Ośrodek Sportu i Rekreacji
w Głogowie Małopolskim
36-060 Głogów Małopolski, ul. Parkowa 15

ZARZĄDZENIE NR 0050.19.2025
DYREKTORA OŚRODKA SPORTU I REKREACJI W GŁOGOWIE MAŁOPOLSKIM
z dnia 5 maj 2025 r.

Na podstawie art. 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 rozporządzenie o ochronie danych), Dz. Urz. UE L Nr 119, s. 1.

zarządzam, co następuje:

§1

Wprowadzam w życie Politykę Ochrony Danych Osobowych w **Ośrodku Sportu i Rekreacji w Głogowie Małopolskim** stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§2

Zobowiązuję pracowników **Ośrodka Sportu i Rekreacji w Głogowie Małopolskim** do bezwzględnego stosowania i przestrzegania zasad zawartych w Polityce Ochrony Danych Osobowych.

§3

Na Inspektora Danych Osobowych sprawującego nadzór nad realizacją niniejszych zapisów wyznacza się Panią Justynę Ciechanowską.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

Dyrektor Ośrodka Sportu
i Rekreacji w Głogowie Małopolskim

Dyrektor OSIR w Głogowie Młp.

Andrzej Zwierzchowski

Andrzej Zwierzchowski

Ośrodek Sportu i Rekreacji
w Głogowie Małopolskim
36-060 Głogów Małopolski, ul. Parkowa 15

Załącznik nr 1 do Zarządzenia
Nr 0050.19.2025 Dyrektora Ośrodka
Sportu i Rekreacji w Głogowie
Małopolskim z dnia 05.05.2025 r.

Polityka Ochrony Danych Osobowych w Ośrodku Sportu i Rekreacji w Głogowie Małopolskim

Wstęp

Niniejszy dokument jest Polityką Ochrony Danych Osobowych w rozumieniu RODO - Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1).

§ 1

Cel i zakres polityki:

1. Celem Polityki jest przedstawienie zasad ochrony danych osobowych obowiązujących w **Ośrodku Sportu i Rekreacji w Głogowie Małopolskim (zwany dalej OSIR).**
2. Zakres przedmiotowy stosowania obejmuje wszystkie procesy przetwarzania danych osobowych w OSIR, zarówno w formie elektronicznej jak i papierowej.
3. Zakres podmiotowy obowiązuje wszystkich pracowników OSIR oraz inne osoby świadczące prace na rzecz OSIR upoważnione do przetwarzania danych osobowych.
4. Polityka ochrony uwzględnia:
   1) przepisy RODO,
   2) przepisy krajowe w zakresie ochrony danych osobowych,
   3) akty prawa wewnętrznego obowiązujące w OSIR,
5. W celu uszczegółowienia Polityki ochrony w OSIR mogą zostać opracowywane i wdrożone procedury, instrukcje i wytyczne dotyczące zidentyfikowanych procesów przetwarzania danych osobowych.

§ 2

Skróty i definicje

Słownik pojęć i definicji używanych w tym dokumencie:

1) **Polityka** lub **PODO** oznacza niniejszą Politykę ochrony danych osobowych,
2) **RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1),

3) **Dane** oznaczają **dane osobowe** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
4) **Szczególne kategorie danych osobowych** oznaczają dane specjalne i dane karne,
5) **Dane specjalne** oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej,
6) **Dane karne** oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa,
7) **Osoba** oznacza osobę fizyczną, której dane dotyczą.
8) **Przetwarzający / Podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora,
9) **Profilowanie** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się,
10) **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,
11) **Pseudonimizacja** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
12) **Anonimizacja** oznacza proces przetworzenia danych osobowych prowadzący do nieodwracalnego braku możliwości identyfikacji osoby, której dane dotyczą,

13) **Eksport danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej,
14) **Organ nadzorczy** oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51; (Prezes Urzędu Ochrony Danych Osobowych).
15) **IOD** lub **Inspektor** oznacza Inspektora Ochrony Danych w OSIR w Głogowie Małopolskim,
16) **ASI** oznacza osobę odpowiedzialną za system informatyczny,
17) **Rejestr** oznacza Rejestr Czynności Przetwarzania Danych Osobowych w OSIR w Głogowie Małopolskim,
18) **IZSI** – instrukcja zarządzania systemem informatycznym w OSIR w Głogowie Małopolskim,
19) **Ośrodek Sportu i Rekreacji w Głogowie Małopolskim** oznacza OSIR,
20) **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; 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,
21) **Odbiorca** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania,
22) **Pracownik** oznacza osobę fizyczną zatrudnioną w OSIR w Głogowie Małopolskim na podstawie stosunku pracy lub wykonującą umowę zlecenia lub inną umowę cywilno-prawną wymagającą dostępu do danych osobowych np. eksperta wykonującego pracę przy ocenie projektów; a także stażystę, praktykanta pracującego pod nadzorem wyznaczonego opiekuna, jeżeli program stażu, praktyki obejmuje wykonywanie zadań związanych z dostępem do danych osobowych,
23) **Współpracownik** oznacza osobę której zadania, dotyczące przetwarzania danych osobowych zostały określone w dokumentach dotyczących nawiązania współpracy mogą to być np. osoby zatrudnione w innych podmiotach świadczące pracę na rzecz OSIR w Głogowie Małopolskim, które w ramach swoich obowiązków służbowych uzyskują dostęp do danych osobowych przetwarzanych w wyżej wymienionym Inspektoracie (jeśli charakter świadczonych usług przez podmiot nie wpisuje się w tryb powierzenia przetwarzania danych),
24) **Zgoda osoby, której dane dotyczą** oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie

oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych,

25) **Podmiot danych** oznacza, osobę której dane są przetwarzane.
26) **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,
27) **Zbiór danych** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,
28) **Dane genetyczne** oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej,
29) **Dane biometryczne** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne,
30) **Dane dotyczące zdrowia** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia,

§3

Zarządzanie bezpieczeństwem danych osobowych

1. Za bezpieczeństwo danych osobowych przetwarzanych w OSIR w Głogowie Małopolskim w tym za wdrożenie i utrzymanie niniejszej Polityki odpowiedzialny jest Dyrektor OSIR, który w myśl przepisów RODO, jako Administrator/Przetwarzający/Współadministrator obowiązany jest zastosować środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia przy uwzględnieniu stanu wiedzy technicznej, kosztu wdrożenia oraz charakteru, zakresu, kontekstu i cele przetwarzania.

2. Za nadzór i monitorowanie przestrzegania Polityki odpowiadają:
   1) Inspektor Ochrony Danych wyznaczony przez Dyrektora OSIR,
   2) ASI wyznaczony przez Dyrektora OSIR,
3. Za stosowanie niniejszej Polityki odpowiedzialni są pracownicy, których zadania dotyczą przetwarzania danych osobowych,

4. Pracownicy których zadania dotyczą przetwarzania danych osobowych są odpowiedzialni za zapewnienie prawidłowego przetwarzania danych osobowych, w ramach zajmowanych stanowisk ponadto zobowiązani są do:
   1) współdziałania z IOD w sprawach związanych z bezpieczeństwem danych osobowych,
   2) wdrożenia w ramach zajmowanych stanowisk rozwiązań organizacyjnych i technicznych umożliwiających skuteczne realizowanie „obowiązku informacyjnego" wynikającego z RODO,
   3) podejmowania odpowiednich środków, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO (Klauzule informacyjne) oraz prowadzić z nią wszelką komunikację na mocy art. 15-22 i 34 RODO w sprawie przetwarzania. Informacji udziela na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie,
   4) jeżeli zgodność przetwarzania danych opiera się na zgodzie wyrażonej przez osobę, której dane dotyczą pracownik jest zobowiązany za posiadanie w formie pisemnej lub elektronicznej zgody z uwzględnieniem określonego celu lub celów przetwarzania i prowadzi rejestr zgód. (Załącznik Nr 1 - Klauzula zgody na przetwarzanie danych osobowych i informacja o prawie do jej cofnięcia),
   5) dopełnienia obowiązku uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych,
   6) powiadamiania IOD o przypadkach naruszenia ochrony danych osobowych nie później niż 24 godz. od stwierdzenia naruszenia (Załącznik Nr 13 - Wzór Raportu o naruszeniu danych osobowych),
   7) przedkładania aktualizacji „Rejestru czynności przetwarzania" lub/i „Rejestru kategorii czynności" dla zbiorów zidentyfikowanych w Urzędzie Miejskim w Głogowie Małopolskim według wzorów załączonych do PODO, przesyłanie pisemne i na e-mail do IOD (Załącznik Nr 2, 3) niezwłocznie po wystąpieniu zmian w zbiorze bądź odnotowaniu nowego zbioru. Rejestry podpisuje IOD, (Załącznik Nr 2 - Wzór Rejestru czynności przetwarzania i Załącznik Nr 3 - Rejestr kategorii czynności),
   8) dokonywania weryfikacji - przed wyborem podmiotu przetwarzającego, czy gwarantuje odpowiednie środki techniczne i organizacyjne dające możliwość spełnienia wymogów RODO,
   9) sporządzania umów (porozumień) powierzenia przetwarzania danych osobowych (w tym zawieranie zapisów dotyczących celu i zakresu przetwarzania, stosowania - zabezpieczeń określonych w RODO z podmiotami zewnętrznymi oraz kontrolowanie ich wykonania,
   10) aktualizacji „Ewidencji osób upoważnionych do przetwarzania danych osobowych" według Załącznika Nr 5, a następnie przedkładanie i przesyłanie jej do Pracownika ds. Kadr oraz IOD niezwłocznie po wystąpieniu zmian,

11) opracowanie dodatkowych procedur przetwarzania danych osobowych, nie ujętych w niniejszym dokumencie, ze względu na specyfikę zakresu działania OSIR, które będą obowiązywały po konsultacji z IOD i wprowadzeniu przez AD,
12) w przypadku zawarcia umów powierzenia, gdzie występujemy jako podmiot przetwarzający (procesor) pracownicy zobowiązani są do wykonania obowiązków nałożonych umowami (np. powiadamiania o incydencie, wykonanie praw osób, których dane dotyczą),
13) sporządzanie umów o współadministrowaniu oraz wykonywanie obowiązków nałożonych tymi umowami,
14) ewidencjonowanie przypadków udostępniania danych osobowych, jeżeli w OSIR wystąpi przetwarzanie danych dziecka wyłącznie dla celów społeczeństwa informacyjnego i w oparciu o zgodę to pracownik postępuje zgodnie zapisami w § 5 ust 1. pkt 6.

5. **Inspektor Ochrony Danych (IOD)** wyznaczony przez Dyrektora OSIR podlega bezpośrednio Dyrektorowi i realizuje w OSIR zadania dotyczące:

1) informowania administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tym zakresie,
2) monitorowania przestrzegania RODO oraz 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,
3) nadzorowania opracowania, wdrożenia i aktualizowania zasad zawartych w dokumentacji określającej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę tych danych,
4) zapewnienia zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
5) udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
6) współpracy z organem nadzorczym,
7) pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
8) pełnienia roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia,

9) prowadzenia zbiorczego rejestru czynności lub/i rejestru kategorii czynności w imieniu administratora,

6. Administrator Systemu informatycznego (ASI), wyznaczany jest przez Dyrektora OSIR lub osobę przez niego upoważnioną, w ramach ochrony przetwarzanych danych osobowych w OSIR w Głogowie Małopolskim, koordynuje i nadzoruje realizację zadań zapewniających prawidłowe funkcjonowanie systemów teleinformatycznych, w których przetwarzane są dane osobowe. Prowadzi wraz z IOD rejestr naruszeń danych osobowych według załącznika Nr 12 do Polityki.

§4

Zasady ochrony danych

W OSIR w Głogowie Małopolskim przetwarza się dane osobowe z poszanowaniem następujących zasad:

1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm - art.6, 9 RODO),
2) rzetelnie i uczciwie (rzetelność),
3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność),
4) w konkretnych celach i nie „na zapas" (celowość, ograniczenie celu),
5) gromadzenie nie więcej niż potrzeba (adekwatność, minimalizacja danych),
6) z dbałością o prawidłowość danych (prawidłowość),
7) nie dłużej niż potrzeba (czasowość),
8) zapewniając odpowiednie bezpieczeństwo danych (integralność i poufność),
9) dokumentując czynności przetwarzania (rozliczalność),
10) umożliwiając realizację przez osoby, których dane są przetwarzane, swoich praw zgodnie z obowiązującymi przepisami prawa (ochrona prywatności osób fizycznych).

