Sprawozdanie z audytu nr 4/2023

Audyt organizacyjno-finansowy Centrum Kultury i Biblioteki Gminy Augustów

Aesco
Audyt

Jednostka:	Urząd Gminy Augustów
Data audytu:	27 października 2023 r.
Data sprawozdania:	8 listopada 2023 r.
Audytor:	Agnieszka Ostrowska, CGAP

Aesco Group Sp. z o.o.
ul. Żelazna 67/77, 00-871 Warszawa tel.: 22 213 81 66 biuro@aesco.pl www.aesco.pl
NIP: 5252515781 KRS: 0000395738 REGON: 145164953

Spis treści

Wstęp

Tematem zadania zapewniającego był audyt organizacyjno-finansowy Centrum Kultury i Biblioteki Gminy Augustów (dalej: „instytucja kultury" lub „jednostka audytowana"). Zadanie audytowe zostało przeprowadzone w dniu 27 października 2023 r., na podstawie umowy zawartej pomiędzy Gminą Augustów, a Aesco Group Sp. z o.o.

Audyt przeprowadziła Agnieszka Ostrowska, CGAP no 6048 – audytor spełniający wymogi, o których mowa w art. 286 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Audyt wynika z planu pracy na rok 2023.

Celem zadania audytowego była ocena systemu kontroli zarządczej jednostki, w obszarze organizacyjno-finansowym, w celu dostarczenia racjonalnego zapewnienia, iż:

- przyjęte w jednostce procedury i regulacje wewnętrzne są zgodne z przepisami prawa,
- funkcjonujący w jednostce system kontroli zarządczej gwarantuje zgodną z przepisami realizację celów i zadań jednostki,
- ustanowione w jednostce mechanizmy kontrolne są adekwatne, skuteczne i efektywne oraz są przestrzegane w procesie realizacji celów i zadań jednostki.

W przypadku stwierdzenia uchybień lub nieprawidłowości w funkcjonującym systemie kontroli zarządczej celem zadania jest przedstawienie zaleceń dotyczących usprawnienia tego systemu.

Zakres przedmiotowy audytu objął:

- ocenę obszaru organizacji jednostki,
- ocenę obszaru gospodarki finansowej jednostki,
- ocenę obszaru ochrony danych osobowych,
- ocenę obszaru realizacji wydatków.

Zakres podmiotowy zadania objął działalność Centrum Kultury i Biblioteki Gminy Augustów, w latach 2022-2023.

Na etapie wstępnego przeglądu w badanym obszarze stwierdzono następujące ryzyka:

- ryzyko nieaktualnych zapisów regulacji wewnętrznych podmiotu audytowanego,
- ryzyko niewłaściwego przetwarzania danych osobowych,
- ryzyko niekompletności dokumentacji, będącej podstawą realizacji wydatków,
- ryzyko niecelowości i niegospodarności wydatków.

Uzgodnione kryteria oceny:

Ocena realizacji zadań pod kątem ich zgodności z przepisami krajowymi, regulacjami wewnętrznymi, wytycznymi organu prowadzącego i dobrymi praktykami.

W trakcie audytu zastosowano następujące narzędzia i techniki realizacji zadania:

- analiza dokumentów organizacyjnych jednostki,
- analiza dokumentacji realizacji zadań jednostki,
- analiza dokumentacji finansowo-rachunkowej,
- wywiady z pracownikami,
- porównanie informacji z różnych źródeł.

W trakcie audytu wyjaśnień udzielała Pani Dyrektor Elżbieta Sierzputowska.

Ustalenia z audytu

Obszar organizacji jednostki audytowanej

Ustaleń stanu faktycznego dokonano w oparciu o zapisy:

- Ustawy z dnia 25 października 1991 r. *O organizowaniu i prowadzeniu działalności kultury* (Dz.U. 2020 poz. 194 tj. ze zm.),
- Ustawy z dnia 8 marca 1990 r. *O samorządzie gminnym* (Dz.U. 2023 poz. 40 tj. ze zm.),
- Ustawy z dnia 26 czerwca 1974 r. *Kodeks pracy* (Dz.U. 2022 poz. 1510 tj. ze zm.),
- Rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 22 października 2015 r. *w sprawie wynagradzania pracowników instytucji kultury* (Dz.U. poz. 1798),
- Rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. *w sprawie dokumentacji pracowniczej* (poz. 2369).

