KAP.430.002.2020
Nr ewid. 32/2020/P/19/007/KAP

Informacja o wynikach kontroli

WDROŻENIE PRZEZ ADMINISTRACJĘ PUBLICZNĄ REGULACJI DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH PO WEJŚCIU W ŻYCIE RODO

DEPARTAMENT
ADMINISTRACJI PUBLICZNEJ

MISJĄ
Najwyższej Izby Kontroli jest dbałość o gospodarność i skuteczność w służbie publicznej dla Rzeczypospolitej Polskiej

WIZJĄ
Najwyższej Izby Kontroli jest cieszący się powszechnym autorytetem najwyższy organ kontroli państwowej, którego raporty będą oczekiwanym i poszukiwanym źródłem informacji dla organów władzy i społeczeństwa

Informacja o wynikach kontroli
Wdrożenie przez administrację publiczną regulacji dotyczących ochrony danych osobowych po wejściu w życie RODO

Dyrektor Departamentu Administracji Publicznej

Bogdan Skwarka

Akceptuję:
Wiceprezes Najwyższej Izby Kontroli

Małgorzata Motylow

Zatwierdzam:
Prezes Najwyższej Izby Kontroli

Marian Banaś
Warszawa, dnia 26.05.2020

Najwyższa Izba Kontroli
ul. Filtrowa 57
02-056 Warszawa
T/F +48 22 444 50 00
www.nik.gov.pl

SPIS TREŚCI

Zdjęcie na okładce:
stock.adobe.com

Wykaz stosowanych skrótów, skrótowców i pojęć

RODO	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)[1];
ustawa o NIK	ustawa z dnia 23 grudnia 1994 r. *o Najwyższej Izbie Kontroli*[2]*;*
ustawa o ochronie danych osobowych	ustawa z dnia 10 maja 2018 r. *o ochronie danych osobowych*[3]*;*
administrator	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO);
dane osobowe	informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (art. 4 pkt 1 RODO);
naruszenie ochrony danych osobowych	naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art. 4 pkt 12 RODO);
IOD/Inspektor	inspektor ochrony danych, o którym mowa w art. 37 RODO; zasadniczą rolą inspektorów ochrony danych jest doradzanie administratorowi oraz podmiotowi przetwarzającemu, a także weryfikacja prawidłowości wykonywania obowiązków wynikających z przepisów prawa dotyczących przetwarzania danych. Administrator i podmiot przetwarzający są obowiązani do wyznaczenia IOD w przypadkach określonych w art. 37 RODO (art. 8 ustawy *o ochronie danych osobowych*);
podmiot przetwarzający	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (art. 4 pkt 8 RODO);
przetwarzanie	operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie (art. 4 pkt 2 RODO);
ryzyko	jest to ocena zagrożenia/niebezpieczeństwa wynikającego z prawdopodobnych zdarzeń lub z konsekwencji podjęcia decyzji, wskaźnik, który wskazuje prawdopodobieństwo wystąpienia strat;
UODO	Urząd Ochrony Danych Osobowych;
MSWiA	Ministerstwo Spraw Wewnętrznych i Administracji.

[1] Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zm.
[2] Dz. U. z 2019 r. poz. 489, ze zm.
[3] Dz. U. z 2019 r. poz. 1781.

1. WPROWADZENIE

Uzasadnienie podjęcia kontroli

RODO jest bezpośrednio stosowane od 25 maja 2018 r. Rozporządzenie to nakłada na organy administracji publicznej szereg obowiązków związanych z ochroną danych osobowych, polegających m.in. na: zmianie zasad i sposobu ochrony danych osobowych przetwarzanych przez organ, wyznaczeniu inspektora ochrony danych, informowaniu osób fizycznych o zakresie i celach przetwarzania ich danych oraz rozpatrywaniu żądań osób fizycznych dotyczących ich danych, informowaniu organu ochrony danych bez zbędnej zwłoki o stwierdzonych naruszeniach. Trzeba podkreślić, że RODO nie zawiera wskazówek ani rozwiązań, które mogłyby być przyjęte u każdego z administratorów. Wymaga ono natomiast aktywności w realizacji wspomnianych obowiązków po stronie administratorów. Z doniesień medialnych wynikało, że pomimo dwuletniego okresu na wejście w życie przepisów rozporządzenia, administracja publiczna była niewystarczająco przygotowana do wdrożenia procedur ochrony danych osobowych zgodnie z RODO. Wiążą się z tym ryzyka ujawnienia (wycieku) danych osobowych objętych obowiązkiem ochrony, nieprawidłowego przetwarzania danych, a w związku z tym ryzyko zapłaty kar finansowych.

Pytanie definiujące cel główny kontroli

Czy organy administracji publicznej wdrożyły w wymaganym zakresie i czasie przepisy dotyczące ochrony danych osobowych po wejściu w życie RODO?

Pytania definiujące cele szczegółowe kontroli

1. Czy organy administracji publicznej prawidłowo przygotowały się do wdrożenia RODO?
2. Czy ochrona danych osobowych jest prowadzona zgodnie z wytycznymi określonymi w RODO oraz efektywnie?

Jednostki kontrolowane

Do kontroli wybrane zostały podmioty publiczne, które w najszerszym zakresie dokonują przetwarzania danych osobowych, tj. urzędy wojewódzkie oraz urzędy gmin/miast większych miejscowości, które charakteryzują się dużą liczbą prowadzonych spraw obywatelskich. Kontrolą objęto także Ministerstwo Spraw Wewnętrznych i Administracji z uwagi na to, że minister właściwy do spraw wewnętrznych m.in. zapewnia funkcjonowanie wydzielonej sieci umożliwiającej organom gminy i wojewodom dostęp do rejestru dowodów osobistych i do Rejestru PESEL.

Skontrolowano łącznie 17 jednostek, tj.:

1. Ministerstwo Spraw Wewnętrznych i Administracji
2. Łódzki Urząd Wojewódzki
3. Małopolski Urząd Wojewódzki
4. Mazowiecki Urząd Wojewódzki
5. Zachodniopomorski Urząd Wojewódzki
6. 12 urzędów miast z terenu województw: łódzkiego, małopolskiego, mazowieckiego i zachodniopomorskiego

Okres objęty kontrolą

Od 25 maja 2018 r do 2019 r. (do zakończenia czynności kontrolnych oraz z uwzględnieniem okresu sprzed 25 maja 2018 r., jeżeli zaistniałe zdarzenia miały wpływ na kontrolowaną działalność).

2. OCENA OGÓLNA

Pozytywna ocena wdrożenia RODO w skontrolowanych jednostkach

Wszystkie jednostki opracowały i wdrożyły procedury dotyczące RODO

Najwyższa Izba Kontroli pozytywnie ocenia przygotowanie kontrolowanych jednostek do wdrożenia RODO. Opracowano i wdrożono procedury dotyczące ochrony danych osobowych spełniające wymagania RODO.

Zarówno w MSWiA, jak i w pozostałych skontrolowanych urzędach, opracowane zostały systemy przetwarzania i zabezpieczania danych osobowych zgodne z wymogami RODO. Pracownicy urzędów byli zapoznawani z wprowadzonymi regulacjami dotyczącymi ochrony danych osobowych. Prowadzono szkolenia z tego zakresu dla osób w nich zatrudnionych, a niekiedy także dla członków rad miejskich. We wszystkich skontrolowanych jednostkach prowadzono rejestry czynności przetwarzania danych i rejestry kategorii czynności przetwarzania. W czterech jednostkach rejestry te były założone z opóźnieniem, w tym w dwóch przypadkach założono je dopiero w trakcie kontroli NIK.

We wszystkich skontrolowanych jednostkach powołany został Inspektor Ochrony Danych (IOD), o czym informowano Prezesa UODO, z tym że w czterech urzędach obowiązek ten został spełniony z naruszeniem ustawowego terminu. Poza jednym przypadkiem administratorzy zapewnili IOD możliwość realizacji zadań w sposób niezależny. Osoby pełniące funkcje IOD miały odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe. W okresie objętym kontrolą nie stwierdzono zaniedbań w realizacji obowiązków IOD.

W większości skontrolowanych jednostek zastosowane środki bezpieczeństwa (techniczne, fizyczne i informatyczne), służące utrzymaniu poufności, integralności oraz dostępności systemów i usług przetwarzania, były zgodne z wewnętrznymi uregulowaniami dotyczącymi ochrony danych osobowych obowiązującymi w tych jednostkach. Zgodnie z tymi procedurami, dostęp do zasobów informatycznych urzędów wymagał odpowiedniego uwierzytelnienia. Pracownicy oraz osoby zatrudniane na podstawie umów cywilno-prawnych mieli upoważnienia do przetwarzania danych osobowych.

