

## **STOSOWANIE MONITORINGU W BIBLIOTECE A OCHRONA DANYCH OSOBOWYCH PRACOWNIKÓW BIBLIOTEKI**

### **Wprowadzenie**

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenie dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej RODO) weszło w życie 24 maja 2016 r., ale jest stosowane od 25 maja 2018 r. i obowiązuje w polskim porządku prawnym bezpośrednio, niezależnie od przyjęcia krajowych aktów prawnych w tym zakresie (Rozporządzenie, 2016). Zgodnie z treścią art. 1 ust. 1 RODO, Rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych. Rozpoczęcie stosowania RODO wywarło wpływ na funkcjonowanie zarówno organów publicznych, przedsiębiorców, jak i instytucji kultury, w tym bibliotek. W obecnej rzeczywistości gospodarczej i społecznej wykorzystywanie różnych form monitoringu jest stałym elementem działalności zarówno instytucji publicznych, jak i prywatnych. Coraz większą wagę przykładają się bowiem do ochrony informacji i kontroli dostępu do zasobów tych podmiotów (Litwiński, Barta, 2017, s. 887). Jednak stosowanie monitoringu wizyjnego wiąże się z przetwarzaniem danych osobowych w postaci wizerunku osoby fizycznej, który utrwalany jest na nagraniach z monitoringu. W bibliotece monitoring służy w szczególności ochronie materiałów bibliotecznych przed zniszczeniem lub kradzieżą, ale może być również niezbędny do zapewnienia bezpieczeństwa pracowników biblioteki oraz osób korzystających z jej zasobów, co wiąże się z przetwarzaniem danych osobowych zarówno osób korzystających

---

<sup>1</sup> Prawnik w Praktyce TMT i Ochrona Własności Intelektualnej Ochrona Danych Osobowych i Cyberbezpieczeństwo w Zięba & Partners.

z zasobów biblioteki, pracowników biblioteki oraz innych osób trzecich. W polskim porządku prawnym prawo pracownika do prywatności i ochrony swoich danych chronione jest zarówno przepisami o ochronie danych osobowych (Ustawa, 2018), jak i Ustawy z 26 czerwca 1974 r. Kodeks pracy (Ustawa, 1974) (dalej k.p.). Monitoring wizyjny jest jednym z powszechnie stosowanych sposobów przetwarzania danych osobowych pracowników przy zastosowaniu nowych technologii, który nie był dotychczas uregulowany w polskim porządku prawnym. Stan prawny w tym zakresie uległ zmianie wraz z uchwaleniem 10 maja 2018 r. Ustawy o ochronie danych osobowych (Ustawa, 2018), która uregulowała stosowanie monitoringu w miejscu pracy poprzez zmianę k.p., polegającą na dodaniu art. 22<sup>2</sup> i art. 22<sup>3</sup>, ustanawiających zasady stosowania monitoringu w miejscu pracy. Nowe przepisy nakładają na pracodawców wiele obowiązków związanych ze stosowaniem monitoringu w miejscu pracy, polegających w szczególności na przejrzystym informowaniu pracowników o tym, że monitoring jest tam stosowany. Dla pracodawców wiąże się to w szczególności z koniecznością przeprowadzenia zmian regulaminu pracy.

### **Wizerunek jako dane osobowe**

Na gruncie art. 4 pkt 1 RODO<sup>2</sup> przez „dane osobowe” należy rozumieć informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”). Wobec powyższego, każda informacja, którą można przypisać do konkretnej osoby fizycznej, będzie uznawana za dane osobowe. Wizerunek twarzy może umożliwiać jednoznaczną identyfikację osoby fizycznej, a w konsekwencji stanowić dane osobowe w rozumieniu art. 4 pkt 1 RODO. Stosowanie monitoringu wizyjnego wiąże się zatem z przetwarzaniem danych osobowych w postaci wizerunku osoby fizycznej, polegającym na utrwalaniu wizerunku, a następnie przechowywaniu nagrań z monitoringu przez okres czasu ustalony przez administratora. W tym miejscu należy wskazać, że dane osobowe dzieli się na dane osobowe zwykłe oraz specjalne kategorie danych osobowych, które wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności osób fizycznych (por. motyw 51 preambuły do RODO). Dane należące do szczególnych kategorii danych osobowych zostały wskazane w art. 9 ust. 1 RODO w sposób enumeratywny i obejmują dane osobowe ujawniające pochodzenie rasowe

<sup>2</sup> „Dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne i dane biometryczne, służące jednoznacznemu zidentyfikowaniu osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej. Wizerunek utrwalony w formie nagrania obrazu co do zasady nie będzie stanowił danych biometrycznych, chyba że dane będą przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznacznie identyfikację osoby fizycznej lub potwierdzenie jej tożsamości, np. monitoring z funkcją rozpoznawania twarzy (por. motyw 51 preambuły do RODO). Wobec powyższego wizerunek utrwalony na nagraniach monitoringu będzie stanowił dane osobowe zwykłe.