Ustalenia stanu faktycznego:

W wyniku przeprowadzonych czynności stwierdzono, iż jednostka audytowana, w obecnej formie funkcjonuje na mocy Uchwały Nr XVI/119/2016 Rady Gminy Augustów z dnia 16 grudnia 2016 *r w sprawie połączenia samorządowych instytucji kultury – Gminnego Ośrodka Kultury w Augustowie z siedzibą w Żarnowie i Biblioteki Publicznej Gminy Augustów w Żarnowie oraz nadania statutu Centrum Kultury i Bibliotece Gminy Augustów z Żarnowie*. W wyniku przeprowadzonych czynności stwierdzono, iż w treści dokumentu zawarto wszystkie elementy wskazane w treści art. 13 ustawy z dnia 25 października 1991 r. *o organizowaniu i prowadzeniu działalności kultury*. Organizację wewnętrzną i zakres działania poszczególnych komórek organizacyjnych jednostki określono w treści regulaminu organizacyjnego jednostki, stanowiącego załącznik do zarządzenia nr 1/2017 Dyrektora Centrum Kultury i Biblioteki Gminy Augustów w Żarnowie z dnia 1 stycznia 2017 r. *w sprawie przyjęcia regulaminu organizacyjnego Centrum Kultury i Biblioteki Gminy Augustów w Żarnowie.* Regulamin został pozytywnie zaopiniowany przez Wójta Gminy Augustów w dniu 25 września 2019 r.

W wyniku przeprowadzonych czynności nie stwierdzono sytuacji nakładania się kompetencji poszczególnych stanowisk pracy, jak również nie stwierdzono występowania dublujących się obszarów decyzyjnych oraz przypadków występowania konfliktów interesów. Wszyscy pracownicy potwierdzili swoim podpisem fakt zapoznania się z postanowieniami Regulaminu Organizacyjnego.

W obszarze ustalenia regulaminu pracy jednostki stwierdzono, iż w treści Zarządzenia Nr 2/2017 Dyrektora Centrum Kultury i Biblioteki Gminy Augustów w Żarnowie z dnia 01.01.2027 r. *w sprawie wprowadzenia Regulaminu Pracy, Wynagradzania i pozostałych świadczeń przyznanych pracownikom w Centrum Kultury i Bibliotece Gminy Augustów w Żarnowie*, określono organizację i porządek w procesie pracy oraz związane z tym prawa i obowiązki pracodawcy i pracowników. W wyniku analizy regulacji wewnętrznych stwierdzono, iż regulacje nie zawierają wszystkich elementów wskazanych w treści art. 104^1 ustawy z dnia 26 czerwca 1974 r. *Kodeks pracy*, a w szczególności zapisów dot.:

- wykazu prac wzbronionych pracownikom młodocianym (art. 104^1 ust. 1 pkt 6),
- rodzajów prac i wykazu stanowisk pracy dozwolonych pracownikom młodocianym w celu odbywania przygotowania zawodowego (art. 104^1 ust. 1 pkt 7),
- wykazu lekkich prac dozwolonych pracownikom młodocianym zatrudnionym w innym celu niż przygotowanie zawodowe (art. 104^1 ust. 1 pkt 7a)).

W ocenie audytora należy dokonać aktualizacji zapisów Regulaminu pracy jednostki, poprzez dostosowanie jego zapisów do treści art. 104^1 ust. 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy.

Zgodnie z art. 31 ust 1 ustawy *o organizowaniu i prowadzeniu działalności kulturalnej* (t.j. Dz. U. z 2020, poz. 194), wynagrodzenia pracowników instytucji kultury składają się z wynagrodzenia zasadniczego przewidzianego dla danego stanowiska pracy oraz dodatku za wieloletnią pracę. Wysokość wynagrodzenia zasadniczego przypisanego poszczególnym stanowiskom została określona w załączniku nr 1 i 2 do Regulaminu Wynagradzania.

W wyniku przeprowadzonych czynności stwierdzono, iż w przypadku pracowników jednostki mających kontakt z dziećmi, nie zawsze dokonywano weryfikacji ich statusu, w trybie określonym w treści art. 21 ustawy z dnia 16 maja 2016 r. *o przeciwdziałaniu zagrożeniem przestępczością na tle seksualnym* (t.j. Dz.U. 2020 poz. 152). Zgodnie z zapisami art. 21 ust. 1

cyt. ustawy *„przed nawiązaniem z osobą stosunku pracy lub przed dopuszczeniem osoby do innej działalności związanej z wychowaniem, edukacją, wypoczynkiem, leczeniem małoletnich lub z opieką nad nimi pracodawcy lub inni organizatorzy w zakresie takiej działalności są obowiązani do uzyskania informacji, czy dane tej osoby są zamieszczone w Rejestrze z dostępem ograniczonym lub w Rejestrze osób, w stosunku do których Państwowa Komisja do spraw wyjaśniania przypadków czynności skierowanych przeciwko wolności seksualnej i obyczajności wobec małoletniego poniżej lat 15 wydała postanowienie o wpisie w Rejestrze"*. Audytor podkreśla, iż zgodnie z treścią art. 23 ust. 2 cyt. ustawy *„kto dopuszcza do pracy lub do innej działalności związanej z wychowaniem, edukacją, wypoczynkiem, leczeniem małoletnich lub z opieką nad nimi osobę bez uzyskania informacji, o której mowa w art. 21 ust. 1, lub wiedząc, że dane tej osoby są zamieszczone w Rejestrze, podlega karze aresztu, ograniczenia wolności albo grzywny nie niższej niż 1000 zł"*.