§5

System ochrony danych osobowych

System ochrony danych osobowych przetwarzanych w OSIR w Głogowie Małopolskim składa się z następujących zasadniczych elementów:

1) Inwentaryzacja danych:
   a) dane osobowe wymagające ochrony zostały wykazane w wykazie zbiorów. Wykaz obejmuje zbiory ze stwierdzonym potencjalnym ryzykiem naruszenia praw lub wolności osób fizycznych. Każdy ze zbiorów jest opisany w sposób umożliwiający przeprowadzenie analizy ryzyka,
   b) Opis zbiorów obejmuje takie informacje, jak:
   — nazwę zbioru,

— opis celów przetwarzania,
— charakter, zakres, kontekst, rodzaj danych (dane zwykłe, dane szczególne),
— odbiorcy,
— podstawę prawną przetwarzania danych osobowych,
— funkcjonalny opis operacji przetwarzania,

c) aktywa służące do przetwarzania danych osobowych (ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, programy, systemy operacyjne, informacja o powierzeniu danych osobowych, informacja o wykonywaniu usług przez podmioty zewnętrzne, źródła pochodzenia danych osobowych),
d) Szczególne kategorie danych osobowych. Identyfikacja przypadków, w których przetwarza lub może przetwarzać szczególne kategorie danych osobowych (dane specjalne i dane karne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. Weryfikuje podstawy prawne przetwarzania takich danych w oparciu o art. 9 i art. 10 RODO oraz zapewnienia szczególnej ochrony przetwarzania tych danych,
e) Dane niezidentyfikowane. Identyfikacja przypadków, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane. Administrator nie odmawia przyjęcia dodatkowych informacji od osoby, której dane dotyczą by ułatwić jej wykonanie jej praw i w takim przypadku dokonuje weryfikacji tożsamości np. poprzez mechanizmy uwierzytelniania,
f) Profilowanie. Identyfikacja przypadków, w których dokonuje się profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i w pełni zautomatyzowanego podejmowania decyzji, Administrator informuje osobę, której dane dotyczą o fakcie profilowania oraz o konsekwencjach takiego profilowania. Jeżeli gromadzi jej dane informuje ją również czy ma ona obowiązek podać te dane oraz o konsekwencjach ich niepodania. Informację można przekazać w połączeniu ze standardowymi znakami graficznym, które w widoczny, zrozumiały i czytelny sposób przedstawiają sens zamierzonego przetwarzania,
g) Przetwarzanie danych dzieci - stosuje przepisy art.8 RODO. Zgodnie z art. 8 ust. 1 RODO w sytuacji, w której przetwarzanie danych odbywa się na podstawie zgody i dotyczy usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku poniżej 16 roku życia, wymagana jest zgoda udzielona lub zaaprobowana przez osobę sprawującą władzę rodzicielską nad dzieckiem lub opiekę. Kluczowe jest zatem, aby przetwarzanie:

— odbywało się na podstawie zgody,
— dotyczyło wyłącznie usług społeczeństwa informacyjnego,
— oferowanych bezpośrednio dziecku w wieku poniżej 16 roku życia,

Realizacja wymogów wynikających z art. 8 RODO jest związana z nałożonym na administratora obowiązkiem weryfikacji wieku. Administrator wprowadza odpowiednie mechanizmy, uwzględniając dostępną technologię i podejmując racjonalne starania, aby zweryfikować, czy odpowiednia osoba udzieliła zgody lub ją zaaprobowała (komunikacja pocztą tradycyjną lub elektroniczną, zgodę pisemną, inne metody autoryzacyjne),

h) Współadministrowanie. W przypadku gdy Administrator określa cele i sposoby przetwarzania wspólnie z innymi podmiotami może dojść między nimi do zawarcia umowy o współadministrowaniu. W takim przypadku przepis art. 26 ust. 1 RODO nakłada na nich jako na współadministratorów obowiązek określenia, w drodze uzgodnień, w przejrzysty sposób odpowiednich zakresów obowiązków. W szczególności powinno zostać określone, który z współadministratorów będzie realizował obowiązki informacyjne i inne obowiązki wynikające z przepisów RODO. W uzgodnieniach może zostać również wskazany punkt kontaktowy dla osób, których dane dotyczą. Zgodnie z przepisem art. 26 ust. 2 RODO zasadnicza treść uzgodnień powinna zostać udostępniona osobom, których dane dotyczą. Ocena w tym zakresie pozostawiona została współadministratorom. Należy przyjąć, że zasadniczy charakter będą miały co najmniej te uzgodnienia, które odnoszą się do podziału obowiązków między współadministratorami oraz sposobu realizacji uprawnień podmiotów danych. Dokonanie uzgodnień między współadministratorami nie zwalnia ich z obowiązków przewidzianych przepisami RODO. Ponadto niezależnie od uzgodnień, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z RODO wobec każdego z administratorów.

i) Upoważnienia:

— odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych,

— Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa,

— Upoważnienia nadawane są w formie pisemnej (dopuszcza się formę elektroniczną) w postaci skierowanego imiennie dokumentu do osoby upoważnionej. Minimalne wymagania co do treści upoważnienia zawarte są w Załączniku Nr 4 - Wzór upoważnienia do przetwarzania danych osobowych,

— Upoważnienia mogą być nadawane w formie pisemnych poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności

służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia,

— Osobę, która po raz pierwszy ma mieć dostęp do przetwarzania danych osobowych można upoważnić po zapoznaniu jej z obowiązującą w Urzędzie Miejskim w Głogowie Małopolskim Polityką oraz przepisami dotyczącymi ochrony danych osobowych. Szkolenie przeprowadza IOD. Po odbyciu szkolenia osoba ta, podpisuje oświadczenie o zapoznaniu z przepisami dotyczącymi ochrony danych osobowych, zachowaniu w tajemnicy przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia (Załącznik Nr 6 - Oświadczenie o poufności). Kserokopię oświadczenia przedstawia pracownik, który przygotuje upoważnienie do przetwarzania danych osobowych załącznik Nr 4 - Wzór upoważnienia do przetwarzania danych osobowych,

j) Nazwa zbioru/zbiorów przetwarzania powinna być zgodna z nazwą zbioru występującą w rejestrze czynności przetwarzania prowadzonym przez IOD,

k) Podpisane oświadczenie jest przechowywane w teczce osobowej pracownika OSIR w Głogowie Małopolskim. W przypadku przejścia pracownika na inne stanowisko i związaną z tym zmianą zakresu czynności nie jest wymagane ponowne szkolenie ani podpisywanie kolejnego oświadczenia o zachowaniu w tajemnicy przetwarzanych informacji,

l) W przypadku osób, które nie są pracownikami OSIR w Głogowie Małopolskim na podstawie umowy o pracę, dokumenty wymienione w pkt. i) (powyżej) są dołączane do dokumentacji określającej zakres współpracy i świadczeń wykonywanych na rzecz OSIR w Głogowie Małopolskim przez te osoby lub mogą stanowić jej część,

m) Zakres upoważnienia może dodatkowo zostać uszczegółowiony w dokumentach określających obowiązki osób wykonujących czynności przetwarzania danych osobowych w OSIR w Głogowie Małopolskim lub na jego rzecz,

n) Szczegółowy zakres oraz poziom uprawnień do przetwarzanych danych osobowych może zostać dodatkowo określony, w zależności od formy współpracy z OSIR w Głogowie Małopolskim w:

— zakresie czynności pracownika oraz opisie dodatkowych zadań wykraczających poza zakres obowiązków pracownika, które są przez niego realizowane,

— planie stażu/praktyki,

— zawartej umowie cywilno-prawnej,

— indywidualnym formularzu dostępu do systemów teleinformatycznych,

o) Pracownik ds. Kadr prowadzi ewidencję osób upoważnionych (Załącznik Nr 5 - Ewidencja osób upoważnionych do przetwarzania danych osobowych), w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych.

p) Podstawy prawne:

— zapewnienie, identyfikowanie, weryfikowanie podstaw prawnych przetwarzania danych i rejestrowanie ich w Rejestrze, w tym:

— — osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów (rejestr zgód). Jeżeli zbierane jest kilka zgód dotyczących różnych celów przetwarzania, zgody te muszą zostać wyrażone osobno. Niedozwolone jest zbiorcze zbieranie zgód,

— — przetwarzanie 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,

— — przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,

— — przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,

— — przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,

— — Prawnie uzasadniony interes administratora nie powinien mieć zastosowania jako podstawa prawna przetwarzania, gdyż jako organ publiczny dokonuje tego realizując swoje zadania określone przez ustawodawcę,

q) Eksport danych

— Administrator weryfikuje czy nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce,

r) Rejestr Czynności Przetwarzania Danych:

— Administrator opracowuje, prowadzi i utrzymuje Rejestr czynności przetwarzania danych, zwany „Rejestrem" (Załącznik Nr 2) oraz „Rejestr kategorii czynności" (Załącznik Nr 3) jako podmiot przetwarzający - procesor w przypadku powierzenia danych osobowych,

— Rejestr stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności,

— IOD wraz z pracownikiem ds. kadr prowadzi „Rejestr Czynności Przetwarzania Danych" oraz „Rejestr Kategorii Czynności" w imieniu Administratora, Procesora, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Wypełnia rejestry (Załącznik Nr 2 i Nr 3) po otrzymaniu rejestrów czynności przetwarzania danych prowadzonych w poszczególnych komórkach organizacyjnych,

— Rejestr czynności prowadzony jest dla każdego zbioru danych osobowych/czynności przetwarzania występującego w OSIR w Głogowie Małopolskim,

— Rejestr jest jednym z podstawowych narzędzi umożliwiających rozliczanie większości obowiązków ochrony danych,

— Wzór Rejestru stanowi Załącznik nr 2 do Polityki - „Wzór Rejestru Czynności Przetwarzania". Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych rejestruje się informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej,

— Rejestry czynności przetwarzania danych mają charakter dokumentów wewnętrznych i z uwagi na zawarte tam informacje odnoszące się do zabezpieczeń nie mogą być udostępniane osobom nieuprawnionym.

§6

Prawa osoby, której dane dotyczą

1. Obsługa praw jednostki. Administrator spełnia obowiązki informacyjne względem osób których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   1) Obowiązki informacyjne. Administrator przekazuje osobom prawem wymagane informacje przy zbieraniu danych oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków,
   2) Możliwość wykonania żądań. Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających,
   3) Obsługa żądań. Administrator zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane. Umożliwia wnoszenie przedmiotowych żądań także drogą elektroniczną,
   4) Zawiadamianie o naruszeniach. Administrator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.
2. Sposób obsługi praw jednostki i obowiązków informacyjnych,
   1) Informacje podawane na mocy art.13 i 14 RODO oraz komunikacja i działania podejmowane na mocy art. 15-22 i 34 RODO są wolne od opłat z zastrzeżeniem ust 4 pkt. 5 niniejszego paragrafu. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza,
   2) Administrator ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej OSIR w Głogowie Małopolskim

informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich, metodach kontaktu z Administratorem w tym celu, ewentualnym cenniku żądań „dodatkowych" itp.,

3) Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób,
4) Administrator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych. Np. takie same dane uwierzytelniające, których osoba, której dane dotyczą użyła, by zalogować się do usług internetowych oferowanych przez administratora,
5) W celu realizacji praw jednostki Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzanych, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
6) Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

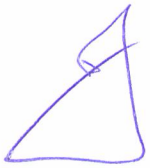
3. Obowiązki informacyjne: Załącznik Nr 7 zawiera wzory - Podstawowe klauzule informacyjne (art.13, 14 RODO).
4. Administrator:
   1) określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych,
   2) informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby,
   3) informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby, gdy przepis szczegółowy nie stanowi inaczej,
   4) informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej, gdy przepis szczegółowy nie stanowi inaczej,
   5) określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
   6) informuje osobę o planowanej zmianie celu przetwarzania danych,
   7) informuje osobę przed uchyleniem ograniczenia przetwarzania,
   8) informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe),
   9) informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą, w przypadku gdy prawo to jej przysługuje,
   10) bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.
5. Żądania osób:

1) Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, Administrator gwarantuje ochronę praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), Administrator może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu,
2) Nieprzetwarzanie. Administrator informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw,
3) Odmowa. Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych,
4) Dostęp do danych. Na żądanie osoby dotyczące dostępu do jej danych, Administrator informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych, nie uzna się za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych,
5) Kopie danych. Na żądanie wydaje się osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Administrator odrębnym zarządzeniem może wprowadzać cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych zgodnie z art. 15 ust. 3 RODO. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych,
6) Sprostowanie danych. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby,
7) Uzupełnienie danych. Administrator uzupełnia i aktualizuje dane na żądanie osoby, ma prawo odmówić uzupełnienia lub aktualizacji danych, jeżeli uzupełnienie lub aktualizacja byłoby niezgodne z celami przetwarzania danych. Administrator może polegać na oświadczeniu osoby, co do uzupełnianych lub aktualizowanych danych, chyba że będzie to niewystarczające w świetle prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne,
8) Usunięcie danych. Na żądanie osoby, Administrator usuwa dane, gdy:
   a) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,



b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
d) dane były przetwarzane niezgodnie z prawem,
e) konieczność usunięcia wynika z obowiązku prawnego,
f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. udział w konkursie na stronie internetowej),
oraz
g) Administrator określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO,
h) W sytuacji gdy przepisy prawa nakładają obowiązek, do którego spełnienia konieczne jest przetwarzanie danych, Administrator nie ma obowiązku spełnienia żądania osoby, której dane dotyczą, odnoszącego się do usunięcia jej danych,
i) Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, podejmuje on rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich,
j) W przypadku usunięcia danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby,

9) Ograniczenie przetwarzania. W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.
Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
a) osoba kwestionuje prawidłowość danych - na okres pozwalający sprawdzić ich prawidłowość,
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, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,



d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją - do czasu stwierdzenia, czy po stronie Administrator zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu,

10) Przenoszenie danych. Na żądanie osoby Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Administratora,

11) Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o powierzone zadanie w interesie publicznym, Administrator uwzględni sprzeciw, o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń,

12) Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych. Jeżeli Administrator prowadzi lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Administrator uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym,

13) Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu. Jeżeli Administrator przetwarza dane w sposób wyłącznie zautomatyzowany, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Administrator zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Administratora, chyba że taka automatyczna decyzja jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Administratorem, lub jest wprost dozwolona przepisami prawa: albo opiera się o wyraźną zgodę odwołującej osoby,

§7

Minimalizacja

1. Administrator dba o minimalizację przetwarzania danych pod kątem: adekwatności danych do celów (ilości danych i zakresu przetwarzania), dostępu do danych, czasu przechowywania danych.