### **Stosowanie monitoringu w bibliotekach**

Podstawy prawne przetwarzania danych osobowych zwykłych zostały wskazane w art. 6 ust. 1 RODO. Zgodnie z treścią tego przepisu, przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

- a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

### **Niezbędność do wypełnienia obowiązku prawnego ciążącego na bibliotece**

Jak zostało wskazane na wstępie, stosowanie monitoringu wizyjnego w bibliotece może służyć w szczególności ochronie materiałów bibliotecznych przed zniszczeniem lub kradzieżą oraz zapewnieniu bezpieczeństwa

pracowników biblioteki oraz osób korzystających z jej zasobów. W tym miejscu należy wskazać, że stosownie do treści art. 4 ust. 1 lit. a) Ustawy z 27 czerwca 1997 r. o bibliotekach (Ustawa, 1997, dalej UOB) do podstawowych zadań bibliotek należy gromadzenie, opracowywanie, przechowywanie i ochrona materiałów bibliotecznych. Z kolei zgodnie z treścią § 8 Rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z 4 lipca 2012 r. w sprawie narodowego zasobu bibliotecznego (Rozporządzenie, 2017), które zostało wydane na podstawie upoważnienia zawartego w art. 6 ust. 3 UOB, narodowy zasób podlega szczególnej ochronie polegającej na zapewnieniu bezpiecznych dla danego rodzaju materiałów bibliotecznych warunków w zakresie: przechowywania, kopiowania i utrwalania na informatycznych nośnikach danych, udostępniania w celach naukowych albo ekspozycyjnych, które nie spowodują pogorszenia stanu ich zachowania lub uniemożliwią ich zniszczenie lub kradzież. Wobec powyższego, przetwarzanie danych osobowych przez bibliotekę w związku ze stosowaniem monitoringu wizyjnego (Ustawa, 2018) może być niezbędne do wypełnienia obowiązków prawnych w zakresie ochrony materiałów bibliotecznych oraz zapewnienia bezpiecznych warunków ich przechowywania wynikających z przepisów UOB (art. 6 ust. 1 lit. c) RODO), o ile spełniony zostanie test równowagi. Mianowicie, wdrożenie monitoringu wymaga przeprowadzenia testu równowagi, polegającego na wyważeniu prawnie uzasadnionych interesów realizowanych przez administratora w związku ze stosowaniem monitoringu, z prawami i wolnościami osób, których dane dotyczą. Wynik testu równowagi określa, czy wdrożenie monitoringu będzie dopuszczalne i nie doprowadzi do zbędnej ingerencji w prawa i wolności osób, których dane dotyczą oraz do bezpodstawnego naruszenia tych praw i wolności. Wdrożenie monitoringu będzie dopuszczalne, jeżeli równowaga przechyli się na korzyść administratora. W ocenie Zespołu roboczego ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (dawna Grupa Robocza Art. 29) przeprowadzenie testu równowagi powinno polegać najpierw na dokonaniu oceny, czy interes administratora jest „prawnie uzasadniony” czy „nieuzasadniony” oraz czy stosowanie monitoringu jest konieczne do osiągnięcia interesu administratora. Stosowanie monitoringu jest niekonieczne, jeżeli istnieją inne, mniej inwazyjne środki do osiągnięcia określonego celu przetwarzania, jakim jest ochrona zasobów bibliotecznych (np. nadzór osobowy). Następnie należy dokonać oceny wpływu na osobę, której dane dotyczą, oraz przeprowadzić porównanie go z oczekiwanymi korzyściami z przetwarzania dla administratora, a kolejno ustalić, czy zostały wdrożone środki techniczne lub organizacyjne, mające na celu zapewnienie prywatności osób, których dane dotyczą, odpowiednie do ryzyka naruszenia praw i wolności tych osób (np. odpowiednie zabezpieczenie zapisów nagrań z monitoringu oraz ograniczenie dostępu do tych zapisów wyłącznie do upoważnionych osób) (Opinia, 2014). Ta przesłanka

znajdzie zastosowanie zarówno do przetwarzania danych osobowych osób korzystających z zasobów biblioteki, wszelkich osób trzecich przebywających na terenie i wokół terenu biblioteki (o ile objęty jest monitoringiem wizyjnym), jak również pracowników biblioteki.