Należy wprowadzić praktykę weryfikacji pracowników realizujących zajęcia z dziećmi i młodzieżą, zgodnie z art. 21 ustawy z dnia 16 maja 2016 r. *o przeciwdziałaniu zagrożeniem przestępczością na tle seksualnym*, każdorazowo przed nawiązaniem każdego stosunku pracy. Stwierdzony jednostkowy przypadek braku udokumentowania sprawdzenia danych pracownika w Rejestrze sprawców przestępstw na tle seksualnym został uzupełniony podczas zadania audytowego.

W obszarze dokumentacji pracowniczej zawartej w teczkach osobowych pracowników jednostki stwierdzono, iż dokumentacja odzwierciedla historię zatrudnienia pracowników jednostki. Audytor zwraca uwagę, iż nie należy w aktach osobowych przechowywać kopii dowodów osobistych. Gromadząc dane osobowe pracowników, należy pamiętać o istotnej w kontekście RODO zasadzie minimalizacji – przetwarza się tylko tyle danych osobowych, ile rzeczywiście jest potrzebne do zatrudnienia, realizacji przebiegu zatrudnienia oraz realizacji obowiązków pracodawcy (jako administratora danych osobowych) wobec ZUS, US czy innych instytucji państwowych. Nie budzi zatem wątpliwości w kontekście przepisów RODO, iż przechowywanie kopii dowodu osobistego jest niedopuszczalne, nawet za zgodą pracownika. Pomimo, iż zgoda na przetwarzanie danych osobowych jest jedną z podstaw przetwarzania, to mając na względzie zasadę minimalizacji danych osobowych nie należy gromadzić ich i przetwarzać w zakresie szerszym, niż jest to konieczne.

Zalecenia w obszarze organizacyjnym:

Lp.	Treść	Termin	Ryzyko
1.	Należy dokonać aktualizacji zapisów regulaminu pracy jednostki, poprzez dostosowanie jego zapisów do treści art. 104^1 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy.	Do końca I kw. 2024	● **niskie**
2.	Należy wprowadzić praktykę weryfikacji pracowników realizujących zajęcia z dziećmi i młodzieżą, zgodnie z art. 21 ustawy z dnia 16 maja 2016 r. *o przeciwdziałaniu zagrożeniem przestępczością na tle seksualnym*, w przypadku każdorazowego podpisania umowy z pracownikiem/podmiotem osobą zewnętrzną. Dokonać przeglądu całości dokumentacji pracowniczej i uzupełnić ją o ewentualne brakujące informacje z Rejestru sprawców przestępstw na tle seksualnym.	niezwłocznie	● ● ● **wysokie**
3.	Usunąć kopie dowodów osobistych z akt osobowych pracowników.	niezwłocznie	● ● **średnie**
Skala ryzyka: ● niskie, ● ● średnie, ● ● ● wysokie, ☠ krytyczne			

Obszar gospodarki finansowej jednostki audytowanej

Kryteria oceny badanego obszaru:

Ustaleń stanu faktycznego dokonano w oparciu o zapisy:

- Ustawy z dnia 29 września 1994 r. *O rachunkowości* (Dz.U. 2023 poz. 120 tj. ze zm.),
- Ustawy z dnia 25 października 1991 r. *O organizowaniu i prowadzeniu działalności kultury* (Dz.U. 2020 poz. 194 tj. ze zm.),
- Ustawy z dnia 11 września 2019 r. *Prawo zamówień publicznych* (Dz.U. 2021 poz. 1129 tj. ze zm.).

Ustalenia stanu faktycznego:

W wyniku przeprowadzonych czynności stwierdzono, iż na poziomie jednostki opracowano zasady/politykę rachunkowości, definiujące zasady gospodarki finansowej. Zasady rachunkowości określono w treści Zarządzenia Nr 8/2017 Dyrektora Centrum Kultury i Biblioteki Gminy Augustów w Żarnowie z dnia 02 stycznia 2017 r. Dokument obejmuje elementy wskazane w treści art. 10 *ustawy o rachunkowości*.

Jednocześnie należy wskazać, że w audytowanym podmiocie nie opracowano *instrukcji obiegu dowodów finansowo księgowych*. Należy pamiętać, że celem prawidłowo skonstruowanej dokumentacji opisującej obieg oraz kontrolę dokumentów finansowo – księgowych jest zapewnienie, że gospodarowanie środkami finansowymi w jednostce będzie się odbywało zgodnie z przepisami a środki powierzone podmiotom będą podlegały procesom kontroli i autoryzacji. Należy więc zaprojektować oraz wdrożyć do stosowania schemat obiegu dokumentów księgowych.

