Dokumentacja Ochrony Danych Osobowych (RODO) – Muzeum Miejskie w Jastrzębiu-Zdroju

Spis treści

Wstęp

Niniejsza dokumentacja została opracowana zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) oraz Ustawą z 10 maja 2018 r. o ochronie danych osobowych. Uwzględnia również wytyczne Urzędu Ochrony Danych Osobowych (UODO) oraz dobre praktyki instytucji kultury w Polsce. Dokumentacja składa się z następujących części:

- **Polityka ochrony danych osobowych** – ogólne zasady, cele i podstawy prawne przetwarzania oraz odpowiedzialność Administratora.
- **Rejestr czynności przetwarzania danych** – ewidencja wszystkich procesów przetwarzania danych w muzeum.
- **Klauzule informacyjne** – obowiązki informacyjne RODO dla pracowników, kontrahentów i gości (zwiedzających, uczestników wydarzeń).
- **Procedura realizacji praw osób, których dane dotyczą** – sposób obsługi żądań dostępu, sprostowania, usunięcia itp.
- **Procedura zgłaszania naruszeń ochrony danych** – postępowanie w razie incydentów i zgłaszanie ich UODO.
- **Upoważnienia do przetwarzania danych i ewidencja upoważnień** – wzory dokumentów autoryzujących personel do przetwarzania danych.
- **Umowy powierzenia przetwarzania danych** – wzory umów z podmiotami przetwarzającymi dane w imieniu muzeum.
- **Polityka retencji danych** – zasady przechowywania i usuwania danych po upływie okresów niezbędnych do celów przetwarzania.
- **Procedury dotyczące nośników danych i dokumentacji papierowej** – bezpieczne obchodzenie się z dokumentami i urządzeniami zawierającymi dane.
- **Zakres obowiązków Inspektora Ochrony Danych (IOD)** – opis zadań IOD, jeśli został powołany.

Poniżej przedstawiono poszczególne elementy dokumentacji w formie gotowej do wdrożenia.

Polityka Ochrony Danych Osobowych

Polityka ochrony danych osobowych jest nadrzędnym dokumentem wewnętrznym określającym ramy przetwarzania danych osobowych w Muzeum Miejskim w Jastrzębiu-Zdroju. Celem polityki jest zapewnienie zgodności działań muzeum z przepisami RODO oraz krajowymi przepisami o ochronie danych. Polityka ustanawia zasady postępowania z danymi osobowymi, obowiązujące wszystkich pracowników i współpracowników

muzeum, a także określa odpowiedzialność Administratora Danych (Dyrektora Muzeum) za przestrzeganie tych zasad.

Podstawy prawne: Przetwarzanie danych osobowych odbywa się w oparciu o art. 6 i 9 RODO oraz odpowiednie przepisy krajowe. Administrator zapewnia, że każda operacja na danych ma swoją podstawę prawną (np. zgoda osoby, obowiązek prawny, wykonanie umowy, zadanie w interesie publicznym lub prawnie uzasadniony interes). Muzeum jako instytucja publiczna przestrzega też szczególnych przepisów branżowych dotyczących przechowywania dokumentacji (np. archiwizacyjnych).

Zakres stosowania: Polityka ma zastosowanie do wszelkich procesów przetwarzania danych osobowych w muzeum – zarówno w formie elektronicznej, jak i papierowej – we wszystkich komórkach organizacyjnych. Dotyczy danych osobowych pracowników, wolontariuszy, kontrahentów, zwiedzających, uczestników wydarzeń oraz innych osób, których dane muzeum przetwarza w związku ze swoją działalnością statutową.

Zasady ochrony danych: Administrator danych zobowiązuje się do przestrzegania ogólnych zasad przetwarzania danych osobowych określonych w art. 5 RODO. W szczególności Muzeum stosuje następujące zasady:

- **Zgodność z prawem, rzetelność i przejrzystość:** Dane osobowe są przetwarzane w sposób zgodny z prawem, rzetelny i zrozumiały dla osoby, której dotyczą. Osoby, których dane dotyczą, informowane są o celach i podstawach przetwarzania (patrz *Klauzule informacyjne*).
- **Ograniczenie celu:** Dane zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie są dalej przetwarzane w sposób niezgodny z tymi celami. Muzeum nie wykorzystuje danych w nowych celach nieprzewidzianych pierwotnie, chyba że dysponuje odrębną podstawą prawną.
- **Minimalizacja danych:** Przetwarzane są wyłącznie dane adekwatne, stosowne oraz ograniczone do niezbędnego minimum wymaganego do realizacji celu. Muzeum unika zbierania danych „na zapas" i nie wymaga podawania informacji niezwiązanych z danym celem.
- **Prawidłowość danych:** Muzeum dba o to, by dane osobowe były poprawne i w razie potrzeby aktualizowane. Wprowadzone zostały mechanizmy korygowania i aktualizacji danych – na żądanie osoby lub z inicjatywy muzeum – aby usunąć lub sprostować nieprawidłowe informacje.
- **Ograniczenie przechowywania:** Dane przechowywane są w formie umożliwiającej identyfikację osoby tylko tak długo, jak to konieczne do realizacji celów przetwarzania. Po osiągnięciu celu dane są usuwane lub anonimizowane zgodnie z *Polityką retencji danych*. Muzeum przestrzega obowiązujących przepisów archiwizacyjnych przy określaniu okresów przechowywania.

- **Integralność i poufność:** Dane przetwarzane są w sposób zapewniający ich bezpieczeństwo – ochronę przed nieuprawnionym lub przypadkowym dostępem, modyfikacją, ujawnieniem, utratą czy zniszczeniem. Wdrożono odpowiednie środki techniczne i organizacyjne (patrz *Procedury nośników i dokumentacji* oraz *Bezpieczeństwo IT*). Dostęp do danych mają wyłącznie osoby upoważnione.
- **Rozliczalność:** Muzeum dokumentuje wszystkie istotne działania związane z przetwarzaniem danych, aby móc wykazać zgodność z przepisami. Polityka ta, wraz z pozostałą dokumentacją RODO, jest elementem realizacji zasady rozliczalności (art. 5 ust.2 RODO), która wymaga od Administratora nie tylko przestrzegania przepisów, ale także zdolności do wykazania tej zgodności.
- **Privacy by design/default:** Już na etapie planowania nowych przedsięwzięć muzeum uwzględnia kwestię ochrony danych. Domyślnie przetwarzane są tylko dane niezbędne do celu (zasada minimalizacji), a w systemach informatycznych wprowadzane są ustawienia zapewniające najwyższy poziom prywatności. Nowe projekty poddawane są ocenie pod kątem wpływu na ochronę danych, a w razie potrzeby przeprowadzana jest formalna **ocena skutków dla ochrony danych (DPIA)** zgodnie z art. 35 RODO.
- **Dokumentacja i nadzór:** Polityka jest poddawana okresowym przeglądom i aktualizacjom w razie zmian przepisów lub procesów. Administrator wyznaczył **Inspektora Ochrony Danych (IOD)** (patrz niżej), który monitoruje przestrzeganie niniejszej Polityki i przepisów prawa. Wszyscy pracownicy zostali zapoznani z Polityką i zobowiązani do jej stosowania w zakresie swoich obowiązków służbowych.

Odpowiedzialność administratora: Muzeum, jako Administrator Danych, ponosi odpowiedzialność za zgodne z prawem przetwarzanie danych i bezpieczeństwo informacji. Administrator wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia ochrony danych (m.in. szyfrowanie, zabezpieczenia fizyczne pomieszczeń, środki kontroli dostępu). Obowiązki Administratora obejmują m.in. prowadzenie wymaganej dokumentacji (np. rejestru czynności), szkolenie personelu z zasad ochrony danych, reagowanie na incydenty naruszenia oraz współpracę z organem nadzorczym. Administrator dba również o to, by każdy pracownik lub współpracownik przetwarzający dane osobowe posiadał odpowiednie upoważnienie i działał zgodnie z nadanymi mu uprawnieniami (szczegóły w sekcji *Upoważnienia*).

Inspektor Ochrony Danych: Zgodnie z art. 37 RODO, muzeum powołało Inspektora Ochrony Danych. IOD podlega bezpośrednio Dyrektorowi muzeum i pełni niezależną rolę doradczą i kontrolną w zakresie zgodności z RODO (szczegółowy zakres zadań IOD opisano w rozdziale poniżej). Dane kontaktowe IOD udostępniono we wszystkich klauzulach informacyjnych, aby osoby, których dane dotyczą, mogły łatwo nawiązać kontakt w sprawach związanych z danymi osobowymi.

Rejestr czynności przetwarzania danych

Muzeum prowadzi **Rejestr Czynności Przetwarzania Danych Osobowych**, zgodnie z art. 30 RODO. Rejestr ten dokumentuje wszystkie główne operacje przetwarzania danych osobowych realizowane przez muzeum jako Administratora. Ma on formę tabelaryczną i jest przechowywany w formie elektronicznej (z możliwością wydruku). Za utrzymanie i aktualizację rejestru odpowiada Administrator Danych we współpracy z IOD.