### **Niezbędność do celów wynikających z prawnie uzasadnionych interesów realizowanych przez bibliotekę jako pracodawcę**

W procesie zatrudnienia status administratora danych posiada pracodawca, ponieważ decyduje on o celach i sposobach przetwarzania danych osobowych pracowników. Stosownie do treści art. 3 k.p. pracodawcą jest jednostka organizacyjna, choćby nie miała osobowości prawnej, a także osoba fizyczna, jeżeli zatrudniają one pracowników. W tym miejscu należy wskazać, że pracodawcą osób zatrudnionych w bibliotece jest instytucja kultury, a nie jej dyrektor, który jedynie podejmuje za pracodawcę czynności w sprawach z zakresu prawa pracy będącego jednostką organizacyjną jako osoba lub organ zarządzający tą jednostką zgodnie z art. 3<sup>1</sup> k.p. Nowe przepisy k.p. nakładają na bibliotekę jako pracodawcę wiele nowych obowiązków w zakresie określenia celów, zakresu oraz sposobu zastosowania monitoringu wobec pracowników. Stosownie do treści art. 22<sup>2</sup> § 1 k.p., jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring). Jak zostało wskazane w treści uzasadnienia do Projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 z dnia 23 maja 2018 r. (Projekt, 2018a) stosowanie projektowanych przepisów dotyczących monitoringu będzie oznaczać, iż pracodawca przetwarza dane osobowe pracowników na potrzeby celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora (Rozporządzenie, 2016 art. 6 ust. 1 lit. f; Uzasadnienie, 2018a, s. 17-18). W ocenie Zespołu roboczego ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, jeżeli pracodawca chce powołać się na podstawę prawną wskazaną w art. 7 lit. f) Dyrektywy o ochronie danych, cel przetwarzania danych musi być uzasadniony, a wybrana metoda lub określona technologia, za pomocą której prowadzone jest przetwarzanie, musi być konieczna z punktu widzenia uzasadnionego interesu pracodawcy (Opinia, 2017). Aby być „prawnie uzasadnionym”, interes musi być zgodny z prawem (czyli zgodny z właściwym prawem UE oraz prawem krajowym), wystarczająco jasno wyrażony, tak aby pozwolić na zastosowanie testu równowagi względem interesów oraz praw podstawowych osoby, której dane dotyczą (tzn. wystarczająco

konkretny) oraz musi być rzeczywisty i obecny (nie spekulatywny) (Opinia, 2017). Wobec powyższego, podstawę prawną przetwarzania danych osobowych w związku ze stosowaniem monitoringu wizyjnego wobec pracowników biblioteki stanowi niezbędność do celów wynikających z prawnie uzasadnionych interesów realizowanych przez bibliotekę, czyli zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić bibliotekę na szkodę. Interesy te są zgodne z prawem, to jest w szczególności art. 22<sup>2</sup> k.p., konkretne oraz rzeczywiste i obecne, gdyż odpowiadają aktualnym działaniom pracodawcy. Zgodnie z treścią art. 22<sup>2</sup> § 2 k.p. monitoring nie obejmuje pomieszczeń sanitarnych, szatni, stołówek oraz palarni, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu określonego w § 1 i nie naruszy to godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik umożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Jednym z warunków stosowania monitoringu jest zatem poszanowanie dóbr osobistych pracownika. Pracodawca uznał zatem, że objęcie monitoringiem pomieszczeń wskazanych w art. 22<sup>2</sup> § 2 k.p. stanowiłoby zbędną i nieuzasadnioną ingerencję w prawa i wolności pracowników, a ponadto byłoby nieproporcjonalne do celu stosowania monitoringu. W tym miejscu należy wskazać, że zgodnie z art. 22<sup>2</sup> § 1<sup>1</sup> k.p. monitoring nie obejmuje pomieszczeń udostępnianych zakładowej organizacji związkowej. W opinii projektodawcy monitoring pomieszczeń związkowych rodzi duże prawdopodobieństwo naruszenia zasady wolności i niezależności związków zawodowych (Uzasadnienie, 2018c, s. 26). Bibliotekarze i pozostali pracownicy bibliotek mają prawo, by tworzyć organizacje i przystępować do tych organizacji w celu reprezentacji i obrony swoich praw i interesów (zob. Ustawa, 1974, art. 18<sup>1</sup> § 1). Jeżeli zatem w bibliotece działa zakładowa organizacja związkowa, to biblioteka jest obowiązana zapewnić, aby monitoring nie obejmował jej pomieszczeń.

