsze musi zawierać uzasadnienie.

miejscowość, data	*podpis osoby fizycznej, której dane dotyczą*

Załącznik Nr 3 do Załącznika Nr 7

Ewidencja udostępnionej dokumentacji

IMIĘ I NAZWISKO PRACOWNIKA	KOMÓRKA ORGANIZACYJNA I STANOWISKO	RODZAJ DOKUMENTU	ZAKRES INFORMACJI ZAWARTYCH W DOKUMENTACH	W JAKIM CELU BĘDĄ POTRZEBNE DOKUMENTY?	TECHNICZNE I ORGANIZACYJNE ŚRODKI BEPIECZEŃSTWA	ADMINISTRATOR ZATWIERDZIŁ / NIE ZATWIERDZIŁ	DATA ZATWIERDZENIA / NIE ZATWIERDZENIA PRZEZ ADMINISTRATORA	DATA UDOSTĘPNIENIA PRACOWNIKOWI KOPII	DATA ZDANIA KOPII PRZEZ PRACOWNIKA

Załącznik Nr 8 do zarządzenia Nr 715/2021
Burmistrza Miasta i Gminy Kąty Wrocławskie
z dnia 08 kwietnia 2021 r.

PROCEDURA USUWANIA DANYCH OSOBOWYCH

PROCEDURA USUWANIA DANYCH OSOBOWYCH

SIPIS TREŚCI

I. WPROWADZENIE

1.Niniejsza procedura jest integralną częścią Polityki, jednakże Polityka jest nadrzędnym dokumentem w stosunku do procedury.
2.Niniejsza procedura określa zasady usuwania danych osobowych
3.Wprowadzenie niniejszej procedury jest niezbędne ze względu na:
a.zapewnienie ograniczenia przechowywania danych osobowych zgodnie z art. 5 rozporządzenia UE 2016/679;
b.zapewnienie rozliczalności przestrzegania zasad przetwarzania danych osobowych, o których mowa w art. 5 rozporządzenia UE 2016/679.
4.Niniejsza procedura ma zastosowanie do wszystkich danych osobowych przetwarzanych w formie tradycyjnej oraz elektronicznej przez administratora, w imieniu administratora lub w imieniu innych administratorów.
5.Jeżeli przepisy unijne lub krajowe w inny sposób regulują postanowienia niniejszej procedury, to niniejsza procedura w zakresie w jakim regulują to przepisy nie obowiązuje.
6.Z niniejszą procedurą musi zapoznać się:
a.każdy pełnomocnik administratora;
b.każdy kierownik;
c.każdy pracownik przechowujący dane osobowe lub je usuwający;
d.cały zespół bezpieczeństwa danych.
7.Zamiany niniejszej procedury lub jej załączników wymagają zgody administratora oraz inspektora ochrony danych i są wprowadzane pod ich ścisłym nadzorem.

II. WYKAZ

1.Kierownik w obrębie własnej komórki organizacyjnej tworzy wykaz zawierający:
a.terminy usunięcia danych osobowych;
b.sposoby ich usunięcia.
2.Opracowany wykaz musi zostać zatwierdzony przez zespół bezpieczeństwa danych.
3.Wszystkie zmiany w wykazie muszą być wprowadzane za zgodą zespołu bezpieczeństwa danych lub na jego polecenie.
4.Wszystkie aktualne wykazy, po zatwierdzeniu przez zespół bezpieczeństwa danych, przekazywane są do IOD.
5.Kierownik odpowiada za aktualizację wykazu i za jego przestrzeganie w obrębie własnej komórki organizacyjnej.

III. USUWANIE

1.Kierownik może wyznaczyć pracownika, własnej komórki organizacyjnej, odpowiedzialnego za usuwanie danych osobowych.
2.Osoba odpowiedzialna za usuwanie danych opisuje cały proces w protokole z usunięcia (załącznik do procedury) oraz wpisuje proces do „rejestru usuwania" (załącznik do procedury), chyba że będzie można w inny sposób otrzymać informacje zawarte w tych załącznikach.

3.Kierownik nadzoruje proces usuwania danych osobowych, w obrębie własnej komórki organizacyjnej.

IV. WZORY I DOKUMENTY

1.Zastosowanie mają następujące wzory dokumentów będące załącznikami do niniejszej procedury:
a.„08. Wykaz terminów i sposobów usunięcia danych osobowych";
b.„08. protokół z usunięcia danych osobowych".
2.W wyniku stosowania niniejszej procedury powstanie dokumentacja zawierająca dane osobowe lub/oraz informacje poufne o jednostce przetwarzającej dlatego administrator wyznacza osoby odpowiedzialne za przechowywanie w następujących zakresach:
a.kierownik w obrębie własnej komórki organizacyjnej – protokoły z przeprowadzonych procesów usunięcia danych osobowych;
b.kierownik w obrębie własnej komórki organizacyjnej – wykazy zwierające aktualne informacje;
c.IOD w obrębie całej jednostki przetwarzającej – wykazy zawierające aktualne informacje z wszystkich komórek organizacyjnych.
3.Przechowywanie, archiwizowanie, modyfikowanie, ujawnianie, udostępnianie, niszczenie lub usuwanie i innego rodzaju przetwarzanie załączników lub treści w nich zawartych odbywa się zgodnie ze stosowną procedurą, chyba, że nie zawierają danych osobowych to zgodnie z przepisami unijnymi lub krajowymi lub uregulowaniami wewnętrznymi.

V. POSTANOWIENIA KOŃCOWE

1.Nadzór nad niniejszą procedurą sprawują:
a.IOD w pełnym zakresie;
b.każdy kierownik w obrębie własnej komórki organizacyjnej;
c.każdy pełnomocnik administratora w zakresie udzielonego pełnomocnictwa:
d.każdy upoważniony w zakresie nadanego upoważnienia;
2.Każdy kto nie przestrzega niniejszej procedury a jest do tego zobowiązany na mocy przepisów unijnych lub krajowych lub na mocy wyrażonego oświadczenia woli, ponosi odpowiedzialność za wszelkie szkody powstałe z powodu tego zaniechania zgodnie z Kodeksem Cywilnym, Kodeksem Pracy, Rozporządzeniem UE 2016/679 bądź innymi przepisami adekwatnymi do zaistniałej sytuacji.
3.Niniejsza procedura obowiązuję z dniem _____.

VI. METRYKA

aktualna wersja:		numer zarządzenia:	

Zakres aktualizacji	Data aktualizacji	Wprowadził aktualizacje	Zatwierdził aktualizacje

Załącznik Nr 1 do Załącznika Nr 8

Wykaz terminów i sposobów usunięcia danych osobowych

Nazwa zbioru danych osobowych	Kategorie danych	Termin przechowywania	Sposób usunięcia	Aktualnie przetwarzane? TAK / NIE

Załącznik Nr 2 do Załącznika Nr 8

PROTOKÓŁ Z USUNIĘCIA DANYCH OSOBOWYCH

PROTOKÓŁ Z USUNIĘCIA DANYCH OSOBOWYCH	
	_____, dnia _____ r.
1. Osoba przeprowadzająca proces usuwania danych osobowych.	
1.1 Imię i nazwisko:	
1.2 Stanowisko:	
1.3 Komórka organizacyjna.	
2. Sposób przeprowadzenia procesu usunięcia.	
2.1 Opis procesu[1]:	
2.2 Forma przetwarzania[2]:	
3. Zakres danych podlegających usunięciu.	
3.1 Nazwa zbioru[3]:	
3.2 Kategorie osób[4]:	
3.3 Zakres danych[5]:	
4. Przyczyna usunięcia.	
4.1 Podstawa usunięcia[6]:	

[1] - jaką metodą będą usuwane dane osobowe, jak będzie przebiegał proces usunięcia;
[2] -czy usunięcie danych osobowych dotyczy dokumentacji papierowej czy danych przetwarzanych elektronicznie; jeżeli dotyczy danych przetwarzanych elektronicznie, to należy wskazać z jakich aplikacji i systemów są usuwane;
[3] – nazwa zbioru danych z którego są usuwane dane osobowe;
[4] – kategoria osób, których dane osobowe są usuwane;
[5] – zakres usuwanych danych osobowych;
[6] – z czego wynika inicjacja usunięcia np. z ustalonej procedury lub z realizacji żądania osoby, której dane dotyczą, itp.

Załącznik Nr 9 do zarządzenia Nr 715/2021
Burmistrza Miasta i Gminy Kąty Wrocławskie
z dnia 08 kwietnia 2021 r.

PROCEDURA UPUBLICZNIANIA DANYCH OSOBOWYCH

SIPIS TREŚCI

I. WPROWADZENIE

1.Niniejsza procedura jest integralną częścią Polityki, jednakże Polityka jest nadrzędnym dokumentem w stosunku do procedury.
2.Niniejsza procedura określa zasady upubliczniania danych osobowych.
3.Wprowadzenie niniejszej procedury jest niezbędne ze względu na:
a.zapewnienie przestrzegania 6 zasad przetwarzania danych osobowych, w tym udostępniania, o których mowa w art. 5 rozporządzenia UE 2016/679;
b.zapewnienie spełnienia co najmniej jednego z sześciu warunków przetwarzania danych osobowych, w tym udostępnienia, o których mowa w art. 6 rozporządzenia UE 2016/679;
c.zapewnienie rozliczalności przestrzegania zasad przetwarzania danych osobowych, o których mowa w art. 5 rozporządzenia UE 2016/679.
4.Niniejsza procedura ma zastosowanie do wszystkich czynności związanych z upublicznianiem danych osobowych.
5.Jeżeli przepisy unijne lub krajowe w inny sposób regulują postanowienia niniejszej procedury to niniejsza procedura w zakresie w jakim regulują to przepisy nie obowiązuje.
6.Z niniejszą procedurą musi zapoznać się:
a.każdy pełnomocnik administratora;
b.każdy kierownik;
c.każdy pracownik odpowiedzialny za publikację informacji, w tym za upublicznianie danych osobowych;
d.cały zespół bezpieczeństwa danych.
7.Zmiany niniejszej procedury lub jej załączników wymagają zgody administratora oraz inspektora ochrony danych i są wprowadzane pod ich ścisłym nadzorem.