2. Minimalizacja zakresu:

1) Administrator weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO. Administrator dokonuje na bieżąco przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania,
2) Administrator przeprowadza weryfikację co do ilości i zakresu przetwarzania danych zgodnie z zasadą ochrony danych w fazie projektowania i zasadą domyślnej ochrony danych („Privacy by design" & „Privacy by default"). W tym celu Administrator już na etapie projektowania zmian analizuje i rekomenduje wdrożenie odpowiednich środków technicznych i organizacyjnych, tak aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności,

3. Minimalizacja dostępu:
   1) Administrator stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe),
   2) W OSIR w Głogowie Małopolskim stosuje się kontrolę dostępu fizycznego. Dokonuje się aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających. Dokonuje się na bieżąco przeglądu i aktualizacji ustanowionych użytkowników systemów. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego (Załącznik Nr 8 „Zasady korzystania z pomieszczeń i sprzętu OSIR w Głogowie Małopolskim oraz i Załącznik Nr 13 – Instrukcja zarządzania systemem informatycznym (IZSI).
4. Minimalizacja czasu:
   1) Administrator przetwarza dane osobowe do czasu osiągnięcia celu. Termin przetwarzania danych określony został na podstawie przepisów prawa lub wynikający z przeprowadzonej analizy ich przydatności i wykazany w Rejestrze,
   2) Dane, których zakres przydatności ulega ograniczeniu są archiwizowane oraz znajdują się na kopiach zapasowych. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych. Zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności wynikają z obowiązujących przepisów prawa w zakresie archiwizacji.

§8

Bezpieczeństwo

Administrator:

1) zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych w OSIR w Głogowie Małopolskim,
2) zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
    a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii. Przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
    b) zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania - wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych,
    c) kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają,
    d) przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia,
    e) ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym ustala przydatność i stosuje takie środki i podejście jak:
    — pseudonimizacja danych osobowych,
    — inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności,
    — integralności, dostępności i odporności systemów i usług przetwarzania,
    — środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
    f) Wzór procedury analizy ryzyka określa Załącznik Nr 9,
    g) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie oraz jest to obowiązkowe na podstawie przepisów prawa (art. 35 RODO). Dla wypełnienia obowiązku przeprowadzenia oceny skutków dla ochrony danych stosuje się metodykę oceny skutków zgodnie z Załącznikiem nr 10 (Wzór - Ocena skutków dla ochrony danych),
    h) dostosowuje środki ochrony danych do ustalonego ryzyka,
    i) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Prezesowi Urzędu Ochrony Danych Osobowych - zarządza incydentami,

3) Środki bezpieczeństwa. W OSIR w Głogowie Małopolskim stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa są bliżej opisane w procedurach przyjętych w OSIR w Głogowie Małopolskim dla tych obszarów,
4) Zestawienie środków organizacyjnych i technicznych zapewniających ochronę danych osobowych w zakresie poufności, integralności i rozliczalności:
   a) Ochrona danych osobowych polega na zabezpieczeniu informacji wprowadzonej, przetwarzanej, przesyłanej w systemie informatycznym oraz na nośnikach informacji przed nielegalnym ujawnieniem, kradzieżą oraz nieuprawnioną modyfikacją lub usunięciem,
   b) W celu ochrony danych przechowywanych w systemach informatycznych należy wykorzystywać wchodzące w ich skład mechanizmy zarówno sprzętowe, jak i programowe oraz inne rozwiązania zwiększające bezpieczeństwo danych,
   c) Dane osobowe mogą przetwarzać wyłącznie pracownicy upoważnieni do ich przetwarzania. Pracownicy upoważnieni do przetwarzania danych osobowych mają obowiązek zachować w tajemnicy dane, które przetwarzają oraz sposoby ich zabezpieczenia,
   d) Wszystkie pomieszczenia, w których przetwarza się dane osobowe, są zamykane na klucz, w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych - także w godzinach pracy,
   e) Dane osobowe w formie papierowej są przechowywane po zakończeniu pracy w zamykanych na klucz szafach biurowych, a najlepiej w szafach metalowych. Klucze od szaf należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych. Zasady korzystania z pomieszczeń i sprzętu OSIR w Głogowie Małopolskim, zabezpieczenia ich po godzinach pracy oraz gospodarki kluczami określa Załącznik Nr 8 „Zasady korzystania z pomieszczeń i sprzętu w OSIR w Głogowie Małopolskim, zabezpieczania ich po godzinach pracy oraz gospodarki kluczami",
   f) Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań (tzw. polityka czystego biurka),
   g) Na biurku nie mogą znajdować się napoje w pojemnikach grożących rozlaniem płynu,
   h) Po zakończonej pracy na biurku może znajdować się jedynie telefon, komputer stacjonarny i przybory biurowe,
   i) Próbne i zepsute wydruki papierowe powinny być niszczone w niszczarce dokumentów odpowiedniej klasy (np.:DIN4) w stopniu uniemożliwiającym ich odczytanie,



j) W przypadku żądania udostępniania danych osobowych pracownicy OSIR postępują zgodnie z przepisami RODO. Decyzję podejmuje Administrator na wniosek pracownika. Udostępnianie danych jest odnotowywane w systemach informatycznych i w formie papierowej,

k) Procedury zarządzania uprawnieniami do systemów informatycznych reguluje instrukcja zarzadzania systemem informatycznym w OSIR w Głogowie Małopolskim (IZSI).

l) Przy przetwarzaniu danych osobowych w systemach informatycznych należy stosować następujące zasady:
— kontrola dostępu do zbiorów danych osobowych,
— indywidualne identyfikatory użytkowników,
— uwierzytelnianie użytkowników systemu,

m) W celu zabezpieczenia danych osobowych przed ich utratą lub uszkodzeniem należy:
— dla wszystkich systemów stosować procedurę sporządzania kopii zapasowych, zgodnie z IZSI,
— wszystkie systemy informatyczne wyposażyć w awaryjne zasilanie,
— stosować oprogramowanie antywirusowe,
— kontrolować dostęp do systemów z publicznej sieci telekomunikacyjnej za pomocą zapory sieciowej, filtrów antyspamowych, oprogramowania antywirusowego, itp.,
— stosować środki fizyczne chroniące urządzenia przed osobami nieupoważnionymi do dostępu do danych osobowych oraz zagrożeniami ze strony sił natury,

n) Użytkowników systemów obowiązuje polityka haseł opisana w IZSI,

o) Użytkownik systemu, który utracił hasło, zobowiązany skorzystać z serwisu odzyskiwania haseł (selfservice), ewentualnie skontaktować się z ASI,

p) W przypadku likwidacji, naprawy lub przekazania nośnika informacji, który zawiera dane osobowe, podmiotowi nieupoważnionemu do przetwarzania danych osobowych, należy zapewnić trwałe wymazanie informacji stanowiących dane osobowe, zgodnie z procedurami zawartymi w IZSI,

q) W przypadku korzystania z komputerów przenośnych, które zawierają dane osobowe należy zachować szczególną ostrożność podczas używania ich poza obszarem przetwarzania danych. Na użytkowanie przenośnych urządzeń komputerowych poza siedzibą OSIR w Głogowie Małopolskim w wymagana jest zgoda Dyrektora bądź osoby przez niego upoważnionej. Decyzja wydawana jest na podstawie indywidualnego wniosku zaakceptowanego wstępnie przez ASI i IOD i opatrzonego uzasadnieniem odnoszącym się do zakresu realizowanych poza siedzibą OSIR w Głogowie Małopolskim. Rejestracja zezwoleń odbywa się w kadrach. Szczegółowe zasady korzystania z komputerów przenośnych określa IZSI,



r) Ekrany komputerów, na których przetwarzane są dane osobowe, są chronione wygaszaczami zabezpieczonymi hasłem. Ekrany należy ustawić tak, aby dane osobowe były niewidoczne dla osób nieupoważnionych do ich przetwarzania lub stosować filtry anonimizacyjne,

s) Elektroniczne nośniki informacji zawierające dane osobowe muszą być zabezpieczone przed dostępem osób nieupoważnionych do ich przetwarzania. Sposób i miejsce ich przechowywania określa IZSI.

§9

Zgłaszanie naruszeń ochrony danych osobowych

1. Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu (instrukcja postępowania z incydentami). W procedurze opisano obowiązek zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, terminy na dopełnienie tego obowiązku, minimalne wymogi co do treści zgłoszenia oraz sposób dokumentowania naruszeń,
   1) Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości,
   2) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do natychmiastowego powiadamiania o wystąpieniu incydentu bezpieczeństwa, bezpośredniego przełożonego i Inspektora Ochrony Danych,
   3) Obsługę zgłoszonych przypadków związanych z naruszeniem bezpieczeństwa danych osobowych OSIR w Głogowie Małopolskim zapewnia ASI i IOD.
   4) Punkt kontaktowy do zgłaszania przypadków związanych z naruszeniem bezpieczeństwa danych osobowych: Inspektor Ochrony Danych, ul. Parkowa 15 36-060 Głogów Małopolski.
2. Do typowych podatności mogących prowadzić do naruszenia bezpieczeństwa danych osobowych należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
3. Pracownicy OSIR winni wzajemnie współpracować w celu minimalizacji podatności systemu ochrony danych osobowych,
4. Do typowych naruszeń bezpieczeństwa danych osobowych należą:

1) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania, nieuprawnione modyfikowanie),
2) przykładowe zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
3) przykładowe zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),

5. W przypadku wykrycia naruszenia bezpieczeństwa danych osobowych należy, o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, oraz uwzględnić w działaniu również ustalenie przyczyn lub sprawców. W szczególności należy:
   1) rozważyć wstrzymanie bieżącej pracy w celu zabezpieczenia miejsca zdarzenia (odłączyć urządzenie od sieci komputerowej, wylogować się z systemu, wyłączyć urządzenie),
   2) zaniechać, o ile to możliwe, dalszych działań, które wiążą się z zaistniałą sytuacją i mogą utrudnić jej udokumentowanie i późniejszą analizę,
   3) w zależności od okoliczności zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałej sytuacji (np. zasady BHP, ewakuacja z budynku, procedury ppoż.),
6. Zgłaszanie incydentu naruszenia bezpieczeństwa danych osobowych:
   1) Z uwagi na wymogi wynikające z RODO, w tym krótki okres na zgłoszenie incydentu naruszenia bezpieczeństwa danych osobowych (72 godziny od stwierdzam/wykrycia naruszenia) informacje w tym zakresie muszą być przekazywane przez osoby lub podmiot przetwarzający dane, po zidentyfikowaniu zagrożenia, najpóźniej w ciągu 24 godz.,
   2) Wykrycia naruszenia lub podejrzenie wystąpienia zdarzenia, które może mieć wpływ na bezpieczeństwo przetwarzanych danych należy zgłosić do punktu kontaktowego,
   3) Zgłoszenie musi zawierać: datę i czas zdarzenia, imię i nazwisko osoby zgłaszającej, miejsce wystąpienia incydentu naruszenia bezpieczeństwa danych osobowych oraz jego krótki opis (wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, opisywać możliwe konsekwencje naruszenia ochrony danych osobowych),
   4) Zgłoszenie o naruszeniu przepisów o ochronie danych osobowych pochodzi najczęściej od osoby zatrudnionej przez OSIR przy przetwarzaniu danych osobowych jak i z informacji od podmiotu przetwarzającego,