Art. 22<sup>2</sup> § 3 dopuszcza przechowywanie nagrań obrazu przez okres nieprzekraczający trzy miesiące od dnia nagrania, chyba że nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu (wówczas termin ten ulega przedłużeniu do czasu prawomocnego zakończenia postępowania). Wprowadzenie tego przepisu do polskiego porządku prawnego ma na celu zapewnienie realizacji zasady ograniczenia przechowywania danych osobowych wyrażonej art. 5 ust. 1 lit. e) RODO (Rozporządzenie, 2016). W przypadku wprowadzenia monitoringu biblioteka powinna oznaczyć pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem (por. Ustawa, 1974, art. 22<sup>2</sup> § 9). Nie zwalnia to jednak z obowiązku spoczywa-

jącego na administratorze na gruncie art. 12 i 13 RODO (Rozporządzenie, 2016)<sup>3</sup>. Niezależnie od powyższego, zgodnie z treścią art. 22<sup>2</sup> § 6 k.p., cele, zakres oraz sposób zastosowania monitoringu wizyjnego oraz innych form monitoringu powinny być ustalone w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy. Ponadto, pracodawca powinien przekazać pracownikowi informacje o celach, zakresie oraz sposobie zastosowania monitoringu na piśmie oraz poinformować pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy, nie później niż dwa tygodnie przed jego uruchomieniem (por. Ustawa, 1974, art. 22<sup>2</sup> § 7 i 8).

Przepisy prawa pracy nakładają na pracodawców zatrudniających co najmniej 50 pracowników obowiązek wprowadzenia regulaminu pracy, chyba że są objęci układem zbiorowym pracy. Regulamin pracy może również zostać wprowadzony fakultatywnie przez pracodawców zatrudniających mniej niż 50 pracowników lub na wniosek zakładowej organizacji związkowej przez pracodawców zatrudniających co najmniej 20 i mniej niż 50 pracowników. Wobec powyższego, pracodawcy którzy wprowadzili regulamin pracy będą obowiązani do przeprowadzenia jego zmiany, jeżeli stosują lub zamierzają wprowadzić monitoring w miejscu pracy. Zmiana regulaminu pracy wymaga zachowania określonej procedury, która może być czasochłonna. Jeżeli u pracodawcy działa zakładowa organizacja związkowa, to zmiana regulaminu pracy powinna być ustalona w uzgodnieniu z taką organizacją. Ponadto pracodawca jest obowiązany do poinformowania pracowników o zmianie regulaminu pracy, co powinno nastąpić poprzez przekazanie jej treści każdemu pracownikowi na piśmie. Potwierdzenie przez pracownika zapoznania się z aneksem do regulaminu pracy będzie równoznaczne z zapoznaniem się przez pracownika z celami, zakresem oraz sposobami zastosowania monitoringu. Zmiana regulaminu pracy wejdzie w życie po upływie dwu tygodni od dnia podania jej do wiadomości pracowników w sposób przyjęty u danego pracodawcy, przy czym przy ustalaniu daty wejścia w życie zmian do regulaminu pracy nie uwzględnia się dnia przekazania ich treści do wiadomości pracowników.

Podsumowując powyższe, stosowanie monitoringu wizyjnego w bibliotece jako miejscu pracy będzie dopuszczalne, jeżeli przetwarzanie danych jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez bibliotekę, a celu przetwarzania nie można osiągnąć w inny sposób, pracodawca przekazuje pracownikom w sposób przejrzysty informacje o celach, zakresie oraz sposobie zastosowania monitoringu oraz inne informacje wymagane na gruncie art. 13 RODO, zastosowane środki

---

<sup>3</sup> Zagadnienie to zostanie szerzej zaprezentowane w dalszej części tekstu poświęconej obowiązkom w zakresie informowania o stosowaniu monitoringu.