Zakres informacji w rejestrze: Dla każdej zidentyfikowanej czynności przetwarzania rejestr zawiera co najmniej następujące informacje:

- **Nazwa procesu przetwarzania:** opis czynności lub obszaru (np. „Rekrutacja pracowników", „Obsługa umów z dostawcami", „Monitoring wizyjny").
- **Cel przetwarzania:** jasne określenie, w jakim celu gromadzone i wykorzystywane są dane (np. rekrutacja i zatrudnienie, realizacja umowy sprzedaży biletów, cele archiwalne, edukacyjne itp.).
- **Podstawa prawna:** podstawa prawna dla danego procesu (np. art. 6 ust.1 lit. b RODO – wykonanie umowy z osobą, art. 6 ust.1 lit. c – obowiązek prawny z ustawy o rachunkowości, art. 6 ust.1 lit. e – zadanie publiczne muzeum itp., a w razie przetwarzania szczególnych kategorii danych – właściwa podstawa z art. 9 ust.2 RODO).
- **Kategorie danych osobowych:** jakie rodzaje danych są przetwarzane (np. dane identyfikacyjne: imię, nazwisko, PESEL; dane kontaktowe: adres, e-mail, telefon; dane finansowe; wizerunek z monitoringu; dane wrażliwe – jeśli dotyczy).
- **Kategorie osób, których dane dotyczą:** grupy osób, których dane obejmuje proces (np. pracownicy, kandydaci do pracy, kontrahenci/osoby kontaktowe u dostawców, zwiedzający, uczestnicy warsztatów edukacyjnych, użytkownicy strony internetowej).
- **Kategorie odbiorców danych:** komu dane są przekazywane lub ujawniane, w tym odbiorcy zewnętrzni (np. firma kadrowa, obsługa IT, biuro rachunkowe) oraz odbiorcy wewnętrzni (działy muzeum, upoważnieni pracownicy). Wskazuje się także ewentualne przekazywanie danych do państw trzecich lub organizacji międzynarodowych (jeśli ma miejsce, wraz z podstawą prawną takiego transferu).
- **Okres przechowywania danych:** przez jaki czas dane będą przechowywane – konkretny okres lub kryterium jego ustalenia (np. „dane kandydatów niewybranych – 6 miesięcy od zakończenia rekrutacji", „dane pracowników – 10 lat od ustania zatrudnienia zgodnie z przepisami prawa pracy", „nagrania monitoringu – 30 dni, następnie automatyczne nadpisanie").

- **Opis środków ochrony:** (opcjonalnie) ogólny opis zastosowanych zabezpieczeń technicznych i organizacyjnych dla danej kategorii przetwarzania, jeżeli jest to potrzebne do zrozumienia ryzyk (np. szyfrowanie bazy danych, dostęp tylko dla określonych pracowników, pomieszczenia zabezpieczone alarmem itp.).
- **Ewentualne uwagi:** dodatkowe informacje, np. jeśli przetwarzanie podlega ocenie skutków (DPIA) lub jest realizowane wspólnie z innym administratorem.

Rejestr czynności jest **aktywnie utrzymywanym dokumentem** – powinien być na bieżąco aktualizowany w razie zmiany procesu lub pojawienia się nowego rodzaju przetwarzania. Przegląd rejestru dokonywany jest co najmniej raz do roku w celu weryfikacji kompletności i poprawności wpisów. UODO wymaga, aby taki rejestr istniał i był udostępniony na żądanie w razie kontroli. Muzeum, choć z racji wielkości i charakteru (podmiot publiczny) jest zobowiązane do posiadania rejestru, traktuje go przede wszystkim jako narzędzie wewnętrzne do monitorowania procesów przetwarzania i identyfikowania obszarów wymagających ewentualnych ulepszeń w zakresie bezpieczeństwa danych.

Klauzule informacyjne (obowiązek informacyjny)

Zgodnie z art. 13 i 14 RODO, muzeum realizuje wobec osób, których dane dotyczą, tzw. **obowiązek informacyjny**. Oznacza to, że przekazuje tym osobom wymagane informacje o przetwarzaniu ich danych. W tym celu przygotowane zostały odrębne **klauzule informacyjne** dostosowane do poszczególnych kategorii osób:

- **Klauzula dla pracowników/ kandydatów do pracy:** wręczana przy zbieraniu danych od kandydatów (np. w formularzu aplikacyjnym) oraz udostępniana pracownikom przy zatrudnieniu. Zawiera informacje m.in. o administratorze (muzeum), celu przetwarzania danych pracowniczych (realizacja procesu rekrutacji lub zatrudnienia), podstawie prawnej (m.in. Kodeks pracy, art. 6 ust.1 lit. b i c RODO), okresie przechowywania akt pracowniczych, odbiorcach danych (np. ZUS, US, firma medycyny pracy), a także o prawach pracownika (dostęp, sprostowanie, itp.). W przypadku rekrutacji zewnętrznej (dane pozyskane z portali lub agencji) stosuje się art. 14 RODO – kandydat informowany jest najpóźniej przy pierwszym kontakcie.
- **Klauzula dla kontrahentów/partnerów biznesowych:** przekazywana osobom fizycznym, z którymi muzeum zawiera umowy cywilnoprawne (np. zleceniobiorcy, artyści, dostawcy usług) lub które reprezentują kontrahentów (np. osoby kontaktowe wskazane w umowach). Informuje m.in. o celu przetwarzania danych w związku z wykonaniem umowy (art. 6 ust.1 lit. b RODO) lub obowiązkami prawnymi (rachunkowość – art. 6 ust.1 lit. c), czasie przechowywania (np. 5 lat dla dokumentów księgowych), odbiorcach (np. bank, kurier, organy kontrolne) oraz prawach tych osób. W przypadku danych pozyskanych nie bezpośrednio od

osoby (np. gdy kontrahent podaje dane swojego pracownika do kontaktu), spełniany jest obowiązek z art. 14 RODO – np. klauzula przesyłana e-mailem.

- **Klauzula dla gości i uczestników wydarzeń:** dostępna np. przy zakupie biletu, rezerwacji zwiedzania, zapisie na newsletter, udziale w konkursach czy warsztatach organizowanych przez muzeum. Informuje zwiedzających i uczestników o tym, że administratorem ich danych jest Muzeum, podaje dane kontaktowe (w tym IOD), określa cele przetwarzania (np. rezerwacja wizyty – art. 6 ust.1 lit. b; marketing – art. 6 ust.1 lit. a – zgoda; zapewnienie bezpieczeństwa na terenie muzeum – art. 6 ust.1 lit. e), czas przechowywania (np. dane rezerwacji – do czasu realizacji usługi + okres archiwizacji, monitoring – 30 dni), odbiorców (np. dostawca systemu biletowego) oraz prawa przysługujące odwiedzającym. W klauzuli tej zawarte są także informacje dotyczące monitoringu wizyjnego, jeżeli jest prowadzony – w szczególności oznaczone są strefy objęte kamerami, a informacja o monitoringu jest wywieszona przy wejściu do muzeum.

Zakres informacji w klauzulach: Każda klauzula informacyjna zawiera wszystkie elementy wymagane przez RODO:

- Tożsamość i dane kontaktowe Administratora: Muzeum Miejskie w Jastrzębiu-Zdroju, adres siedziby, dane kontaktowe (telefon, e-mail).
- Dane kontaktowe Inspektora Ochrony Danych: adres e-mail lub numer telefonu IOD do bezpośredniego kontaktu.
- Cele przetwarzania danych oraz podstawy prawne: wyszczególnione oddzielnie dla każdego celu (np. cel marketingowy – zgoda, cel realizacji umowy – niezbędność do umowy, cel archiwalny – obowiązek prawny lub interes publiczny, itp.). Jeśli muzeum przetwarza dane szczególne (np. zdrowotne przy organizacji wydarzeń z zapewnieniem opieki medycznej) – wskazana jest podstawa z art. 9 ust.2.
- Informacja o odbiorcach danych: wskazanie podmiotów, którym dane mogą być ujawniane na mocy umowy powierzenia lub przepisu prawa (np. firmy współpracujące, organy publiczne uprawnione do otrzymania danych).
- Ewentualne przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej: z podaniem podstaw zabezpieczeń (np. standardowe klauzule umowne, decyzja KE o adekwatności) lub informacji o braku takiego przekazywania.
- Okres przechowywania danych lub kryteria jego ustalenia: jasno określone, jak długo dane będą przechowywane (np. „dane przetwarzane na podstawie zgody – do czasu wycofania zgody", „dane uczestników wydarzeń – przez czas trwania projektu i rozliczeń + 5 lat w celach archiwalnych").