5) Jeśli zgłoszenia dokonuje podmiot przetwarzający na podstawie Umowy powierzenia lub podmiot świadczący usługi serwisowe to zgłoszenie musi nastąpić w ciągu 24 godz.,

7. Analiza przypadków naruszenia bezpieczeństwa danych osobowych:
   1) Każdy zgłoszony przypadek musi zostać poddany analizie, w zakresie ustalenia czy naruszenie bezpieczeństwa danych osobowych jest incydentem bezpieczeństwa (prowadzi do utraty, zniszczenia, ujawnienia itd.), a w szczególności czy naruszenie to skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych np. jeśli naruszenie może prowadzić do kradzieży lub fałszowania tożsamości, straty finansowej, naruszenia dobrego imienia czy też naruszenia tajemnic prawnie chronionych,
   2) W trakcie analizy należy brać pod uwagę następujące elementy:
      a) wdrożone zabezpieczenia i ich funkcjonowanie (potwierdzenie ich skuteczności),
      b) zapisy (logi systemowe/rejestry) systemu teleinformatycznego, jeśli zachodzi podejrzenie utraty poufności przetwarzanych danych (np. kradzież danych z bazy),
      c) poprawność funkcjonowania systemu - bazy danych jeśli zachodzi podejrzenie utraty integralności przetwarzanych danych (np. uszkodzenie bazy danych),
      d) zapisy (logi systemowe/nagrania/rejestry) systemów zabezpieczeń wspomagających ochronę systemów teleinformatycznych oraz przetwarzanych danych, jeśli zachodzi podejrzenie nieautoryzowanego dostępu do danych,
   3) Analiza przeprowadzana jest przez pracownika OSIR w Głogowie Małopolskim we współpracy z IOD i ASI.
8. W zależności od charakteru naruszenia w czynnościach, o których mowa w ust. 6 mogą zostać zaangażowani:
   1) inni pracownicy OSIR (w tym w szczególności pracownicy komórki organizacyjnej OSIR, w której wystąpiło naruszenie),
   2) ASI (w szczególności jeśli naruszenie jest związane z funkcjonowaniem systemu informatycznego),
9. W wyniku analizy i stwierdzenia wystąpienia incydentu, ustalenia zakresu, przyczyny incydentu oraz jego ewentualnych skutków, ASI wraz z IOD :
   1) działa na rzecz przywrócenia działania organizacji po wystąpieniu incydentu,
   2) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia,
   3) inicjuje ewentualne działania dyscyplinujące.
10. IOD dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte

działania zaradcze. Dokumentacja naruszeń prowadzona jest według Załącznika Nr 10 - „Rejestr naruszeń ochrony danych osobowych",

11. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych osobowych,
12. O wystąpieniu sytuacji naruszenia bezpieczeństwa danych osobowych przetwarzanych w OSIR jest informowany Administrator danych (Załącznik Nr 11 - Wzór Raportu o naruszeniu danych osobowych),
13. Zawiadomienie organu nadzorczego o sytuacji naruszenia bezpieczeństwa danych osobowych,
    1) Jeżeli przeprowadzona analiza, o której mowa w ust. 7 wskazuje na to że doszło do naruszenia bezpieczeństwa danych osobowych (incydent bezpieczeństwa), które może skutkować ryzykiem naruszenia praw i wolności osób z dużym prawdopodobieństwem, informacja o tym zdarzeniu jest kierowana do Prezesa Urzędu Ochrony Danych Osobowych,
    2) Zgłoszenia naruszenia bezpieczeństwa danych osobowych dokonywane jest w sposób określony przez organ nadzorczy nie później niż 72 godziny od stwierdzenia (wykrycia) zdarzenia,
    3) Jeżeli zgłoszenie naruszenia bezpieczeństwa danych osobowych dokonane zostanie po upływie 72 godzin od stwierdzenia (wykrycia) zdarzenia musi ono zwierać wyjaśnienie przyczyn opóźnienia,
    4) Zgłoszenia naruszenia bezpieczeństwa danych osobowych dokonuje ASI wraz z IOD lub osoba działająca w jego zastępstwie. Art.33 ust.3 RODO określa minimalne informacje, które musi zawierać zgłoszenie,
14. Zawiadomienie osoby której dane dotyczą o sytuacji naruszenia bezpieczeństwa jej danych osobowych,
    1) Jeżeli przeprowadzona analiza, o której mowa w ust. 7 wskazuje, że doszło do naruszenia bezpieczeństwa danych osobowych, które może skutkować wysokim ryzykiem naruszenia praw i wolności osób, informacja o tym zdarzeniu jest kierowana bez zbędnej zwłoki do osób których dane dotyczą,
    2) W myśl przepisu art. 34 ust. 2 RODO zawiadomienie osoby, której dane dotyczą, powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz przynajmniej:
        a) zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
        b) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
        c) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków,

3) Zawiadomienia o naruszeniu powinno zostać przekazane zainteresowanym osobom, biorąc pod uwagę dostępne kanały komunikacji z nimi oraz koszty wysyłki korespondencji np. z uwagi na liczbę osób objętych zawiadomieniem:
   a) na adres e-mail (jeśli znany),
   b) sms (jeśli znany nr telefonu),
   c) listownie (jeśli znany adres),
4) Zawiadomienie w formie, o której mowa powyżej nie jest wymagane jeśli:
   a) w celu zabezpieczenia danych Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
   b) Administrator po stwierdzeniu naruszenia zastosował (następnie) środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
   c) bezpośrednie zawiadomienie nie jest również wymagane jeśli powodowałoby to poniesienie niewspółmiernie dużych nakładów pracy i środków finansowych ze strony Administratora. W tym przypadku należy wydać publiczny komunikat (informacja na stronie OSIR - BIP i stronie promocyjnej, jednorazowe ogłoszenie w dzienniku o zasięgu regionalnym),

15. Usuwanie naruszenia bezpieczeństwa danych osobowych:
   1) Po wykryciu naruszenia bezpieczeństwa danych osobowych analizowane są okoliczności związane z jego wystąpieniem oraz ustalany jest sposób rozwiązania problemu oraz, jeśli to konieczne, zabezpieczenie materiału dowodowego,
   2) W usuwanie naruszenia bezpieczeństwa danych osobowych zaangażowani są pracownicy OSIR w Głogowie Małopolskim, którzy w ramach powierzonych obowiązków zapewniają i nadzorują funkcjonowanie systemu służącego do przetwarzania danych osobowych,
   3) W przypadku gdy problem może zostać rozwiązany samodzielnie przez pracowników OSIR w Głogowie Małopolskim, należy to wykonać bez zbędnej zwłoki,
   4) W przypadku konieczności wykonania działań przez podmiot zewnętrzny, pracownik zajmujący się rozwiązaniem problemu powinien, używając ustalonych metod, poinformować o zdarzeniu ten podmiot, oraz razem z jego przedstawicielem uczestniczyć w rozwiązywaniu problemu,
   5) Po przywróceniu prawidłowego stanu bezpieczeństwa danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości,
   6) Jeżeli przyczyną naruszenia bezpieczeństwa danych osobowych:

a) był błąd osoby przetwarzającej dane, w szczególności użytkownika systemu teleinformatycznego, można przeprowadzić dodatkowe szkolenie lub przesłać stosowną informację do wszystkich użytkowników systemu o sposobie postępowania przy przetwarzaniu danych osobowych oraz zapewnieniu ich bezpieczeństwa,
b) było uaktywnienie złośliwego kodu, należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe,
c) było zaniedbanie lub umyślne działanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy powiadomić przełożonego i ewentualnie wyciągnąć konsekwencje służbowe,
d) było włamanie lub uszkodzenie systemu zabezpieczeń w celu pozyskania danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony danych osobowych,
e) był zły stan urządzeń lub sposób działania oprogramowania, należy niezwłocznie przeprowadzić kontrolne czynności serwisowe,

16. Naruszenia bezpieczeństwa danych osobowych są omawiane na posiedzeniach z udziałem Administratora, ASI i IOD oraz pracowników komórek OSIR, w których wykryto naruszenie.

§ 10

Przetwarzający

1. Administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Wymogi dotyczące powierzenia określa art.28 RODO,
2. Przepisy RODO wskazują, że podmiot przetwarzający może wykazać, iż daje wystarczające gwarancje m in. poprzez stosowanie odpowiedniego zatwierdzonego przez Prezesa Urzędu Ochrony Danych Osobowych kodeksu postępowania albo poddał się procesowi certyfikacji i uzyskał certyfikat. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora,
3. 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,

4. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie pisemnej umowy lub innego instrumentu prawnego 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. Umowa bądź porozumienie nie musi się ograniczać do kwestii powierzenia, może być ona elementem szerszej umowy (np. umowy o współpracę, umowy serwisowej). Umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:
   1) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora (pisemna umowa powierzenia),
   2) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
   3) podejmuje wszelkie środki wymagane na mocy art. 32 RODO,
   4) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 3,
   5) 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 RODO,
   6) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36 RODO,
   7) przekazuje Administratorowi, w ciągu 24 godzin od wykrycia zdarzenia, informacje o naruszeniu ochrony powierzonych mu danych osobowych, w tym informacje niezbędne Administratorowi do zgłoszenia naruszenia ochrony danych organowi nadzorczemu, o którym mowa w art. 33 ust. 3 RODO. Zgłoszenie takie powinno odbywać się adres: ul. Parkowa 15 36-060 Głogów Małopolski.
   8) zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania danych, w tym rejestru kategorii czynności przetwarzania danych osobowych (wymóg art. 30 RODO) Przetwarzający udostępniania na żądanie Administratora prowadzony rejestr czynności przetwarzania danych przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego,
   9) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie,
   10) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym paragrafie oraz umożliwia



administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich,

11) jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nakłada - na mocy umowy lub innego aktu prawnego, te same obowiązki ochrony danych jakie zostały na niego nałożone umową z administratorem, o których to obowiązkach mowa w niniejszym ustępie, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO,

12) jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym,

§ 11

Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

1. W przypadku wystąpienia przekazania danych osobowych do państw trzecich lub organizacji międzynarodowych Administrator zastosuje zasady opisane w Rozdziale V RODO,
2. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w art. 45 ust 3 RODO lub braku odpowiednich zabezpieczeń określonych w art. 46 RODO, w tym wiążących reguł korporacyjnych, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej nastąpi wyłącznie pod warunkiem, spełnienia wymagań określonych w art.49 RODO,
3. pracownicy są odpowiedzialni za monitorowanie i rejestrację wszystkich przypadków eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy, który stanowią kraje członkowskie Unii Europejskiej oraz Islandia, Lichtenstein i Norwegia,
4. O każdym przypadku wystąpienia konieczności przekazania danych osobowych do państw trzecich lub organizacji międzynarodowych pracownik informuje IOD,
5. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych w Inspektoracie.
6. weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne,
7. Informacja o przekazaniu danych osobowych poza Europejski Obszar Gospodarczy zostanie zawarta w „ Rejestrze" oraz „Rejestrze kategorii czynności przetwarzania"

§ 12

Ochrona danych w fazie projektowania i domyślna ochrona danych

1. Ochrona danych w fazie projektowania procesów odnoszących się do danych osobowych uwzględnia:
   1) stan wiedzy technicznej,
   2) koszt wdrażania,
   3) charakter, zakres, kontekst i cele przetwarzania,
   4) ryzyko naruszenia praw lub wolności osób fizycznych,

   tak aby zaprojektować i wdrożyć odpowiednie środki techniczne i organizacyjne w celu nadania przetwarzaniu danych niezbędnych zabezpieczeń chroniących prawa osób, których dane dotyczą,

2. Domyślna ochrona danych gwarantuje aby przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Dotyczyć to będzie ilości zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.
3. Zasada uwzględniania ochrony danych w fazie projektowania oraz zasada domyślnej ochrony danych ma zastosowanie przy realizacji zamówień publicznych.

§ 13

Szkolenia

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi zostaje poddana przeszkoleniu i zapoznana z przepisami PODO oraz RODO,
2. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania (Załącznik Nr 6 - Wzór Oświadczenie o poufności),
3. Szkolenie organizuje IOD,
4. Szkolenie wewnętrzne z zasad ochrony danych osobowych odbywa za zgodnie z Załącznikiem Nr 13 - „Wzór - Plan szkolenia z zakresu znajomości zasad ochrony danych osobowych".