Administratorzy prawidłowo realizowali obowiązki wynikające z RODO w stosunku do swoich pracowników, jak też i osób ubiegających się o zatrudnienie oraz zadania podmiotów przetwarzających.

W większości przypadków prawidłowo prowadzone były działania w reakcji na stwierdzone naruszenia ochrony danych osobowych oraz żądania usunięcia lub sprostowania danych osobowych.

3. SYNTEZA WYNIKÓW KONTROLI

Opracowanie dokumentacji wymaganej przepisami RODO

1. NIK nie stwierdziła zaniedbań w przygotowaniach skontrolowanych jednostek do wdrażania RODO. W ich ramach przeprowadzano analizy ryzyk, przeglądy dotychczas stosowanych rozwiązań, analizę posiadanych zasobów i dokumentacji. W wyniku tych działań opracowano nowe dokumenty lub odpowiednio dostosowano dotychczasowe. We wszystkich jednostkach pracownicy zostali poinformowani o nowych regulacjach dotyczących ochrony danych osobowych. [str. 12–13]

Wyznaczanie i realizacja zadań Inspektora Ochrony Danych

2. We wszystkich kontrolowanych jednostkach wyznaczono Inspektora Ochrony Danych. W czterech z 17 jednostek stwierdzono opóźnienia w przekazaniu informacji do Prezesa UODO o powołaniu IOD, które wyniosły od czterech do 53 dni. Wszystkie badane jednostki, zgodnie z art. 37 ust. 7 RODO, zamieściły dane kontaktowe do IOD na swoich stronach internetowych. Inspektorzy mieli odpowiednie kwalifikacje do pełnienia tej funkcji, w tym m.in. brali udział w szkoleniach kierunkowych. Administratorzy, poza jednym przypadkiem, zapewnili IOD niezależność w wykonywaniu ich zadań. Nie stwierdzono nieprawidłowości w wykonywaniu przez IOD obowiązków określonych w art. 39 RODO. [str. 13–15]

Infografika nr 1
Obowiązki Inspektora Ochrony Danych

Źródło: opracowanie własne NIK.

Szkolenia dotyczące ochrony danych osobowych

3. Wszystkie kontrolowane jednostki zapewniły swoim pracownikom szkolenia dotyczące nowych regulacji wynikających z RODO oraz szeroko pojętej ochrony danych osobowych. Szkolenia te były prowadzone zarówno przez IOD, w ramach wykonywania jego zadań wynikających z art. 39 RODO, jak i przez wyspecjalizowane podmioty zewnętrzne. W niektórych jednostkach prowadzono także szkolenia w systemie e-learningu. [str. 15–16]

Koszty wdrożenia RODO

4. Wydatki szacowane przez skontrolowane jednostki związane z wprowadzeniem RODO wyniosły od 1,8 tys. zł do 560 tys. zł. Dotyczyły one głównie kosztów szkoleń, zakupu sprzętu i oprogramowania oraz zadań inwestycyjnych związanych z koniecznością stworzenia fizycznych zabezpieczeń w obrębie użytkowanych budynków.

Jednostki objęte kontrolą nie były obciążone karami finansowymi za nieprawidłowe stosowanie RODO. [str. 16]

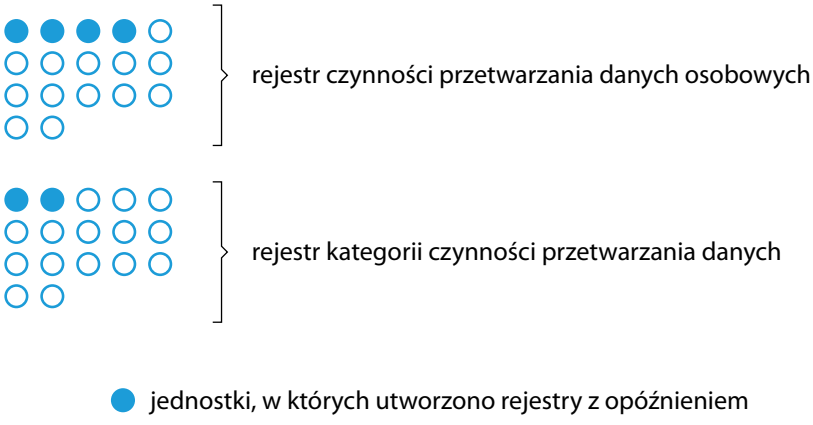
Nadzór urzędów gmin nad jednostkami podległymi w zakresie stosowania RODO

5. Współpraca urzędów 11 gmin, w zakresie stosowania RODO, z ich jednostkami podległymi nie miała charakteru ścisłego nadzoru i polegała głównie na roboczych kontaktach oraz doraźnej pomocy w sytuacjach problematycznych. Spośród 12 skontrolowanych urzędów gmin, jednostki podległe 11 z nich samodzielnie powoływały IOD, opracowywały wewnętrzne procedury dotyczące bezpieczeństwa i ochrony danych osobowych. Jedynie Miasto Kraków ściślej i kompleksowo współpracowało z jednostkami podległymi, m.in. w Urzędzie Miasta byli usytuowani IOD dla jednostek podległych. [str. 16–18]

Rejestry: czynności przetwarzania danych i kategorii czynności przetwarzania danych

6. Trzynaście jednostek wywiązało się z obowiązku utworzenia i prowadzenia rejestru czynności przetwarzania danych i rejestru kategorii czynności przetwarzania danych. Natomiast w czterech rejestry te zostały założone z opóźnieniem, w tym rejestry kategorii czynności przetwarzania danych w dwóch jednostkach zostały utworzone dopiero w wyniku kontroli NIK. Rejestry te, poza jednym przypadkiem, zawierały dane określone w art. 30 ust. 1 i 2 RODO. Nie stwierdzono natomiast ujmowania w rejestrach informacji nadmiernych lub nieadekwatnych i niestosownych do celów ich przetwarzania, co było zgodne z art. 5 ust. 1 pkt c RODO. [str. 18–19]

Infografika nr 2
Opóźnienia w utworzeniu rejestrów



Źródło: opracowanie własne NIK.

Upoważnienia do przetwarzania danych

7. Administratorzy w 14 spośród 17 jednostek objętych kontrolą wywiązywali się z obowiązku określonego w art. 32 ust. 4 RODO, tj. zapewnili, aby każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora. W większości badanych przypadków osoby mające dostęp do danych osobowych miały upoważnienia administratora do ich przetwarzania. Stwierdzone w tym zakresie w trzech jednostkach nieprawidłowości, miały charakter sporadyczny. [str. 19–21]

Unieważnianie dostępu do systemów informatycznych

8. W sześciu z 17 kontrolowanych jednostek nie wywiązywano się z obowiązku niezwłocznego odbierania byłym pracownikom uprawnień do systemów informatycznych tych jednostek. [str. 21–22]

Powierzanie przetwarzania danych osobowych podmiotom zewnętrznym

9. Wszystkie kontrolowane jednostki powierzały przetwarzanie danych osobowych podmiotom zewnętrznym. Nieprawidłowość w tym obszarze stwierdzono tylko w jednej jednostce. Polegała ona na zawarciu porozumienia dotyczącego powierzenia przetwarzania danych z opóźnieniem i nieuwzględnieniu w nim wszystkich elementów wymaganych przez RODO. We wszystkich z nich prowadzono rejestry umów powierzenia, z tym że w dwóch jednostkach rejestry te były prowadzone nierzetelnie. [str. 22]

Wypełnianie obowiązków podmiotu przetwarzającego

10. Nie stwierdzono nieprawidłowości w realizowaniu zadań podmiotu przetwarzającego. Wszystkie kontrolowane jednostki wykonywały te zadania prawidłowo, na podstawie ustaw, umów i porozumień. [str. 22–23]

Infografika nr 3
Podstawy prowadzenia rejestru kategorii czynności przetwarzania

rejestr kategorii czynności przetwarzania prowadzony jest na podstawie

- **ustaw** np. o ewidencji ludności, o dowodach osobistych, Prawo o aktach stanu cywilnego
- **umów** np. dotyczących realizacji projektów dofinansowywanych z budżetu Unii Europejskiej, świadczenia usług rekreacyjno-sportowych
- **porozumień** np. dotyczących realizacji programów Karta Rodziny, Karta Seniora

Źródło: opracowanie własne NIK.