II. PODSTAWOWE ZASADY

1.Kierownik, w obrębie własnej komórki organizacyjnej, prowadzi rejestr upublicznionych danych osobowych zawierający co najmniej:
a.zakres danych osobowych, który będzie upubliczniany;
b.podstawę prawną do upublicznienia;
c.miejsce upublicznienia danych osobowych;
d.terminy usunięcia upublicznionych danych osobowych.
2.Kierownik przed dokonaniem zmian lub wprowadzaniem nowych pozycji do rejestru musi otrzymać pozytywną rekomendację IOD oraz administratora.
3.Administrator lub IOD nadzoruje, monitoruje i kontroluje prowadzenie rejestru upublicznionych danych osobowych przez kierowników.
4.IOD w oparciu o przekazywane rejestry upublicznianych danych osobowych, prowadzi rejestr wszystkich upublicznianych danych osobowych w jednostce przetwarzające.

III. PODSTAWY PRAWNE I CEL

1.Kierownik odpowiedzialny jest za ustalenie podstawy prawnej do upublicznienia danych osobowych.
2.Podsiadanie bezspornej podstawy prawnej do upublicznienia danych osobowych jest warunkiem koniecznym.
3.Następujące podstawy prawne we wskazanym zakresie dopuszczają możliwość upublicznienia danych osobowych:
a.zgoda osoby fizycznej, której dane dotyczą (lub opiekuna prawnego), w zakresie niezbędnym do realizacji celu przetwarzania danych osobowych wskazanego podczas pobierania zgody;
b.umowa z osobą fizyczną, której dane osobowe dotyczą w zakresie niezbędnym do realizacji tej umowy;
c.obowiązek prawny, wynikający z przepisów prawa, w zakresie niezbędnym do realizacji tego obowiązku;
d.ochrona i obrona żywotnych interesów osób fizycznych, w zakresie niezbędnym do zapewnienia tej ochrony i obrony;
e.interes publiczny lub władza publiczna wynikająca z przepisów prawa w zakresie niezbędnym do realizacji tego interesu lub władzy publicznej;
f.interes prawny wynikający z przepisów prawa, w zakresie niezbędnym do realizacji tego interesu.
4.Zgoda na upublicznienie danych osobowych wyrażona przez osobę, której dane dotyczą, musi być przedstawiona w sposób pozwalający ją wyraźnie odróżnić od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem oraz w sposób możliwy do wykazania, że faktycznie zgoda został wyrażona.
5.Upubliczniając dane osobowe w ramach umowy z osobą fizyczną, której dane dotyczą należy upewnić się, że upublicznienie danych jest warunkiem koniecznym do realizacji tej umowy.
6.Realizując obowiązek prawny, interes publiczny lub władzę publiczną, osoba upubliczniająca dane osobowe musi upewnić się, że faktycznie przepisy zobowiązują do upublicznienia danych osobowych we wskazanym zakresie lub, że upublicznienie danych osobowych jest niezbędne do realizacji obowiązku prawnego, interesu publicznego lub władzy publicznej.
7.Upubliczniając dane osobowe w ramach żywotnego interesu należy upewnić się, że upublicznienie danych osobowych jest warunkiem niezbędnym do obrony lub ochrony życia lub zdrowia osoby fizycznej.
8.Upubliczniając dane osobowe w ramach prawnie uzasadnionego interesu musimy się upewnić czy faktyczny interes prawny jest nadrzędny w stosunku do interesów osoby fizycznej, której dane osobowe dotyczą i czy nie narusza jej prywatności i prawa do ochrony danych osobowych.

IV. ZAKRES DANYCH

1.Zakres upublicznianych danych musi być zgodny z zasadną minimalizacji danych, czyli dane muszą być adekwatne, stosowne i ograniczone do tego co niezbędne aby zrealizować cel upublicznienia danych.
2.Jeżeli zakres upublicznianych danych osobowych nie wynika z przepisów unijnych lub krajowych to ich zakres musi być ograniczony do tego co niezbędne do realizacji celu upublicznienia.

V. OKRES UPUBLICZNIANIA

1.Każda upubliczniona dana osobowa musi mieć ustalony okres publikacji.
2.Jeżeli przepisy krajowe lub unijne wskazują okres upublicznienia należy bezwzględnie stosować się do tego terminu.
3.Jeżeli przepisy unijne lub krajowe nie wskazują okres upublicznienia danych, musi on zostać ustalony zgodnie z zasadą ograniczenia przechowywania, czyli mogą być one upubliczniane przez okres nie dłuższy niż jest to niezbędne do realizacji celu upublicznienia.

VI. WZORY I DOKUMENTY

1.Zastosowanie mają następujące wzory dokumentów będące załącznikami do niniejszej procedury:
a.„09. Rejestr upublicznionych danych osobowych"
2.Przechowywanie, archiwizowanie, modyfikowanie, ujawnianie, udostępnianie, niszczenie lub usuwanie i innego rodzaju przetwarzanie załączników lub treści w nich zawartych odbywa się zgodnie ze stosowną procedurą, chyba, że nie zawierają danych osobowych to zgodnie z przepisami unijnymi lub krajowymi lub uregulowaniami wewnętrznymi.

VII. POSTANOWIENIA KOŃCOWE

1.Nadzór nad niniejszą procedurą sprawuję:
a.IOD w pełnym zakresie;

b.każdy kierownik w obrębie własnej komórki organizacyjnej;
c.każdy pełnomocnik administratora w zakresie udzielonego pełnomocnictwa:
d.każdy upoważniony w zakresie nadanego upoważnienia;
2.Każdy kto nie przestrzega niniejszej procedury a jest do tego zobowiązany, na mocy przepisów unijnych lub krajowych lub na mocy wyrażonego oświadczenia woli, ponosi odpowiedzialność za wszelkie szkody powstałe z powodu tego zaniechania zgodnie z Kodeksem Cywilnym, Kodeksem Pracy, Rozporządzeniem UE 2016/679 bądź innymi przepisami adekwatnymi do zaistniałej sytuacji.
3.Niniejsza procedura obowiązuję z dniem _____.

VIII. METRYKA

aktualna wersja:		numer zarządzenia:	

Zakres aktualizacji	Data aktualizacji	Wprowadził aktualizacje	Zatwierdził aktualizacje

Załącznik Nr 1 do Załącznika Nr 9

Rejestr upublicznionych danych osobowych

OPIS UPUBLICZNIANYCH DANYCH OSOBOWYCH	ZAKRES DANYCH OSOBOWYCH	MIEJSCE UPUBLICZNIENIA DANYCH OSOBOWYCH	DATA PUBLIKACJI DANYCH OSOBOWYCH	TRERMIN USUNIĘCIA DANYCH OSOBOWYCH	PODSTAWA PRAWNA UPUBLICZNIENIA DANYCH OSOBOWYCH

Załącznik Nr 10 do zarządzenia Nr 715/2021
Burmistrza Miasta i Gminy Kąty Wrocławskie
z dnia 08 kwietnia 2021 r.

PROCEDURA PRACY ZDALNEJ

PROCEDURA PRACY ZDALNEJ

SPIS TREŚCI

I. WPROWADZENIE

1.Niniejsza procedura jest integralną częścią Polityki, jednakże Polityka jest nadrzędnym dokumentem w stosunku do procedury.
2.Niniejsza procedura określa zasady przetwarzania danych osobowych podczas wykonywania pracy zdalnej.
3.Wprowadzenie niniejszej procedury jest niezbędne ze względu na:
a.zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych podczas pracy zdalnej oraz zapewnienie realizacji obowiązków administratora, o których mowa między innymi w art. 24 i 32 rozporządzenia UE 2016/679;
b.zapewnienie przestrzegania zasad przetwarzania danych osobowych, o których mowa w art. 5 rozporządzenia UE 2016/679;
c.zapewnienie rozliczalności przestrzegania zasad przetwarzania danych osobowych, o których mowa w art. 5 rozporządzenia UE 2016/679.
4.Niniejsza procedura ma zastosowanie do wszystkich przypadków pracy zdalnej bez względu na czas jej trwania, jeżeli podczas niej mają być przetwarzane dane osobowe.
5.Jeżeli przepisy unijne lub krajowe w inny sposób regulują postanowienia niniejszej procedury, to niniejsza procedura, w zakresie w jakim regulują to przepisy, nie obowiązuje.
6.Z niniejszą procedurą musi zapoznać się:
a.każdy pełnomocnik administratora;
b.każdy kierownik;
c.każdy pracownik wykonujący pracę zdalną;
d.cały zespół bezpieczeństwa danych.
7.Zmiany niniejszej procedury lub jej załączników wymagają zgody administratora oraz IOD i są wprowadzane pod ich ścisłym nadzorem.

II. OBOWIĄZKI

1.Administrator zobowiązuję zespół bezpieczeństwa danych do:
a.ustalenia minimalnych wymagań zapewniających bezpieczeństwo podczas pracy zdalnej;
b.ustalenia zasad wykonywania pracy zdalnej;
c.ustalenia procedury zgłaszania awarii i naruszeń podczas pracy zdalnej;
d.przygotowania sprzętu niezbędnego do wykonania pracy zdalnej.
2.Administrator zobowiązuję kierowników, w obrębie własnej komórki organizacyjnej, do:
a.prowadzenia ewidencji sprzętu wykorzystywanego do pracy zdalnej;
b.prowadzenia ewidencji udostępnianej papierowo dokumentacji wykorzystywanej do pracy zdalnej;

c.ustalenia zadań do wykonania dla każdego pracownika oddelegowanego do pracy zdalnej;
d.przekazania wszystkich ważnych merytorycznie informacji pracownikowi oddelegowanemu do pracy zdalnej;
e.oddelegowania pracownika na szkolenia dotyczące bezpieczeństwa podczas wykonywania pracy zdalnej.
3.Każdy pracownik oddelegowany do pracy zdalnej zobowiązany jest:
a.przestrzegania Polityki i innych procedur dotyczących pracy zdalnej;
b.wykonywania poleceń przełożonych i zespołu bezpieczeństwa danych;
c.zobowiązany jest być dyspozycyjny w godzinach ustalonych z kierownikiem;
d.realizować wszystkie zadania zgodnie z obowiązującymi umowami i poleceniami;
e.zapewnić poufność swojej pracy i bezpieczeństwo danych osobowych i innych poufnych informacji.