§ 14

Audyty

1. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Administrator jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych z roczną częstotliwością lub częściej,
2. Programy audytów będą opracowywane biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. W planie audytu określone zostaną kryteria audytu, jego cel, zakres i ewentualnie metody,
3. Audytor jest zobowiązany do przygotowania się do przeprowadzenia audytu, zapoznając się z opisem audytowanego obszaru, stosowanych procedur i wyników poprzednich audytów,

§ 15

Punkt kontaktowy RODO

1. W celu usprawnienia procesu obsługi spraw związanych z czynnościami przetwarzania danych osobowych w OSIR w Głogowie Małopolskim Administrator organizuje „Punkt kontaktowy RODO".
2. Obsługę „Punktu kontaktowego RODO" zapewniają pracownicy administracyjni OSIR.
3. „Punkt kontaktowy RODO" zlokalizowany jest w siedzibie OSIR w Głogowie Małopolskim (ul. Parkowa 15, 36-060 Głogów Małopolski) i funkcjonuje w godzinach pracy 7.30 – 15.30
4. Do głównych zadań „Punktu kontaktowego RODO" należy:
   1) udzielanie ustnych i pisemnych informacji osobom, których dane dotyczą we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych w OSIR w Głogowie Małopolskim,
   2) koordynacja spraw związanych z załatwianiem wniosków i udzielanie informacji osobom, których dane są przetwarzane w wyżej wymienionej szkole trybie art. 15- 20 RODO,
   3) przyjmowanie zgłoszeń o wystąpieniu naruszenia bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miejskim w Głogowie Małopolskim.

§ 16

Udostępnianie danych osobowych

RODO wyróżnia dwa rodzaje udostępniania danych:

1. udostępnianie innemu administratorowi - jeden administrator udostępnia dane drugiemu i każdy z nich wykorzystuje je do realizacji własnych celów,

2. współadministrowanie - opisane § 5 ust.1 lit.7.
   1) Udostępnianie danych innemu administratorowi następuje:
      a) za wyraźną zgodą osoby, której dane dotyczą,
      b) na podstawie przepisów prawa (np. udostępnienie danych policji, prokuraturze, sądom),
      c) innemu administratorowi, jeżeli przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem (dochodzenie roszczeń, zapobieganie oszustwom, marketing bezpośredni),
   2) W przypadku żądania udostępniania danych osobowych decyzję podejmuje Administrator na wniosek pracownika.

§ 17

Przeglądy i aktualizacje

1. PODO podlega przeglądowi i aktualizacji w przypadku:

1) zmian w przepisach prawa wymagających aktualizacji PODO,
2) innych znaczących zmian dotyczących bezpieczeństwa przetwarzania danych osobowych,
3) w celu realizacji rekomendacji i zaleceń wynikających z przeprowadzonych kontroli i audytów.

Dyrektor OSiR w Głogowie Młp.
Andrzej Zwierzchowski
Ośrodek Sportu i Rekreacji
w Głogowie Małopolskim
36-060 Głogów Małopolski, ul. Parkowa 15

Załącznik nr 1 do Polityki Ochrony Danych Osobowych

Klauzula zgody na przetwarzanie danych osobowych i informacja o prawie do jej cofnięcia

.....

(miejscowość, data)

.....

Imię i nazwisko

Zgoda na przetwarzanie danych osobowych

Zgodnie z art. 6 ust.1 lit. a oraz art. 9 ust 2 lit a[1] ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016 (RODO) wyrażam zgodę na przetwarzanie moich danych osobowych zwykłych oraz [1] danych osobowych szczególnych kategorii* w zakresie:

.....

przez Administratora.....

w celu.....

Ponadto oświadczam, ze zostałem poinformowany, iż w dowolnym momencie przysługuje mi prawo do wycofania zgody na przetwarzanie danych osobowych. Cofnięcie zgody nie będzie wpływać na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

data.....

czytelny podpis.....

*Dane szczególnych kategorii to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne wykorzystywane do identyfikacji, dane dotyczące zdrowia, seksualności lub orientacji seksualnej

1 niepotrzebne skreślić

Informacja o prawie cofnięcia zgody

W dowolnym momencie przysługuje Pani/Panu prawo do wycofania zgody na przetwarzanie Pani/Pana danych osobowych. Cofnięcie zgody nie będzie wpływać na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Załącznik nr 2 do Polityki Ochrony Danych Osobowych

Rejestr czynności przetwarzania danych osobowych

Administrator danych

Nazwa	
Adres	
Email	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)

Nazwa	
Adres	
Email	
Telefon	

Przedstawiciel (jeśli wyznaczono)

Nazwa	
Adres	
Email	
Telefon	

Proces[1] .....

Dział, departament, jednostka organizacyjna	
Cel przetwarzania danych[2]	
Kategorie osób, których dane dotyczą[3]	
Podstawa prawna	
Kategorie danych przetwarzane w procesie [4]	
Kategorie odbiorców danych *(jeśli dotyczy)* [5]	
Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane oraz dokumentacja odpowiednich zabezpieczeń *(jeżeli dotyczy)*	
Planowany termin usunięcia danych osobowych *(jeżeli jest to możliwe)* [6]	
Opis zabezpieczeń technicznych i organizacyjnych *(jeżeli jest to możliwe)* [7]	

Załącznik nr 3 do Polityki Ochrony Danych Osobowych

Rejestr kategorii czynności przetwarzania

Podmiot przetwarzający

Nazwa	
Adres	
Email	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)

Nazwa	
Adres	
Email	
Telefon	

Przedstawiciel (jeśli wyznaczono)

Nazwa	
Adres	
Email	
Telefon	

Kategoria przetwarzania [1)]

Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa *(jeżeli jest to możliwe)* [2)]	
Nazwa i dane kontaktowe Administratora danych	
Nazwa i dane kontaktowe Przedstawiciela administratora *(jeśli wyznaczono)*	
Inspektor Ochrony Danych *(jeśli powołano)*	
Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane oraz dokumentacja odpowiednich zabezpieczeń *(jeżeli dotyczy)*	

.....

.....

Data

Podpis Inspektora Ochrony Danych
/ osoby upoważnionej przez Administratora danych

[3)]

[1)] Np. Udostępnienie i utrzymywanie zdalnej platformy programistycznej do prowadzenia sklepu internetowego. Należy opisać wszystkie realizowane przez podmiot kategorie przetwarzań w oddzielnych tabelach.

[2)] Np. Kontrola dostępu do infrastruktury, aplikacji i baz danych, Dostęp do danych otrzymują wyłącznie osoby wskazane przez przetwarzającego na zlecenie administratora (czynności związane z modyfikacją funkcjonalności, konserwacyjne, naprawcze), szyfrowana transmisja danych. Jeśli dotyczy, należy umieścić dopisek: szczegółowe procedury znajdują się w polityce bezpieczeństwa - link/numer

.....

.....

Data

Podpis Inspektora Ochrony Danych
/ osoby upoważnionej przez Administratora danych

8)

[1] Nazwa procesu, np. Realizacja zamówienia, rekrutacja pracowników, prowadzenie ewidencji pracowników zgodnie z Kodeksem Pracy. Należy opisać wszystkie realizowane przez podmiot procesy w oddzielnych tabelach.

[2] Np. zgłoszenia pracownika i członków jego rodziny do ZUS, ich aktualizacja oraz przekazywanie informacji o zwolnieniach, prowadzenie rozliczeń z pracownikami, naliczanie potrąceń, obliczanie składek ZUS.

[3] Np. kandydaci do pracy, pracownicy, klienci.

[4] Np. dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych.

[5] Np. banki, kurierzy, Poczta Polska, itd.

[6] Np. 2 lata, 50 lat, itp.

[7] Wpisać, np. Kontrola dostępu do infrastruktury, aplikacji i baz danych; Dostęp do danych otrzymują wyłącznie osoby wskazane przez przetwarzającego na zlecenie administratora (czynności związane z modyfikacją funkcjonalności, konserwacyjne, naprawcze), szyfrowana transmisja danych. Jeśli dotyczy, należy umieścić dopisek: szczegółowe procedury znajdują się w polityce bezpieczeństwa - link/numer dokumentu.

[8] Wybrać w zależności, czy został powołany Inspektor Ochrony Danych

Załącznik nr 4 do Polityki
Ochrony Danych Osobowych

....

Numer upoważnienia (miejscowość, data)

UPOWAŻNIENIE

do przetwarzania danych osobowych

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), niniejszym: z dniem ..... upoważniam Panią/Pana..... do przetwarzania danych osobowych administrowanych przez....., w postaci papierowej oraz w ramach nadanych dostępów do systemów informatycznych, zgodnie z zajmowanym stanowiskiem.

Jednocześnie, wraz z nadanym upoważnieniem, zobowiązuję Panią/Pana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz obowiązującej w OSIR w Głogowie Małopolskim dokumentacji ochrony danych osobowych, w tym zasad przetwarzania danych osobowych.

Niniejsze upoważnienie traci moc: najpóźniej z dniem odwołania albo rozwiązania lub wygaśnięcia umowy o pracę, umowy zlecenia, umowy o dzieło lub innej umowy cywilnoprawnej łączącej Pana/Panią z OSIR w Głogowie Małopolskim.

Jednocześnie odwołuje upoważnienie z dnia . ....., znak .....

.....

.

(podpis osoby upoważniającej

Potwierdzam odbiór

.....

(data i podpis)

Załącznik nr 5 do Polityki Ochrony Danych Osobowych

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Numer upoważnienia	Data nadania upoważnienia	Zakres upoważnienia	Zmiana zakresu upoważnienia	Data ustania upoważnienia
1.						
2.						
3.						
4.						
5.						

Załącznik nr 6 do Polityki Ochrony Danych Osobowych

....

Nazwa jednostki organizacyjnej (miejscowość, data)

OŚWIADCZENIE O POUFNOŚCI

.....
(imię i nazwisko)

Oświadczam, iż zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych, w szczególności z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz. Urz. UE.L Nr 119, str. 1), ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000) oraz obowiązującą w OSIR w Głogowie Małopolskim dokumentacją ochrony danych osobowych, w szczególności z Polityką ochrony danych osobowych jak i Instrukcją zarządzania systemami informatycznymi, w tym z zasadami przetwarzania danych osobowych przez użytkownika końcowego.

W szczególności zobowiązuję się do:

- zachowania w tajemnicy danych osobowych jak również innych informacji stanowiących tajemnicę przedsiębiorcy w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2018 poz. 419 t.j.), do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych,
- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach
- zachowania w tajemnicy danych osobowych do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych

- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych, nieuprawnionym przetwarzaniem danych osobowych.
- niewykorzystywania danych osobowych oraz innych informacji w celach pozasłużbowych, o ile informacje te nie są jawne,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych oraz innych informacji, o ile informacje te nie są jawne,
- korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora,
- należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją przetwarzania danych osobowych,
- korzystania z komputerów przenośnych i innych urządzeń mobilnych zgodnie z zasadami przetwarzania danych osobowych przez użytkownika końcowego,
- nieudostępniania sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.

Jednocześnie zobowiązuję się do zachowania w tajemnicy przetwarzanych informacji oraz sposobów ich zabezpieczenia, także po zaprzestaniu ich przetwarzania lub ustaniu zatrudnienia.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów RODO oraz obowiązków służbowych.

.....

data i czytelny podpis oświadczającego

Załącznik nr 7 a) do Polityki Ochrony Danych Osobowych

Klauzula informacyjna dla kandydatów do pracy

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) informuję, iż:

1) administratorem Pani/Pana danych osobowych przetwarzanych w
2) kontakt z Inspektorem Ochrony Danych – adres mailowy: ....., listownie: na adres: ..... osobiście w siedzibie .....,
3) Pani/Pana dane osobowe przetwarzane będą w celu rekrutacji / przyszłych rekrutacji *- na podstawie Art. 6 ust. 1 lit. a ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.,
4) w przypadku podawania dodatkowych danych osobowych które nie są wymagane przepisami prawa proszę o wyraźne wskazanie zgody na ich przetwarzanie, gdyż brak takiej zgody będzie skutkować odrzuceniem Pani/Pana oferty,
5) Pani/Pana dane osobowe przechowywane będą przez okres rekrutacji / okres tej i przyszłych rekrutacji*,
6) posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, oraz prawo do cofnięcia zgody w dowolnym momencie. Cofnięcie zgody nie będzie wpływać na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem,
7) ma Pani/Pan prawo wniesienia skargi do Prezesa Ochrony Danych Osobowych,
8) podanie danych osobowych jest dobrowolne jednakże niepodanie danych może skutkować,
9) odbiorcami Pani/Pana danych osobowych będą.....