W zakresie postępowań o szacunkowej wartości do kwoty 130 tys. zł netto stwierdzono, iż na poziomie jednostki zasady udzielania tych zamówień określono w treści Zarządzenia Nr 12/2020 Dyrektora Centrum Kultury i Biblioteki Gminy Augustów w Żarnowie z dnia 31 grudnia 2020 roku *w sprawie wprowadzenia regulaminu udzielania przez Centrum Kultury i Biblioteki Gminy Augustów w Żarnowie zamówień, których wartość nie przekracza wyrażonej w złotych równowartości kwoty 130 000 PLN*. Stwierdzono, iż w treści regulacji wewnętrznych dokonano rozgraniczenia trybów udzielanych zamówień, poprzez wskazanie, iż:

- zamówienia o wartości do 30 tys. zł realizowane są w sposób celowy i oszczędny kierując się zasadą należytej staranności i uzyskiwania najlepszych efektów z danych nakładów,
- zamówienia o wartość 30 tys. -130 tys. zł realizowane są w oparciu o pisemne, lub elektroniczne rozeznanie rynku.

W wyniku przeprowadzonych czynności stwierdzono, iż w treści regulacji wewnętrznych nie zapewniono wszystkich zasad traktatowych wskazanych w treści Komunikatu Wyjaśniającego Komisji, dotyczącego prawa wspólnotowego obowiązującego w dziedzinie udzielania zamówień, które nie są lub są jedynie częściowo objęte dyrektywami w sprawie zamówień publicznych (2006/C 179/02). Regulacje wewnętrzne jednostki nie definiują kwestii:

- *właściwego upublicznienia informacji o zamówieniu*. Zasady równego traktowania i niedyskryminacji pociągają za sobą obowiązek przejrzystości, który polega na zagwarantowaniu wszystkim potencjalnym oferentom odpowiedniego poziomu upublicznienia informacji umożliwiającego rynkowi otwarcie na konkurencję. Obowiązek przejrzystości oznacza, iż przedsiębiorstwo z siedzibą w innym państwie członkowskim ma dostęp do odpowiednich informacji odnoszących się do zamówienia przed jego udzieleniem i w konsekwencji jest w stanie wyrazić swoje ewentualne zainteresowanie otrzymaniem takiego zamówienia. Według Komisji praktyka kontaktowania się z licznymi potencjalnymi oferentami nie jest wystarczająca w tym zakresie, nawet jeżeli podmiot zamawiający zwraca się do przedsiębiorstw z innych państw członkowskich lub próbuje nawiązać kontakt z wszystkimi potencjalnymi dostawcami. Stosując tego rodzaju selektywne podejście nie można wykluczyć dyskryminacji względem potencjalnych oferentów z innych państw członkowskich, w szczególności nowych uczestników rynku. To samo odnosi się do wszystkich form „biernej" publikacji, w przypadku której podmiot zamawiający nie upublicznia informacji w sposób aktywny, lecz udziela odpowiedzi na pytania wnioskodawców, którzy sami dowiedzieli się o planowanym udzieleniu zamówienia. Dlatego w ocenie Komisji jedynym sposobem na spełnienie wymogów ustanowionych przez ETS jest publikacja wystarczająco dostępnego ogłoszenia przed udzieleniem zamówienia. Takie ogłoszenie powinno być opublikowane przez podmiot zamawiający w celu otwarcia udzielania zamówień na konkurencję.

Stwierdzono, iż w treści Regulaminu określono przesłanki braku stosowania procedur. Audytor podkreśla, iż dyrektywy w sprawie zamówień publicznych zawierają konkretne odstępstwa umożliwiające, pod pewnymi warunkami, zastosowanie procedur bez uprzedniej publikacji ogłoszenia[1]. Najważniejsze przypadki dotyczą wystąpienia pilnej konieczności spowodowanej nieprzewidywalnymi wydarzeniami oraz zamówień, które z przyczyn technicznych bądź artystycznych lub związanych z ochroną praw wyłącznych mogą zostać wykonane jedynie przez określony podmiot gospodarczy. Według Komisji odpowiednie odstępstwa mogą mieć zastosowanie do udzielania zamówień nieobjętych tymi dyrektywami. Dlatego też podmioty zamawiające mogą udzielać takich zamówień bez uprzedniej publikacji ogłoszenia, pod warunkiem, że spełniają one warunki ustanowione we wskazanych dyrektywach w odniesieniu do jednego z odstępstw[2].

W ocenie audytora należy dokonać aktualizacji regulacji wewnętrznych jednostki, poprzez wprowadzenie do ich treści zapisów wypełniających wymogi przytoczonego Komunikatu w obszarze:

- właściwego upublicznienia informacji o zamówieniu – wprowadzenie do procedur obowiązku powszechnego zamieszczania ogłoszeń o zamówieniach na stronach internetowych jednostki dla postępowań o wartości z przedziału od 30 tys. zł (jednocześnie audytor sugeruje zmniejszenie tej wartości do 10.000 zł netto), przy jednoczesnym zachowaniu wymogów w zakresie zamówień współfinansowanych ze środków unijnych określonych w wytycznych właściwych Instytucji Zarządzających Programami Operacyjnymi,
- określenie i przypisanie przedziałów wartości zamówień do poszczególnych trybów zakupowych w których:
  - ✓ wystarczającym potwierdzeniem wydatku będzie dokument finansowy – np. zamówienia do 1.500 zł,
  - ✓ należy przeprowadzić rozeznanie cenowe (oferty, wydruki cenowe, itp.) lub zapytanie ofertowe przesłane do min. 3 wykonawców – np. 1.500zł – 10.000zł.