Monitoring wizyjny

11. We wszystkich jednostkach, w których prowadzony był monitoring wizyjny jego zasięg obejmował miejsca dozwolone i prawidłowo oznaczone. Stwierdzona w jednej jednostce nieprawidłowość dotyczyła okresu przechowywania nagrań z monitoringu. [str. 23–24]

Ochrona systemów informatycznych

12. Wszystkie jednostki objęte kontrolą, zgodnie z art. 32 ust. 1 RODO, opracowały i wdrożyły wewnętrzne procedury dotyczące ochrony fizycznej i technicznej posiadanych zasobów informatycznych. Jednak w czterech z nich stwierdzono nieprawidłowości dotyczące utrzymywania serwerowni w nieodpowiednim stanie technicznym. Ustalono też, że w trzech jednostkach niewłaściwie chronione były dane osobowe przechowywane w systemach informatycznych. Stwierdzono, że stosowano w nich hasła dostępu o mniejszej liczbie znaków niż przewidziano w procedurach wewnętrznych. [str. 24–26]

Postępowanie w przypadku naruszenia ochrony danych osobowych

13. Wszystkie skontrolowane jednostki opracowały i stosowały procedury wewnętrzne dotyczące postępowania w razie stwierdzenia naruszeń ochrony danych osobowych i zgłaszania ich do organu nadzorczego (Prezes UODO). Nieprawidłowości, w dwóch jednostkach, dotyczyły nieterminowego przekazania takiego zawiadomienia oraz niezgłoszenia Prezesowi UODO przypadku naruszenia ochrony danych osobowych, co stanowiło naruszenie art. 33 ust. 1 RODO. [str. 27–28]

Postępowanie w przypadku żądań usunięcia lub sprostowania danych osobowych

14. Poza jednym przypadkiem, nie stwierdzono nieprawidłowości w postępowaniu administratorów przy procedowaniu dotyczącym żądań osób fizycznych w sprawach usunięcia danych osobowych, jak również ich sprostowania lub uzupełnienia. Liczba takich żądań w poszczególnych jednost-

kach, poza Miastem Stołecznym Warszawa, była znikoma i nie przekroczyła siedmiu żądań o usunięcie danych, a w przypadku żądania sprostowania danych dotyczyła pojedynczych spraw. Natomiast w Mieście Stołecznym Warszawa w okresie objętym kontrolą zarejestrowano 344 żądania usunięcia danych osobowych i 46 wniosków o sprostowanie takich danych.
[str. 28–29]

Postępowanie z danymi osobowymi w jednostce

15. W skontrolowanych jednostkach, administratorzy na ogół prawidłowo postępowali z danymi osobowymi znajdującymi się w tych jednostkach, tj. prawidłowo informowali pracowników, jak również osoby zatrudnione na podstawie umów cywilno-prawnych oraz osoby ubiegające się o zatrudnienie o przetwarzaniu ich danych osobowych. Nieprawidłowości stwierdzono w jednej jednostce i dotyczyło to nieinformowania kandydatów ubiegających się o zatrudnienie o przetwarzaniu ich danych osobowych. Prawidłowo informowano gości i petentów o przetwarzaniu ich danych osobowych, a w przypadku monitoringu wizyjnego, również o przetwarzaniu ich wizerunku. W trakcie kontroli nie stwierdzono przypadków upubliczniania w miejscach ogólnodostępnych (np. tablice informacyjne) nadmiernych (inne niż niezbędne) danych osobowych. W każdej kontrolowanej jednostce opracowano i wdrożono, a także stosowano procedury związane z niszczeniem dokumentów papierowych i elektronicznych. Poza jednym wyjątkiem, przekazywanie na zewnątrz dokumentów do niszczenia następowało na podstawie umowy powierzenia przetwarzania danych osobowych. [str. 30–32]

4. UWAGI

Ochrona danych osobowych jest istotnym elementem działalności administracji publicznej. Nowe regulacje prawne postawiły przed administracją nowe zadania z którymi, jak wynika z ustaleń kontroli, jednostki radzą sobie w sposób zadawalający. Należy jednak mieć na uwadze, że kontrola przeprowadzona była m.in. w urzędach wojewódzkich i urzędach dużych i stosunkowo dużych miast. Jednostki tej wielkości mają odpowiednie zasoby ludzkie (kadrowe), które pozwalają na dokonanie profesjonalnych analiz i właściwe zdiagnozowanie ewentualnych zagrożeń związanych z bezpieczeństwem danych osobowych. Nie bez znaczenia jest również dysponowanie środkami finansowymi pozwalającymi na wdrożenie odpowiednich zabezpieczeń zarówno fizycznych, jak i technicznych, mających na celu niwelowanie tzw. „błędu ludzkiego". Doświadczenie NIK z innych kontroli oraz publikacje w mediach wskazują natomiast, że małe jednostki (np. gminy wiejskie) mogą nie dysponować odpowiednimi zasobami kadrowymi i finansowymi dla rzetelnej organizacji ochrony danych osobowych, co może powodować trudności w należytym zabezpieczeniu danych osobowych gromadzonych w tych jednostkach.

Zdaniem NIK ustalenia zawarte w tej Informacji mogą być pomocne jednostkom niekontrolowanym, w szczególności administracji samorządowej, w prawidłowej organizacji ochrony danych osobowych w swoich jednostkach.

Kierownicy jednostek administracji publicznej

Na podstawie analizy wniosków pokontrolnych skierowanych do kierowników skontrolowanych jednostek NIK podkreśla, że w związku z koniecznością ochrony danych osobowych, każda z jednostek administracji publicznej musi zwracać w szczególności uwagę na niżej wymienione obowiązki:

- upoważnianie pracowników do przetwarzania danych osobowych z chwilą powstania stosownego obowiązku;
- niezwłoczne odbieranie uprawnień dostępu do systemów informatycznych byłym pracownikom;
- zabezpieczanie pomieszczenia serwerowni przed utratą danych poprzez zminimalizowanie ryzyka nieautoryzowanego dostępu oraz zagrożenia pożarowego;
- stosowanie bezpiecznych rozwiązań informatycznych związanych m.in. z systemem autoryzacji dostępu do elektronicznych zasobów danych osobowych gromadzonych w jednostce oraz z tworzeniem i przechowywaniem kopii bezpieczeństwa zgromadzonych danych.

5. WAŻNIEJSZE WYNIKI KONTROLI

5.1. Organizacja ochrony danych osobowych w jednostce

Działania związane z identyfikacją ryzyk

Wszystkie jednostki przeprowadziły oceny dotychczasowych działań dotyczących ochrony danych oraz zasobów będących przedmiotem ochrony, a także zidentyfikowały słabości tych rozwiązań. Analiza ryzyka była prowadzona w pierwszej połowie 2018 r., przed powstaniem obowiązku stosowania RODO lub na początku jego obowiązywania, tj. czerwiec–lipiec 2018 r., co w ocenie NIK potwierdza rzetelne przygotowanie tych jednostek do wdrożenia RODO.

Analizy ryzyka były wykonywane przez Inspektorów Ochrony Danych lub przez powołane w jednostkach specjalnie w tym celu zespoły wdrożeniowe RODO. Stwierdzono również przypadki zlecania firmom zewnętrznym kompleksowego przygotowania jednostek do wdrożenia RODO, tj. przeprowadzenia analizy ryzyka, zaopiniowania lub opracowania projektów dokumentów, przeprowadzenie audytu w obszarze bezpieczeństwa informacji i ochrony danych osobowych. Działania te prowadziły do zidentyfikowania zasobów urzędów podlegających ochronie, wskazywały, które z obowiązujących dokumentów należy zmienić lub uaktualnić. Proponowano także plany działań naprawczych i szacowano poziom ryzyka dla poszczególnych procesów wraz z planem reakcji na ewentualne wystąpienie ryzyka.

Przykłady

W **Urzędzie Miasta Krakowa** analizy ryzyk związanych z przetwarzaniem danych osobowych, sporządzanie raportów z przeprowadzonych analiz oraz przyjmowanie planów postępowania w stosunku do ryzyk opisanych w tych analizach przygotowywano w ramach systemów informatycznych wdrożonych i stosowanych w Urzędzie.

W **Urzędzie Miasta Siedlce** podpisano umowę z firmą zewnętrzną, na podstawie której firma ta wykonała audyt Urzędu, przeprowadziła analizę i ocenę ryzyka oraz opracowała raport z audytu. W dokumentach tych, przedstawionych Prezydentowi w maju i czerwcu 2018 r., dokonano oceny ryzyka wynikającego ze sposobu działania Urzędu oraz stosowanych środków i procedur, a także zaproponowano określone działania.