będą proporcjonalne do celu wprowadzenia monitoringu, a przetwarzanie danych w związku ze stosowaniem monitoringu będzie odbywało się z poszanowaniem dóbr osobistych pracownika. W odniesieniu do danych osobowych pracowników biblioteki podstawę przetwarzania danych osobowych w związku ze stosowaniem monitoringu wizyjnego będzie zatem stanowić, oprócz niezbędności do wypełnienia obowiązków prawnych w zakresie ochrony materiałów bibliotecznych oraz zapewnienia bezpiecznych warunków ich przechowywania wynikających z przepisów UOB (art. 6 ust. 1 lit. c) RODO, także niezbędność do celów wynikających z prawnie uzasadnionych interesów realizowanych przez bibliotekę, a to zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić bibliotekę na szkodę (art. 6 ust. 1 lit. f) RODO).

### **Obowiązki w zakresie informowania o stosowaniu monitoringu**

Art. 13 RODO reguluje obowiązek przekazania osobie, której dane dotyczą, informacji w sytuacji zbierania danych osobowych od osoby, której dane dotyczą (dalej „obowiązek informacyjny”). Z kolei art. 12 RODO wymaga w szczególności, aby przedmiotowe informacje były zwięzłe, przejrzyste, zrozumiałe i łatwo dostępne. Art. 12 RODO stanowi doprecyzowanie zasady przejrzystości wyrażonej w art. 5 ust. 1 lit. a) RODO, zgodnie z którym dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Zasada przejrzystości ma kluczowe znaczenie dla rzetelnego przetwarzania danych osobowych, gdyż wymaga, aby operacje przetwarzania danych osobowych były transparentne dla osób, których dane dotyczą (Drobek, 2018, s. 328). Przejrzystość stanowi nadrzędny wymóg na mocy RODO mający zastosowanie do trzech głównych obszarów: po pierwsze zapewniania informacji osobom, których dane dotyczą, związanych z rzetelnym przetwarzaniem, po drugie sposobów, w jakie administratorzy danych komunikują się z osobami, których dane dotyczą, w związku z ich prawami wynikającymi z RODO oraz po trzecie sposobów umożliwiania przez administratorów danych wykonywania swoich praw przez osoby, których dane dotyczą (Wytyczne, 2017). Stosownie do treści art. 13 RODO w przypadku, gdy dane pozyskano od osoby, której dane dotyczą, należy tę osobę poinformować o:

a) tożsamości i danych kontaktowych Administratora oraz, gdy ma to zastosowanie, tożsamości i danych kontaktowych przedstawiciela Administratora;

b) gdy ma to zastosowanie – o danych kontaktowych Inspektora Ochrony Danych;

c) celach przetwarzania danych osobowych oraz podstawie prawnej przetwarzania;



d) jeżeli przetwarzanie odbywa się na podstawie prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f) RODO) – prawnie uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią;

e) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

f) gdy ma to zastosowanie – o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

g) okresie czasu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;

h) prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

i) jeżeli przetwarzanie odbywa się na podstawie zgody (art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO) – prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

j) prawie wniesienia skargi do organu nadzorczego;

k) dobrowolności podania danych osobowych oraz ewentualnych konsekwencjach niepodania danych;

l) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, które wywołuje skutki prawne wobec osoby, której dane dotyczą, lub w podobny sposób istotnie na nią wpływa – istotne informacje o zasadach ich podejmowania.

RODO nie określa formy realizacji obowiązku informacyjnego, ale zgodnie z zasadą rozliczalności pracodawca powinien być w stanie wykazać, że przekazał osobom ubiegającym się o zatrudnienie oraz pracownikom informacje wymagane na gruncie art. 13 RODO. Obecnie powszechną praktyką jest informowanie o stosowaniu monitoringu wizyjnego w postaci tablicy z piktogramem. Umieszczenie takiego oznaczenia w monitorowanym obszarze nie stanowi jednak wypełnienia obowiązku informacyjnego, o którym mowa w art. 13 RODO, wobec osób, których dane dotyczą. Co istotne, zasada przejrzystości w RODO nie jest ograniczona do wprowadzenia jej w życie po prostu poprzez komunikację językową (czy to pisemną czy ustną). RODO przewiduje narzędzia służące do wizualizacji (wskazując w szczególności na znaki graficzne, mechanizmy certyfikacji oraz znaki jakości i oznaczenia w zakresie ochrony danych), gdy to właściwe (Wytyczne, 2017). Wobec powyższego, stosowanie oznaczeń graficznych w postaci piktogramów jest jednym ze sposobów realizacji obowiązku oznaczenia obszaru monitorowanego, ale nie powinno zastępować obowiązku przekazania podmiotom danych informacji wymaganych na gruncie art. 13 RODO. Ze względu na obszerność informacji, do których przekazania obowiązany jest administra-