W obszarze spełnienia obowiązku planistycznego, określonego w treści art. 23 ust. 1 ustawy Pzp, jednostka audytowana nie opracowała planów zamówień publicznych na lata 2022-2023

[1] Artykuł 31 dyrektywy 2004/18/WE i art. 40 ust. 3 dyrektywy 2004/17/WE
[2] opinia rzecznika generalnego Jacobsa w sprawie C-525/03 Komisja przeciwko Włochom, pkt 46 do 48

oraz nie dokonała ich publikacji na stronie Biuletynu Informacji Publicznej jednostki oraz w Biuletynie Zamówień Publicznych. Jednostka w tym okresie nie realizowała postępowań determinujących stosowanie trybów określonych w treści ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. 2022 poz. 1710 tj. ze zm.).

W ramach czynności audytowych weryfikacji poddano wybrane pozycje wydatków jednostki, poniesionych w okresie październik – listopad 2023 r.

W obszarze obiegu dokumentów stwierdzono, iż dokumenty finansowe zatwierdzane są do realizacji przez kierownika jednostki audytowanej. W obszarze obiegu dokumentów finansowych stwierdzono, iż dokumenty:

- poddawane są kontroli merytorycznej,
- poddawane są kontroli formalno-rachunkowej,
- zatwierdzane są do realizacji przez kierownika jednostki audytowanej, przy kontrasygnacie głównego księgowego jednostki.

Wydatki poniesione zostały z zachowaniem zasad określonych w treści art. 44 ust. 3 ustawy o finansach publicznych, tj. w sposób celowy i oszczędny, z zachowaniem zasad uzyskiwania najlepszych efektów z danych nakładów optymalnego doboru metod i środków służących osiągnięciu założonych celów, w sposób umożliwiający terminową realizację zadań oraz w wysokości i terminach wynikających z wcześniej zaciągniętych zobowiązań.

Zalecenia w obszarze gospodarki finansowej:

Lp.	Treść	Termin	Ryzyko
1.	Opracować i wdrożyć Instrukcję obiegu dokumentów księgowych.	Do końca I kw. 2024	● ● średnie
2.	Należy dokonać aktualizacji regulacji wewnętrznych jednostki, poprzez: 1. wprowadzenie do ich treści zapisów wypełniających wymogi przytoczonego Komunikatu w obszarze właściwego upublicznienia informacji o zamówieniu, przy jednoczesnym zachowaniu wymogów w zakresie zamówień współfinansowanych ze środków unijnych określonych w wytycznych właściwych Instytucji Zarządzających Programami Operacyjnymi, 2. określenie przedziałów wartości zamówień i przypisanie im trybów postępowań.	Do końca I kw. 2024	● ● średnie
Skala ryzyka: ● niskie, ● ● średnie, ● ● ● wysokie, ☠ krytyczne			

Obszar ochrony danych osobowych

Kryteria oceny badanego obszaru:

Weryfikacji stanu faktycznego dokonano w oparciu o zgodność z zapisami:

- 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*) (L 119/1 z dnia 4 maja 2016) – (dalej: „Rozporządzenie RODO"),
- ustawy z dnia 10 maja 2018 r. *o ochronie danych osobowych* (Dz.U. poz. 1000 ze zm.) wraz z aktami wykonawczymi,
- ustawy z dnia 21 lutego 2019 r. *o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych) (Dz.U. poz. 730),

Ustalenia stanu faktycznego:

W wyniku przeprowadzonych czynności stwierdzono, iż regulacje w zakresie ochrony danych osobowych wdrożono w treści Polityki Bezpieczeństwa Informacji z dnia 6.12.2018 r. oraz w dokumentach:

- Procedura wynoszenia dokumentacji,
- Procedura korzystania ze sprzętu IT i systemów,
- Procedura zapewnienia prawidłowego przetwarzania danych przy korzystaniu ze sprzętu IT i systemów.

Audytor zwraca uwagę, że należy stosować mechanizm corocznych przeglądów regulacji i w razie konieczności ich uaktualniania. Przeglądy takie należałoby udokumentować.

Funkcję Inspektora ochrony danych powierzono usługodawcy zewnętrznemu (dalej: „Inspektor" lub „IOD"). Inspektor został formalnie powołany Zarządzeniem nr 7/2021 Dyrektora Centrum Kultury i Biblioteki Gminy Augustów w Żarnowie z dnia 31 grudnia 2021 r.