**niepotrzebne skreślić*

nr 7 b) do Polityki Ochrony Danych Osobowych

Klauzula informacyjna dla pracowników

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) informuję, iż:

1) administratorem Pani/Pana danych osobowych przetwarzanych w
2) kontakt z Inspektorem Ochrony Danych – adres mailowy: ....., listownie: na adres: ..... osobiście siedzibie.....,
3) Pani/Pana dane osobowe przetwarzane będą w celu zatrudniania i przyznawania świadczeń socjalnych - na podstawie art. 6 ust. 1 lit. a, c, art. 9 ust.2 lit. b ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.,
4) w przypadku podania danych osobowych które nie są wymagane przepisami prawa proszę o wyraźne wskazanie zgody na ich przetwarzanie,
5) odbiorcami Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa lub podmioty świadczące usługi na rzecz administratora na podstawie umowy powierzenia,
6) Pani/Pana dane osobowe przechowywane będą przez okres wskazany przepisami prawa, zgodnie z instrukcją kancelaryjną, jednolitym rzeczowym wykazem akt oraz instrukcją archiwalną oraz w oparciu o uzasadniony interes realizowany przez administratora ,
7) posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania a także prawo do cofnięcia zgody w dowolnym momencie*,
8) ma Pani/Pan prawo wniesienia skargi do Prezesa Ochrony Danych Osobowych
9) podanie danych osobowych jest obligatoryjne w oparciu o przepisy prawa a w pozostałym zakresie jest dobrowolne, niepodanie danych może skutkować niezawarciem umowy,
10) Pani/Pana dane będą/ nie będą* poddane zautomatyzowanemu podejmowaniu decyzji (profilowaniu) w celu* ....., (przewidywane konsekwencje takiego przetwarzania dla osoby, której dane dotyczą)
11) Pani/Pana dane będą/nie będą* przekazane odbiorcy w państwie trzecim lub organizacji międzynarodowej.

.....
(data i podpis)

* niepotrzebne skreślić

Załącznik nr 7 c) do Polityki Ochrony Danych Osobowych

Klauzula informacyjna dla umów-zleceń, umów o dzieło oraz z kontrahentami (osobami z bazy CEIDG)

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) informuję, iż:

1) administratorem Pani/Pana danych osobowych przetwarzanych w
2) kontakt z Inspektorem Ochrony Danych – adres mailowy: ....., listownie: na adres: .....osobiście siedzibie .....
3) Pani/Pana dane osobowe przetwarzane będą w celu realizacji umowy - na podstawie Art. 6 ust. 1 lit. b ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.,
4) odbiorcami Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa lub podmioty świadczące usługi na rzecz administratora na podstawie umowy powierzenia
5) Pani/Pana dane osobowe przechowywane będą przez czas określony przepisami prawa, nie krócej niż przez okres niezbędny do czasu zrealizowania celu oraz przedawnienia roszczeń w związku z zawartą umową.
6) posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz przenoszenia danych*
7) ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych
8) podanie danych osobowych jest dobrowolne, jednakże odmowa podania danych może skutkować odmową zawarcia umowy
9) Pani/Pana dane będą/nie będą* przekazane odbiorcy w państwie trzecim lub organizacji międzynarodowej.

.....
(data i podpis)

*niepotrzebne skreślić

Załącznik nr 7 d) do Polityki Ochrony Danych Osobowych

klauzula informacyjna ma zastosowanie w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą.

Zgodnie z art. 14 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) informuję, iż:

1. administratorem Pani/Pana danych osobowych przetwarzanych w
2. kontakt z Inspektorem Ochrony Danych – adres mailowy: ....., listownie: na adres: .....osobiście w siedzibie .....
3. Pani/Pana dane osobowe przetwarzane będą w celu .... na podstawie Art. 6 ust. 1 lit. a, b, c, d, e lub Art. 9 ust. l lit. a, b, c, d, h, i, j** ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.,
4. kategoria danych osobowych: dane
5. Pana/Pani dane osobowe pozyskano z (podać źródło [w tym źródło publiczne])
6. odbiorcami Pana/Pani danych osobowych będą (podać nazwę odbiorców lub kategorię odbiorców jeżeli istnieją) *
7. Pana/Pani dane osobowe przechowywane będą przez okres dni/lat, lub kryteria ustalania okresu (okres przechowywania może wynikać z instrukcji kancelaryjnej)
8. posiada Pani/Pan prawo do: żądania od administratora dostępu do danych osobowych, do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych, prawie do cofnięcia zgody w każdym momencie*
9. ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych
10. Pana/Pani dane będą/nie będą poddane zautomatyzowanym podejmowaniu decyzji (profilowaniu) w celu, (podać przewidywane konsekwencje takiego przetwarzania dla osoby, której dane dotyczą) *
11. Pani/Pana dane będą/nie będą* przekazane odbiorcy w państwie trzecim lub organizacji międzynarodowej

.....
(data i podpis)

* niepotrzebne skreślić
** wybrać podstawę w konkretnym przypadku

Załącznik nr 7 e) do Polityki Ochrony Danych Osobowych

Klauzula informacyjna

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) informuję, iż

1. administratorem Pani/Pana danych osobowych jest
2. kontakt z Inspektorem Ochrony Danych – adres mailowy: ....., listownie na adres:....., kontakt osobisty w siedzibie:
3. Pani/Pana dane osobowe przetwarzane będą w celu wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 c) RODO), wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 e) RODO), realizacji zawartych umów (art. 6 ust. 1 b) RODO).
4. odbiorcami Pana/Pani danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa lub podmioty świadczące usługi na rzecz administratora na podstawie umowy powierzenia.
5. Pana/Pani dane osobowe przechowywane będą przez okres wskazany przepisami prawa, zgodnie z instrukcją kancelaryjną, jednolitym rzeczowym wykazem akt oraz instrukcją archiwalną oraz w oparciu o uzasadniony interes realizowany przez administratora.
6. posiada Pani/Pan prawo do: żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie.
7. ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. podanie danych osobowych jest wymogiem ustawowym/ warunkiem zawarcia umowy/ dobrowolne/ *, jednakże niepodanie danych w zakresie wymaganym przez administratora będzie skutkować niezrealizowaniem Pani/Pana wniosku.
9. Pani/Pana dane będą/ nie będą* poddane zautomatyzowanemu podejmowaniu decyzji

   (profilowaniu) w celu* .....

   (przewidywane konsekwencje takiego przetwarzania dla osoby, której dane dotyczą)

   .....
10. Pani/Pana dane będą/nie będą* przekazane odbiorcy w państwie trzecim lub organizacji międzynarodowej.

* niepotrzebne skreślić

.....

(data i podpis)

Załącznik Nr 8 do Polityki Ochrony Danych

„Zasady korzystania z pomieszczeń i sprzętu OSIR w Głogowie Małopolskim, zabezpieczania ich po godzinach pracy oraz gospodarki kluczami"

1. Budynek OSIR w Głogowie Małopolskim wyposażony jest w zewnętrzny i wewnętrzny całodobowy monitoring wizyjny obsługiwany i nadzorowany przez upoważnionego pracownika. Zadaniem monitoringu jest obserwowanie i rejestrowanie ruchu osobowego na zewnątrz i wewnątrz budynku celem ustalenia i przeciwdziałania różnego rodzaju zagrożeniom bezpieczeństwa, w tym z zakresu ochrony danych osobowych.
2. W sprawach przebywania pracowników OSIR w budynku OSIR po godzinach urzędowania, mają zastosowanie odpowiednie przepisy Regulaminu Pracy OSIR w Głogowie Małopolskim.
3. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń sprzętu biurowego, komputerowego i innego wyposażenia, a także składowanej w tych pomieszczeniach dokumentacji. W przypadku stwierdzenia zmian lub naruszeń stanu zabezpieczeń , pracownik, który to stwierdził, natychmiast podejmuje niezbędne czynności zabezpieczające i powiadamia o zaistniałej sytuacji Dyrektora OSIR w Głogowie Małopolskim.
4. Pracownik opuszczający po pracy pomieszczenie powinien wyłączyć komputer, drukarkę, listwę zasilającą komputer i inne urządzenia elektryczne, jeżeli są w pomieszczeniu, zamknąć okna, zgasić światło, zamknąć na klucz szafy i biurka oraz pomieszczenie biurowe.
5. Klucze do pomieszczeń biurowych otrzymują wszyscy pracownicy, o ile dalsze przepisy niniejszego załącznika nie stanowią inaczej.
6. Pracownicy zatrudnieni na czas określony, w tym pracownicy interwencyjni, otrzymują klucze do pomieszczeń biurowych za zgodą Dyrektora OSIR w Głogowie Małopolskim, o ile występuje taka potrzeba.
7. Od momentu pobrania kluczy do momentu ich zdania, na pracownikach spoczywa pełna odpowiedzialność za ich zabezpieczenie w czasie pracy i po pracy przed utratą oraz nieudostępnianie osobom nieupoważnionym.
8. Klucze do pomieszczeń szczególnie chronionych np. serwerowni, pozostają pod osobistym nadzorem osób upoważnionych. Dostęp osób trzecich do tych pomieszczeń odbywa się pod ścisłym nadzorem osób upoważnionych.
9. Pomieszczenia biurowe podczas nieobecności pracowników powinny być zamykane.
10. W przypadku utraty klucza do pomieszczenia, pracownik winien ten fakt bezwzględnie zgłosić Dyrektorowi OSiR, która na tę okoliczność odbierze od pracownika pisemne oświadczenie. Niedopuszczalne jest dorabianie kluczy przez pracowników we własnym zakresie.
11. Za sprawdzenie stanu zabezpieczenia pomieszczeń i całego budynku OSiR, nadzorowanie systemów ochronnych (alarm przeciwpożarowy i alarm antywłamaniowy po godzinach urzędowania, odpowiedzialni są pracownicy ochraniarskiej, z którą OSiR ma zawartą umowę współpracy.

Procedura analizy ryzyka

Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Analiza ryzyka jest elementem procesu zarządzania ryzykiem.

Definicje

1. Zasoby (aktywa) - środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych
2. Naruszenie (Incydent) ochrony danych osobowych - to 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
3. Zagrożenie - potencjalne naruszenie (istnieje możliwość incydentu)
4. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia)
5. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów

Metodyka analizy ryzyka

1. Wyznaczenie zasobów podlegających analizie ryzyka
2. Opis przyjętego katalogu zagrożeń
3. Sposób wyliczenia ryzyka
4. Ryzyko akceptowalne
5. Reakcja na wartość ryzyka
6. Postępowanie z ryzykiem (zarządzanie ryzykiem)
7. Ponowna analiza ryzyka

WYZNACZENIE ZASOBÓW DO ANALIZY RYZYKA

Przyjęto, że analiza ryzyka przeprowadzana jest dla zasobów związanych z ochroną danych osobowych.

Zasobem związanym z ochroną danych osobowych nazywamy informacje w nim przetwarzane, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji.

W ramach identyfikacji ryzyka określono następujące kategorie zasobów systemu ochrony danych osobowych:

Kategorie zasobów systemu ochrony danych osobowych:

Kategorie zasobów systemu ochrony danych osobowych	Opis zasobów
INFORMACJE	zbiory danych osobowych, dane dostępowe (loginy, hasła, piny), dane dotyczące zabezpieczeń (klucze szyfrujące, certyfikaty), logi systemowe, dokumentacja techniczna, polityki bezpieczeństwa, procedury postępowania, umowy prawne

OPROGRAMOWANIE	systemy operacyjne, oprogramowanie użytkowe (pakiety biurowe, oprogramowanie dziedzinowe), serwery usługowe (www, poczta, serwery plików, bazy danych, usługi katalogowe), oprogramowanie administracyjne (wirtualizacja, inwentaryzacja, monitoring, backup), oprogramowanie układowe (firmware), strony www i aplikacje webowe
SPRZĘT KOMPUTEROWY	serwery (fizyczne i wirtualne), storage (macierze, NAS-y), stacje robocze (PC, laptopy, A-in-O), urządzenia mobilne (tablety, smartfony, komórki), urządzenia peryferyjne (drukarki, skanery), drukarki sieciowe,
NOSNIKI DANYCH	dokumentacja papierowa, dyski twarde (HDD i SSD) będące składnikami komputerów, komputerów przenośnych, macierzy dyskowych, przenośne dyski twarde (HDD i SSD). pen-drive, karty pamięci typu flash,, płyty CD/DVD, dyskietki, taśmy magnetyczne
OBSZARY CHRONIONE	Serwerownie , punkty dystrybucyjne sieci, punkty składowania i przetwarzania danych (elektronicznych i papierowych), rozdzielnie elektryczne, stanowiska portierni i monitoringu,
PERSONEL	Kompetencje, doświadczenie, szkolenia
DOSTAWCY	sprzęt i oprogramowanie, usługi chmurowe, usługi internetowe (hosting, dns), łącza telekomunikacyjne, usługi serwisowe i gwarancyjne, wsparcie techniczne

*Kategorie zasobów można rozszerzyć lub zawęzić w zależności od specyfiki i właściwości wydziału/komórki organizacyjnej.