- Prawa osób, których dane dotyczą: wyszczególnienie przysługujących praw, w tym prawa dostępu do danych, sprostowania, usunięcia („prawo do bycia zapomnianym”), ograniczenia przetwarzania, przenoszenia danych, sprzeciwu wobec przetwarzania oraz prawa do cofnięcia zgody (jeśli przetwarzanie odbywa się na podstawie zgody). Każdorazowo dodana jest informacja, że skorzystanie z tych praw odbywa się na zasadach określonych w RODO (np. prawo do usunięcia nie jest bezwzględne i zależy od spełnienia przesłanek z art. 17 RODO).
- Prawo wniesienia skargi do organu nadzorczego: informacja, że w razie uznania, iż przetwarzanie narusza przepisy, osoba ma prawo złożyć skargę do Prezesa UODO. Podany jest adres urzędu lub przynajmniej nazwa organu.
- Informacja o wymogu/dobrowolności podania danych: czy podanie danych jest obowiązkowe (np. wymóg ustawowy lub umowny, niezbędny do zawarcia umowy), oraz jakie są ewentualne konsekwencje niepodania danych. Np. dla pracowników – obowiązek ustawowy (brak danych uniemożliwi zatrudnienie), dla gości – dobrowolność (ale brak zgody na przetwarzanie np. adresu e-mail uniemożliwi otrzymywanie newslettera).
- Informacja o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu: (jeśli ma miejsce) – muzeum obecnie nie stosuje profilowania w odniesieniu do danych osobowych, a wszelkie decyzje mają charakter indywidualny, co jest wyraźnie zaznaczone. Standardowo wskazuje się, że dane nie będą przetwarzane w sposób zautomatyzowany prowadzący do decyzji wywołujących skutki prawne dla osoby (chyba że w danym przypadku jest inaczej – wtedy opis takiego procesu i jego konsekwencji).

Klauzule informacyjne są przekazywane w przystępnej formie: drukowane na formularzach (w przypadku dokumentów papierowych, np. zgody, umowy) lub przesyłane e-mailem/udostępniane na stronie internetowej muzeum. Muzeum dba o jasność języka klauzul – sformułowane są one **językiem formalnym**, ale zrozumiałym. W razie zmian w przetwarzaniu (np. nowy cel) klauzule są aktualizowane, a osoby informowane ponownie, jeśli wymaga tego art. 13 ust.3/ art. 14 ust.4 RODO.

Ponadto, w miejscach szczególnych: np. przy wejściu do budynku objętego monitoringiem CCTV, umieszczone są skrócone informacje (tzw. krótkie klauzule: piktogram kamery plus podstawowe dane administratora i odnośnik do pełnej informacji). Na stronie internetowej muzeum dostępna jest pełna **polityka prywatności** zawierająca skonsolidowane informacje RODO dla użytkowników strony oraz odwiedzających.

Procedura realizacji praw osób, których dane dotyczą

RODO gwarantuje osobom, których dane są przetwarzane, szereg praw. Muzeum wdrożyło **procedurę obsługi żądań podmiotów danych**, aby zapewnić skuteczne

wykonywanie tych praw w przewidzianych prawem terminach. Prawa osób fizycznych obejmują m.in.:

- **Prawo dostępu** do swoich danych (art. 15 RODO) – osoba ma prawo uzyskać informację, czy muzeum przetwarza jej dane, a jeśli tak, to jakie to dane, w jakim celu, jak długo, komu ujawniane itp., oraz otrzymać kopię danych.
- **Prawo sprostowania** (art. 16) – do poprawienia nieprawidłowych danych lub uzupełnienia brakujących.
- **Prawo do usunięcia danych** („prawo do bycia zapomnianym", art. 17) – w określonych sytuacjach (np. dane nie są już potrzebne, zgoda została wycofana, dane przetwarzane niezgodnie z prawem, brak nadrzędnego prawnie uzasadnionego interesu) osoba może żądać usunięcia dotyczących jej danych.
- **Prawo do ograniczenia przetwarzania** (art. 18) – np. w czasie kwestionowania prawidłowości danych lub podstaw przetwarzania osoba może żądać, by muzeum czasowo wstrzymało operacje na jej danych poza przechowywaniem.
- **Prawo do przenoszenia danych** (art. 20) – dotyczy danych przetwarzanych w sposób zautomatyzowany na podstawie zgody lub umowy; osoba ma prawo otrzymać od muzeum swoje dane w ustrukturyzowanym formacie lub zażądać ich przesłania bezpośrednio innemu administratorowi, o ile to technicznie możliwe.
- **Prawo sprzeciwu** (art. 21) – w dowolnym momencie osoba może wnieść sprzeciw wobec przetwarzania jej danych na podstawie prawnie uzasadnionego interesu administratora lub w interesie publicznym – z przyczyn związanych z jej szczególną sytuacją. Wtedy muzeum oceni, czy nadal może przetwarzać te dane (musi wykazać ważne prawnie uzasadnione podstawy nadrzędne nad interesami osoby albo że dane są potrzebne do ustalenia, dochodzenia lub obrony roszczeń). Jeśli sprzeciw dotyczy marketingu bezpośredniego – jest skuteczny z mocy prawa i muzeum zaprzestanie takiego przetwarzania.
- **Prawo do niepodlegania zautomatyzowanym decyzjom** (art. 22) – muzeum nie podejmuje decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu (w tym profilowaniu), które wywoływałyby skutki prawne wobec osoby lub istotnie na nią wpływały, bez zapewnienia możliwości interwencji ludzkiej. Gdyby jednak takie operacje miały miejsce, osoba ma prawo do uzyskania wyjaśnień co do zasad podjęcia decyzji, zakwestionowania jej i uzyskania interwencji człowieka.

Zgłaszanie żądań: Osoba, której dane dotyczą, może zgłosić swoje żądanie realizacji prawa osobiście w siedzibie muzeum (w formie pisemnej), pocztą tradycyjną, a także drogą elektroniczną – wysyłając wiadomość na adres muzeum lub bezpośrednio do IOD.

Muzeum udostępnia również wzór formularza wniosku, ułatwiającego sformułowanie żądania (skorzystanie z niego nie jest obowiązkowe).

Weryfikacja tożsamości: W celu ochrony danych przed dostępem osób nieuprawnionych, muzeum weryfikuje tożsamość wnioskodawcy. Jeśli wniosek składany jest:

- pisemnie – przy odbiorze odpowiedzi osoba może zostać poproszona o okazanie dokumentu tożsamości (chyba że wysyłamy odpowiedź na adres będący już w naszych kontaktach ewidencyjnych);
- mailowo – odpowiedź wysyłana jest z zasady na ten sam adres, z którego przyszło żądanie, jeśli adres ten figuruje w naszej bazie; w razie wątpliwości muzeum może poprosić o dodatkowe potwierdzenie tożsamości (np. podanie pewnych danych kontrolnych lub stawienie się osobiście).

Terminy realizacji: Muzeum realizuje prawa niezwłocznie – co do zasady **najpóźniej w ciągu miesiąca** od otrzymania żądania. Jeżeli charakter żądania jest skomplikowany lub wpłynęła duża liczba żądań, termin ten może zostać przedłużony maksymalnie o kolejne dwa miesiące. W każdym przypadku, jeżeli muzeum nie jest w stanie odpowiedzieć w ciągu miesiąca, poinformuje osobę w tym terminie o przedłużeniu oraz poda przyczyny opóźnienia (zgodnie z art. 12 ust.3 RODO).

Sposób realizacji: Po otrzymaniu żądania, IOD lub upoważniony pracownik rejestruje wniosek w **Rejestrze żądań podmiotów danych** (wewnętrzny spis pozwalający śledzić termin i sposób załatwienia sprawy). Następnie:

- Jeśli żądanie jest niejasne, muzeum zwróci się o doprecyzowanie (wstrzymuje to bieg terminu do wyjaśnienia zakresu żądania).
- Muzeum analizuje zasadność żądania w świetle przepisów (np. czy zachodzą przesłanki do usunięcia danych, czy istnieją ustawowe obowiązki wymagające dalszego przechowywania danych pomimo żądania).
- W razie potrzeby, IOD konsultuje się z właściwym działem (np. kadr, marketingu, księgowości) celem zebrania informacji niezbędnych do udzielenia odpowiedzi.
- Przy przygotowaniu odpowiedzi IOD czuwa, aby zawierała ona wymagane elementy (np. przy dostępie – kopię danych lub informację, że dane nie są przetwarzane; przy odmowie – uzasadnienie i pouczenie o prawie skargi).

Odpowiedź na żądanie: Udzielana jest w formie zgodnej z formą złożenia wniosku (o ile to możliwe i chyba że osoba zażądała innej formy). Jeżeli muzeum nie realizuje żądania (np. odmawia usunięcia danych ze względu na obowiązek prawny ich dalszego przechowywania), w terminie również informuje osobę o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do UODO oraz skorzystania z ochrony sądowej.