Na poziomie jednostki, dnia 5 stycznia 2022 r. dokonano zgłoszenia Inspektora Ochrony Danych do Prezesa Urzędu Ochrony Danych Osobowych.

Zgodnie z brzmieniem art. 37 ust. 5 RODO,

> *Inspektor ochrony danych jest **wyznaczany na podstawie kwalifikacji zawodowych**, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39.*

Jednostka nie dysponuje informacjami na temat kwalifikacji Inspektora, jedynie polega na oświadczeniu, zawartym w umowie. Dla dołożenia należytej staranności, jednostka powinna dysponować dokumentacją, którą może wykazać spełnienie obowiązków wynikających z RODO.

Inspektora Ochrony Danych powołuje administrator, tym samym administrator powinien móc wykazać zasadność powołania Inspektora w kontekście posiadanych przez niego kwalifikacji. Brakujące informacje na temat IOD należy niezwłocznie uzupełnić.

Zgodnie z art. 39 RODO, obowiązki IOD przedstawiają się następująco:

> *1. Inspektor ochrony danych ma następujące zadania:*
>
> *a) **informowanie administratora**, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, **o obowiązkach spoczywających na nich** na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;*
>
> *b) **monitorowanie** przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz **polityk administratora** lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, **szkolenia personelu** uczestniczącego w operacjach przetwarzania oraz powiązane z tym **audyty**;*

W zakresie udokumentowania działań Inspektora Ochrony Danych, przedstawiono następującą dokumentację:

- niedatowaną informację dotyczącą przeprowadzenia szkolenia w zakresie cyberbezpieczeństwa,
- kartę audytową z 2022 r.,

Pamiętać należy o konieczności cyklicznych szkoleń dla wszystkich pracowników, w zakresie zasad ochrony danych osobowych, celem przypominania zasad bezpieczeństwa i informowania o nowych zagrożeniach. Przeprowadzenie szkoleń należy dokumentować.

Dla łatwiejszego zapanowania nad realizowanymi zadaniami, sugeruje się wprowadzenie rocznego planu pracy Inspektora Ochrony Danych a następnie jego egzekwowanie. Jako dobrą praktykę z zakresu ochrony danych osobowych uznaje się przygotowanie i wdrożenia przez inspektorów ochrony danych planu działań z uwzględnieniem działań o charakterze stałym oraz incydentalnym. Plan ten powinien objąć m. in. audyty, sprawdzenia, dedykowane szkolenia.

Również Prezes UODO wskazuje:

> *W aktualnym stanie prawnym nie ma przepisów, które wprost i jednakowo dla wszystkich wskazywałyby okres, na jaki należy opracować plan audytów. Niemniej, aby prawidłowo realizować zadanie z art. 39 ust. 1 lit. b RODO, warto planować swoje działania, tj. posiadać plan audytów. [...] Inspektor odpowiada m.in. za monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz wewnętrznych polityk ustanowionych w tym zakresie przez administratora lub podmiot przetwarzający. Realizacja tego zadania przez inspektora nie powinna mieć charakteru jednorazowego, lecz charakter ciągły i długofalowy. [...] Zaplanowanie audytów [...] pozwoli mu dobrze wywiązywać się z powyższego zadania. Taki plan powinien uwzględniać wiele czynników zależnych od specyfiki danego administratora i prowadzonych przez niego procesów (czynności) przetwarzania danych. Konieczne jest jego dostosowanie do przeprowadzonej w organizacji oceny ryzyka. [...] Plan ułatwia jak najlepsze i realne wykorzystanie zasobów, którymi IOD dysponuje. [...] Sporządzając plan audytów, warto przemyśleć takie jego elementy, jak: częstotliwość przeprowadzania, metody, kryteria i zakres poszczególnych audytów (w zależności od obszaru poddawanego ocenie), tryb uruchamiania audytów, zasady i sposób jego dokumentowania (w tym czas przechowywania raportu z audytu), zasady i sposób raportowania jego wyników. Trzeba pamiętać, że - z uwagi na podejście oparte na ryzyku i nieprzewidziane zdarzenia, na które należy szybko reagować – plan audytów powinien przewidywać tryb doraźny.*

> *Zarówno plan audytów, jak i wyniki z audytów są dla administratora (kierownictwa, kadry zarządzającej) ważnym elementem rozliczalności (art. 5 ust. 2 RODO), sprawowania kontroli, jak wykonywane są obowiązki z zakresu ochrony danych, czy funkcjonujące w podmiocie rozwiązania techniczne i organizacyjne są zgodne z przepisami oraz wewnętrznymi politykami, a także czy zostały skutecznie wdrożone. Mogą wskazywać, jakie obszary organizacji potrzebują pomocy i wiedzy fachowej, aby prawidłowo wykonywać powierzone zadania.*

Źródło: https://archiwum.uodo.gov.pl/pl/225/1870

Zgodnie z art. 24 RODO:

> *Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.*

Celem realizacji powyższych wymagań, w Centrum Kultury i Biblioteki w 2022 r. została przeprowadzona analiza ryzyka. Należy pamiętać o konieczności systematycznej oceny ryzyka przetwarzania danych osobowych obejmujących w szczególności elementy oceny funkcjonujących rozwiązań technicznych i organizacyjnych, a w uzasadnionych przypadkach oceny skutków przetwarzania danych.