III. ROZPOCZĘCIE PRACY ZDALNEJ

1.Oddelegowanie do pracy zdalnej odbywa się na podstawie złożonego przez pracownika wniosku.
2.Wniosek o oddelegowanie do pracy zdalnej pracownik składa kierownikowi i zwierać musi co najmniej:
a.uzasadnienie;
b.okres wykonywania pracy zdalnej;
c.informacje opisowe dotyczące sposobu wykonywania pracy zdalnej;
d.zapotrzebowanie na sprzęt niezbędny do wykonywania pracy zdalnej.
3.Kierownik po otrzymaniu wniosku kolejno:
a.sprawdza czy wniosek zawiera wszystkie niezbędne informacje;
b.opiniuje zasadność wniosku;
c.przekazuje administratorowi do rozpatrzenia wniosek i swoje uzasadnienie.
4.Administrator uzasadnia każdą swoją decyzję a w przypadku wyrażenia zgody na pracę zdalną kolejno:
a.przekazuje swoją decyzję kierownikowi, którego pracownik będzie wykonywać pracę zdalną;
b.przekazuje zespołowi bezpieczeństwa danych konieczność przygotowania stanowiska do pracy zdalnej.
5.ZBD wraz z kierownikiem ustala:
a.jaki sprzęt i jakie systemy będą wykorzystywane do pracy zdalnej;
b.jaki będzie dostęp do baz danych i informacji niejawnych podczas pracy zdalnej;
c.jakie minimalne wymagania musi spełniać obszar, na którym wykonywana będzie praca zdalna;
d.jakie dokumenty może pobrać pracownik i w jakiej formie;
e.jak będzie odbywała się komunikacja z pracownikiem wykonującym pracę zdalną.

IV. ZAKOŃCZENIE PRACY ZDALNEJ

1.Po zakończeniu pracy zdalnej pracownik kolejno:
a.zdaje sprzęt przeznaczony do pracy zdalnej;
b.zadaje dokumentację pobraną do pracy zdalnej;
2.Kierownik po zakończeniu pracy zdalnej pracownika kolejno:
a.sprawdza czy sprzęt został zdany w niepogorszonym stanie;
b.odnotowuje w prowadzonej ewidencji zdanie sprzętu;
c.sprawdza kompletność zdanej dokumentacji;
d.odnotowuje w prowadzonej ewidencji zdają dokumentacje

V. ZASADY I ZAKAZY

1.Wykonując pracę zdalną pracownik musi przestrzegać następujących zasad:
a.minimalizacji danych – należy wykorzystywać tylko te dane osobowe i informacje, które są niezbędne do wykonania pracy zdalnej;
b.rzetelność i przejrzystość – należy rzetelnie wykonywać pracę zdalną w sposób przejrzysty dla potrzeb ewentualnych kontroli;
c.poufność – należy zachować najwyższą poufność co do sposobu wykonywania pracy zdalnej, zastosowanych rozwiązań zapewniających bezpieczeństwo, wykorzystywanych danych osobowych i innych informacji niejawnych;
d.integralność – należy niezwłocznie uaktualniać wszystkie pozyskane dane osobowe i inne informację poufne w taki sposób aby inne osoby upoważnione do ich wykorzystania dysponowały aktualnymi danymi;
e.bezpieczeństwo – należy stosować co najmniej takie środki bezpieczeństwa jakie panują w jednostce przetwarzającej chyba, że inne wymagania zostaną wskazane przez kierownika bądź zespół bezpieczeństwa danych;
f.dostępność – należy być dyspozycyjnym, w zakresie wcześniej ustalonym,, zapewniając ciągłość wykonywania

zadań służbowych;
g.rozliczalność – należy być w stanie wykazać realizację powyższych zasad i poddawać się ewentualnym kontrolom.
2.Wykonując pracę zdalną pracownik musi przestrzegać następujących zakazów:
a.sprzęt – zakaz korzystania z innego sprzętu niż przeznaczonego do pracy zdalnej;
b.konta – zakaz korzystania z innych kont niż przeznaczonych do pracy zdalnej;
c.dokumenty – zakaz zabierania oryginałów dokumentów z jednostki przetwarzającej;
d.niszczenie – zakaz niszczenia dokumentacji wykorzystywanej do pracy zdalnej poza jednostką przetwarzającą

VI. NARUSZENIA I AWARIE

1.Każdy pracownik, który zaobserwuje, że doszło do naruszenia niezwłocznie zobowiązany jest postępować zgodnie z procedurą postępowania z naruszeniem.
2.Każdy pracownik, który zaobserwuje, że doszło do awarii urządzenia, systemu, aplikacji lub programu ma obowiązek niezwłocznie poinformować o tym zespół bezpieczeństwa danych i działać zgodnie z ich wytycznymi.
3.W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić je do zespołu bezpieczeństwa danych i postępować zgodnie z ich wytycznymi oraz procedurą postępowania z naruszeniem.

VII. KONTROLE

1.Następujące osoby we wskazanych zakresach mogą dokonywać kontroli:
a.administrator – w każdym zakresie;
b.inspektor ochrony danych – w zakresie bezpieczeństwa przetwarzanych danych osobowych;
c.zespół bezpieczeństwa danych – w każdym zakresie adekwatnym do przyczyny kontroli.
2.Pracownik nie może utrudniać kontroli kontrolującemu, ma obowiązek wykonywać jego polecenia i wspierać go w przeprowadzanej kontroli.
3.Kontrolujący ma prawo:
a.wglądu do danych poufnych w zakresie niezbędnym do przeprowadzenia kontroli;
b.żądać od kontrolowanego wyjaśnień, informacji, dokumentów niezbędnych do prowadzenia kontroli;
c.nakazać pracownikowi w określonym terminie uregulować wykryte uchybienia;
d.zakazać dalszej pracy pracownikowi, jeżeli wykryte zostało wysokie ryzyko naruszenia bezpieczeństwa.

VIII. WZORY I DOKUMENTY

1.Zastosowanie mają następujące wzory dokumentów będące załącznikami do niniejszej procedury:
a.„10. Ewidencja udostępnionej dokumentacji";
b.„10. Ewidencja urządzeń wykorzystywanych do pracy zdalnej";
c.„10. Oświadczenie."
2.W wyniku stosowania niniejszej procedury powstanie dokumentacja zawierająca dane osobowe lub/oraz informacje poufne o jednostce przetwarzającej dlatego administrator wyznacza osoby odpowiedzialne za przechowywanie w następujących zakresach:
a.Ewidencje w oryginale przechowuję kierownik, zgodnie z obowiązującymi instrukcjami archiwalnymi;
b.Podpisane oświadczenia przechowywane są w aktach pracowniczych.
3.Przechowywanie, archiwizowanie, modyfikowanie, ujawnianie, udostępnianie, niszczenie lub usuwanie i innego rodzaju przetwarzanie załączników lub treści w nich zawartych odbywa się zgodnie ze stosowną procedurą, chyba, że nie zawierają danych osobowych to zgodnie z przepisami unijnymi lub krajowymi lub uregulowaniami wewnętrznymi.

IX. POSTANOWIENIA KOŃCOWE

1.Nadzór nad niniejszą procedurą sprawuję:
a.IOD w pełnym zakresie;
b.każdy kierownik w obrębie własnej komórki organizacyjnej;
c.każdy pełnomocnik administratora w zakresie udzielonego pełnomocnictwa:
d.każdy upoważniony w zakresie nadanego upoważnienia;
2.Każdy kto nie przestrzega niniejszej procedury a jest do tego zobowiązany, na mocy przepisów unijnych lub krajowych lub na mocy wyrażonego oświadczenia woli, ponosi odpowiedzialność za wszelkie szkody powstałe z powodu tego zaniechania zgodnie z Kodeksem Cywilnym, Kodeksem Pracy, Rozporządzeniem UE 2016/679 bądź innymi przepisami adekwatnymi do zaistniałej sytuacji.

3.Niniejsza procedura obowiązuję z dniem _____.

X. METRYKA			
aktualna wersja:		numer zarządzenia:	

Zakres aktualizacji	Data aktualizacji	Wprowadził aktualizacje	Zatwierdził aktualizacje

Załącznik Nr 1 do Załącznika Nr 10

Ewidencja udostępnionej dokumentacji

IMIĘ I NAZWISKO PRACOWNIKA	KOMÓRKA ORGANIZACYJNA I STANOWISKO	RODZAJ DOKUMENTU	ZAKRES INFORMACJI ZAWARTYCH W DOKUMENTACH	W JAKIM CELU BĘDĄ POTRZEBNE DOKUMENTY?	TECHNICZNE I ORGANIZACYJNE ŚRODKI BEPIECZEŃSTWA	ADMINISTRATOR ZATWIERDZIŁ / NIE ZATWIERDZIŁ	DATA ZATWIERDZENIA / NIE ZATWIERDZENIA PRZEZ ADMINISTRATORA	DATA UDOSTĘPNIENIA PRACOWNIKOWI KOPII	DATA ZDANIA KOPII PRZEZ PRACOWNIKA

Załącznik Nr 2 do Załącznika Nr 10

Ewidencja urządzeń wykorzystywanych do pracy zdalnej

NUMER EWIDENCYJNY URZĄDZENIA	RODZAJ URZĄDZENIA	APLIKACJE, SYSTEMY I PROGRAMY	URZĄDZENIE WŁASNE LUB SŁUŻBOWE	ZASTOSOWANE ZABEZPIECZENIA	UŻYTKOWNIK	OSOBA KONTROLUJĄCA	DATA ROPOCZĘCIA PRACY ZDALNEJ	DATA ZAKOŃCZENIA PRACY ZDALNEJ	UWAGI

Załącznik Nr 3 do Załącznika Nr 10

Oświadczenie

OŚWIADCZENIE
pracownika wykonującego pracę zdalną

miejscowość i data:

Pracownik
Imię i nazwisko:

Komórka organizacyjna:

Stanowisko:

Pracodawca
Nazwa jednostki:

Adres siedziby:

Administrator:

Oświadczam, że administrator przekazał mi a ja zapoznałem się z:
a. procedurą pracy zdalnej;
b. politykami bezpieczeństwa informacji;
c. zasadami bezpieczeństwa i higieny pracy.