tor, mogą pojawić się praktyczne trudności w zamieszczeniu wszystkich tych informacji na tablicy informacyjnej w obszarze objętym monitoringiem wizyjnym. Wówczas możliwe będzie zastosowanie warstwowej informacji dotyczącej przetwarzania danych osobowych, obejmującej co najmniej informację o tożsamości administratora, celu stosowania monitoringu oraz danych kontaktowych w celu uzyskania informacji w sprawach związanych z przetwarzaniem danych osobowych.

### **Prawa osób, których dotyczą dane, przysługujące w związku ze stosowaniem monitoringu w bibliotece**

RODO wprowadza w art. 15-21 prawa osób, których dane dotyczą, czyli prawo dostępu do danych, prawo do sprostowania danych, prawo do usunięcia danych („prawo do bycia zapomnianym”), prawo do ograniczenia przetwarzania, prawo do przenoszenia danych oraz prawo do sprzeciwu. Biblioteka jako administrator danych ma obowiązek zapewnić osobom, których dane dotyczą, możliwość realizacji tych praw. Należy przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na RODO, w tym mechanizmy żądania – i gdy ma to zastosowanie bezpłatnego uzyskiwania – w szczególności dostępu do danych osobowych i ich sprostowania lub usunięcia oraz możliwości wykonywania prawa do sprzeciwu. Administrator powinien zapewnić możliwość wnoszenia odnośnych żądań także drogą elektroniczną, w szczególności gdy dane osobowe są przetwarzane drogą elektroniczną (por. motyw 59 preambuły do RODO). Wobec powyższego należy uznać, że administrator powinien zamieścić procedurę określającą zasady wykonania wniosku o realizację praw osoby, której dane osobowe są przetwarzane, w tym przetwarzane w związku ze stosowaniem monitoringu wizyjnego, w widocznym miejscu w siedzibie biblioteki (np. na tablicy informacyjnej) czy też na stronie internetowej biblioteki. W celu zapewnienia osobie fizycznej możliwości przesłania wniosku o realizację jej praw przyznanych w rozdziale III RODO, biblioteka może udostępnić także publicznie dedykowany do tego celu adres poczty elektronicznej oraz tradycyjny adres korespondencyjny.

### **Odpowiedzialność biblioteki za naruszenie przepisów o ochronie danych osobowych w związku ze stosowaniem monitoringu**

Ogólne warunki nakładania administracyjnych kar pieniężnych za naruszenie przepisów RODO zostały określone w art. 83 RODO. Co do zasady, naruszenie przepisów RODO podlega administracyjnej karze pieniężnej w wysokości do 10 milionów lub do 20 milionów euro, a w przypadku przedsiębiorstwa – w wysokości do 2% lub 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności

od dokonanego naruszenia. Prawodawca unijny przewidział jednak w art. 83 ust. 7 możliwość określenia przez państwa członkowskie czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne. Polski prawodawca skorzystał z możliwości przyjęcia szczegółowych przepisów w tym zakresie i określił maksymalną wysokość administracyjnej kary pieniężnej, jaką można nakładać na organy i podmioty publiczne, w tym instytucje kultury. Stosownie do treści art. 102 ust. 2 Prezes Urzędu Ochrony Danych Osobowych (dalej PUODO) może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 tysięcy złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 Ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Ustawa, 2009) (tj. państwowe i samorządowe instytucje kultury). Ustawodawca polski uzasadnił ograniczenie maksymalnych kwot kar nakładanych na instytucje kultury, wskazując na konieczność realizacji konstytucyjnych zasad upowszechniania dóbr kultury, mającej istotne znaczenie dla poznawania kultury, uczestniczenia w niej, tworzenia wspólnoty narodowej oraz procesu patriotycznego wychowania i kształtowania postaw obywatelskich oraz zapewnienia równego dostępu do tych dóbr, które stanowią źródło tożsamości narodu, jego trwania i rozwoju. Ustawodawca wskazał również, że zagrożenie wysokimi karami administracyjnymi zniechęciłoby do prowadzenia tej działalności kulturalnej, a tym samym pozbawiłoby, a w każdym razie znacznie ograniczyło, obywatelom możliwość dostępu do kultury, w szczególności w wymiarze lokalnym (Uzasadnienie, 2018b s. 43-44).