Opłaty: Realizacja praw co do zasady jest **bezpłatna**. Jeżeli jednak żądania osoby są ewidentnie nieuzasadnione lub nadmierne (np. zgłaszane często i powtarzające się), muzeum może pobrać uzasadnioną opłatę (odzwierciedlającą koszty administracyjne udzielenia informacji) albo odmówić podjęcia działań – zgodnie z art. 12 ust.5 RODO. Taka sytuacja będzie jednak każdorazowo analizowana z udziałem IOD.

Rejestrowanie i raportowanie: Wszystkie żądania i sposób ich załatwienia są odnotowywane. IOD prowadzi rejestr wniosków, co pozwala m.in. wykazać realizację zasady rozliczalności oraz monitorować najczęstsze obszary, w których osoby korzystają ze swoich praw. Informacje z tego rejestru (anonimowe, pozbawione danych osobowych) mogą być wykorzystywane do raportowania kierownictwu muzeum o skali realizacji praw podmiotów danych oraz ewentualnych potrzebach (np. dodatkowe szkolenia personelu z obsługi żądań).

Procedura realizacji praw jest częścią polityki ochrony danych i jest znana personelowi. Pracownicy pierwszej linii (np. sekretariat, dział kadr) są przeszkoleni, aby wiedzieć jak rozpoznać żądanie RODO i przekazać je niezwłocznie do IOD lub osoby odpowiedzialnej. Dzięki temu muzeum zapewnia, że prawa osób są respektowane w praktyce, wzmacnia zaufanie interesariuszy oraz minimalizuje ryzyko skarg do organu nadzorczego.

Procedura zgłaszania naruszeń ochrony danych

Muzeum wdrożyło formalną **procedurę reagowania na incydenty bezpieczeństwa danych osobowych**, zgodną z art. 33 i 34 RODO oraz wskazówkami UODO. Celem procedury jest zapewnienie szybkiego wykrywania, oceny i raportowania **naruszeń ochrony danych osobowych** zarówno do wewnątrz (kierownictwo, IOD), jak i na zewnątrz (Prezes UODO, a w razie konieczności – osoby, których dane dotyczą).

Definicja naruszenia: Naruszenie ochrony danych osobowych to każde zdarzenie skutkujące przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub dostępem do danych osobowych. Obejmuje m.in. sytuacje takie jak: utrata urządzenia zawierającego dane, włamanie do systemu informatycznego, wysłanie danych do nieuprawnionego odbiorcy, kradzież dokumentacji papierowej, przypadkowe skasowanie danych bez kopii zapasowej, awaria bazy danych itp.

Obowiązek zgłaszania incydentów: Każdy pracownik muzeum lub współpracownik, który stwierdzi lub podejrzewa wystąpienie naruszenia danych, ma obowiązek **niezwłocznie poinformować** o tym fakcie Inspektora Ochrony Danych lub, w razie jego nieobecności, bezpośrednio Dyrektora muzeum. Informacja może być przekazana osobiście, telefonicznie lub drogą elektroniczną (na dedykowany adres alarmowy). Muzeum promuje kulturę bezpieczeństwa, w której zgłaszanie incydentów jest traktowane priorytetowo i bez poszukiwania winnych – celem jest szybkie opanowanie sytuacji.

Kroki postępowania po wykryciu incydentu:

1. **Zabezpieczenie danych:** osoba zgłaszająca lub odpowiedzialny pracownik podejmuje działania, by ograniczyć skutki incydentu (np. odłącza wadliwy system od sieci, odzyskuje omyłkowo wysłany e-mail jeśli to możliwe, zabezpiecza miejsce zdarzenia).

2. **Zebranie informacji:** IOD (lub wyznaczony członek zespołu ds. incydentów) zbiera szczegóły: kiedy, gdzie i jak doszło do naruszenia, jakiego rodzaju dane i ilu osób dotyczą, jakie zabezpieczenia zawiodły, kto brał udział, itp.

3. **Ocena ryzyka:** Zespół ocenia, czy naruszenie może skutkować **ryzykiem naruszenia praw lub wolności osób fizycznych**, a jeśli tak – czy jest to **wysokie ryzyko**. Ocena ryzyka uwzględnia m.in. charakter danych (zwykłe vs wrażliwe), konsekwencje dla osób (np. ryzyko kradzieży tożsamości, szkód finansowych, naruszenia dóbr osobistych) oraz okoliczności (np. czy dane były zaszyfrowane, czy osoba nieuprawniona mogła je wykorzystać).

4. **Decyzja o zgłoszeniu do UODO:** Jeśli stwierdzono, że jest prawdopodobne ryzyko naruszenia praw lub wolności osób wskutek incydentu, Administrator (działając przez Dyrektora w porozumieniu z IOD) **zgłasza naruszenie Prezesowi UODO nie później niż w ciągu 72 godzin od stwierdzenia naruszenia**. Zgłoszenie składane jest poprzez elektroniczny formularz udostępniony przez UODO i zawiera informacje wymagane art. 33 ust.3 RODO (opis naruszenia, kategorie i przybliżoną liczbę osób oraz zapisów danych, dane kontaktowe IOD, opis możliwych konsekwencji naruszenia oraz środków podjętych lub proponowanych w celu zaradzenia naruszeniu). Jeżeli pełne informacje nie są dostępne w 72h, muzeum składa zgłoszenie wstępne, a brakujące informacje uzupełnia w kolejnym zgłoszeniu. Gdy ocena wykaże, że incydent **nie powoduje ryzyka** dla osób (np. dane były zaszyfrowane i nie doszło do ich ujawnienia), zgłoszenie do UODO nie jest wymagane – jednak muzeum **dokumentuje** wewnętrznie naruszenie i motywy uznania, że nie było obowiązku zgłoszenia.

5. **Zawiadomienie osób, których dane dotyczą:** Jeżeli oceniono, że naruszenie może powodować **wysokie ryzyko** negatywnych skutków dla osób, muzeum **niezwłocznie** (bez zbędnej zwłoki) informuje te osoby o zaistniałym naruszeniu (zgodnie z art. 34 RODO). Komunikat do osób opisuje w prosty sposób charakter naruszenia i jego możliwe konsekwencje oraz wskazuje podjęte środki zaradcze (np. zalecenie zmiany haseł, zwrócenie się do banku o obserwację rachunku, itp.). Informacja zawiera także dane kontaktowe do punktu informacyjnego (np. IOD), od którego osoby mogą uzyskać więcej szczegółów. Obowiązek informowania osób nie zachodzi, jeśli zostały wdrożone odpowiednie techniczne środki ochrony (np. szyfrowanie uniemożliwiające odczyt utraconych danych) lub

podjęto działania eliminujące wysokie ryzyko, albo gdy wymagałoby to niewspółmiernie dużego wysiłku – wtedy publikowany jest komunikat publiczny.

6. **Działania naprawcze:** Muzeum podejmuje kroki w celu **usunięcia przyczyn naruszenia** i minimalizacji skutków. Może to obejmować przywrócenie danych z kopii zapasowej, naprawę luk bezpieczeństwa, zmianę procedur, ukaranie naruszeń dyscyplinarnych, dodatkowe szkolenia personelu itp.

7. **Dokumentowanie naruszenia:** Każdy incydent, niezależnie od tego czy podlega zgłoszeniu do UODO czy nie, jest wpisywany do **Rejestru naruszeń ochrony danych** prowadzonego przez IOD. W rejestrze odnotowuje się datę i okoliczności zdarzenia, jego opis, kategorie i przybliżoną liczbę poszkodowanych osób oraz rekordów, opis podjętych działań i wniosków na przyszłość. Taki rejestr wymagany jest art. 33 ust.5 RODO i może być sprawdzany przez UODO podczas kontroli. Prowadzenie rejestru wpisuje się w zasadę rozliczalności – Administrator musi udokumentować naruszenie i działania naprawcze.

Procedura 72 godzin: Muzeum przywiązuje szczególną wagę do 72-godzinnego terminu notyfikacji organu nadzorczego. IOD został zobowiązany do bezzwłocznego informowania Dyrektora o każdym incydencie i wspólnej oceny ryzyka natychmiast po wykryciu. Procedura wewnętrzna przewiduje, że **czas na stwierdzenie naruszenia** (od momentu zaistnienia do momentu, gdy administrator się o nim dowiedział) jest ograniczany przez odpowiednie szkolenie personelu i mechanizmy wykrywania (np. systemy informatyczne z alertami). Dopiero od momentu formalnego stwierdzenia naruszenia biegnie 72-godzinny termin na zgłoszenie – dlatego tak ważne jest szybkie raportowanie incydentów wewnątrz organizacji.

Współpraca z podmiotem przetwarzającym: Jeśli muzeum powierza pewne operacje przetwarzającemu (np. zewnętrznej firmie IT) to umowa powierzenia obliguje ten podmiot do informowania muzeum o incydentach **bez zbędnej zwłoki** po ich wykryciu. W procedurze uregulowano, że w takiej sytuacji uruchamiany jest analogiczny tryb oceny i raportowania, jak dla incydentu wewnętrznego.