Ponadto zobowiązuję się do:
a. stosowania postanowień procedury pracy zdalnej oraz innych polityk bezpieczeństwa informacji oraz zasad bezpieczeństwa i higieny pracy;
b. zachowania w poufności wszystkich informacji pozyskanych związku z wykonywaniem pracy, a w szczególności informacji dotyczących danych osobowych, danych poufnych, technicznych i organizacyjnych środków bezpieczeństwa;
c. przetwarzania danych osobowych tylko w zakresie adekwatnym, stosownym i ograniczonym do zakresu obowiązków służbowych zgodnie z zasadą minimalizacji danych osobowych;
d. zgłaszania każdego naruszenia bezpieczeństwa niezwłocznie po wykryciu;
e. zapewnienia największego możliwego bezpieczeństwa przetwarzanych danych osobowych i danych poufnych;
f. wspierania osób kontrolujących bezpieczeństwo pracy zdalnej i wykonywania ich poleceń.

Oznajmiam, że zostałem przeszkolony z następujących zakresów:
a. bezpieczeństwo i higiena pracy;
b. bezpieczeństwo informacji w systemach;
c. bezpieczeństwo danych osobowych;
d. _____

Zostałem poinformowany, że złamanie zasad określonych w Regulaminie Pracy Zdalnej lub złamanie postanowień złożonego oświadczenia będzie stanowić naruszenie obowiązków pracowniczych.

podpis administratora (pracodawca)
podpis oświadczającego (pracownik)

	miejscowość i data:	
Pracownik		**Pracodawca**

Imię i nazwisko: Komórka organizacyjna: Stanowisko:	Nazwa jednostki: Adres siedziby: Administrator:

Oświadczam, że administrator przekazał mi a ja zapoznałem się z:

a. procedurą pracy zdalnej;

b. politykami bezpieczeństwa informacji;

c. zasadami bezpieczeństwa i higieny pracy.

Ponadto zobowiązuję się do:

a. stosowania postanowień procedury pracy zdalnej oraz innych polityk bezpieczeństwa informacji oraz zasad bezpieczeństwa i higieny pracy;

b. zachowania w poufności wszystkich informacji pozyskanych związku z wykonywaniem pracy, a w szczególności informacji dotyczących danych osobowych, danych poufnych, technicznych i organizacyjnych środków bezpieczeństwa;

c. przetwarzania danych osobowych tylko w zakresie adekwatnym, stosownym i ograniczonym do zakresu obowiązków służbowych zgodnie z zasadą minimalizacji danych osobowych;

d. zgłaszania każdego naruszenia bezpieczeństwa niezwłocznie po wykryciu;

e. zapewnienia największego możliwego bezpieczeństwa przetwarzanych danych osobowych i danych poufnych;

f. wspierania osób kontrolujących bezpieczeństwo pracy zdalnej i wykonywania ich poleceń.

Oznajmiam, że zostałem przeszkolony z następujących zakresów:

a. bezpieczeństwo i higiena pracy;

b. bezpieczeństwo informacji w systemach;

c. bezpieczeństwo danych osobowych;

d. _____

Zostałem poinformowany, że złamanie zasad określonych w Regulaminie Pracy Zdalnej lub złamanie postanowień złożonego oświadczenia będzie stanowić naruszenie obowiązków pracowniczych.

podpis administratora (pracodawca)	podpis oświadczającego (pracownik)

Załącznik Nr 11 do zarządzenia Nr 715/2021
Burmistrza Miasta i Gminy Kąty Wrocławskie
z dnia 08 kwietnia 2021 r.

PROCEDURA POSTĘPOWANIA Z NARUSZENIEM

SPIS TREŚCI

I. WPROWADZENIE

1.Niniejsza procedura jest integralną częścią Polityki, jednakże Polityka jest nadrzędnym dokumentem w stosunku do procedury.
2.Niniejsza procedura określa sposób postępowania w przypadku wykrycia naruszenia ochrony danych osobowych
3.Wprowadzenie niniejszej procedury jest niezbędne ze względu na:
a.zapewnienie poprawnej realizacji obowiązków wynikających z art. 33 i 34 rozporządzenia UE 2016/679;
b.zapewnienie zgodności z prawem, o której mowa w art. 5 rozporządzenia UE 2016/679;
c.zapewnienie rozliczalności przestrzegania zasad przetwarzania danych osobowych, o których mowa w art. 5 rozporządzenia UE 2016/679.
4.Niniejsza procedura dotyczy wszystkich naruszeń ochrony danych osobowych bez względu na wielkość ryzyka.
5.Jeżeli przepisy unijne lub krajowe w inny sposób regulują postanowienia niniejszej procedury, to niniejsza procedura w zakresie w jakim regulują to przepisy nie obowiązuje.
6.Z niniejszą procedurą musi się zapoznać:
a.każdy pełnomocnik administratora;
b.każdy kierownik;
c.każdy pracownik przetwarzający dane osobowe;
d.cały zespół bezpieczeństwa danych.
7.Zmiany niniejszej procedury lub jej załączników wymagają zgody administratora oraz inspektora ochrony danych i są wprowadzane pod ich ścisłym nadzorem.

II. IDENTYFIKACJA NARUSZENIA

1.Do naruszenia dochodzi jeżeli mamy do czynienia z przypadkowym lub niezgodnym z prawem:
a.zniszczeniem danych osobowych;
b.utraceniem danych osobowych;
c.zmodyfikowaniem danych osobowych;
d.ujawnieniem danych osobowych;
e.udostępnieniem danych osobowych.
2.Ustalając, czy mamy do czynienia z naruszeniem bierzemy pod uwagę tylko powyższe okoliczności natomiast skala ryzyka nie ma znaczenia.

III. ZGŁOSZENIE NARUSZENIA

1.Pracownik, który zaobserwował, że doszło do naruszenia zobowiązany jest niezwłocznie powiadomić bezpośredniego przełożonego.
2.Ponadto pracownik, który zaobserwował, że doszło do naruszenia zobowiązany jest:
a.zaprzestać przetwarzania danych osobowych do czasu otrzymania innych poleceń od przełożonego;
b.sporządzić notatkę (załącznik „Notatka uczestnika NODO") z naruszenia i przekazać ją do IOD, administratora i kierownika;
c.zachować wszystkie okoliczności naruszenia w poufności.

IV. DZIAŁANIA ZARADCZE

1.Kierownik po otrzymaniu informacji o naruszeniu niezwłocznie podejmuje wszystkie niezbędne działania minimalizujące ryzyko naruszenia prawa i wolności osób, których dane osobowe są przetwarzane.
2.Kierownik w szczególności zobowiązany jest do:
a.wstrzymania przetwarzania danych osobowych, których naruszanie dotyczy, do czasu upewnienia się, że ponowne przetwarzanie danych osobowych nie będzie powodować kolejnych naruszeń;
b.podjęcia możliwych do natychmiastowej realizacji działań minimalizujących skutki naruszenia;
c.poinformowania zespołu bezpieczeństwa danych i administratora o powstałym naruszeniu;
d.działania zgodnie z wytycznymi administratora i zespołu bezpieczeństwa danych.
3.Zespół bezpieczeństwa danych po otrzymaniu informacji o naruszeniu, nie później niż w ciągu 24 godzin, przygotowuje zalecenia dotyczące dalszego działania i przekazuje je:
a.administratorowi;
b.kierownikowi komórki organizacyjne, w której naruszenie wstąpiło;
c.odpowiednim członkom bezpieczeństwa danych.

V. ANALIZA RYZYKA

1.IOD po otrzymaniu notatki z naruszenia niezwłocznie ale nie później niż w ciągu 24 godzin przeprowadza analizę ryzyka naruszenia praw i wolności osób, których dane osobowe dotyczą.
2.IOD przekazuje administratorowi oraz kierownikowi komórki organizacyjnej w której naruszenie wystąpiło:
a.wyniki analizy;
b.wytyczne dotyczące dalszych działań.
3.IOD nadzoruje realizację wszystkich dalszych działań.

VI. ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ

1.Jeżeli wyniki analizy ryzyka wskazują, że doszło do naruszenia, które powoduje wysokie ryzyko naruszenia prawa i wolności osoby fizycznej to należy niezwłocznie zawiadomić tę osobę o naruszeniu.
2.Zawiadamianie, o którym mowa powyżej, nie jest obowiązkowe w przypadku gdy:
a.administrator wdrożył odpowiednie techniczne i organizacyjne środki zaradcze, w szczególności takie jak szyfrowanie uniemożliwiające odczyt danych osobowych;
b.administrator zastosował środki eliminujące wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą;
c.wymagałoby ono niewspółmiernie dużego wysiłku - w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostanie podobny środek, za pomocą którego osoby, których dane dotyczą zostaną poinformowane w równie skuteczny sposób o naruszeniu.
3.Jeżeli stwierdzono, że nie ma obowiązku zawiadamiania osoby fizycznej o naruszeniu to musi to pisemnie potwierdzić IOD uzasadniając taką decyzję.
4.Jeżeli IOD stwierdzi po dokonaniu dodatkowej analizy, że należy zawiadomić osobę fizyczną o naruszeniu, to zawiadomienie musi być dokonane niezwłocznie.
5.Za przygotowanie treści zawiadomienia o naruszeniu odpowiedzialny jest kierownik komórki organicznej, w której wystąpiło.
6.Przed wysłaniem zawiadomienia o naruszeniu IOD musi zaopiniować jego treść i formę.