W **Zachodniopomorskim Urzędzie Wojewódzkim** w lutym 2018 r. powołano Zespół do spraw wdrożenia RODO, którego zadaniem było m.in. przeprowadzenie analizy i oceny ryzyka wiążącego się z przetwarzaniem danych oraz przegląd dokumentacji ich przetwarzania. Podsumowanie działań Zespołu zostało przedstawione Wojewodzie w sprawozdaniu z 30 kwietnia 2018 r.

Wywiązywanie się z obowiązku opracowania dokumentacji wymaganej przepisami RODO

Wszystkie jednostki poddane kontroli wdrożyły nowe lub odpowiednio dostosowały dotychczasowe dokumenty do nowych regulacji[4]. Przede wszystkim opracowywano polityki bezpieczeństwa przetwarzania i ochrony danych. Dokumenty te określały podstawowe zasady obowiązujące w jednostce m.in. w zakresie dostępu, przetwarzania i nadawania upoważnień do przetwarzania danych. Dokumentacja ta była uzupełnia-

[4] Jednym z obowiązków wskazanych w art. 24 ust. 1 RODO jest wdrożenie przez administratora odpowiednich środków technicznych i organizacyjnych zapewniających przetwarzanie danych osobowych zgodnie z rozporządzeniem. Wymagane jest wdrożenie odpowiednich polityk ochrony danych. W związku z tym jednostki miały obowiązek opracować i wdrożyć odpowiednie regulacje.

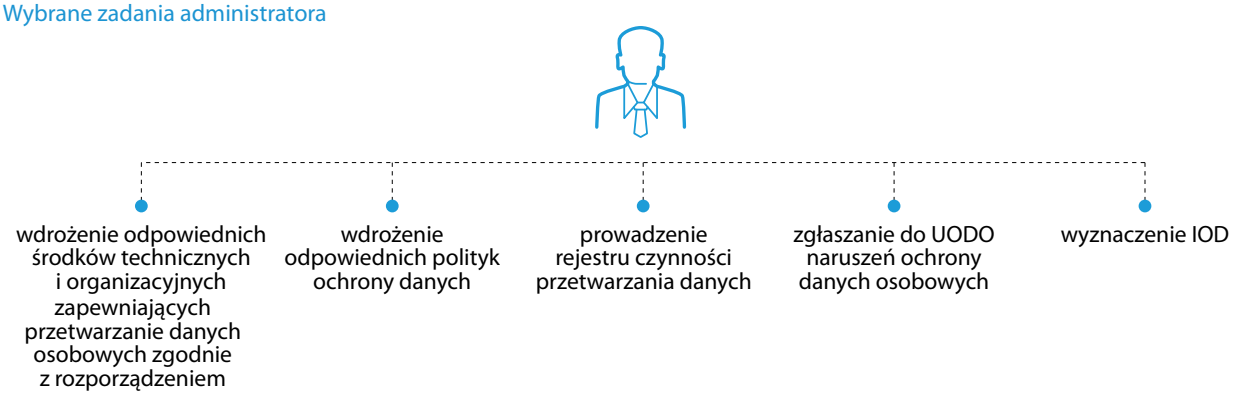
nia instrukcjami/zasadami dotyczącymi zarządzania systemami informatycznymi, zasadami dotyczącymi sposobu zawierania umów z podmiotami zewnętrznymi, regulacjami dotyczącymi postępowania w razie stwierdzenia naruszeń ochrony danych osobowych, zasadami prowadzenia monitoringu w jednostce oraz zasadami prowadzenia, określonych w art. 30 ust. 1 i 2 RODO, rejestrów: czynności przetwarzania danych osobowych i kategorii czynności przetwarzania.

Opracowanie projektów dokumentacji wewnętrznej było także (w dwóch przypadkach) powierzane podmiotom zewnętrznym. Podstawą ich sporządzenia był audyt przedwdrożeniowy przeprowadzany przez ten podmiot w obszarze bezpieczeństwa informacji.
Sytuacja taka miała miejsce w Urzędzie Miejskim w Chrzanowie. Umowa pomiędzy tym urzędem a wynajętym podmiotem obejmowała zarówno przeprowadzenie szczegółowego badania i oszacowania ryzyka oraz opracowanie projektów dokumentów wewnętrznych dostosowanych do przepisów RODO.

Informacje o wejściu w życie nowych regulacji przekazywane były pracownikom pocztą elektroniczną, w trakcie szkoleń lub poprzez zamieszczenie takiej informacji w zasobach intranetowych jednostki.

W jednym urzędzie (Mazowiecki Urząd Wojewódzki) ustalono, że zapoznanie się pracowników z wdrożoną dokumentacją miało być potwierdzone przez nich w sposób pisemny. Nie wszyscy pracownicy (dziewięć z 70 objętych kontrolą) dochowali tego obowiązku i nie przekazali w wymaganym terminie oświadczeń o zapoznaniu się z dokumentacją.

Infografika nr 4
Wybrane zadania administratora



Źródło: opracowanie własne NIK.

Wywiązanie się jednostek z obowiązku wyznaczenia Inspektora Ochrony Danych

We wszystkich kontrolowanych urzędach został wyznaczony IOD[5]. W jednej z 17 badanych jednostek (Urząd Miasta i Gminy Wieliczka) funkcję IOD pełniła firma świadcząca usługi w zakresie wdrożeń systemów ochrony danych, szkoleń o ochronie danych osobowych oraz pełnienia funkcji IOD. Firma ta została wybrana na podstawie konkursu ofert. W pozostałych przypadkach IOD był etatowym pracownikiem urzędu. Informacje o wyznaczeniu Inspektora Ochrony Danych oraz kontakt do niego były zamieszczane na stronach internetowych jednostek, zgodnie z art. 37 ust. 7 RODO.

[5] Obowiązek wyznaczenia Inspektora Ochrony Danych wynika z art. 37 ust. 1 RODO.

WAŻNIEJSZE WYNIKI KONTROLI

Stosownie do art. 10 ust. 1 i 6 ustawy *o ochronie danych osobowych* we wszystkich kontrolowanych jednostkach dochowano obowiązku powiadomienia Prezesa UODO o powołaniu IOD. Jednakże w czterech przypadkach powiadomienie zostało dokonane z opóźnieniem. W Urzędach Miast w: Ciechanowie, Kutnie i Krakowie kilkudniowe opóźnienia wynikały z problemów technicznych, które uniemożliwiały wysłanie drogą elektroniczną zgłoszenia do UODO. Natomiast 53 dniowe opóźnienie stwierdzone w Urzędzie Miasta i Gminy Wieliczka było spowodowane, jak wyjaśniono, dużym obciążeniem innymi obowiązkami służbowymi.

Zgodnie z art. 37 ust. 5 RODO, we wszystkich kontrolowanych jednostkach IOD miał odpowiednie kwalifikacje zawodowe związane z prawem i praktyką w dziedzinie ochrony danych osobowych. Pracownicy wyznaczeni na ww. stanowiska mieli wyższe wykształcenie, w tym prawnicze, a także ukończone studia podyplomowe z zakresu ochrony danych osobowych i informacji niejawnych lub bezpieczeństwa informacji (np. IOD w Urzędzie Miasta Stołecznego Warszawy, Urzędzie Miasta Ciechanów, Urzędzie Miejskim w Stargardzie, Urzędzie Miejskim w Policach). IOD brali udział w kursach, szkoleniach i konferencjach dotyczących ochrony danych osobowych.

Przestrzeganie zasady niezależności IOD

W kontrolowanych jednostkach Inspektorzy mieli zapewnioną niezależność[6] poprzez uregulowanie ich podległości tylko w stosunku do administratora, tj. ministra, wojewody czy prezydenta miasta, z wyjątkiem Urzędu Miejskiego w Stargardzie, gdzie IOD, zgodnie ze schematem organizacyjnym, podlegał także, pod względem merytorycznym, Sekretarzowi Miasta. Zdaniem Prezydenta Miasta wskazana w schemacie organizacyjnym dodatkowa podległość IOD Sekretarzowi Miasta dotyczyła głównie bieżących spraw administracyjnych, a Sekretarz nie ingerował w realizację zadań przez IOD. W ocenie NIK merytoryczny nadzór Sekretarza nad IOD stwarza możliwość władczego oddziaływania na istotne sprawy pozostające w gestii IOD i jest niezgodny z art. 38 ust. 3 RODO.

W 10 jednostkach pracownik wyznaczony do pełnienia funkcji IOD wykonywał także inne obowiązki.