Niezależnie od powyższego, zgodnie z treścią art. 82 ust. 1 RODO biblioteka jako administrator danych odpowiada za szkodę majątkową lub niemajątkową poniesioną przez osobę fizyczną w wyniku naruszenia przepisów RODO przez bibliotekę. Ponadto w przypadku naruszenia zasad dotyczących stosowania monitoringu w miejscu pracy, określonych w art. 22<sup>2</sup> k.p. biblioteka jako pracodawca może ponosić ponadto odpowiedzialność za naruszenie praw pracownika na gruncie k.p.

## **Podsumowanie**

Rozpoczęcie stosowania RODO oraz uchwalenie krajowych przepisów prawnych mających na celu zapewnienie stosowania RODO w polskim porządku prawnym niewątpliwie wywrze istotny wpływ na zasady przetwarzania danych osobowych bibliotekarzy i innych pracowników bibliotek. Dodanie w k.p. art. 22<sup>2</sup> i art. 22<sup>3</sup>, ustanawiających zasady stosowania monitoringu w miejscu pracy pozwoliło na usunięcie stanu niepewności prawnej, co do konkretnych ram i wymogów związanych z przetwarzaniem danych osobowych pracowników w związku ze stosowaniem monitoringu. Nowe unijne i krajowe przepisy prawne oznaczają wyzwanie dla instytucji kultury, takich jak biblioteki, w zakresie dostosowania działalności do

nowych wymogów prawnych. Jednym z najistotniejszych obowiązków, które spoczywają na bibliotekach jako administratorach danych, jest informowanie osób, których dane dotyczą, o stosowaniu monitoringu wizyjnego oraz o wszelkich okolicznościach związanych z przetwarzaniem ich danych osobowych, w szczególności przysługujących prawach i sposobie ich realizacji. Biblioteki powinny zadbać, aby przekazywanie podmiotom danych informacji było zgodne z zasadą przejrzystości, tj. w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Brak realizacji obowiązków wynikających z przepisów o ochronie danych osobowych może narazić bibliotekę na odpowiedzialność administracyjną i cywilnoprawną za naruszenie przepisów ogólnego rozporządzenia o ochronie danych, a w zakresie stosowania monitoringu w miejscu pracy – także na odpowiedzialność za naruszenie praw pracownika na gruncie k.p. Jednakże, z uwagi na ograniczenie maksymalnej wysokości administracyjnej kary pieniężnej, jaką można nakładać na instytucje kultury, do 10 tysięcy zł, ewentualne kary nie będą tak dotkliwe, jak mogą być dla przedsiębiorców. Przyjęcie szczegółowych przepisów w zakresie określenia maksymalnej wysokości administracyjnej kary pieniężnej dla instytucji kultury należy ocenić pozytywnie, gdyż ewentualne nałożenie administracyjnej kary pieniężnej nie zniechęci instytucji do dalszego prowadzenia działalności kulturalnej, a ponadto między wysokością kary a rocznym budżetem instytucji nie będzie zachodziła rażąca dysproporcja.

## Bibliografia

- Litwiński, P. (red.), Barta, P., Kawecki, M. (2018). *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych : komentarz*. Warszawa: Wydawnictwo C. H. Beck.
- Drobek P. (2018). W: E. Bielak-Jomaa, D. Lubasz (red.), *RODO - ogólne rozporządzenie o ochronie danych : komentarz* (s. 317-344). Warszawa: Wolters Kluwer.
- (Opinia, 2014). Grupa Robocza Art. 29 ds. Ochrony Danych, Opinia 6/2014 sprawie pojęcia prawnie uzasadnionych interesów administratora danych na mocy artykułu 7 dyrektywy 95/46/WE, przyjęta w dniu 09.04.2014 r., 844/14/EN
- WP 217. Pobrane 5 listopada 2018, z: <https://giodo.gov.pl/pl/1520203/7813>
- (Opinia, 2017). Grupa Robocza Art. 29 ds. Ochrony Danych, Opinia 2/2017 na temat przetwarzania danych w miejscu pracy, przyjęta w dniu 08.06.2017 r., 17/PL WP 249. Pobrane 5 listopada 2018, z: <https://giodo.gov.pl/pl/1520296/10060>
- (Projekt, 2018a). Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 z dnia 23 maja 2018 r. Pobrane 5 listopada 2018, z: <https://legislacja.rcl.gov.pl/projekt/12302951/>