Komunikacja i wsparcie: W ramach procedury określono gotowe **formularze**: zgłoszenia incydentu wewnętrznego (dla pracowników), wzór raportu dla UODO oraz wzór zawiadomienia osób. Pracownicy zostali przeszkoleni, jak rozpoznać naruszenie i kogo poinformować. Procedura jest regularnie testowana i oceniana – np. poprzez ćwiczenia scenariuszowe – aby upewnić się, że w sytuacji realnej muzeum zadziała sprawnie. UODO podkreśla, że kluczowy jest czas reakcji i dobrze wdrożony schemat postępowania.

Upoważnienia do przetwarzania danych i ewidencja upoważnień

Aby zapewnić, że dostęp do danych osobowych mają wyłącznie uprawnione osoby, muzeum wprowadziło system **imiennych upoważnień do przetwarzania danych**

osobowych. Każdy pracownik lub współpracownik muzeum, który w ramach swoich obowiązków potrzebuje dostępu do danych osobowych, musi otrzymać pisemne upoważnienie nadane przez Administratora Danych (Dyrektora muzeum). Upoważnienie jest udzielane przed dopuszczeniem danej osoby do przetwarzania danych.

Podstawa wymogu: Zgodnie z art. 29 RODO, każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego może przetwarzać dane osobowe wyłącznie na polecenie administratora. W praktyce oznacza to konieczność wyraźnego wyznaczenia, komu i w jakim zakresie wolno przetwarzać dane – czemu służy właśnie system upoważnień. Jest to także kontynuacja dobrej praktyki wykształconej na gruncie poprzedniej ustawy o ochronie danych (gdzie imienne upoważnienia były obowiązkowe).

Forma upoważnienia: Sporządza się dokument zatytułowany „Upoważnienie do przetwarzania danych osobowych nr _/__" (numer kolejny/upoważnienie, rok). W treści wskazuje się:

- **Dane osoby upoważnionej:** imię, nazwisko, stanowisko/funkcja.
- **Zakres upoważnienia:** opis obszarów danych, do których osoba może mieć dostęp oraz czynności, jakie może wykonywać. Zakres ten jest powiązany z zakresem obowiązków służbowych. Np. pracownik działu kadr – upoważnienie do przetwarzania danych pracowników i kandydatów do pracy; edukator muzealny – dane uczestników zajęć edukacyjnych; specjalista IT – dane w systemach, do których ma administracyjny dostęp itp.
- **Okres obowiązywania:** najczęściej upoważnienie wydaje się na czas nieokreślony (na okres zatrudnienia/współpracy), z zastrzeżeniem wygaśnięcia wraz z ustaniem podstawy prawnej (np. rozwiązanie umowy). Można też wskazać datę od–do, jeśli dotyczy to np. kontraktowego współpracownika przy projekcie.
- **Administrator danych:** nazwa i adres muzeum, reprezentowany przez Dyrektora, który podpisuje upoważnienie.
- **Pouczenie o obowiązkach i odpowiedzialności:** standardowa klauzula stwierdzająca, że osoba upoważniona zobowiązana jest do zachowania danych w poufności i do przestrzegania przepisów o ochronie danych oraz wewnętrznych polityk (w tym Polityki ochrony danych muzeum). Zawiera się również zapis o odpowiedzialności dyscyplinarnej i prawnej za nieuprawnione działania na danych.
- **Data i podpisy:** data nadania upoważnienia, podpis Administratora (Dyrektora) udzielającego upoważnienia, a także podpis osoby upoważnionej potwierdzającej zapoznanie się z nim i przyjęcie obowiązków.

Tak sporządzone upoważnienie przekazuje się pracownikowi (otrzymuje kopię), a oryginał przechowuje dział kadr lub IOD w dokumentacji ochrony danych.

Ewidencja upoważnień: Muzeum prowadzi rejestr (ewidencję) wydanych upoważnień. Ewidencja ma formę tabeli zawierającej co najmniej: numer upoważnienia, imię i nazwisko osoby upoważnionej, stanowisko, zakres upoważnienia (można odwołać się do kategorii danych lub działu), datę nadania, datę ustania upoważnienia (np. data odwołania lub rozwiązania umowy) oraz kolumnę na uwagi (np. przyczynę odwołania upoważnienia). Każdorazowo po odejściu pracownika lub zmianie jego zakresu obowiązków, upoważnienie jest cofane lub modyfikowane na piśmie, a ewidencja uaktualniana.

IOD okresowo (np. raz w roku) przegląda ewidencję upoważnień we współpracy z działem kadr, aby upewnić się, że nie ma osób z upoważnieniami, które nie są już potrzebne lub aktualne. Pracownicy, którym cofnięto upoważnienie (np. z powodu zmiany stanowiska), tracą dostęp do odpowiednich systemów i akt – co jest realizowane w ramach procedur zarządzania dostępem IT i obiegiem dokumentów.

Cel upoważnień: System upoważnień zapewnia, że każda osoba mająca do czynienia z danymi osobowymi w muzeum posiada wyraźne umocowanie prawne do ich przetwarzania oraz zna zakres swojej odpowiedzialności. Minimalizuje to ryzyko przypadkowego dostępu osób postronnych do danych. Jest to także dowód na stosowanie zasady „need-to-know" (dostępu ograniczonego do niezbędnego zakresu) i element spełniania zasady rozliczalności – muzeum może wykazać, że kontroluje kto i na jakiej podstawie przetwarza dane osobowe.

Poufność: Wszyscy upoważnieni pracownicy złożyli (w ramach upoważnienia lub odrębnie) **oświadczenie o zachowaniu poufności** danych osobowych, które obowiązuje zarówno w trakcie zatrudnienia, jak i po jego ustaniu. Oświadczenie to przypomina o zakazie ujawniania lub wykorzystywania danych do celów innych niż wynikające z obowiązków służbowych.

Umowy powierzenia przetwarzania danych

Muzeum jako administrator może w pewnych sytuacjach powierzać przetwarzanie danych osobowych innym podmiotom (procesorom). Dzieje się tak np. gdy korzysta z usług zewnętrznej firmy w zakresie hostingu danych, obsługi informatycznej, ochrony fizycznej, mailingu newslettera, sprzedaży biletów online, czy też zleca przetwarzanie list płac biuru rachunkowemu. W takich przypadkach, zgodnie z art. 28 RODO, **niezbędne jest zawarcie umowy powierzenia przetwarzania danych osobowych** z tym podmiotem.

Wymogi formalne: Umowa powierzenia musi mieć formę pisemną (w tym elektroniczną) i zawierać postanowienia wymagane przez art. 28 ust. 3 RODO. Muzeum opracowało wzór takiej umowy, który może być dostosowywany do konkretnych kontrahentów. Wzór uwzględnia także rekomendacje Europejskiej Rady Ochrony Danych co do klauzul umownych. Kluczowe elementy umowy powierzenia to:

- **Przedmiot i czas trwania przetwarzania:** Co zlecamy procesorowi – np. utrzymanie systemu rezerwacji biletów, wraz z danymi klientów; oraz jak długo będzie on przetwarzał dane (np. przez czas obowiązywania umowy plus okres niezbędny do przekazania/ usunięcia danych).
- **Charakter i cel przetwarzania:** Charakter czyli rodzaj czynności (np. przechowywanie danych na serwerach, analizowanie danych ankietowych), cel – np. realizacja umowy o świadczenie usługi określonej w umowie głównej.
- **Rodzaj danych osobowych i kategorie osób, których dane dotyczą:** Precyzyjne określenie, jakie dane powierzamy (np. imiona, nazwiska, adresy e-mail uczestników newslettera; dane pracowników, w tym PESEL i adresy; dane klientów sklepu internetowego itp.) oraz kogo one dotyczą (np. uczestnicy newslettera, pracownicy, klienci). Ten element jest często pomijany, co UODO piętnuje – w jednej z decyzji nałożono karę za brak określenia w umowie kategorii osób i rodzaju danych.
- **Obowiązki i uprawnienia administratora:** Podkreślenie, że to muzeum jako administrator określa cele przetwarzania i ma prawo kontrolować procesora. Administrator może wydawać polecenia co do przetwarzania (co procesor musi odnotować).
- **Obowiązki podmiotu przetwarzającego (procesora):** W umowie szczegółowo wymienione są obowiązki procesora wynikające z art. 28 RODO, w tym m.in.:
    - *Przetwarzanie wyłącznie na udokumentowane polecenie administratora* – procesor nie może wykorzystywać danych do własnych celów ani poza zakresem zleconym przez muzeum.
    - *Zapewnienie, że osoby upoważnione do przetwarzania danych u procesora zobowiązały się do poufności* lub podlegają odpowiedniemu ustawowemu obowiązkowi poufności.
    - *Podejmowanie środków bezpieczeństwa* wymaganych na mocy art. 32 RODO – np. szyfrowanie, kontrola dostępu, odporność systemów, regularne testy bezpieczeństwa. W umowie bądź załączniku opisuje się wymagane środki lub poziom bezpieczeństwa.
    - *Niezatrudnianie dalszych podprocesorów bez zgody administratora:* Procesor nie może podpowierzać danych innemu podmiotowi bez uprzedniej osobnej zgody lub ogólnej zgody wyrażonej w umowie (w tym ostatnim przypadku musi informować o zmianach i umożliwić sprzeciw administratora). Jeśli zgoda jest dana, kolejny podprocesor musi mieć nałożone takie same obowiązki jak pierwszorzędny procesor.