Przykłady

W **Urzędzie Miejskim w Chrzanowie** IOD był także Inspektorem w Biurze ds. Bezpieczeństwa, w **Urzędzie Miasta Ciechanów** był także Pełnomocnikiem ds. ochrony informacji niejawnych, inspektorem bezpieczeństwa teleinformatycznego oraz operatorem drona, w **Urzędzie Miasta Siedlce** był podinspektorem w Wydziale Bezpieczeństwa i Zarządzania Kryzysowego, w **Urzędzie Miasta Kutno** był specjalistą ds. BHP, w **Urzędzie Miasta Sieradza** był zatrudniony na samodzielnym stanowisku ds. audytu i kontroli, w **Urzędzie Miasta Łodzi** był dyrektorem Biura Bezpieczeństwa Informacji i Ochrony Danych Osobowych, **w Mazowieckim UW** był Pełnomocnikiem ds. ochrony informacji niejawnych, **w Łódzkim UW** był na samodzielnym stanowisku ds. funkcjonowania systemów teleinformatycznych, w **Małopolskim UW** był Pełnomocnikiem ds. ochrony informacji niejawnych.

[6] Przepisy RODO (art. 38 ust. 3 i 6) nakazują, aby IOD był niezależny, a inne wykonywane przez niego zadania w jednostce nie powodowały konfliktu interesów.

WAŻNIEJSZE WYNIKI KONTROLI

Kontrola NIK nie wykazała przypadków wskazujących na ryzyko konfliktu interesów.
Należy mieć jednak na uwadze, że zgodnie z art. 38 ust. 6 RODO IOD może wykonywać inne zadania i obowiązki, jednakże to administrator ma obowiązek zapewnienia, by ich wykonywanie nie powodowało konfliktu interesów.

Realizacja zadań IOD

Inspektorzy prawidłowo realizowali swoje zadania określone w art. 39 RODO, tj. poprzez informowanie administratora i pracowników urzędów o obowiązkach związanych z ochroną danych, powiadamianie w sprawach zmieniających się przepisów prawa, monitorowanie przestrzegania przepisów dotyczących RODO oraz przyjętych regulacji wewnętrznych w swoich urzędach, współpracę w przypadku zawierania umów powierzenia przetwarzania danych oraz upoważnianie pracowników do przetwarzania danych osobowych, prowadzenie spraw związanych z naruszeniem danych osobowych, współpracę z organem nadzorczym oraz szkolenia z zakresu ochrony danych.

Prowadzenie szkoleń dotyczących ochrony danych osobowych

Kontrola nie ujawniła przypadków braku szkoleń specjalistycznych z zakresu ochrony danych osobowych. W większości jednostek szkoleniami z tego tematu obejmowano wszystkich pracowników urzędu, jedynie w jednym urzędzie (Urząd Miasta Siedlce) przeszkolono 20% pracowników, w zależności od zakresu obowiązków związanych z przetwarzaniem danych osobowych oraz przydatności tej wiedzy na stanowisku pracy.

Szkolenia prowadzone były przez IOD, a także przez podmioty zewnętrzne. Stosowano również formę szkoleń e-learningu (np. w Urzędzie Miasta Stołecznego Warszawy, Małopolskim Urzędzie Wojewódzkim, Urzędzie Miasta Łodzi, Urzędzie Miasta Szczecin). Tematyka prowadzonych szkoleń odnosiła się w szczególności do przepisów prawnych dotyczących ochrony danych osobowych, definicji danych osobowych, kategorii danych, praktycznych zasad przetwarzania danych osobowych, obowiązków administratora, IOD, pracowników, praw osób, których dane dotyczą, odpowiedzialności, naruszeń ochrony danych, ryzyka, zasad bezpieczeństwa związanych z użytkowaniem systemów informatycznych.

Szkolenia były też zróżnicowane pod kątem poszczególnych grup odbiorców, tj. odrębnie dla kadry kierowniczej urzędu, radnych rady miejskiej, pracowników urzędu, grupy pracowników obsługującej media. Szkolenia nowo zatrudnionych pracowników odbywały się na bieżąco, tak aby każdy nowy pracownik miał niezbędną wiedzę w tym zakresie. Nowo zatrudnieni pracownicy byli szkoleni przez IOD albo odbywali obowiązkowe szkolenie e-learningowe.

Infografika nr 5
Forma prowadzenia szkoleń pracowników

Źródło: opracowanie własne NIK.

Koszty wdrożenia RODO

Kontrola nie stwierdziła przypadków braku środków na pokrycie kosztów wdrożenia RODO. Wejście w życie przepisów RODO w każdej ze skontrolowanych jednostek wiązało się z dodatkowymi wydatkami. Szacowane przez kontrolowane jednostki koszty wdrożenia RODO wyniosły od 1,8 tys. zł do ok. 560 tys. zł. Wydatki te dotyczyły np. kosztów szkoleń, przeprowadzenia audytów, zakupu specjalistycznego oprogramowania, licencji, sprzętu, dostosowania infrastruktury do konieczności zwiększenia bezpieczeństwa i niekiedy kosztów zatrudnienia nowego pracownika do pełnienia funkcji IOD.

Przykłady

W **Małopolskim UW** koszty wdrożenia RODO oszacowano na 1,8 tys. zł – dotyczyły one kosztów szkolenia IOD.

W **Zachodniopomorskim UW** wydatkowano 5,7 tys. zł na szkolenia i uczestnictwo w konferencjach.

W **Urzędzie Miasta Krakowa** wydatkowano 130,0 tys. zł na szkolenia i modernizację aplikacji informatycznych.

W **Urzędzie Miasta Ciechanów** wydatkowano 194,7 tys. zł na usługi prawne i audytowe, zakup sprzętu i oprogramowania, szkolenia, refundację studiów podyplomowych, zakup systemów komputerowych.

W **MSWiA** wydatkowano ok 560,0 tys. zł na wykonanie niezbędnych inwestycji.

Ponoszenie konsekwencji w przypadkach naruszenia ochrony danych osobowych. Kary nakładane przez organ nadzorczy

W trzech z 17 kontrolowanych jednostek była przeprowadzona kontrola UODO. Na żadną z tych jednostek nie nałożono kar finansowych[7], natomiast w jednym przypadku (Urząd Miasta Stołecznego Warszawy) Prezes UODO w ramach swojego uprawnienia określonego w art. 102 ustawy o ochronie danych osobowych, nałożył karę upomnienia. Kara ta nałożona została w związku z nieuprawnionym przetwarzaniem danych osobowych osoby, która złożyła skargę do UODO, odnoszącą się do jej adresu zamieszkania.

Nadzór urzędów gmin nad jednostkami podległymi w zakresie stosowania RODO

Każdy z kontrolowanych 12 urzędów gmin miejskich posiadał jednostki podległe, tj. np. szkoły, przedszkola, spółki z udziałem miasta. Jednostki te były odrębnymi i samodzielnymi administratorami, ustanawiającymi samodzielnie zasady ochrony danych. Badaniem objęto współpracę urzę-

[7] Prezes UODO, w przypadku stwierdzenia nieprawidłowości związanych z ochroną danych osobowych, zgodnie z art. 102 ustawy *o ochronie danych osobowych*, może nałożyć na jednostki sektora finansów publicznych kary pieniężne w wysokości do 100 tys. zł.

dów miast z podległymi jednostkami w zakresie określania wspólnych zasad ochrony danych osobowych, wzajemnej pomocy lub wyznaczaniu kierunków działań.

Urzędy miast, poza jednym przypadkiem, nie uczestniczyły w opracowywaniu zasad ochrony danych oraz nie sprawowały bezpośredniego nadzoru w obszarze stosowania RODO w podległych jednostkach organizacyjnych. W ramach współpracy organizowano cykliczne spotkania z przedstawicielami jednostek, na których omawiano aktualne problemy dotyczące przetwarzania danych osobowych, udzielano merytorycznego i prawnego wsparcia. Jedną z metod nadzoru było też zlecenie audytu firmie zewnętrznej, dotyczącego ochrony danych osobowych (np. w Szczecinie, gdzie audyt został przeprowadzony w 149 podległych jednostkach oświatowych) oraz przeprowadzanie kontroli w podległych jednostkach w tym obszarze (np. w Łodzi i w Kutnie).