- (Rozporządzenie, 2016). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). (Dz. Urz. UE L 2016, nr 119).
- (Rozporządzenie, 2017). Rozporządzenie Ministra Kultury i Dziedzictwa Narodowego z dnia 4 lipca 2012 r. w sprawie narodowego zasobu bibliotecznego. (Dz.U. 2017, poz. 1948).
- (Ustawa, 1974). Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy. (Dz.U. z 2018 r. poz. 917).
- (Ustawa, 1997). Ustawa z dnia 27 czerwca 1997 r. o bibliotekach. (Dz.U. 2018, poz. 574.).
- (Ustawa, 2009). Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. 2010, poz. 2077).
- (Ustawa, 2018). Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. (Dz.U. 2018, poz. 1000).
- (Uzasadnienie, 2018a). Uzasadnienie do projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 z dnia 23 maja 2018 r. Pobrane 5 listopada 2018, z: <https://legislacja.rcl.gov.pl/projekt/12302951/>
- (Uzasadnienie, 2018b). Uzasadnienie projektu ustawy o ochronie danych osobowych, *Druk sejmowy* nr 2410, z dnia 5 kwietnia 2018 roku. Pobrane 5 listopada 2018, z: <http://orka.sejm.gov.pl/Druki8ka.nsf/0/8CCAC91A3C6B-BF62C125826C0033588C/%24File/2410.pdf>
- (Uzasadnienie, 2018c). Uzasadnienie do projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 z dnia 22 października 2018 r. Pobrane 5 listopada 2018, z: [https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/149781\\_projekt-ustawy-o-zmianie-niektorych-ustaw-w-zwiazku-z-zapewnieniem-stosowania-rozporzadzenia-2016-679.html](https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/149781_projekt-ustawy-o-zmianie-niektorych-ustaw-w-zwiazku-z-zapewnieniem-stosowania-rozporzadzenia-2016-679.html)
- (Wytyczne, 2017). Grupa Robocza Art. 29 ds. Ochrony Danych, *Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679*, 17/PL WP 260, przyjęte w dniu 28 listopada 2017 roku. Pobrane 5 listopada 2018, z: <https://www.giodo.gov.pl/pl/1520346/10402>

**Karolina Kulikowska**

***Library monitoring and the protection of personal data of library staff***

**Abstract**

The introduction of the General Data Protection Regulation (GDPR) has had an impact on the functionality of cultural institutions such as libraries. The libraries use video monitoring, which involves processing of personal data of people using library resources, library employees

---

and other third parties. Due to the implementation of GDPR new provisions have been added to the Polish employment law which, among others, regulate the monitoring in the workplace. The new regulations outlines the circumstances under which monitoring is permissible. The libraries as employers have to adhere to this legislation by informing employees about the use of monitoring in the workplace.

**Keywords:** video monitoring, facial image, personal data, workplace monitoring, processing of personal data, GDPR

**Karolina Kulikowska**

***Stosowanie monitoringu w bibliotece a ochrona danych osobowych pracowników biblioteki***

**Streszczenie**

Rozpoczęcie stosowania ogólnego Rozporządzenia o ochronie danych (RODO) wywarło wpływ na funkcjonowanie instytucji kultury takich jak biblioteki. Biblioteki stosują monitoring wizyjny, co wiąże się w szczególności z przetwarzaniem danych osobowych pracowników biblioteki, jak również innych osób trzecich. Konieczność zapewnienia stosowania RODO w polskim porządku prawnym doprowadziła do uregulowania stanu prawnego w zakresie stosowania monitoringu w miejscu pracy poprzez zmianę przepisów prawa pracy. Nowe przepisy nakładają na biblioteki jako pracodawców szereg obowiązków związanych ze stosowaniem monitoringu w miejscu pracy, które wiążą się z koniecznością poinformowania pracowników o stosowaniu monitoringu, w szczególności poprzez wprowadzenie zmian do regulaminu pracy.

**Słowa kluczowe:** monitoring wizyjny, wizerunek, dane osobowe, monitoring w miejscu pracy, przetwarzanie danych, RODO