Zbiory i zestawy danych osobowych mogą być przetwarzane w formie elektronicznej i/lub papierowej i mogą zawierać zarówno dane osobowe zwykłe jak i szczególne kategorie danych osobowych. W procesie analizy ryzyka powyższe zbiory i zestawy danych podlegają identyfikacji wg kategorii Szczegółowe dane - potrzebne w procesie analizy ryzyka - opisujące zbiory i zestawy danych osobowych przetwarzanych w Urzędzie zawiera Rejestr Czynności Przetwarzania.
Zbiory i zestawy danych osobowych w formie elektronicznej i papierowej zlokalizowane są zarówno w Urzędzie jak poza Urzędem - na podstawie Umów powierzenia, w których firmy (procesor) zobowiązane są do wykonywania własnej analizy ryzyka i udostępnienia wyników powierzającemu.

System teleinformatyczny służący do przetwarzania danych osobowych podlega analizie ryzyka jak dla szczególnych kategorii danych ze względów technicznych (brak wydzielonej sieci teleinformatycznej, wspólny dostęp do sieci publicznych, wspólna infrastruktura teleinformatyczna).

2 WYZNACZENIE ZAGROŻEŃ

1 Zagrożenia powinny być identyfikowane w odniesieniu do zasobów.

WYZNACZENIE KATALOGU MOŻLIWYCH ZAGROŻEŃ

Definicja: **zagrożenie** - potencjalne naruszenie (potencjalny incydent)

L. p.	Zagrożenia
1	Sfałszowanie, zniszczenie, zmiana dokumentów / danych
2	Błędy aplikacji, pomyłki administratorów, użytkowników
3	Złośliwe oprogramowanie, wirusy, hackerzy
4	Pożar, zalanie, wybuch obiektu/pomieszczeń
5	Brak / błędy w wykonywaniu kopii bezpieczeństwa
6	Nieaktualizowana / błędna dokumentacja
7	Wydawanie informacji /dokumentacji osobom nieuprawnionym
8	Pomyłkowe wysłanie danych do osób nieuprawnionych
9	Upublicznienie danych w internecie
10	Kradzież tożsamości
11	Zagubienie / kradzież dokumentacji / nośników poza organizacją
12	Porzucanie dokumentacji na zewnątrz, wyrzucanie na śmietnik
13	Przejęcie danych podczas przesyłania danych (internet, mail)
14	Niezabezpieczona naprawa zewnętrzna
15	Włamanie / nieautoryzowany dostęp do obiektu/pomieszczeń
16	Nieautoryzowany dostęp / włamanie do systemu
17	Nieuprawnione kopiowanie danych z aplikacji i systemów
18	Brak / niewłaściwe umowy współpracy / serwisu
19	Upadek firmy outsourcingowej dostawczej,
20	Zakończenie wsparcia oprogramowania / usługi outsourcingowej
21	Kradzież sprzętu
22	Utrata łączności internetowej
23	Braki zasilania

Kategorie zagrożeń można zawęzić lub rozszerzyć w zależności od specyfiki i właściwości wydziału/komórki organizacyjnej

3 WYLICZENIE RYZYKA DLA ZAGROŻEŃ

1. Administrator określa Prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń dla zasobów.
2.Proponowaną skalę prawdopodobieństwa prezentuje Tabela A
3.Administrator określa Skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne
4.Proponowaną Skalę skutków prezentuje Tabela B
5.Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: R = P * S

Definicja: ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów

Tabela A PRAWDOPODOBIEŃS TWO WYSTĄPIENIA ZAGROŻENIA (P)	SKALA (WAGA)
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Definicja: skutki - rezultat niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia)

Skalę prawdopodobieństwa wystąpienia zagrożenia można rozszerzyć (np.: 1 - 5)

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA (S)	SKALA (WAGA)
Małe	1
Średnie	2
Duże	3

Skalę skutków wystąpienia zagrożenia można rozszerzyć (np.: 1 - 5)

4 OKREŚLENIE RYZYKA AKCEPTOWALNEGO

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem
2. Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	WARTOŚĆ [R = P*S]
ryzyko pomijalne i akceptowalne	1-3
ryzyko jest opcjonalne	4-6
ryzyko jest nieakceptowalne	8-9

WARTOŚĆ RYZYKA ORAZ POZIOMY WYNIKA Z PRZYJĘTEJ SKALI SKUTKÓW I PRAWDOPODBIEŃSTWA.

5 REAKCJA NA WARTOŚĆ RYZYKA

1. Ryzyko akceptowalne: zabezpieczenia są właściwe - brak potrzeby stosowania dodatkowych zabezpieczeń,
2. Ryzyko opcjonalne: wymaga akceptacji lub działań obniżających ryzyko, które może zastosować Administrator:

a. Przeniesienie - przerzucenie ryzyka (outsourcing, ubezpieczenie)

b. Unikanie - eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji)

c. Redukcja - zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie nośników z danymi wynoszonych poza firmę)

3. Ryzyko nieakceptowalne: administrator musi podjąć koniecznie działania obniżające lub eliminujące ryzyko.

6 PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

Możliwe sposoby zabezpieczeń obniżające poziom ryzyka:

Lp.	Zabezpieczenia

1	Uregulowania dot. ochrony danych osobowych dla pracowników i współpracowników
2	Szkolenia personelu
3	Audyty
4	Testy penetracyjne
5	Procedury przywracania w razie incydentu
6	Polityka kluczy / polityka kontroli dostępu
7	Monitorowany dostęp do pomieszczeń i sprzętu
8	Zabezpieczenie dostępu do pomieszczeń (w tym biurowych)
9	Zabezpieczenie dostępu do serwerowni
10	Zabezpieczenie dostępu do archiwum
11	Zabezpieczenie dokumentacji w pomieszczeniach
12	Systemy alarmowe / zabezpieczenia antywłamaniowe
13	Ochrona fizyczna obiektu / pomieszczeń
14	Strefy dostępu
15	System kontroli dostępu
16	System ppoż.
17	Monitoring środowiskowy
18	Klimatyzacja
19	Monitoring wizyjny
20	Systemy UPS / agregaty prądotwórcze
21	Systemy antywirusowy i antyspamowy
22	Serwery proxy i bramki filtrujące
23	Systemy firewall, Sondy IDS / IPS, NG firewall, UTM
24	SIEM - Security Information and Event Management
25	Skanery podatności
26	Systemy do inwentaryzacji
27	Szyfrowanie i pseudonimizacja
28	Redundancja krytycznych zasobów
29	Aktualizacje systemu
30	Backupy i archiwizacja
31	Rozliczalność operacji
32	Procedury postępowania z nośnikami
33	Wirtualizacja
34	Zarządzanie uprawnieniami
35	Uwierzytelnianie
36	Umowy serwisowe
37	Procedury napraw w serwisach zewnętrznych

7 PONOWNA ANALIZA RYZYKA

Ponowna analiza ryzyka, wynikająca z przepływu i ochrony danych, przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne). Towarzyszący analizie ryzyka proces komunikacji w ramach jednostki organizacyjnej (zbieranie i wymiana informacji) jest procesem ciągłym w Urzędzie.

Ocena skutków dla ochrony danych

Obowiązek oceny skutków dla ochrony danych nie ma charakteru powszechnego, gdyż, zgodnie z art. 35 ust. 1 RODO, dotyczy administratorów, u których przetwarzanie danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Ocena skutków powinna odnosić się do skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

Organ nadzorczy określa i podaje do publicznej wiadomości wykaz rodzajów operacji, w odniesieniu do których przeprowadzenie oceny jest obligatoryjne, jak również wykaz operacji niepodlegających wymogowi dokonania oceny skutków dla ochrony danych.

Artykuł 35 ust. 7 RODO określa minimalne wymogi co do zawartości oceny skutków dla ochrony danych. Obowiązek przeprowadzenia oceny został wyłączony gdy przetwarzanie jest niezbędne do:

1) wypełnienia obowiązku prawnego ciążącego na administratorze,
2) wykonania zadania realizowanego w interesie publicznym oraz

w ramach sprawowania władzy publicznej powierzonej administratorowi, a oceny skutków dokonano na etapie prac legislacyjnych.

Administrator dokonuje przeglądu dla sprawdzenia, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych. Jeżeli ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko, a administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator (działając zgodnie z art. 36 RODO) powinien skonsultować się z organem nadzorczym.

Krok: zamiar przetwarzania danych osobowych

Przed przystąpieniem do przetwarzania danych administrator powinien sprawdzić, czy dany rodzaj przetwarzania nie wymaga przeprowadzenia oceny skutków dla ochrony danych.

Krok: sprawdzenie, czy ocena skutków dla ochrony danych została przeprowadzona w ramach prac legislacyjnych

Administrator nie ma obowiązku przeprowadzania oceny skutków dla ochrony danych w przypadku, gdy:

1) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (tzn. opiera się na podstawie wskazanej w art. 6 ust. 1 lit. c RODO)
2) administrator wykonuje zadanie realizowane w interesie publicznym (art. 6 ust. 1 lit. e RODO)
3) administrator w ramach sprawowania władzy publicznej ma podstawę prawną, a oceny skutków dokonano na etapie prac legislacyjnych.

Krok: brak obowiązku przeprowadzenia oceny skutków dla ochrony danych

We wskazanych w art. 35 RODO przypadkach administrator nie ma obowiązku przeprowadzania oceny dla ochrony danych. W tych przypadkach wystarczy dokonanie

analizy ryzyka oraz przyjęcie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzanych danych.

Krok: sprawdzenie, czy dany rodzaj przetwarzania podlega obowiązkowej ocenie skutków

Przeprowadzenie oceny skutków dla ochrony danych jest wymagane w przypadku:

1) 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,

2) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO jak również danych osobowych dotyczących wyroków skazujących i naruszeń prawa (o których mowa w art. 10 RODO),

3) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Organ nadzorczy określa wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych.

Krok: ocena, czy dany rodzaj przetwarzania został wskazany jako niepodlegający ocenie skutków

Organ nadzorczy określa wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych.

Krok: sprawdzenie, czy dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób

Zgodnie z przepisem art. 35 ust. 1 RODO, jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania powinien dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

Jeżeli administrator stwierdzi, że ryzyko nie jest wysokie, to nie ma obowiązku przeprowadzać oceny skutków dla ochrony danych.

Krok: przeprowadzenie oceny skutków dla ochrony danych

Ocena skutków dla ochrony danych powinna zawierać co najmniej (art. 35 ust. 7) RODO:

1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora;

2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;

3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;

4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia

5) środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób. których dane dotyczą, i innych osób, których sprawa dotyczy.

Z uwagi na zasadę rozliczalności, wyniki przeprowadzonej przez administratora oceny skutków dla ochrony danych powinny być utrwalone na piśmie (w postaci tradycyjnej lub elektronicznej).

Krok: konsultacje z inspektorem ochrony danych

Przy dokonywaniu oceny skutków dla ochrony danych administrator powinien konsultować się z inspektorem ochrony danych, jeżeli został on wyznaczony.

Krok: zasięgnięcie opinii osób, których dane dotyczą

Administrator w stosownych przypadkach (art. 35 ust. 9 RODO) zasięga opinii osób. których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych albo bezpieczeństwa operacji przetwarzania. Oznacza to, że administrator nie ma obowiązku zasięgania opinii w każdym przypadku, a jedynie wówczas, gdy takie opinie mogą mieć istotne znaczenie dla oceny skutków, natomiast przy zasięganiu opinii administrator nie ma obowiązku podawania informacji, które mogłyby powodować zagrożenie jego interesów handlowych (np. ujawnienie tajemnicy przedsiębiorstwa) lub bezpieczeństwa operacji przetwarzania (np. ujawnienie szczegółowych informacji o zabezpieczeniach).

Krok: dokonanie przeglądu zgodności przetwarzania z oceną skutków dla ochrony danych

Zgodnie z art. 35 ust. 11 RODO w razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych. O potrzebie dokonania przeglądu decyduje administrator, przy czym przegląd powinien być dokonany wówczas, gdy zmieni się ryzyko, natomiast administrator może zdecydować o dokonywaniu przeglądów także w innych przypadkach.

Krok: konsultacje z organem nadzorczym

Jeżeli ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko, a administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator powinien skonsultować się z organem nadzorczym, zgodnie z art. 36 RODO.