VII. ZAWIADOMIENIE UODO

1.Jeżeli wyniki analizy ryzyka wskazują, że doszło do naruszenia, które powoduje ryzyko naruszenia prawa i wolności osoby fizycznej to należy niezwłocznie, ale nie później niż w ciągu 72 godzin od wykrycia naruszenia, powiadomić o tym Prezesa Urzędu Ochrony Danych Osobowych.
2.Zawiadomienie o naruszeniu sporządza i przesyła do Urzędu Ochrony Danych Osobowych administrator lub jego

pełnomocnik.
3.Zawiadomienie o naruszeniu sporządza się zgodnie wytycznymi Prezesa Urzędu Ochrony Danych Osobowych znajdującymi się pod linkiem: https://uodo.gov.pl/pl/134/233.

VIII. ZAWIADOMIENIE ADMINISTRATORA

1.Jeżeli doszło do naruszenia powierzonych danych osobowych to należy niezwłocznie powiadomić administratora tych danych lub współadministratora.
2.Powyższe zawiadomienie przeprowadza kierownik komórki organizacyjnej odpowiedzialnej za współpracę z administratorem tych danych lub współadministratorem.

IX. RAPORT Z NARUSZENIA

1.Administrator lub jego pełnomocnik po realizacji działań zaradczych i dokonaniu niezbędnych zawiadomień sporządza raport z naruszenia i przesyła go do zespołu bezpieczeństwa danych.
2.Raport wykonywany jest zgodnie z załącznikiem „raport administratora z NODO".
3.Zespół bezpieczeństwa danych zatwierdza raport oraz wskazane w nim działania zapobiegawcze, może także wskazać konieczność zastosowania innych lub dodatkowych działań.
4.Jeżeli zespół bezpieczeństwa danych wskaże konieczność zastosowania innych lub dodatkowych działań zapobiegawczych to musi to uzasadnić i przekazać administratorowi do realizacji.

X. REJESTR NARUSZEŃ

1.Administrator dokumentuje wszelkie naruszenia, w tym jego okoliczności, skutki oraz podjęte działania zaradcze.
2.Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania niniejszej procedury.
3.Rejestr naruszeń jest załącznikiem do niniejszej procedury.

XI. DZIAŁANIA ZAPOBIEGAWCZE

1.Administrator na podstawie sporządzonego i zatwierdzonego przez zespół bezpieczeństwa danych raportu zleca realizację działań zapobiegawczych.
2.Wdrażane działa zapobiegawcze są nadzorowane przez administratora.

XII. WZORY I DOKUMENTY

1.Zastosowanie mają następujące wzory dokumentów będące załącznikami do niniejszej procedury:
a.Analiza Ryzyka NODO;
b.Notatka uczestnika NODO;
c.Raport administratora z NODO;
d.Rejestr NODO;
e.zawiadomienie o naruszeniu.
2.W wyniku stosowania niniejszej procedury powstanie dokumentacja zawierająca dane osobowe lub/oraz informacje poufne o jednostce przetwarzającej dlatego administrator wyznacza IOD jako osobę odpowiedzialną za przechowywanie całej dokumentacji wynikającej z NODO.
3.Przechowywanie, archiwizowanie, modyfikowanie, ujawnianie, udostępnianie, niszczenie lub usuwanie i innego rodzaju przetwarzanie załączników lub treści w nich zawartych odbywa się zgodnie ze stosowną procedurą, chyba, że nie zawierają danych osobowych to zgodnie z przepisami unijnymi lub krajowymi lub uregulowaniami wewnętrznymi.

XIII. POSTANOWIENIA KOŃCOWE

1.Nadzór nad niniejszą procedurą sprawuję:
a.IOD w pełnym zakresie;
b.każdy kierownik w obrębie własnej komórki organizacyjnej;
c.każdy pełnomocnik administratora w zakresie udzielonego pełnomocnictwa:
d.każdy upoważniony w zakresie nadanego upoważnienia;
2.Każdy kto nie przestrzega niniejszej procedury a jest do tego zobowiązany, na mocy przepisów unijnych lub krajowych lub na mocy wyrażonego oświadczenia woli, ponosi odpowiedzialność za wszelkie szkody powstałe z powodu tego zaniechania zgodnie z Kodeksem Cywilnym, Kodeksem Pracy, Rozporządzeniem UE 2016/679 bądź innymi przepisami adekwatnymi do zaistniałej sytuacji.
3.Niniejsza procedura obowiązuję z dniem _____.

XIV. METRYKA			
aktualna wersja:		numer zarządzenia:	

Zakres aktualizacji	Data aktualizacji	Wprowadził aktualizacje	Zatwierdził aktualizacje

Analiza Ryzyka NODO

ANALIZOWANY OBSZAR| jakie elementy bierzemy pod uwagę dokonując analizy ryzyka |	**DOKŁADNE INFORMACJE**| wpisujemy dokładnie jakich informacji dotyczy analizowany obszar |	**WYTYCZNE DOTYCZĄCE ANALIZY**| na jakiej podstawie należy ustalić skale ryzyka |	**SKALA RYZYKA**| punkty do wyboru|	**MAKS PKT.**
RODZAJ DANYCH OSOBOWYCH		**Punkty sumujemy**1 pkt. - imię i nazwisko, numer klienta, ID, login, numer polisy, numer zamówienia; 2 pkt - PESEL, numer dokumentu tożsamości; 3 pkt - telefon kontaktowy, adres e-mail (nie zawierający danych); 4 pkt - adres korespondencyjny, adres e-mail (zawierający dane), konta społecznościowe; 5 pkt - adres zamieszkania, adres pobytu, informacje o podróżach; 6 pkt - zdjęcia, nagrania, informacje o rodzinie; 7 pkt - zarobki, renta, emerytur; 8 pkt - świadczenia, zobowiązania, sytuacja finansowa; 9 pkt - niedyspozycyjność zdrowotna, L4, opiekuńcze, wychowawcze; 10 pkt - pochodzenie rasowe i etniczne, poglądy polityczne, przekonania religijne i światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualność i orientacja seksualna, wyroki skazujące, naruszenia prawa.		55
LICZBA OSÓB, KTÓRYCH DOTYCZY NODO		**za każdą osobę 1 pkt.**Powyżej 50 osób zgłaszamy do UODO		50
ILOŚĆ DANYCH OSOBOWYCH		**za każdą pojedynczą dane 2 pkt.**powyżej 20 danych zgłaszamy do UODO		40
MOŻLIWOŚĆ IDENTYFIKACJI OSOBY FIZYCZNEJ NA PODSTAWIE DANYCH OSOBOWYCH, KTÓRYCH DOTYCZY NODO		**wybieramy jedną pozycję**1 pkt. nie ma możliwości identyfikacji 10 pkt. osoba jest możliwa do zidentyfikowania 20 pkt. osoba jest zidentyfikowana w otoczeniu powstania naruszenia		20
AKTUALNOŚĆ DANYCH		**wybieramy jedną pozycję**1 pkt - dane osobowe były niepoprawne; 10 pkt - dane osobowe były już nieaktualne; 20 pkt - dane osobowe były niepełne lub niekompletne; 30 pkt - dane osobowe były aktualne		30
CZY DANE OSOBOWE MIAŁY JAKIEŚ ZNACZENIE W MIEJSCU NARUSZNIA?		**wybieramy jedną pozycję**1 pkt - nie miały żadnego znaczenia; 50 pkt - mogły mieć jakieś znaczenie		50

MAX PKT (100%)	195

UZYSKANO PKT	**0**
PROCENTOWO	**0%**

Notatka uczestnika NODO

NOTATKA UCZESTNIKA NARUSZENIA OCHRONY DANYCH OSOBOWYCH	
DANE UCZESTNIKA	
Imię i nazwisko:	
Komórka organizacyjna:	
Stanowisko:	
Telefon:	
E-mail:	
SZCZEGÓŁOWY OPIS ZDARZENIA	
Gdzie miało miejsce zdarzenie?	
Kiedy miało miejsce zdarzenie (data i godzina)?	
Czy byli inni uczestnicy zdarzenia? Jeżeli tak to należy podać dane identyfikacyjne tych osób.	
OPIS ZDARZENIA	
MATERIAŁY DOWODOWE	
Należy opisać załączone materiały dowodowe (np. wiadomość e-mail, SMS).	
Nazwa załącznika	Opis zawartości
1.	
2.	
3.	
4.	
data sporządzenia, miejscowość	czytelny podpis uczestnika

Raport administratora z NODO

RAPORT ADMINISTRATORA Z NODO	
DANE ADMINISTRATORA LUB PEŁNOMOCNIKA	
Imię i nazwisko:	
Stanowisko:	
SZCZEGÓŁOWY OPIS ZDARZENIA	
Data powstania NODO:	
Data wykrycia NODO:	
Jakich danych osobowych NODO dotyczy?	
Opis zdarzenia zawierający w szczególności: - kategorie osób; - kategorie danych; - sposób przetwarzania; - sposób uzyskania informacji o NODO; - inne istotne okoliczności.	

PODJĘTE DZIAŁANIA ZARADCZE
Działania zaradcze – działania minimalizujące skutki powstałego NODO
1.
2.
3.
4.
5.

ANALIZA RYZYKA I SKUTKI NODO	
Czy wynik analizy ryzyka wskazuje na wysokie ryzyko naruszenia prawa lub wolności osoby fizycznej, której NODO dotyczy?	
Jakie skutki prawne może powodować NODO w stosunku do osoby fizycznej, której naruszenie dotyczy?	
ZAWIADOMIENIA	
Czy powiadomiono osobę fizyczną o NODO?	
Dlaczego nie powiadomiono osoby fizycznej o NODO?	
W jaki sposób powiadomiono osobę fizyczną o NODO?	
Kiedy powiadomiono osobę	

fizyczną o NODO?	
Czy powiadomiono UODO o NODO?	
Dlaczego nie powiadomiono UODO o NODO?	
W jaki sposób powiadomiono UODO o NODO?	
Kiedy powiadomiono UODO o NODO?	