- *Wspomaganie administratora w realizacji obowiązków wobec osób i organu:* Procesor zobowiązuje się pomagać muzeum w zakresie realizacji praw osób (poprzez odpowiednie organizacyjne i techniczne środki – np. jeśli osoba żąda usunięcia danych, procesor na żądanie muzeum usuwa dane z swoich systemów) oraz w obowiązkach związanych z naruszeniami (niezwłocznie zgłasza własne incydenty, dostarcza informacji do zgłoszenia UODO) i oceną skutków dla ochrony danych (jeśli dotyczy).
- *Po zakończeniu świadczenia usług dotyczących przetwarzania – usunięcie lub zwrot danych:* Procesor po zakończeniu umowy głównej musi, wedle wyboru administratora, usunąć wszelkie dane osobowe przekazane mu do przetwarzania lub zwrócić je administratorowi, a także usunąć wszelkie ich istniejące kopie (chyba że prawo UE lub polskie nakazuje przechowywanie tych danych).
- *Udostępnienie informacji potrzebnych do wykazania spełnienia obowiązków i umożliwienie audytów:* Procesor zobowiązuje się poddać audytom i inspekcjom prowadzonym przez administratora (lub audytora zewnętrznego zmandatowanego przez administratora) oraz przekazywać wszelkie informacje potrzebne do potwierdzenia zgodności jego działań z RODO. Musi również niezwłocznie poinformować muzeum, jeśli uzna, że jakieś polecenie narusza RODO lub inne przepisy o danych.

Odpowiedzialność i kary: W umowie określono, że naruszenie lub niewykonanie powyższych obowiązków przez procesora upoważnia administratora do rozwiązania umowy i może skutkować żądaniem odszkodowania. Procesor ponosi też odpowiedzialność za ewentualne kary nałożone na administratora wskutek zaniedbań procesora (regres).

Dobór podmiotu przetwarzającego: Przed zawarciem umowy muzeum weryfikuje wiarygodność i zdolność potencjalnego procesora do zapewnienia ochrony danych na wymaganym poziomie (zgodnie z art. 28 ust.1 RODO). Stosuje się w tym celu listę kontrolną pytań bezpieczeństwa bądź wymaga od kontrahenta przedstawienia certyfikatów, polityk bezpieczeństwa itp. Wzór umowy przewiduje możliwość załączenia takiej **listy kontrolnej** lub **raportu z audytu** jako załącznika, co potwierdza spełnianie gwarancji przez procesora.

Rejestr umów powierzenia: IOD lub inna wyznaczona osoba prowadzi spis wszystkich obowiązujących umów powierzenia danych, z informacją jaki podmiot, z jaką datą i zakresem został dopuszczony do danych. Każda nowa umowa jest przed podpisaniem konsultowana z IOD co do treści klauzul związanych z ochroną danych.

Konsekwencje braku umowy: Powierzenie danych bez umowy grozi poważnymi konsekwencjami. Prezes UODO może nałożyć administracyjną karę pieniężną na

administratora, który przekazał dane podmiotowi trzeciemu **bez wymaganej umowy lub z umową niepełną**. Przykładem jest kara 100 tys. zł wymierzona szkole wyższej za powierzenie danych firmie zewnętrznej bez odpowiednich zapisów w umowie (brak zobowiązania do działania wyłącznie na polecenie administratora, brak określenia kategorii danych i osób). Dlatego muzeum dokłada staranności, by każda współpraca związana z dostępem do danych osobowych była sformalizowana umownie. Brak spełnienia obowiązków z art. 28 RODO stanowi naruszenie przepisów mogące skutkować administracyjną karą finansową (grzywną do 10 mln euro lub 2% obrotu).

Polityka retencji danych

Muzeum wdrożyło **politykę retencji danych osobowych**, określającą maksymalne okresy przechowywania danych w poszczególnych kategoriach zbiorów i dokumentów. Polityka ta wynika bezpośrednio z zasady ograniczonego przechowywania danych (art. 5 ust.1 lit. e RODO), zgodnie z którą dane osobowe mogą być przechowywane w formie umożliwiającej identyfikację osoby tylko przez czas nie dłuższy, niż to niezbędne do celów, w których dane te są przetwarzane. Innymi słowy, **cel przetwarzania wyznacza okres retencji** – po realizacji celu dane należy usunąć albo zanonimizować.

Określanie okresów przechowywania: W polityce retencji muzeum wyszczególniono różne kategorie danych i przypisano im okresy przechowywania, uwzględniając wymogi prawa polskiego oraz potrzeby działalności kulturalnej. Przykładowe ustalenia:

- Dane kandydatów do pracy (CV, listy motywacyjne) – przechowywane do 3 miesięcy od zakończenia procesu rekrutacji na dane stanowisko, chyba że kandydat wyraził zgodę na dłuższe przechowywanie dla celów przyszłych rekrutacji (wówczas nie dłużej niż 12 miesięcy). Po tym czasie dokumenty są niszczone chyba, że osobno uzyskano zgodę na archiwizację np. w celu historycznym.
- Akta osobowe pracowników – zgodnie z przepisami prawa pracy **10 lat** od zakończenia zatrudnienia (okres ustawowy). Po 10 latach dokumentacja pracownicza jest komisyjnie brakowana (zniszczona) lub przekazywana do archiwum państwowego, jeżeli tak stanowią odrębne przepisy.
- Dokumenty księgowe zawierające dane (faktury, rachunki, listy płac) – **5 lat** od zakończenia roku obrachunkowego, którego dotyczą, zgodnie z ustawą o rachunkowości.
- Danych klientów (np. kupujących bilety online) – przechowywanie do czasu zrealizowania usługi i rozliczeń, a następnie przez okres przedawnienia roszczeń cywilnoprawnych (co do zasady 6 lat, konsumenckich 6 lat) lub dłużej, jeśli wymagają tego przepisy podatkowe (5 lat) – przyjęto okres 6 lat od końca roku, w którym zrealizowano usługę.

- Dane uczestników wydarzeń (np. warsztatów, konkursów) – przechowywane przez czas trwania danego projektu/eventu i niezbędny okres sprawozdawczy/ewaluacyjny (np. 1 rok po wydarzeniu), a następnie usuwane. Jeżeli była zbierana zgoda marketingowa – dane marketingowe trzymane do czasu wycofania zgody lub ustania aktywności kontaktu (np. 2 lata od ostatniej interakcji).
- Monitoring wizyjny (nagrania z kamer CCTV) – przechowywane przez **30 dni**, po czym następuje automatyczne nadpisanie lub usunięcie nagrań (chyba że dane konkretnego fragmentu są zabezpieczone na potrzeby dochodzenia, wtedy zgodnie z przepisami – np. do czasu zakończenia postępowania).
- Dane w newsletterze (adresy e-mail subskrybentów) – do czasu wypisania się przez użytkownika (co może zrobić w każdej chwili) lub likwidacji newslettera przez muzeum. Po rezygnacji adres e-mail jest niezwłocznie usuwany z bazy.

Dokumentacja i uzasadnienie: Dla każdej kategorii danych w polityce retencji podano **uzasadnienie** okresu przechowywania: albo konkretny przepis prawa (jeśli istnieje) określający minimalny lub maksymalny okres, albo kryterium oparte na celach biznesowych i przedawnieniu ewentualnych roszczeń. Muzeum kieruje się zasadą, że **nie przechowuje danych „na zapas”** – po ustaniu celu przetwarzania dane są co do zasady usuwane. W sytuacjach, gdy dane mogą być dalej przetwarzane do innego, zgodnego celu (np. archiwalne w interesie publicznym, cele badawcze lub statystyczne), w polityce wskazano, że następuje zmiana podstawy prawnej i ewentualne dodatkowe zabezpieczenia, jak anonimizacja części danych.