Z 12 skontrolowanych urzędów miast tylko **Urząd Miasta Krakowa** podjął ścisłą współpracę z jednostkami podległymi, polegającą na wspólnym opracowaniu zasad ochrony danych osobowych, a także zatrudnieniu IOD dla jednostek podległych. Prace nad opracowaniem zasad ochrony danych osobowych w miejskich jednostkach organizacyjnych rozpoczęto we wrześniu 2017 r. w ramach projektu powiązanego ze zmianą przepisów o ochronie danych osobowych i potrzeby kompleksowego wdrożenia zarządzania bezpieczeństwem informacji w gminie miejskiej Kraków (GMK). Projektem objęto wszystkie 340 jednostki gminy, tj. żłobki, przedszkola, szkoły, poradnie psychologiczno-pedagogiczne, domy kultury i inne. Projekt miał na celu m.in. wspomaganie zarządzania bezpieczeństwem informacji w tych jednostkach, a jego realizacja zaplanowana została do marca 2022 r. Nadzór nad jednostkami realizowany był przez Urząd na podstawie zarządzenia Prezydenta Miasta powołującego w GMK Radę Inspektorów Ochrony Danych[8] (w skład Rady wchodzili IOD wyznaczeni w 10 jednostkach GMK np. Straż Miejska, MOPS, IOD Urzędu oraz pracownicy komórki organizacyjnej Urzędu obsługującej IOD). Do zadań Rady należało m.in. opracowanie wspólnych metodyk analizy ryzyka i oceny skutków dla ochrony danych, wytyczanie kierunków polityki bezpieczeństwa informacji, ustalanie standardów zarządzania naruszeniami ochrony danych osobowych, wspieranie administratorów w jednostkach podległych. Ponadto zarządzeniem Prezydenta Miasta w sprawie określenia zasad współpracy Urzędu z miejskimi jednostkami organizacyjnymi wskazano sześć osób jako IOD dla miejskich jednostek, którzy byli pracownikami Zespołu Inspektora Ochrony Danych Urzędu, który organizacyjnie znajdował się w Wydziale Organizacji i Nadzoru Urzędu (w skład Zespołu wchodziło 10 pracowników Urzędu, w tym IOD Urzędu i trzy osoby wspierające go oraz sześć osób sprawujących funkcję IOD dla wybranych miejskich jednostek organizacyjnych).

W jednej gminie (Ciechanów), mimo obowiązku określonego w art. 37 ust. 7 RODO oraz art. 11 ustawy *o ochronie danych osobowych*, na stronach internetowych podległych jednostek (ośmiu z 25) nie zostały zamieszczone dane kontaktowe do IOD.

[8] Zarządzenie nr 1350/2018 z dnia 29 maja 2018 r.

W pięciu przypadkach (na 12 badanych) urzędy skorzystały z możliwości określonej w art. 37 ust. 6 RODO, powierzając zadania IOD firmom zewnętrznym.

Przykłady

W **Chrzanowie** we wszystkich 29 jednostkach organizacyjnych Gminy wyznaczono IOD, z czego w ośmiu przypadkach był to pracownik jednostki, a w pozostałych (21) zawarto umowy z firmą zewnętrzną.

W **Ciechanowie** na 25 jednostek podległych funkcję IOD w czterech przypadkach pełnił pracownik danej jednostki, a w pozostałych jednostkach (21) zawarto umowy z firmą zewnętrzną.

W **Szczecinie** w placówkach edukacyjnych, przedszkolnych i żłobkach zawarto umowę na pełnienie funkcji IOD ze Szczecińskim Parkiem Naukowo-Technologicznym.

W **Policach** na 25 jednostek podległych w 15 przypadkach IOD byli pracownikami jednostek, a w pozostałych dziesięciu zawarto odrębne umowy z podmiotem zewnętrznym.

W **Stargardzie** na 32 jednostki w sześciu przypadkach funkcję IOD pełnił pracownik tej jednostki, a w pozostałych 26 jednostkach zawarto umowy z podmiotem zewnętrznym.

5.2. Wykorzystanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych

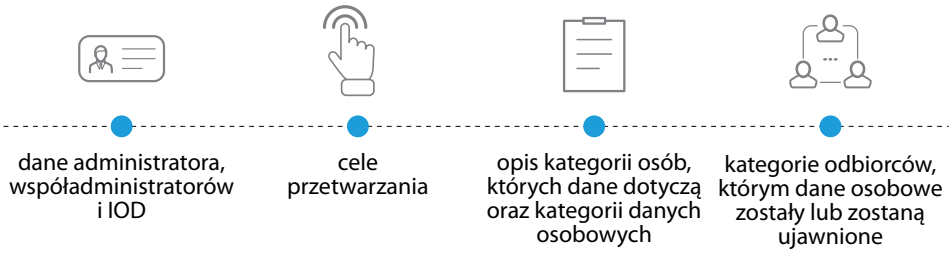
Wywiązywanie się z obowiązku założenia i prowadzenia rejestru czynności przetwarzania danych

W czterech urzędach nie wypełniono obowiązku utworzenia rejestru czynności przetwarzania danych[9] od chwili rozpoczęcia stosowania RODO, tj. od 25 maja 2018 r. Ustalono że w Chrzanowie rejestr prowadzony był od 28 sierpnia 2018 r., w Siedlcach od 24 sierpnia 2018 r., w Stargardzie od 1 czerwca 2018 r., w Ciechanowie od 30 maja 2018 r.

Ponadto rejestr czynności przetwarzania danych prowadzony w Urzędzie Miasta Ciechanów nie zawierał kompletnych danych, ponieważ brak było opisów czynności takich jak: prowadzenie rejestrów upoważnień do przetwarzania danych osobowych, zarządzeń, decyzji wydawanych przez Prezydenta Miasta, realizacji zadań audytowych i kontrolnych, zawierania i realizacji umów cywilnoprawnych. Powodem tej nieprawidłowości były błędy w kartach informacyjnych sporządzanych przez pracowników Urzędu, które stanowiły dla IOD podstawę do ujmowania w rejestrze procesów zachodzących w Urzędzie.

[9] RODO nakłada na administratorów obowiązek prowadzenia rejestru czynności przetwarzania danych. W rejestrze tym, zgodnie z art. 30 ust. 1 RODO, zamieszcza się m.in. imię i nazwisko oraz dane kontaktowe administratora oraz IOD; cele przetwarzania danych; opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych, które są przetwarzane; kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione.

Infografika nr 6
Wybrane informacje zamieszczane w rejestrze czynności przetwarzania danych osobowych



Źródło: opracowanie własne NIK.

W rejestrach czynności przetwarzania danych ujmowano kategorie zbiorów danych takie jak np. akta pracowników, rekrutacje, ubezpieczenia pracowników, oświadczenia majątkowe, sprawy sądowe i egzekucyjne, ewidencje podatków lokalnych, wynagrodzenia z tytułu umów zleceń i umów o dzieło, pomoc społeczną, zdrowie publiczne, działania w ramach profilaktyki antyalkoholowej, akta stanu cywilnego.

Wywiązywanie się z obowiązku założenia i prowadzenia rejestru kategorii czynności przetwarzania danych

W dwóch spośród 17 jednostek objętych kontrolą, rejestr kategorii czynności[10] został założony dopiero w trakcie kontroli NIK, tj. w Urzędzie Miasta Ciechanów 9 grudnia 2019 r. i w Urzędzie Miasta Siedlce 15 października 2019 r., pomimo obowiązku jego prowadzenia od 25 maja 2018 r., tj. powstania obowiązku stosowania RODO.
Prezydent Miasta Siedlce wyjaśnił, że komórki organizacyjne Urzędu nie poinformowały IOD o istnieniu umów powierzenia, w których podmiotem przetwarzającym jest Prezydent i dopiero kontrola NIK ujawniła takie umowy. Natomiast Prezydent Miasta Ciechanów stwierdził, że rejestr ten był prowadzony, ale w formie rejestru umów powierzenia przetwarzania. Kontrola NIK wykazała jednak, że rejestr umów powierzenia nie zawierał danych określonych w art. 30 ust. 2 RODO, w związku z czym, nie można było go uznać za rejestr kategorii czynności przetwarzania danych, o którym mowa w RODO.

Przestrzeganie obowiązku administratorów upoważniania pracowników do przetwarzania danych

W większości badanych urzędów zarówno pracownicy etatowi, jak i osoby zatrudnione na podstawie umów cywilno-prawnych, mający dostęp do danych osobowych, mieli stosowne upoważnienia administratorów do przetwarzania tych danych[11]. Chociaż z przepisów nie wynika obowiązek wydawania upoważnień do przetwarzania danych osobowych w formie pisemnej, jednak w kontrolowanych jednostkach, w odniesieniu do pracowników etatowych, stosowano pisemne upoważnienia. Prowadzono także rejestry wydanych upoważnień. Z analizy przepisów RODO wynika, że przyjęcie takiej formy upoważniania jest wskazane z uwagi na zasadę rozliczalności określoną w art. 5 ust. 2 RODO, który stanowi, że administrator musi być w stanie wykazać przestrzeganie zasad RODO dotyczących przetwarzania danych osobowych.