PLANOWANE DZIAŁANIA ZAPOBIEGAWCZE
Działania zapobiegawcze – działania, które mają zapobiegać powstaniu podobnych naruszeń w przyszłości.
1.
2.
3.
4.
5.

MATERIAŁ DOWODOWY	
Należy opisać załączone materiały dowodowe (np. wiadomość e-mail, SMS, notatki uczestników, zawiadomienia, opinie specjalistów).	
Nazwa załącznika	Opis zawartości
1.	
2.	
3.	
4.	

OPINIA INSPEKTORA OCHRONY DANYCH	
1.Czy zaobserwowano wysokie ryzyko naruszenia prawa lub wolności osoby fizycznej, której dane dotyczą?	
2.Czy podjęto wystarczające środki zaradcze, ewentualnie jakie jeszcze powinny zostać podjęte?	
3.Jakie działania zapobiegawcze należy podjąć, w jakim terminie?	

data sporządzenia, miejscowość	czytelny podpis administratora
data sporządzenia, miejscowość	czytelny podpis inspektora ochrony danych

Załącznik Nr 4 do Załącznika Nr 11

Rejestr NODO

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH										
LP.	DATA POWSTANIA NODO	DATA WYKRYCIA NODO	Kategoria naruszenia	OPIS NODO| liczba osób, których dotyczy NODO |liczba danych, rodzaj danych, kategorie przetwarzania, sposób przetwarzania, umyślność, osoby biorące udział w NODO, wszystkie istotne okoliczności |	SKUTKI NODO| dla osoby fizycznej, której dane dotyczą | potencjalne i faktyczne |	PODJĘTE DZIAŁANIA ZARADCZE| jakie działania podjęto w celu minimalizacji skutków NODO oraz jakie działania podjęto w celu zaradzeniu na przyszłość NODO |	WYNIK ANALIZY RYZYKA	DATA ZGŁOSZENIA DO UODO| jeżeli jest wysokie ryzyko (ryzyko = lub > 50%) |	NUMER NOTATKI| osoby, która brała udział w naruszeniu |	NUMER RAPORTU| wypełniony przez administratora |

Załącznik Nr 5 do Załącznika Nr 11

zawiadomienie o naruszeniu

ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

_____, _____

miejscowość, data

_____

_____

_____

_____

_____

Związku z obowiązkiem wynikającym z rozporządzenia 2016/679 (RODO) z przykrością informujemy, że doszło do naruszenia ochrony danych osobowych, mogącego powodować naruszenia Pani/Pana praw lub wolności. Posiada Pani/Pan prawo do złożenia skargi do Urzędu Ochrony Danych Osobowych oraz obrony swoich praw przed Sądem. We własnym zakresie poinformowaliśmy Prezesa Urzędu Ochrony Danych Osobowych o powstałym naruszeniu.

Poniżej podajemy szczegóły dotyczące naruszania.

1.OPIS ZDARZENIA PROWADZĄCEGO DO NARUSZNEIA

opisywać:

- kiedy powstało naruszanie;
- kiedy zostało wykryte naruszenia;
- jakich danych dotyczy naruszenie;
- w jaki sposób doszło do naruszenia;

2.MOŻLIWE KONSEKWENCJE
3.ZASTOSOWANE ŚRODKI ZARADCZE
4.DANE ADMINISTRATORA
5.DANE INSPEKTORA OCHRONY DANYCH

_____

czytelny podpis osoby uprawnionej

Załącznik Nr 12 do zarządzenia Nr 715/2021
Burmistrza Miasta i Gminy Kąty Wrocławskie
z dnia 08 kwietnia 2021 r.

PROCEDURA MONITORINGU

PROCEDURA MONITORINGU

SPIS TREŚCI

I. WPROWADZENIE

1.Niniejsza procedura jest integralną częścią Polityki, jednakże Polityka jest nadrzędnym dokumentem w stosunku do procedury.
2.Niniejsza procedura określa zasady funkcjonowania monitoringu wizyjnego.
3.Wprowadzenie niniejszej procedury jest niezbędne ze względu na:
a.zapewnienie realizowania zasad przetwarzania o których mowa w art. 5 rozporządzenia UE 2016/679;
b.zapewnienie rozliczalności przestrzegania zasad przetwarzania danych osobowych, o których mowa w art. 5 rozporządzenia UE 2016/679;
c.zapewnienia bezpieczeństwa danych, o którym mowa w art. 32 rozporządzenia UE 2016/679;
d.zapewnienie realizacji obowiązków administratora, o których mowa w art. 24 rozporządzenia UE 2016/679.
4.Niniejsza procedura ma zastosowanie do wszystkich danych osobowych pozyskanych związku z monitoringiem wizyjnym.
5.Jeżeli przepisy unijne lub krajowe w inny sposób regulują postanowienia niniejszej procedury to niniejsza procedura w zakresie w jakim regulują to przepisy nie obowiązuje.
6.Z niniejszą procedurą musi się zapoznać:
a.każdy pełnomocnik administratora;
b.każdy kierownik;
c.każdy pracownik mający dostęp do monitoringu;
d.każdy członek zespoły bezpieczeństwa danych.
7.Zmiany niniejszej procedury lub jej załączników wymagają zgody Administratora oraz IOD i są wprowadzane pod ich ścisłym nadzorem.

II. PODSTAWA PRAWNA I CELE

1.Monitoring wprowadzony jest na podstawie prawnie uzasadnionego interesu realizowanego przez administratora w celu:
a.zapewnienia bezpieczeństwa;
b.zapewnienia ochrony mienia;
c.ograniczenia zachowań niepożądanych i niedozwolonych oraz identyfikacja ich sprawców;
d.dochodzenia i obrony ewentualnych powstałych roszczeń.
2.Monitoring nie służy i nie może służyć do badania jakości wykonywanej pracy przez pracowników.

III. ZAKRES MONITORINGU

1.Monitoring składa się z 9 rejestratorów i obejmuje następujące lokalizacje:
a.Miejscowość Gniechowice – monitoring ustawiony na skrzyżowanie ulic kąteckiej i wrocławskiej;

b.Miejscowość Kąty Wrocławskie, ul. Zwycięstwa - monitoring ustawiony na Dom Kultury;
c.Miejscowość Kąty Wrocławskie, ul. Zwycięstwa - monitoring ustawiony na Targowisko Miejskie;
d.Miejscowość Kąty Wrocławskie, ul. Kościuszki - monitoring ustawiony na Stadion Miejski;
e.Miejscowość Kąty Wrocławskie - monitoring ustawiony na skrzyżowanie ulic 1-Maja i wrocławskiej;
f.Miejscowość Kąty Wrocławskie, ul. Drzymały - monitoring ustawiony na Przedszkole Publiczne w Kątach Wrocławskich;
g.Miejscowość Kąty Wrocławskie, ul. Kościuszki - monitoring ustawiony na plac zabaw;
h.Miejscowość Kąty Wrocławskie, ul. 1-Maja - monitoring ustawiony na Komisariat Policji w Kątach Wrocławskich;
i.Miejscowość Kąty Wrocławskie, ul Rynek-Ratusz 1 - monitoring ustawiony w budynku Urzędu Miasta i Gminy na główne drzwi wejściowe.
2.Monitoring nie rejestruje dźwięku.
3.Monitoring rejestruje obraz całodobowo.

IV. TERMIN PRZECHOWYWANIA

1.Nagrania z monitoringu przechowywane są przez 14 dni od utworzenia nagrania, chyba że:
a.osoba fizyczna, której dane dotyczą wniosła o usunięcie nagrania, na którym się znajduje;
b.osoba fizyczna, której dane dotyczą wniosła o ograniczenie przetwarzania;
c.nagranie jest niezbędne do obrony lub dochodzenia roszczeń;
d.nagranie jest niezbędne do toczącego się postępowania.
2.Po upływie określonego terminu nagrania podlegają usunięciu lub modyfikacji, która uniemożliwi identyfikację osób znajdujących się na nagraniach.

V. PRAWA OSÓB FIZYCZNYCH

1.Każda osoba fizyczna, której wizerunek został zarejestrowany i jest możliwa do identyfikacji ma prawo:
a.dostępu do informacji o przetwarzaniu oraz do treści niniejszego regulaminu;
b.uzyskać kopie nagrania, na którym został utrwalony jej wizerunek, chyba, że narusza to prawa innej osoby fizycznej;
c.żądać usunięcia jej nagrania, na którym został utrwalony jej wizerunek chyba, że administrator posiada inną podstawę prawną przechowywania nagrania;
d.żądać ograniczenia przetwarzania do ustalonego czasu i nie wolno wykorzystywać i usuwać tych nagrań chyba, że administrator posiada inną podstawę prawną.
2.Osoba fizyczna, która chce otrzymać kopie nagrania na którym została zarejestrowana musi złożyć wniosek zgodnie z Procedurą realizacji praw osób fizycznych.
3.Wnioski rozpatruje pracownik upoważniony do dostępu do nagrań po wcześniejszym zaopiniowaniu przez inspektora ochrony danych.

VI. ZAKRES DOSTĘPU DO DANYCH

1.Nagrania z monitoringu podlegają ochronie i mogą mieć do nich dostęp jedynie:
a.administrator;
b.osoby pisemnie upoważnione;
c.uprawnieni odbiorcy zgodnie z Procedurą udostępnienia danych;
d.podmioty przetwarzające na podstawie powierzenia przetwarzania;
e.osoby fizyczne, których wizerunek został zarejestrowany, na podstawie złożonego wniosku zgodnie z Procedurą realizacji praw osób fizycznych;
f.organy publiczne, które na mocy obowiązujących przepisów mogą mieć dostęp do danych, na podstawie złożonego wniosku zgodnie z „Procedurą udostępnienia danych osobowych".
2.Udostępniając nagranie anonimizujemy wizerunki osób, których cel udostępnienia nagrania nie dotyczy.
3.Udostępnione nagrania nie mogą naruszać prawa i wolności innych osób fizycznych.
4.Jeżeli anonimizacja, o której mowa w pkt. 2 nie jest technicznie możliwa, nagranie nie może zostać udostępnione.