Procedura usuwania: Polityka retencji jest powiązana z procedurami operacyjnymi usuwania danych. Przykładowo, ustanowiono mechanizmy:

- Okresowe przeglądy baz danych (np. system kadr co roku oznacza pracowników, których akta przekroczyły 10 lat od zwolnienia, do usunięcia; system CRM co kwartał usuwa klientów nieaktywnych dłużej niż X lat).
- Automatyczne skrypty czyszczące w systemach informatycznych, gdzie to możliwe (np. usuwanie kont użytkowników po określonym czasie nieaktywności).
- Procedura niszczenia dokumentów papierowych: dokumentacja po upływie okresu przechowywania jest przekazywana do zniszczenia przez uprawnioną firmę lub niszczona we własnym zakresie (niszczarka, protokół zniszczenia).
- W przypadku gdy dane mają być **zarchiwizowane** (np. materiały historyczne zawierające dane osobowe – kroniki, fotografie z wydarzeń wraz z opisami osób), dokonuje się ich selekcji i anonimizacji tam, gdzie nie potrzebujemy pełnych danych (np. pseudonimizacja nazwisk osób na potrzeby archiwum

internetowego). W razie archiwizacji w interesie publicznym (art. 89 ust.1 RODO) muzeum stosuje wymagane zabezpieczenia ograniczające zakres danych.

Przeglądy retencji: Za nadzór nad realizacją polityki retencji odpowiada IOD wspólnie z kierownikami poszczególnych działów. Co roku przeprowadzany jest audyt retencji – sprawdzane jest, czy dane nie są przechowywane ponad zadeklarowane okresy. Jeżeli w jakimś obszarze wymagana jest zmiana (np. zmiana przepisów wydłużająca okres przechowywania dokumentów finansowych), polityka jest aktualizowana, a personel informowany.

Dowody przestrzegania zasady: Posiadanie i stosowanie polityki retencji jest również dowodem na wypełnianie zasady ograniczenia przechowywania. Prezes UODO wyraźnie wskazuje, że **brak wdrożonej polityki retencyjnej może skutkować nałożeniem kary** – znany jest przypadek nałożenia wysokiej kary na przedsiębiorcę, który przechowywał dane bezterminowo, nie mając ustalonych okresów i procedur usuwania. Muzeum traktuje więc politykę retencji jako obowiązkowy element zgodności z RODO – formalne procedury przechowywania i usuwania danych nie są „nadgorliwością", lecz wymogiem prawnym i organizacyjnym.

Procedury postępowania z nośnikami danych i dokumentacją papierową

Bezpieczeństwo danych osobowych dotyczy nie tylko systemów informatycznych, ale także fizycznych nośników i dokumentów papierowych. Muzeum wprowadziło **procedury obchodzenia się z nośnikami danych** (pendrive'ami, dyskami zewnętrznymi, komputerami itp.) oraz **zasady zarządzania dokumentacją papierową**, aby zapobiegać utracie lub nieuprawnionemu dostępowi do danych.

Nośniki danych (informatyczne): W ramach polityki bezpieczeństwa informacji obowiązują następujące reguły:

- Przenośne nośniki danych zawierające dane osobowe (np. pendrive, dysk USB, laptop służbowy) muszą być **zaszyfrowane** i zabezpieczone hasłem. Dotyczy to zwłaszcza urządzeń używanych poza siedzibą muzeum. W razie utraty nośnika z danymi w postaci niezaszyfrowanej mogłoby dojść do poważnego naruszenia – co potwierdza przykład ukarania przez UODO Prezesa pewnego sądu za zagubienie niezabezpieczonego pendrive'a z danymi kilkuset osób.
- **Zakaz używania prywatnych nośników** do przechowywania danych służbowych: pracownicy nie mogą kopiować danych osobowych na prywatne pendrive'y, dyski czy chmury. Wszelkie dane muszą być przechowywane w systemach muzeum lub na nośnikach dostarczonych i zatwierdzonych przez muzeum.

- **Ewidencja nośników:** Działy IT/administracyjne prowadzą rejestr wydanych nośników przenośnych (numer urządzenia, komu wydany, data wydania i zwrotu). Wdrożenie ewidencjonowania i obowiązkowego szyfrowania nośników jest efektem wniosków z decyzji UODO, który wskazał, że takie środki są konieczne po incydencie zagubienia pendrive'a.
- **Zasady transportu i przechowywania:** Nośniki z danymi nie powinny być pozostawiane bez nadzoru. Podczas transportu (np. laptop z danymi) muszą znajdować się pod opieką pracownika lub w zamknięciu. W pomieszczeniach muzeum przewidziano zamykane szafki/sejfy do przechowywania nośników po godzinach pracy.
- **Kopie zapasowe:** Nośniki z kopiami zapasowymi (backupami) danych osobowych są szczególnie chronione – trzymane w zabezpieczonym, innym fizycznie miejscu (np. ognioodporny sejf w innej lokalizacji). Dostęp do nich ma ograniczona liczba osób.
- **Usuwanie danych z nośników:** Przy przekazywaniu nośnika do innego użytku lub utylizacji stosuje się bezpieczne usuwanie danych (nadpisywanie, demagnetyzacja) lub fizyczne zniszczenie nośnika, tak by dane nie mogły być odzyskane.
- **Incident handling:** W razie zagubienia lub kradzieży nośnika pracownik jest zobowiązany niezwłocznie zgłosić ten fakt (procedura naruszeń). Muzeum analizuje incydent, a UODO podkreśla, że sam fakt szkolenia pracowników to za mało – muszą być wdrożone *techniczne* środki zabezpieczenia, bo pracownicy mogą nie wiedzieć jak właściwie chronić nośniki lub zignorować polecenia. Dlatego ciężar zabezpieczenia spoczywa na administratorze, a nie na użytkowniku nośnika.

Wszystkie laptopy służbowe oraz komputery stacjonarne używane do pracy z danymi osobowymi mają szyfrowane dyski i są zabezpieczone hasłami o odpowiedniej złożoności. Porty USB na komputerach mogą być zablokowane programowo, jeśli nie ma uzasadnionej potrzeby ich użycia, aby zapobiegać niekontrolowanemu kopiowaniu danych na zewnętrzne media. Dostęp administracyjny (np. instalacja oprogramowania) na komputerach mają tylko uprawnieni informatycy.

Dokumentacja papierowa: Również tradycyjne dokumenty zawierające dane osobowe (umowy, wnioski, listy obecności, ankiety od zwiedzających itp.) są chronione poprzez ustalone procedury:

- Dokumenty są **przechowywane w zamykanych szafach lub pomieszczeniach**. Każdy dział posiada szafy na akta osobowe, dokumenty finansowe itd., do których dostęp mają tylko upoważnione osoby. Pomieszczenia archiwum

zakładowego są wyposażone w drzwi zamykane na klucz (dostęp ograniczony), a także system przeciwpożarowy.

- **Reguła czystego biurka:** Pracownicy zobowiązani są nie pozostawiać dokumentów z danymi w miejscach ogólnodostępnych po zakończeniu pracy. Ważne akta powinny być chowane do szuflad/pomieszczeń zamykanych. Dotyczy to zwłaszcza dokumentów zawierających dane wrażliwe (np. orzeczenia lekarskie pracowników).
- **Kopiowanie i skanowanie:** Wprowadzono ograniczenia co do wykonywania kopii dokumentów z danymi. Urządzenia wielofunkcyjne są zabezpieczone (np. kod PIN do odbioru wydruku) – aby wydruki nie pozostały na tacy dostępne dla przypadkowych osób. Skanowanie dokumentów do e-maila odbywa się na zasady określone (skan bezpiecznym kanałem na skrzynkę dedykowaną).
- **Przesyłanie dokumentów:** Jeśli dokumenty z danymi osobowymi są wysyłane na zewnątrz (poczta, kurier), używa się bezpiecznych opakowań (koperty zaklejone, ewentualnie z oznaczeniem „dane osobowe – otworzyć wyłącznie przez adresata"). Wysyłka wewnątrz budynku między działami odbywa się w zamkniętych teczkach poprzez wyznaczonych pracowników.
- **Niszczenie dokumentów:** W muzeum dostępne są niszczarki (co najmniej klasy P-3) do bieżącego niszczenia zbędnych wydruków zawierających dane. Dodatkowo, regularnie organizowane jest brakowanie dokumentacji archiwalnej – odbywa się to protokolarnie, a same dokumenty są niszczone mechanicznie lub przekazywane do profesjonalnej utylizacji (z umową powierzenia, jeśli zawierają dane). Istnieje szczegółowa *Procedura niszczenia dokumentów papierowych*, która określa, że niedozwolone jest wyrzucanie dokumentów zawierających dane do zwykłych koszy – muszą trafić do niszczarki lub specjalnego pojemnika na dokumenty do zniszczenia.
- **Szkolenia personelu:** Pracownicy administracyjni są szkoleni z zasad bezpiecznego obchodzenia się z dokumentacją. Wiedzą, jak rozpoznawać dokumenty zawierające dane chronione i jak je zabezpieczać. Ustalono także odpowiedzialność dyscyplinarną za rażące naruszenia, np. wyniesienie dokumentów poza obszar muzeum bez zgody, porzucenie dokumentów w miejscu publicznym itp.