[10] Obowiązek prowadzenia rejestru kategorii czynności przetwarzania danych wynika z art. 30 ust. 2 RODO i nałożony jest na podmioty przetwarzające. Rejestr ten zawiera m.in. imię i nazwisko oraz dane kontaktowe podmiotu przetwarzającego oraz administratora, w imieniu którego działa podmiot, a także IOD, a także kategorie przetwarzań dokonywanych w imieniu administratorów.

[11] Zgodnie z RODO (art. 29 oraz art. 32 ust. 4) każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego, mająca dostęp do danych osobowych, przetwarza je wyłącznie na polecenie administratora.

Niestosowanie pisemnej formy wydawania upoważnień do przetwarzania danych osobowych stwierdzono w Urzędzie Miasta Ciechanów w przypadku dwóch umów zleceń oraz w Urzędzie Miasta Siedlce. Badanie 12 umów zleceń zawartych przez Urząd Miasta Siedlce po 25 maja 2018 r. wykazało, że w czterech przypadkach, dotyczących zadań związanych z pracą komisji egzaminacyjnych, zleceniobiorcy nie mieli pisemnych upoważnień i przetwarzali dane osobowe na podstawie prawa powszechnie obowiązującego, tj. art. 9g ust. 2 ustawy z dnia 26 stycznia 1982 r. *Karta Nauczyciela*[12], który normuje obowiązek powoływania przez organ prowadzący szkołę, komisji egzaminacyjnych dla nauczycieli ubiegających się o awans na stopień nauczyciela mianowanego, spośród osób wskazanych na podstawie tego przepisu. Prezydent wyjaśnił, że poufność przetwarzania danych osobowych została zapewniona poprzez stosowanie procedur wewnętrznych odnoszących się do fizycznego zabezpieczenia dokumentów i zapewnienia dostępu do dokumentów jedynie członkom powoływanych komisji egzaminacyjnych. Dodał także, że członkowie komisji egzaminacyjnych realizowali swoje obowiązki zgodnie z powszechnie obowiązującym prawem oraz regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych.
Zdaniem NIK, brak w umowach zapisów, że zleceniobiorcy przetwarzają dane osobowe na wyraźne polecenie administratora, zgodnie z art. 29 RODO, stwarza ryzyko niezapewnienia poufności, o której mowa w art. 5 ust. 1 pkt f RODO. Należy podkreślić, że art. 5 RODO nakłada obowiązki nie tylko na administratora, ale na wszystkie podmioty uczestniczące w procesie przetwarzania danych, a zatem w omawianej sprawie bezpośrednio oddziałuje również na zleceniobiorców, z którymi podpisano umowy.

W obszarze upoważniania pracowników do przetwarzania danych stwierdzono także nieprawidłowości, które miały charakter sporadyczny i związane były przede wszystkim z wydawaniem upoważnień do przetwarzania danych osobowych z opóźnieniem w stosunku do terminów rozpoczęcia faktycznego przetwarzania tych danych przez pracowników urzędów. Dotyczyło to m.in. następujących jednostek.

Przykłady

W **Łódzkim Urzędzie Wojewódzkim** spośród 290 skontrolowanych pracowników, pięciu nowo zatrudnionych w okresie od lipca do września 2019 r. nie miało upoważnienia do przetwarzania danych osobowych. Przyczyną, jak wyjaśniono, było nieprzekazanie do odpowiedniej komórki organizacyjnej urzędu wniosków o wystawienie upoważnień. W wyniku kontroli NIK wydano tym osobom stosowne upoważnienia.

W **Urzędzie Miejskim w Stargardzie**, w okresie od 25 maja do 6 września 2018 r., 19 spośród 21 skontrolowanych pracowników urzędu przetwarzało dane osobowe bez upoważnienia administratora. Prezydent Miasta wyjaśnił, że miało to związek z opóźnieniem wdrożenia dokumentacji przystosowującej Urząd do wymagań RODO.

W **Mazowieckim Urzędzie Wojewódzkim** spośród 40 skontrolowanych pracowników, dwóm nie zmieniono upoważnień w związku ze zmianą miejsca zatrudnienia, a w przypadku jednej osoby upoważnienie do przetwarza-

[12] Dz. U. z 2019 r. poz. 2215, ze zm.

nia danych wydano po dwóch miesiącach od momentu zatrudnienia w urzędzie. Wyjaśniono, że miało to związek z niezłożeniem odpowiednich wniosków o zmianę i wystawienie stosownych upoważnień.

Przestrzeganie obowiązku unieważniania dostępu do systemów informatycznych

W kontrolowanych jednostkach polecenie administratora dotyczące przetwarzania danych osobowych przyjęło formę pisemnych upoważnień dla pracowników przetwarzających dane osobowe. Tym samym osoby, które nie są już pracownikami jednostki, nie mogły działać z upoważnienia administratora i nie mogły dokonywać żadnych czynności związanych z przetwarzaniem danych osobowych.

Wśród 17 kontrolowanych jednostek w sześciu stwierdzono przypadki nie blokowania dostępu do zasobów informatycznych w chwili rozwiązania stosunku pracy, a także przypadki logowań do kont byłych pracowników.

Przykłady

W **Urzędzie Miasta Stołecznego Warszawy** zablokowanie kont dostępu w domenie Urzędu w przypadku 16 z 21 byłych pracowników Urzędu Dzielnicy Ochota zostało dokonane w terminie od jednego do 345 dni od zakończenia stosunku pracy przez tych pracowników. Ponadto ustalono, że do kont czterech byłych pracowników dokonywane były logowania w systemach informatycznych Urzędu Miasta po zakończeniu stosunku pracy.

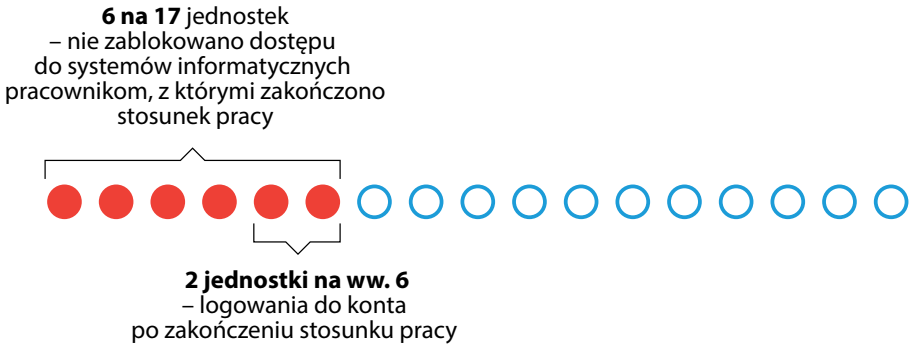
W **Urzędzie Miasta Siedlce** nie zostały wyłączone konta dostępu do systemów informatycznych siedmiu z 16 pracowników, z którymi rozwiązano stosunek pracy. Ponadto w przypadku dwóch spośród 16 ww. osób, po dacie rozwiązania z nimi stosunku pracy wystąpiły przypadki logowania do ich kont domenowych umożliwiających dostęp do komputerów, w których przetwarzane są dane osobowe, tj. osiem i 10 dni po odejściu danego pracownika z pracy.

W **Urzędzie Miasta Kutno** ośmiu osobom na 14 skontrolowanych pozostawiono, po rozwiązaniu stosunku pracy, aktywne konta poczty e-mail. Konta te usunięto dopiero w trakcie kontroli NIK, tj. po upływie od czterech do 16 miesięcy od rozwiązania umów o pracę. Ponadto czterem osobom usunięto konta dostępu do jednego z systemów informatycznych również dopiero na skutek kontroli NIK, tj. po upływie od jednego do sześciu miesięcy od wygaśnięcia stosunku pracy. W przypadku jednej osoby konto w domenie zablokowano po 14 miesiącach od rozwiązania umowy o pracę, także w wyniku kontroli NIK.

W **Urzędzie Miasta Szczecin**, w 19 przypadkach na 23 zbadane, dostęp do systemów informatycznych Urzędu zawierających dane osobowe był unieważniany w terminie od jednego do 22 dni od rozwiązania stosunku pracy. Ponadto trzem osobom zmieniającym miejsce pracy w ramach Urzędu nie odebrano uprawnień do systemów informatycznych z poprzedniego Wydziału/Biura.