VII. OBOWIĄZEK INFORMACYJNY

1.Przy wejściu na teren monitorowany zawieszone są tabliczki informujące o monitoringu i wskazujące administratora oraz dane kontaktowe do niego.
2.Przy rejestratorach w widocznych miejscach zamieszczone są tabliczki z informacją

o monitorowaniu.
3.Przy wejściu do jednostki przetwarzającej w widocznym miejscu zamieszcza się załącznik „klauzula monitoring".

VIII. WZORY I DOKUMENTY

1.W wyniku stosowania niniejszej procedury powstanie dokumentacja zawierająca dane osobowe lub/oraz informacje poufne o jednostce przetwarzającej dlatego administrator ustala iż za dokumenty wytworzone odpowiadają pracownicy merytorycznie prowadzący daną sprawę.
2.Przechowywanie, archiwizowanie, modyfikowanie, ujawnianie, udostępnianie, niszczenie lub usuwanie i innego rodzaju przetwarzanie załączników lub treści w nich zawartych odbywa się zgodnie ze stosowną procedurą, chyba, że nie zawierają danych osobowych to zgodnie z przepisami unijnymi lub krajowymi lub uregulowaniami wewnętrznymi.

IX. POSTANOWIENIA KOŃCOWE

1.Nadzór nad niniejszą procedurą sprawuję:
a.IOD w pełnym zakresie;
b.każdy kierownik w obrębie własnej komórki organizacyjnej;
c.każdy pełnomocnik administratora w zakresie udzielonego pełnomocnictwa:
d.każdy upoważniony w zakresie nadanego upoważnienia;
2.Każdy kto nie przestrzega niniejszej procedury a jest do tego zobowiązany, na mocy przepisów unijnych lub krajowych lub na mocy wyrażonego oświadczenia woli, ponosi odpowiedzialność za wszelkie szkody powstałe z powodu tego zaniechania zgodnie z Kodeksem Cywilnym, Kodeksem Pracy, Rozporządzeniem UE 2016/679 bądź innymi przepisami adekwatnymi do zaistniałej sytuacji.
3.Niniejsza procedura obowiązuję z dniem _____.

X. METRYKA

aktualna wersja:		numer zarządzenia:	

Zakres aktualizacji	Data aktualizacji	Wprowadził aktualizacje	Zatwierdził aktualizacje

Załącznik Nr 1 do Załącznika Nr 12

Klauzula monitoringu

MONITORING – INFORMACJE DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

TOŻSAMOŚĆ I DANE KONTAKTOWE ADMINISTRATORA

Administratorem przetwarzającym dane osobowe jest Burmistrz Miasta i Gminy Kąty Wrocławskie. Z administratorem można skontaktować się:

·telefonicznie – 71 390 72 00;

·osobiście lub pisemnie – Rynek 1, 55-080 Kąty Wrocławskie.

DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH

Z inspektorem ochrony danych można skontaktować się:

·telefonicznie – 513 850 227;

·pisemnie – rodo@katywroclawskie.pl;

·osobiście lub pisemnie - Rynek 1, 55-080 Kąty Wrocławskie.

CEL I PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH

Dane osobowe przetwarzane są lub będą:

·w celu _____ na podstawie _____;

·w celu _____ na podstawie _____.

ZAKRES MONITORINGU

Zakres monitoringu wskazany jest w procedurze monitoringu.

INFORMACJE O ODBIORCACH DANYCH OSOBOWYCH

Dostęp do nagrań z monitoringu mają tylko uprawnieni następujący odbiorcy:

·wyznaczeni pracownicy Urzędu Miasta i Gminy Kąty Wrocławskie.

CZAS PRZETWARZANIA DANYCH OSOBOWYCH

Nagrania monitoringu przechowywane są:

·przez _____ a następnie nagrania _____;

·do czasu zakończenia obrony lub dochodzenia roszczeń jeżeli zostały użyte w tym celu;

·do czasu zakończenia postępowań wszczętych na podstawie przepisów prawa jeżeli w takim celu zostały użyte.

PRAWA OSÓB FIZYCZNYCH

Każda osoba fizyczna, którą zarejestrował monitoring ma następujące prawa wynikające z rozporządzenia 2016/679:

·prawo dostępu do informacji o przetwarzaniu danych osobowych i do kopii nagrań, na których został zarejestrowany wizerunek;

·prawo do usunięcia nagrań, na których został utrwalony jej wizerunek lub anonimizacji wizerunku jeżeli na nagraniu utrwalone są także inne osoby fizyczne;

·prawo do ograniczenia przetwarzania (nie usuwania nagrania) do wskazanego przez nią czasu;

·prawo do złożenia skargi do Urzędu Ochrony Danych Osobowych.

Załącznik Nr 13 do zarządzenia Nr 715/2021
Burmistrza Miasta i Gminy Kąty Wrocławskie
z dnia 08 kwietnia 2021 r.

PROCEDURA WSPÓŁADMINISTROWANIA

SIPIS TREŚCI

I. WPROWADZENIE

1.Niniejsza procedura jest integralną częścią Polityki, jednakże Polityka jest nadrzędnym dokumentem w stosunku do procedury.
2.Niniejsza procedura określa zasady współadministrowania danych osobowych.
3.Wprowadzenie niniejszej procedury jest niezbędne ze względu na:
a.zapewnienie realizacji zasad przetwarzania, o których mowa w art. 5 rozporządzenia UE 2016/679;
b.zapewnienie rozliczalności przestrzegania zasad przetwarzania danych osobowych, o których mowa w art. 5 rozporządzenia UE 2016/679;
c.zapewnienie realizacji zasad wynikających z art. 24, 25 i 26 rozporządzenia UE 2016/679;
4.Jeżeli przepisy unijne lub krajowe w inny sposób regulują postanowienia niniejszej procedury to niniejsza procedura w zakresie w jakim regulują to przepisy nie obowiązuje.
5.Z niniejszą procedurą musi się zapoznać:
a.każdy pełnomocnik administratora;
b.każdy kierownik;
c.każdy pracownik.
6.Zamiany niniejszej procedury lub jej załączników wymagają zgody administratora oraz inspektora ochrony danych i są wprowadzane pod ich ścisłym nadzorem.

II. WSPÓŁADMINISTRATOR

1.Ze współadministrowaniem mamy do czynienia w następujących przypadkach:
a.kiedy przepisy unijne lub krajowe wskazują co najmniej dwóch administratorów do realizacji tej samej czynności przetwarzania;
b.kiedy co najmniej dwóch administratorów realizuje tą samą czynność przetwarzania i wspólnie ustalają cele i sposoby przetwarzania.

III. ZASADY

1.Jeżeli mamy do czynienia ze współadministrowaniem danymi osobowymi to należy nawiązać porozumienie regulujące następujące kwestie:
a.jakich kategorii osób fizycznych będzie dotyczyć przetwarzanie;
b.jaki zakres danych osobowych będzie przetwarzany;
c.w jakich celach będą przetwarzane dane osobowe;
d.jak długo będą przetwarzane dane osobowe;
e.czy wszyscy współadministratorzy dają gwarancję realizacji obowiązków wynikających z rozporządzenia (UE) 2016/679;
f.jakie są obowiązki współadministratorów związku z przetwarzaniem danych osobowych;
g.w jaki sposób realizowane są prawa osób fizycznych;
h.jak postępować w sytuacji wystąpienia naruszenia ochrony danych osobowych;

i.na jakich zasadach realizować powierzenie przetwarzania danych osobowych.
2.Szablon porozumienia stanowi załącznik do niniejszej procedury.
3.Kierownik komórki organizacyjnej, która odpowiedzialna jest za realizowanie czynności przetwarzania, która będzie współadministrowana, odpowiedzialny jest za nawiązanie porozumienia zgodnie z niniejszą procedurą.
4.Każde porozumienie dotyczące współadministrowania danymi osobowymi musi zostać zaakceptowane przez IOD i podpisane przez administratora.
5.Każdy współadministrator musi zostać wpisany do rejestru czynności przetwarzania przez IOD po zgłoszeniu nowego współadministratora, przez kierownika odpowiedzialnego za czynność przetwarzania.
6.Jeżeli którykolwiek współadministrator nie daje wystarczającej gwarancji realizacji wymogów niniejszej procedury to nie można z nim podpisać porozumienia, dopóki takiej gwarancji nie będzie mógł zapewnić.

IV. WZORY I DOKUMENTY

1.Zastosowanie mają następujące wzory dokumentów będące załącznikami do niniejszej procedury:
a.„13. Porozumienie" – dotyczące współadministrowania.
2.W wyniku stosowania niniejszej procedury powstanie dokumentacja zawierająca dane osobowe lub/oraz informacje poufne o jednostce przetwarzającej dlatego administrator wyznacza osoby odpowiedzialne za przechowywanie w następujących zakresach:
a.IOD – kopię zawartego porozumienia;
b.Pracownik merytoryczny – oryginał zawartego porozumienia.
3.Przechowywanie, archiwizowanie, modyfikowanie, ujawnianie, udostępnianie, niszczenie lub usuwanie i innego rodzaju przetwarzanie załączników lub treści w nich zawartych odbywa się zgodnie ze stosowną procedurą, chyba, że nie zawierają danych osobowych to zgodnie z przepisami unijnymi lub krajowymi lub uregulowaniami wewnętrznymi.