Załącznik nr 12 do Polityki Ochrony Danych Osobowych

Rejestr naruszeń

Naruszenie (stypizowany opis naruszeń)	
Data i godzina zgłoszenia podejrzenia naruszenia	
Data i godzina stwierdzenia naruszenia	
Data naruszenia/okres którego dotyczy	
Zakres danych lub kategorii danych, którego dotyczy naruszenie	
Osoba/ źródło informacji o zdarzeniu	
Miejsce naruszenia	
Okoliczności naruszeń- opis charakteru naruszeń, analiza zdarzeń, przyczyny	
Opis skutków/ konsekwencji naruszeń	
Podjęte działania, opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu, w tym zastosowania środków w celu	

zminimalizowania jego negatywnych skutków	
Osoba odpowiedzialna za wdrożenie działań naprawczych	
Rezultat działań naprawczych	
Czy zachodzi potrzeba poinformowania Prezesa Urzędu Ochrony danych Osobowych (jeżeli tak data godzina zgłoszenia, jeżeli wystąpiło opóźnienie – przyczyny)	
Czy zachodzi potrzeba poinformowania osoby, której naruszenie danych osobowych dotyczy (jeżeli tak, data zgłoszenia)	
Ocena skuteczności	

Załącznik nr 13 do Polityki Ochrony Danych Osobowych

Raport o naruszeniu danych osobowych

1. Opis naruszenia ochrony danych osobowych

W dniu ..... zidentyfikowano w Urzędzie Miejskim w Głogowie Małopolskim naruszenie ochrony danych osobowych w zakresie ujawnienia (wskazać rodzaj danych osobowych):

- .....
- .....
- .....

2. Kategoria i przybliżona liczba osób/wpisów danych których dotyczy naruszenie

.....

.....

3. Możliwe konsekwencje naruszenia ochrony danych osobowych

.....

.....

4. Opis środków zastosowanych lub proponowanych do zastosowania w celu zaradzenia naruszeniu ochrony danych osobowych.

.....

.....

.....

(data i podpis)

Załącznik nr 15 do Polityki Ochrony Danych Osobowych

Plan szkolenia z zakresu znajomości zasad ochrony danych osobowych

Program szkolenia układany w porozumieniu z Burmistrzem Głogowa Małopolskiego

Lista uczestników szkolenia z zakresu Ochrony Danych Osobowych

Prowadzący:

Miejsce i data szkolenia:

L.P.	Imię i nazwisko	Podpis

Załącznik nr 13 do Polityki Ochrony Danych

Instrukcja zarządzania systemem informatycznym w Ośrodku Sportu i Rekreacji w Głogowie Małopolskim

§ 1

Postanowienia ogólne

Użyte w Instrukcji określenia i skróty oznaczają:

1. Administrator danych osobowych Ośrodku Sportu i Rekreacji w Głogowie Małopolskim (dalej: OSIR), reprezentowany przez Dyrektora OSIR w Głogowie Małopolskim ,
2. Dane osobowe - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
3. Hasło –ciąg znaków literowych, cyfrowych, lub innych, znane jedynie użytkownikowi,
4. Identyfikator – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
5. Integralność danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
6. Użytkownik – osoba upoważniona do przetwarzania danych osobowych, której nadano hasło i przyznano identyfikator,
7. Poufność danych – to właściwość, że dane nie są udostępniane nieupoważnionym podmiotom,
8. Sieć telekomunikacyjna - sieć telekomunikacyjna w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 roku – Prawo telekomunikacyjne (Dz.U.2017.1907 j.t.),
9. Teletransmisja – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
10. System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, stosowanych w celu przetwarzania danych osobowych,
11. Uwierzytelnienie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§2

Procedury nadawania i rejestrowania uprawnień do przetwarzania danych osobowych w systemach informatycznych

1. Przetwarzać dane osobowe może wyłącznie pracownik upoważniony przez administratora danych, który posiada nadane hasło i identyfikator.
2. Hasła dostępu opracowuje się indywidualnie dla każdego uprawnionego użytkownika systemu i natychmiast zmienia w wypadku podejrzenia lub stwierdzenia ujawnienia ich osobom trzecim.
3. Każdemu pracownikowi / użytkownikowi Administrator Systemu Informatycznego (ASI) ustala hasła dostępu do systemów informatycznych i jeśli to możliwie system wymusza automatyczną zmianę hasła po pierwszym logowaniu.
4. Hasło do systemu informatycznego ASI przekazuje właściwemu użytkownikowi.
5. Hasła dostępu zapisywane są na ekranie monitora w formie niejawnej i mogą być znane użytkownikowi i ASI. Hasła dostępu nie mogą powtarzać się w danym roku.
6. Zmianę hasła do systemu informatycznego wymusza serwer automatycznie co 30 dni co powoduje, że wszyscy użytkownicy / pracownicy OSIR są zmuszeni do jego zmiany (o ile jest to możliwe).
7. Osobą odpowiedzialną za techniczny sposób ustalania, przechowywania i wprowadzania haseł jest ASI.
8. Identyfikatory dla użytkowników przydziela ASI. Identyfikator po wyrejestrowaniu danej osoby z systemu nie może być przydzielony innemu użytkownikowi.
9. Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemach informatycznych przy użyciu identyfikatora i hasła, którymi się posługuje lub posługiwał.
10. Użytkownik zobowiązany jest do utrzymania haseł dostępu w tajemnicy, nawet po ustaniu ich ważności.

§3

Rejestrowanie i wyrejestrowanie użytkowników

1. Rejestrowanie i wyrejestrowania użytkowników z systemu informatycznego dokonuje ASI na podstawie informacji o zatrudnieniu lub ustaniu zatrudnienia uzyskanej od Dyrektora OSIR.
2. Zarejestrowanie użytkownika w systemie wymaga spełnienia następujących warunków:

a) złożenie pisemnego wniosku przez Dyrektora OSIR do KASI lub osoby upoważnionej przez niego o udzielenie wskazanej osobie dostępu do przetwarzania danych osobowych, według wzoru zawartego w załączniku Nr 1 do Instrukcji,

3. Z chwilą zarejestrowania w systemie użytkownik jest informowany przez KASI o ustalonym dla niego identyfikatorze i obowiązku posługiwania się hasłem dostępu.
4. Użytkownika wyrejestrowuje się z systemu na pisemny wniosek Dyrektora do KASI / IOD – po utracie uprawnień dostępu do przetwarzania danych osobowych, co może mieć miejsce w sytuacjach:
   a) ustania zatrudnienia użytkownika w OSIR,
   b) zmiany zakresu obowiązków użytkownika.

5. Ustanie zatrudnienia powoduje utratę dostępu do przetwarzania danych i natychmiastowe wyrejestrowanie użytkownika z systemu do przetwarzania danych i natychmiastowe wyrejestrowanie użytkownika z systemu oraz unieważnienie jego hasła.

§4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy użytkowników systemu informatycznego

1. Użytkownik rozpoczynający pracę, zobowiązany jest przestrzegać procedury mającej na celu sprawdzenie zabezpieczeń systemu, a w szczególności:
   a) sprawdzenie zabezpieczeń fizycznych pomieszczenia,
   b) sprawdzenie ogólnego stanu sprzętu informatycznego oraz miejsca przechowywania nośników zawierających dane osobowe,
2. Użytkownik rozpoczyna pracę od:
   a) włączenia komputera,
   b) uwierzytelnienia się za pomocą loginu i hasła,
3. Zakończenie pracy w systemie następuje po wylogowaniu się z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, dokumenty, wydruki zawierające dane osobowe przed dostępem osób nieupoważnionych,
4. W przypadku dłuższego opuszczenia stanowiska pracy, użytkownik zobowiązany jest wylogować się lub wygasić ekran monitora,
5. Przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji dotyczące pracy na komputerach stacjonarnych,
6. Pracownicy, którym zostały powierzone komputery przenośne powinni je chronić przed uszkodzeniem, kradzieżą i dostępem osób postronnych.

§ 5

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.
2. W celu zapewnienia bezpieczeństwa w systemie informatycznym, przetwarzającym dane osobowe, istnieje obowiązek tworzenia kopii zapasowych.
3. Kopie zapasowe przeznaczone są odtworzenia zbioru danych lub systemu, w przypadku całkowitej lub częściowej zmiany, utraty, uszkodzenia czy tez zniszczenia zbioru danych bądź systemu,

4. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w szafkach zamykanych na klucz,
5. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.

§6

Sposoby, miejsca i okresy przechowywania nośników informacji z danymi osobowymi

Urządzenia, dyski lub inne nośniki informacji, zawierające dane osobowe, przeznczone do:

1. Likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
2. Przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
3. Naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§7

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie dostępu do systemu informatycznego

1. Obszarami systemu informatycznego narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są m.in. :
   a) Dysk twardy,
   b) Pamięć RAM,
   c) Elektroniczne nośniki informacji np. płyty CD/DVD, pamięci USB,
2. Droga przedostania się wirusów i szkodliwego oprogramowania do systemu mogą być sieci informatyczne, zainfekowane elektroniczne nośniki danych oraz załączniki poczty e-mail, pochodzące od nieznanych nadawców,
3. Sprawdzenie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu specjalistycznego oprogramowania antywirusowego, zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych,
4. Za ochronę antywirusową systemu informatycznego odpowiada administrator danych osobowych,
5. System antywirusowy zainstalowany jest w każdym komputerze,
6. Program antywirusowy jest uaktywniony przez cały czas pracy każdego komputera w systemie informatycznym,
7. Wszystkie pliki otrzymane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów, z zastosowaniem najnowszej dostępnej wersji programu antywirusowego.

8. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić administratora danych osobowych.
9. Urządzenia i nośniki, zawierające dane osobowe, które są przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez hasło dostępu,
10. W przypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy zastosować szczególne środki bezpieczeństwa, które obejmują:
    a) Zastosowanie mechanizmów szyfrowania danych osobowych,

§ 8
Procedury wykonywania przeglądów, napraw i konserwacji systemów oraz nośników informacji, służących do przetwarzania danych osobowych

1. KSI dokonuje przeglądów i konserwacji systemu informatycznego, które mają na celu:
    a) Przegląd stosowanych elementów bezpieczeństwa,
    b) Kontrolowanie właściwej konfiguracji systemu,
    c) Sprawdzenie funkcjonalności i jakości pracy systemu,
    d) Zakwalifikowanie sprzętu i urządzeń do naprawy lub modyfikacji,
2. Zakres czynności, o których mowa w ust. 1 pkt a, obejmuje w szczególności:
    a) Sprawdzenie działania urządzeń zabezpieczających przed nieuprawnionym dostępem,
    b) Kontrolę działania awaryjnego zasilania,
    c) Kontrole czasu uaktywnienia wygaszaczy ekranu oraz sposobu ich zabezpieczenia,
    d) Sprawdzenie poprawności wykonania kopii bezpieczeństwa
3. Zakres czynności, o których mowa w ust. 1 pkt b i c, obejmuje:
    a) Sprawdzenie poprawności zainstalowanych aplikacji i urządzeń,
    b) Inwentaryzację zainstalowanego oprogramowania, służącego do przetwarzania danych osobowych,
4. Naprawy prowadzone są pod nadzorem i w siedzibie administratora (jeśli to możliwe) lub poza siedzibą administratora po zobowiązaniu serwisanta do zachowania tajemnicy i ochrony danych osobowych, na podstawie zawartej umowy.

§9
Przeglądy i aktualizacje

Instrukcja zarządzania systemami informatycznymi podlega przeglądowi i aktualizacji w przypadku:

1. zmian w przepisach prawa wymagających aktualizacji Instrukcji zarzadzania systemami informatycznymi,
2. innych znaczących zmian dotyczących bezpieczeństwa przetwarzania danych osobowych,
3. w celu realizacji rekomendacji i zaleceń wynikających z przeprowadzonych kontroli i audytów.

§10
Sposób postępowania w zakresie komunikacji w sieci komputerowej

1. Przeglądarka Internet Explorer powinna mieć ustawione opcje tak, by nie zapamiętywała nazwy użytkownika oraz hasła.
2. Komunikacja w sieci komputerowej dozwolona jest tylko po odpowiednim zalogowaniu się i podaniu indywidualnego hasła użytkownika
3. Przekazywanie danych osobowych za pomocą komunikacji internetowej jest możliwe każdorazowo po uzyskaniu zgody Administratora Danych Osobowych.
4. Dotyczy to także danych zamieszczanych na stronie placówki.

Załącznik Nr 1 do „ Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w OSIR w Głogowie Małopolskim".

.....
(pieczęć komórki organizacyjnej)

Głogów Małopolski dn. .....

Administrator Danych Osobowych
w OSIR
w Głogowie Małopolskim

Na podstawie § 3 „ Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w OSIR w Głogowie Małopolskim".

w n i o s k u j ę o udzielenie (pozbawienie)*

Pani/Pana/*.....
dostępu do przetwarzania danych osobowych w systemach informatycznych w OSIR w Głogowie Małopolskim **z powodu :/** przyjęcia do pracy, przejścia na inne stanowisko, zwolnienia z pracy?* lub innego (jakiego?):

.....
(Zgodnie z nadanym zakresem obowiązków)

1. **Uprawnienia**: .....
   .....
   (wymienić nazwy programów)

2. Miejsce przetwarzania (adres siedziby).....
   danych osobowych (piętro, nr pokoju).....

3. Wprowadzono poprawki do obowiązków pracownika, dotyczące zakresu przetwarzania danych osobowych i odpowiedzialności za to: **tak/ nie***

4. ASI dodaje adnotacje o nadaniu uprawnień

   .....
   .....

.....
(data i podpis)