Monitoring i kontrole: IOD we współpracy z kierownictwem okresowo przeprowadza **kontrole przestrzegania procedur** – np. sprawdza po godzinach, czy na biurkach nie pozostały jakieś dokumenty, czy szafy są pozamykane, czy pendrive'y są zaszyfrowane. Przeprowadza również testy polegające na próbie wyniesienia dokumentu przez osobę nieuprawnioną (tzw. audyt społeczny) w celu sprawdzenia czujności personelu.

Ustanowienie tych procedur ma na celu minimalizację ryzyka czynników ludzkich. Nawet najlepsze systemy informatyczne nie pomogą, jeśli np. pracownik zgubi teczkę z danymi lub pendrive z plikami. **Przykład**: Prezes UODO ukarał Prezesa Sądu Rejonowego karą 10 000 zł za to, że kurator zgubił służbowy pendrive z danymi 400 osób, który nie był zaszyfrowany – w decyzji podkreślono, że to administrator (Prezes Sądu) ponosi odpowiedzialność za brak odpowiednich środków technicznych (szyfrowania) i niewłaściwe przerzucenie obowiązku zabezpieczenia na pracownika. Muzeum wyciąga wnioski z takich przykładów – dlatego procedury kładą nacisk na **systemowe zabezpieczenia** i jasne instrukcje dla personelu, a nie tylko ogólne zalecenia.

W przypadku stwierdzenia uchybień w przestrzeganiu powyższych zasad, IOD zaleca działania korygujące, a kierownictwo może wyciągać konsekwencje służbowe. Wszelkie incydenty (np. znalezienie niezabezpieczonych dokumentów) są analizowane jako potencjalne naruszenia i mogą skutkować wszczęciem procedury zgłaszania naruszeń (jeśli doszło do ryzyka dla danych).

Zakres obowiązków Inspektora Ochrony Danych (IOD)

Muzeum powołało **Inspektora Ochrony Danych (IOD)**, spełniającego wymogi art. 37-39 RODO, ponieważ jako podmiot publiczny zobligowane jest do takiego powołania. IOD pełni kluczową rolę w systemie ochrony danych w muzeum – jest niezależnym specjalistą nadzorującym przestrzeganie przepisów. Do jego głównych **zadań** należy:

1. **Informowanie i doradzanie Administratorowi oraz pracownikom w kwestiach ochrony danych osobowych:** IOD na bieżąco przypomina o obowiązkach wynikających z RODO oraz polskich przepisów, wyjaśnia wątpliwości, rekomenduje rozwiązania. Opracowuje wewnętrzne wytyczne i polityki, konsultuje nowe przedsięwzięcia pod kątem zgodności z przepisami.
2. **Monitorowanie przestrzegania przepisów oraz polityk wewnętrznych:** IOD regularnie sprawdza, czy muzeum stosuje się do RODO, ustawy o ochronie danych oraz własnych procedur i polityk. Obejmuje to m.in. **podział obowiązków** związanych z przetwarzaniem (czy jest właściwie uregulowany), działania zwiększające świadomość i szkolenia personelu oraz **audyty** wewnętrzne. IOD dokumentuje ustalenia z kontroli i przedstawia Administratorowi zalecenia poprawy.
3. **Udzielanie zaleceń co do oceny skutków dla ochrony danych (DPIA) i monitorowanie ich wykonania:** jeśli muzeum planuje operacje mogące istotnie wpłynąć na prywatność (np. wprowadzenie nowego systemu śledzenia zwiedzających), IOD ocenia, czy wymagane jest przeprowadzenie DPIA. Doradza, jak ją przeprowadzić, pomaga zidentyfikować ryzyka i środki zaradcze, a następnie nadzoruje realizację zaleceń wynikających z DPIA.

4. **Współpraca z Prezesem Urzędu Ochrony Danych Osobowych:** IOD jest głównym punktem kontaktu pomiędzy muzeum a organem nadzorczym. W przypadku kontroli lub zapytań ze strony UODO, IOD współdziała w przekazywaniu informacji, zapewnia obecność przy czynnościach kontrolnych, wykonuje zalecenia pokontrolne. IOD także konsultuje się z UODO w razie potrzeby (np. co do interpretacji przepisów).
5. **Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w sprawach przetwarzania, w tym konsultacji uprzednich:** Jeżeli muzeum musiałoby zwrócić się o uprzednią konsultację do UODO (np. gdy planowany proces mimo środków zaradczych generuje wysokie ryzyko), IOD przygotowuje to zgłoszenie i służy jako osoba kontaktowa w tej procedurze.
6. **Pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą:** IOD udostępnia swoje dane kontaktowe osobom (są w klauzulach informacyjnych) i jest gotowy przyjmować od nich zgłoszenia dotyczące przetwarzania ich danych – pytania, skargi, realizację praw. W praktyce, IOD asystuje przy odpowiedziach na żądania osób, wyjaśnia wątpliwości co do wykorzystania danych przez muzeum itp. W razie sporu, IOD pełni rolę mediatora starając się wyjaśnić osobie kwestie związane z ochroną danych.

Inspektor Ochrony Danych ma zapewnioną **niezależność i środki** do działania. Oznacza to, że w strukturze organizacyjnej podlega bezpośrednio najwyższemu kierownictwu (Dyrektorowi), ma gwarancję, że nie będzie karany ani odwoływany za wykonywanie swoich zadań (chyba że rażąco je zaniedbuje). IOD nie otrzymuje instrukcji co do sposobu realizacji zadań z zakresu ochrony danych – jest samodzielny w wydawaniu zaleceń. Oczywiście musi respektować politykę organizacji, ale jeśli uzna jakieś działania za niezgodne z RODO, ma obowiązek o tym poinformować Administratora.

Dostęp do informacji: IOD ma prawo dostępu do wszelkich danych osobowych i operacji przetwarzania w muzeum, które są mu niezbędne do realizacji zadań. Pracownicy mają obowiązek współpracować z IOD – udzielać informacji, wypełniać ankiety audytowe, zgłaszać incydenty, konsultować projekty. W ramach organizacji IOD może uczestniczyć w spotkaniach dotyczących zmian w systemach IT, nowych projektów wystawienniczych (gdy zbierane są dane zwiedzających) itp., aby z góry doradzać w kwestii ochrony danych (zasada *privacy by design*).

Raportowanie: IOD co najmniej raz w roku przygotowuje dla Dyrektora muzeum raport podsumowujący stan ochrony danych – przedstawia zidentyfikowane niezgodności, ryzyka, incydenty, działania podjęte i plan rekomendowanych usprawnień. Raport ten służy kierownictwu do oceny skuteczności wdrożonych środków ochrony i ewentualnie alokacji dodatkowych zasobów (np. potrzeba zakupu sejfów, aktualizacji oprogramowania zabezpieczającego, dodatkowych szkoleń).

Współpraca z innymi podmiotami: Jeżeli w ramach swojej działalności muzeum współpracuje z innymi instytucjami kultury i dochodzi do wspólnego administrowania danymi lub powierzeń – IOD kontaktuje się z IOD tamtych podmiotów celem wypracowania wspólnych standardów i rozwiązań (to element dobrych praktyk w sektorze kultury).

Dopuszcza się możliwość, że funkcję IOD pełni zewnętrzny podmiot (outsourcing) – wówczas zakres obowiązków jest taki sam, ale usługa jest realizowana na podstawie umowy o świadczenie usług IOD. W muzeum, obecny IOD jest pracownikiem etatowym (lub np. pracuje na część etatu pełniąc równolegle inne funkcje, co jest dopuszczalne, o ile nie powoduje konfliktu interesów).

Podsumowując, Inspektor Ochrony Danych jest gwarantem, że muzeum **nie tylko spełnia wymogi RODO, ale czyni to w sposób świadomy i systematyczny**. IOD zapewnia fachowe wsparcie w codziennym zapewnianiu prywatności osób odwiedzających i związanych z muzeum. Jego obowiązki zostały formalnie określone zgodnie z art. 39 RODO i wewnętrznym regulaminem muzeum, a wszyscy pracownicy zostali poinformowani o roli IOD i możliwości zwracania się do niego w sprawach ochrony danych.

Źródła: Polityka opracowana w oparciu o przepisy RODO oraz krajowe (Dz.U. 2018 poz. 1000), wytyczne UODO, a także wzorce z instytucji kultury, rekomendacje portalu UODO oraz decyzje Prezesa UODO stanowiące wskazówki co do dobrych praktyk i błędów do unikania). Dokumentacja jest przygotowana do natychmiastowego wdrożenia – stanowi komplet procedur i instrukcji spełniających wymogi RODO i dostosowanych do specyfiki Muzeum Miejskiego w Jastrzębiu-Zdroju. Wszystkie osoby zaangażowane w przetwarzanie danych w Muzeum powinny zostać zapoznane z tą dokumentacją i stosować się do niej w codziennej pracy.