Ustalono, że nie dla wszystkich zbiorów danych/procesów przetwarzania danych zidentyfikowano podstawę prawną oraz warunki ich przetwarzania. Prowadzony w jednostce Rejestr Czynności Przetwarzania jest niekompletny. Należy jak najszybciej zidentyfikować wszystkie procesy związane z przetwarzaniem danych osobowych i skatalogować je w przedmiotowym rejestrze. Ponadto, Inspektor Ochrony Danych powinien systematycznie dokonywać przeglądów rejestru, pod kątem jego ewentualnej konieczności aktualizacji. Dokonanie przeglądu należy dokumentować.

Co do zasady, zakres informacji Rejestru Czynności Przetwarzania jest zgodny z zapisami art. 30 ust. 1 Rozporządzenia RODO.

Zgodnie z art.29 przepisów RODO:

> *Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych **przetwarzają je wyłącznie na polecenie administratora**, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.*

W ramach czynności audytowych przeanalizowano próbę upoważnień do przetwarzania danych osobowych. Wszystkie posiadały datę utworzenia, zakres i zostały zaakceptowane przez administratora danych. Administrator prowadzi rejestr wydanych upoważnień do przetwarzania danych osobowych w sposób umożliwiający identyfikację wszystkich pracowników biorących udział w tym procesie. Rejestr jest kompletny – są w nim zaewidencjonowane wszystkie wydane upoważnienia.

Zalecenia

Lp.	Treść	Termin	Ryzyko
1.	Dokumentację jednostki uzupełnić o informacje w zakresie kwalifikacji Inspektora Ochrony Danych	Do 31.12.2023 r.	● **niskie**
2.	Opracować roczny plan pracy Inspektora Ochrony Danych i go systematycznie realizować	Do 31.12.2023 r.	● ● **średnie**
3.	Uzupełnić Rejestr Czynności Przetwarzania	niezwłocznie	● ● **średnie**
Skala ryzyka: ● niskie, ● ● średnie, ● ● ● wysokie, ☠ krytyczne			

Podsumowanie

Na podstawie przeprowadzonych czynności audytor wydaje ocenę **pozytywną** w obszarze organizacyjno-finansowym Centrum Kultury i Biblioteki Gminy Augustów, z zastrzeżeniami wskazanymi w treści sprawozdania.

Na poziomie jednostki funkcjonuje adekwatny, efektywny i skuteczny system kontroli zarządczej w obszarze organizacyjnym oraz finansowym.

Audytor w treści sprawozdania wskazuje na możliwość materializacji ryzyka oraz na słabości systemu kontroli zarządczej, w obszarze regulacji wewnętrznych jednostki audytowanej, zasad ochrony danych osobowych oraz organizacji systemu gospodarki finansowej jednostki, w tym obszaru udzielania zamówień. W treści dokumentu wydano stosowne zalecenia.

Agnieszka Ostrowska
Audytor wewnętrzny CGAP 6048

Podpisane elektronicznie przez Agnieszka Ostrowska (Certyfikat kwalifikowany) w dniu 2023-11-08.

Zapoznałam się ze sprawozdaniem:
DYREKTOR Centrum Kultury i Biblioteki Gminy Augustów w Żarnowie *mgr Elżbieta Sierzputowska* 09.11.2023 r.
Dyrektor Centrum Kultury i Biblioteki Gminy Augustów (data i podpis)

Zapoznałem się ze sprawozdaniem:
WÓJT *mgr inż. Zbigniew Buksiński* 09.11.2023
Wójt Gminy Augustów (data i podpis)

Pouczenie

1. Jednostka audytowana w terminie 7 dni od daty otrzymania sprawozdania może zgłosić uwagi lub zastrzeżenia do treści ustaleń.
2. W przypadku braku uwag do treści ustaleń wstępnych z audytu należy traktować przedmiotowe sprawozdanie jako sprawozdanie końcowe.
3. Audytowany, w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania, ustala sposób i termin realizacji zaleceń oraz wyznacza osoby odpowiedzialne za realizację zaleceń, powiadamiając o tym na piśmie audytora wewnętrznego oraz Wójta.
4. W przypadku odmowy realizacji zaleceń audytowany przedstawia, w terminie 7 dni kalendarzowych od dnia otrzymania sprawozdania, pisemne stanowisko audytorowi wewnętrznemu oraz Wójtowi.
5. Wójt podejmuje decyzję dotyczącą realizacji zaleceń, informując o tym Audytowanego i audytora wewnętrznego.
6. Wszelką korespondencję do audytora wewnętrznego proszę kierować na adres:
   agnieszka.ostrowska@aesco.com.pl