V. POSTANOWIENIA KOŃCOWE

1.Nadzór nad niniejszą procedurą sprawuję:
a.IOD w pełnym zakresie;
b.każdy kierownik w obrębie własnej komórki organizacyjnej;
c.każdy pełnomocnik administratora w zakresie udzielonego pełnomocnictwa:
d.każdy upoważniony w zakresie nadanego upoważnienia.
2.Każdy kto nie przestrzega niniejszej procedury a jest do tego zobowiązany, na mocy przepisów unijnych lub krajowych lub na mocy wyrażonego oświadczenia woli, ponosi odpowiedzialność za wszelkie szkody powstałe z powodu tego zaniechania zgodnie z Kodeksem Cywilnym, Kodeksem Pracy, Rozporządzeniem UE 2016/679 bądź innymi przepisami adekwatnymi do zaistniałej sytuacji.
3.Niniejsza procedura obowiązuję z dniem _____.

VI. METRYKA

aktualna wersja:		numer zarządzenia:	

Zakres aktualizacji	Data aktualizacji	Wprowadził aktualizacje	Zatwierdził aktualizacje

Załącznik Nr 1 do Załącznika Nr 13

Porozumienie

Porozumienie dotyczące współadministrowania danymi osobowymi

zawarte w dniu _____ pomiędzy:

nazwa podmiotu: _____
adres siedziby: _____
reprezentowany przez: _____

zwaną dalej **„Współadministratorem"**

a

nazwa podmiotu: _____
adres siedziby: _____
reprezentowany przez: _____

zwaną dalej **„Współadministratorem"**.

a

nazwa podmiotu: _____
adres siedziby: _____
reprezentowany przez: _____

zwaną dalej **„Współadministratorem"**.

a

nazwa podmiotu: _____
adres siedziby: _____
reprezentowany przez: _____

zwaną dalej **„Współadministratorem"**.

Łącznie zwanych **„Stronami"**

Mając na uwadze, że:

·Współadministratorzy wspólnie ustalają cele i sposoby przetwarzania danych osobowych związku z _____.

·Współadministratorzy mają zapewnić aby współadministrowanie danymi osobowymi odbywało się zgodnie z prawem, a zwłaszcza zgodnie z art. 26 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679.

Strony postanowiły zawrzeć porozumienie o następującej treści:

§ 1. Definicje

Użyte w porozumieniu określenia będą miały następujące znaczenie:

1. **Rozporządzenie (UE) 2016/679** – oznacza 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);

2. **Dane Osobowe** – oznacza dane w rozumieniu art. 4 pkt 1) Rozporządzenia (UE) 2016/679, tj. wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

3. **Naruszenie**– oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

4. **Przetwarzanie** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

§ 2. Przedmiot porozumienia

1. Przedmiotem niniejszego porozumienia jest określenie zasad przetwarzania oraz zabezpieczania danych osobowych, które wspólnie przetwarzają współadministratorzy.

2. Każdy współadministrator będzie odpowiednio wykonywał obowiązki określone w niniejszym porozumieniu również w przypadku uznania, że jest on samodzielnym administratorem.

§ 3. Przetwarzane dane osobowe

1. Strony oświadczają wspólnie, że w ramach niniejszego porozumienia przetwarzać będą następujące kategorie danych osobowych we wskazanych celach:

Kategoria osób fizycznych	Dane osobowe	Cel powierzenia przetwarzania	Termin usunięcia

2. Każdy ze współadministratorów oświadcza, że zarówno przed podpisaniem niniejszego porozumienia i w trakcie jego trwania wypełnia wszystkie obowiązki prawne wynikające z rozporządzenia (UE) 2016/679.

3. Jeżeli którykolwiek ze współadministratorów uzna, że podjęte działania zgodnie z niniejszym porozumieniem stanowią naruszenie prawa, zobowiązany jest niezwłocznie powiadomić wszystkich pozostałych współadministratorów.

§ 4. Obowiązki współadministratorów

1. Każdy współadministrator jest uprawniony do przetwarzania danych osobowych wyłącznie na potrzeby realizacji wskazanych celów.

2. Każdy współadministrator przetwarzając dane osobowe na podstawie zgody, zobowiązany jest do pobrania oświadczenia o wyrażeniu zgody w formie pisemnej, korzystając z załącznika do niniejszego porozumienia „zgoda - ____". Wszystkie pobrane zgody należy dostarczyć w formie skanu wszystkim pozostałym współadministratorom.

3. Osoby upoważnione przez każdego współadministratora do przetwarzania danych osobowych będą zobowiązane do zachowania ich oraz informacji o ich zabezpieczeniach w tajemnicy.

4. Każdy współadministrator podejmuje wszelkie środki wymagane na mocy art. 32 rozporządzenia (UE) 2016/679
w celu zapewnienia bezpieczeństwa danych osobowych.

5. Każdy ze współadministratorów zobowiązany jest realizować prawa osób fizycznych zgodnie z niniejszym porozumieniem i z rozdziałem III rozporządzenia (UE) 2016/679.

6. Każdy ze współadministratorów zobowiązany jest do udzielenia wszelkich niezbędnych informacji pozostałym współadministratorom niezbędnych do przeprowadzenia oceny skutków wynikającej z art. 35 rozporządzenia (UE) 2016/679 w przypadkach kiedy ona jest wymagana.

7. Każdy ze współadministratorów zobowiązany jest poinformować pozostałych współadministratorów o podjętych działaniach, które mogą wpłynąć na proces przetwarzania danych osobowych objętego niniejszym porozumieniem.

§ 5. Sposób realizacji praw osób fizycznych, których dane osobowe są przetwarzane

1. Jeżeli którykolwiek ze współadministratorów pozyskuje dane osobowe, których pozostali współadministratorzy nie posiadali, bezpośrednio od osoby fizycznej lub z innego źródła zobowiązany jest wypełnić obowiązek informacyjny zgodnie z art. 12-14 rozporządzenia (UE) 2016/679.

2. Spełniając obowiązek informacyjny należy korzystać z załącznika „obowiązek informacyjny - ____".

3. Jeżeli osoba fizyczna, której dane osobowe są przetwarzane, zażąda realizacji praw wynikających z rozdziału III rozporządzenia (UE) 2016/679 to rozpatruje i realizuje je współadministrator do którego ta osoba złożyła żądanie.

4. Jeżeli udzielenie odpowiedzi bądź zrealizowanie żądania wymaga zaangażowania innego lub wszystkich pozostałych współadministratorów, to należy niezwłocznie poinformować odpowiednich współadministratorów.

§ 6. Naruszenie ochrony danych osobowych

1. Współadministrator po stwierdzeniu naruszenia ochrony danych osobowych jest zobowiązany niezwłocznie poinformować wszystkich pozostałych współadministratorów o naruszeniu oraz wskazać następujące pozostałe informacje:

a.kiedy miało miejsce naruszenie i kiedy je stwierdzono;

b.jakiego zakresu danych dotyczy naruszenie;

c.jakiej liczby osób dotyczy naruszenie;

d.co było przyczyną naruszenia;

e.jakie konsekwencje mogą wyniknąć z naruszenia;

f.jakie działania zaradcze i zapobiegawcze podjęto.

2. Współadministrator, z winy którego powstało naruszenie, zobowiązany jest zrealizować wszystkie wymogi zgodnie z art. 33-34 rozporządzenia (UE) 2016/679.

3. Jeżeli związku z ryzykiem naruszenia praw osoby fizycznej należało zgłosić do Urzędu Ochrony Danych Osobowych zaistniałe naruszenie, to wszyscy współadministratorzy informowani są o wszystkich sprawach w ramach toczącego się postępowania.

4. Wszystkie kary finansowe związane z naruszaniem ochrony danych osobowych regulowane są przez współadministratora z winy, którego powstało naruszenie.

§ 7. Punkt kontaktowy

1. Każdy współadministrator z osobna ustala punkt kontaktowy dla osób fizycznych, których dane dotyczą.

2. W ramach punktu kontaktowego osoby fizyczne, których dane osobowe są przetwarzane mogą:

a.otrzymywać informacje dotyczące przetwarzania;

b.składać żądania dotyczące realizacji jej praw;

c.dostarczać i otrzymywać dokumenty dotyczące przetwarzania.

3. Ustala się następujące punkty kontaktowe:

Imię i nazwisko osoby kontaktowej	Adres punktu	Telefon do punktu	Adres e-mail punktu

§ 8. Powierzenie przetwarzania danych osobowych

1. Jeżeli, którykolwiek ze współadministratorów zamierza powierzyć przetwarzanie danych osobowych objętych niniejszym porozumieniem zewnętrznemu podmiotowi, zobowiązany jest poinformować o tym pozostałych współadministratorów.

2. Współadministrator, który powierza przetwarzanie danych osobowych zewnętrznemu podmiotowi przekazuje pozostałym współadministratorom następujące informacje:

a.nazwę i siedzibę podmiotu przetwarzającego;

b.zakres powierzonych danych osobowych;

c.cel powierzenia przetwarzania.

3. Współadministrator, który powierza dane osobowe jest zobowiązany zapewnić, iż podmiot przetwarzający, z którego usług zamierza korzystać przy przetwarzaniu danych osobowych, daje wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia (UE) 2016/679, a w szczególności art. 28 i chroniło prawa osób, których dane dotyczą.

4. Jeżeli którykolwiek ze współadministratorów złoży sprzeciw do powierzenia przetwarzania wskazanemu podmiotowi, to nie wolno już temu podmiotowi powierzyć danych osobowych.

5. Sprzeciw w stosunku do powierzenia danych osobowych podmiotowi zewnętrznemu musi zawsze zawierać uzasadnienie pod rygorem nieważności.

6. Jeżeli podmiot, któremu miało być powierzone przetwarzanie wykaże, że uregulował wszystkie uchybienia wskazane w uzasadnieniu do sprzeciwu i nie pojawiły się żadne nowe uchybienia, to może zostać ponownie rozpatrzone powierzenie mu przetwarzania danych osobowych.

§ 9. Postanowienia końcowe

1. Niniejsze porozumienie zostaje zawarte na czas _____.

2. Niniejsze porozumienie zostało sporządzone w ____ egzemplarzach.

3. Wszelkie zmiany lub uzupełnienia niniejszego porozumienia wymagają zachowania formy pisemnej pod rygorem nieważności.