Lista weryfikacyjna oceny jakości wykonania zadania zapewniającego	
Temat zadania zapewniającego:	**Audyt organizacyjno-finansowy Centrum Kultury i Biblioteki Gminy Augustów**
Numer zadania:	**4/2023**

l.p.	Zagadnienie	Odpowiedź audytora	
		Tak	Nie
1.	Czy sporządzono program zadania?	X	
2.	Czy wszystkie czynności programu zadania zakończono?	X	
3.	Czy udokumentowano powody wszelkich pominięć niektórych czynności?	X	
4.	Czy wszystkie ustalenia i zalecenia poparte są materiałem dowodowym?	X	
5.	Czy we wszystkich notatkach z czynności audytowych podano, z kim omówiono ustalenia?	X	
6.	Czy notatki z czynności audytowych są jasne, zwięzłe i obiektywnie odzwierciedlają stan rzeczy?	X	
7.	Czy dokumentacja robocza zadania zapewniającego zawiera wszystkie niezbędne elementy określone w obowiązujących przepisach?	X	
8.	Czy wszystkie dokumenty robocze odpowiadają czynnościom programu zadania pod względem zakresu audytu?	X	
9.	Czy dokumentacja robocza nie zawiera nieistotnych lub niepotrzebnych dokumentów?	X	
10.	Czy dokumenty robocze są sporządzone czytelnie i schludnie oraz logicznie ułożone zgodnie z rozwojem informacji od ogólnej do szczegółowej?	X	
11.	Czy z akt audytu usunięto niepotrzebne dokumenty robocze?	X	
12.	Czy zadanie wykonano w sposób obiektywny?	X	
13.	Czy zadanie osiągnęło cele ustalone w ramach procesu planowania?	X	
14.	Czy są jakieś obszary warte zbadania, którymi nie zajmowano się w tym audycie, a powinny zostać uwzględnione w ramach systematycznej oceny ryzyka?		X
15.	Czy czas trwania audytu nie przekraczał czasu określonego w corocznym planie audytu?	X	

16.	Czy sprawozdanie z zadania zostało przedstawione w ciągu 30 dni od zakończenia audytu?	X	
17.	Czy sprawozdanie jest jasne i zwięzłe?	X	

Podpisane elektronicznie przez Agnieszka Ostrowska (Certyfikat kwalifikowany) w dniu 2023-11-08.

Data i podpis audytora wewnętrznego

Aesco
Audyt

Urząd Gminy Augustów	
Program działania audytowego	
Temat zadania:	Audyt organizacyjno-finansowy Centrum Kultury i Biblioteki Gminy Augustów
Cel zadania:	Celem zadania audytowego była ocena systemu kontroli zarządczej jednostki, w obszarze organizacyjno-finansowym, w celu dostarczenia racjonalnego zapewnienia, iż: • przyjęte w jednostce procedury i regulacje wewnętrzne są zgodne z przepisami prawa, • funkcjonujący w jednostce system kontroli zarządczej gwarantuje zgodną z przepisami realizację celów i zadań jednostki, • ustanowione w jednostce mechanizmy kontrolne są adekwatne, skuteczne i efektywne oraz są przestrzegane w procesie realizacji celów i zadań jednostki.
Zakres podmiotowy i przedmiotowy zadania:	Zakres przedmiotowy audytu objął: • ocenę obszaru organizacji jednostki, • ocenę obszaru gospodarki finansowej jednostki, • ocenę obszaru ochrony danych osobowych, • ocenę obszaru realizacji wydatków. Zakres podmiotowy zadania objął działalność Centrum Kultury i Biblioteki Gminy Augustów, w latach 2022-2023.
Istotne ryzyka w obszarze działalności jednostki objętym zadaniem:	• ryzyko nieaktualnych zapisów regulacji wewnętrznych podmiotu audytowanego, • ryzyko niewłaściwego przetwarzania danych osobowych, • ryzyko niekompletności dokumentacji, będącej podstawą realizacji wydatków, • ryzyko niecelowości i niegospodarności wydatków.

Sposób zrealizowania zadania, w szczególności opis doboru próby do badania oraz technik badania:	• analiza dokumentów organizacyjnych jednostki, • analiza dokumentacji realizacji zadań jednostki, • analiza dokumentacji finansowo-rachunkowej, • wywiady z pracownikami, • porównanie informacji z różnych źródeł.
Uzgodnione kryteria oceny:	Ocena realizacji zadań pod kątem ich zgodności z przepisami krajowymi, regulacjami wewnętrznymi, wytycznymi organu prowadzącego i dobrymi praktykami.
Data rozpoczęcia i zakończenia zadania:	27.10.2023 r.
Audytor:	27.10.2023 r. Agnieszka Ostrowska, CGAP Agnieszka Ostrowska