Przyczyną powyższych nieprawidłowości, według wyjaśnień osób odpowiedzialnych w poszczególnych Urzędach za ten obszar działalności, było przede wszystkim niedopatrzenie i nieprawidłowy obieg informacji między odpowiednimi komórkami organizacyjnymi w jednostkach.

Infografika nr 7
Nieprawidłowości w unieważnianiu dostępu do systemów informatycznych



Źródło: opracowanie własne NIK.

Przestrzeganie warunków powierzania przetwarzania danych osobowych podmiotom zewnętrznym

We wszystkich jednostkach objętych kontrolą miało miejsce powierzanie przetwarzania danych osobowych podmiotom zewnętrznym. Podstawą powierzeń były umowy, które, poza niżej wymienionym przypadkiem, zawierały elementy wymagane przepisami RODO[13].

W **Urzędzie Miasta Szczecin** jedna umowa zawarta przed 25 maja 2018 r. została zaktualizowana o odpowiednie postanowienia dotyczące powierzenia przetwarzania danych osobowych po upływie 18 dni od powstania obowiązku stosowania RODO. Stwierdzono też, że porozumienie w sprawie powierzenia przetwarzania danych osobowych Zakładowi Budynków i Lokali Komunalnych zawarto po upływie pięciu miesięcy i 22 dni od rozpoczęcia stosowania RODO. Ponadto w porozumieniu tym nie określono kategorii osób, których dane dotyczą, co było niezgodne z art. 28 ust. 3 RODO. Według wyjaśnień IOD przyczyną powyższego było długotrwałe uzgadnianie treści umów i porozumień, aby spełniały wszystkie wymogi RODO.

Nierzetelne prowadzenie rejestrów umów powierzenia stwierdzono w Urzędach Miast w Kutnie i w Sieradzu. Polegało to na nieujęciu w nich odpowiednio 38% i 68% umów powierzenia zawartych w tych jednostkach. Było to niezgodne z procedurami wewnętrznymi obowiązującymi w tych Urzędach. Przyczyną tych nieprawidłowości było niedopatrzenie ze strony pracowników urzędu oraz niewłaściwy przepływ danych między komórkami organizacyjnymi urzędu.

Wypełnianie obowiązków podmiotu przetwarzającego

Wszystkie jednostki objęte kontrolą realizowały zadania podmiotu przetwarzającego dane osobowe na polecenie administratora. Podstawą przetwarzania były ustawy, umowy i porozumienia zawierane z administratorami.

Przykładowo, urzędy gmin wykonywały zadania podmiotu przetwarzającego z tytułu zadań zleconych z zakresu administracji rządowej w imieniu: Ministra Cyfryzacji oraz Ministra Spraw Wewnętrznych

[13] Zgodnie z art. 28 ust. 3 RODO przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które określają przedmiot, czas trwania, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób których dotyczą, a także obowiązki i prawa administratora. Dokumenty te muszą mieć formę pisemną, w tym formę elektroniczną (art. 28 ust. 9 RODO).

i Administracji na podstawie ustawy z dnia 28 listopada 2014 r. *Prawo o aktach stanu cywilnego*[14], ustawy z dnia 24 września 2010 r. *o ewidencji ludności*[15], ustawy z dnia 6 sierpnia 2010 r. *o dowodach osobistych*[16] oraz w imieniu Ministra Edukacji Narodowej na podstawie ustawy z dnia 15 kwietnia 2011 r. *o systemie informacji oświatowej*[17].

W związku z wykonywaniem zadań podmiotu przetwarzającego z tytułu realizacji zadań zleconych z zakresu administracji rządowej, urzędy gmin otrzymały od administratorów wytyczne i instrukcje odnośnie prowadzenia baz danych lub stosowania obowiązujących przepisów, w tym m.in.:

- Minister Spraw Wewnętrznych i Administracji wspólnie z Ministrem Cyfryzacji w związku z realizacją zadań z zakresu spraw obywatelskich przygotowali i przekazali informacje na temat stosowania przepisów RODO wraz ze wzorami klauzul informacyjnych w zakresie rejestru stanu cywilnego, ewidencji ludności i dowodów osobistych;
- Minister Edukacji Narodowej przekazywał wytyczne odnośnie pracy w Systemie Informacji Oświatowej.

Urzędy gmin realizowały także zadania podmiotów przetwarzających na podstawie umów i porozumień, np.: umowa z Krajowym Biurem Wyborczym w sprawie realizacji wyborów, porozumienia dotyczące realizacji programów Karta Rodziny i Karta Seniora, umowy dotyczące realizacji projektów dofinansowywanych z budżetu Unii Europejskiej.

Wojewodowie przetwarzali dane osobowe na podstawie np. ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[18], ustawy z dnia 24 sierpnia 2007 r. *o udziale RP w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym*[19], ustawy z dnia 22 listopada 2013 r. *o systemie powiadamiania ratunkowego*[20], ustawy z dnia 8 września 2006 r. *o Państwowym Ratownictwie Medycznym*[21], ustawy z dnia 13 lipca 2006 r. *o dokumentach paszportowych*[22].

Wojewodowie przetwarzali dane osobowe również na podstawie umów i porozumień, np. umowy dotyczące realizacji projektów dofinansowywanych z budżetu Unii Europejskiej, świadczenia usług rekreacyjno-sportowych, aktywizacji zawodowej młodych.

Przestrzeganie zasad funkcjonowania monitoringu wizyjnego

Spośród 17 jednostek objętych kontrolą, monitoring wizyjny prowadzony był w 14, w jednej jednostce nie był prowadzony, a w dwóch prowadzona była jedynie transmisja z obrad rady miejskiej[23]. Monitoringiem objęte były

[14] Dz. U. z 2018 r. poz. 2224, ze zm.

[15] Dz. U. z 2019 r. poz. 1397, ze zm.

[16] Dz. U. z 2020 r. poz. 332.

[17] Dz. U. z 2019 r. poz. 1942.

[18] Dz. U. z 2020 r. poz. 346.

[19] Dz. U. z 2019 r. poz. 1844.

[20] Dz. U. z 2019 r. poz. 1077.

[21] Dz. U. z 2019 r. poz. 993, ze zm.

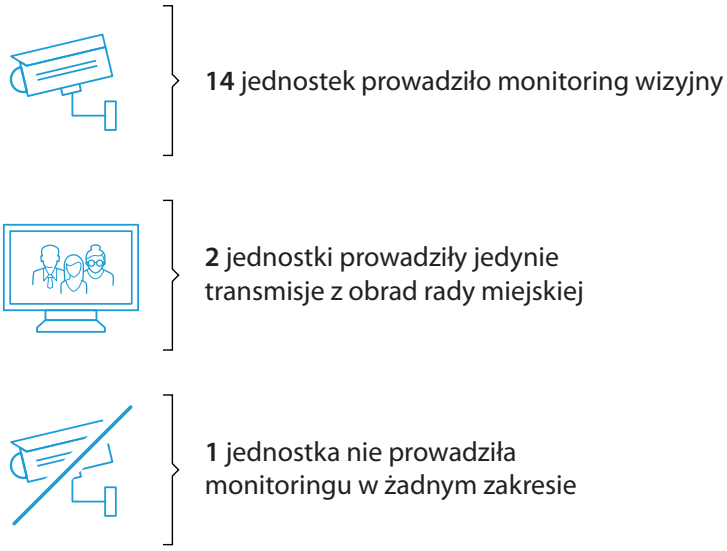
[22] Dz. U. z 2018 r. poz. 1919, ze zm.

[23] Zgodnie z art. 88 ust. 1 RODO państwa członkowskie mogą zawrzeć w swoich przepisach bardziej szczegółowe uregulowania mające zapewnić ochronę praw i wolności przy przetwarzaniu danych osobowych pracowników. Na tej podstawie zasady prowadzenia monitoringu wizyjnego w miejscach pracy zostały uregulowane w ustawie z dnia 26 czerwca 1974 r. *Kodeks pracy* Dz. U. z 2019 r. poz. 1040, ze zm.

najczęściej wejścia do urzędów wraz z recepcjami oraz ciągi komunikacyjne. Nie stwierdzono monitoringu wizyjnego w miejscach niedozwolonych, o których mowa w art. 22^2 Kodeksu pracy, tj. m.in. pomieszczeń sanitarnych, stołówek, palarni. Miejsca objęte monitoringiem wizyjnym były właściwie oznakowane w sposób widoczny i czytelny. W kontrolowanych jednostkach były wewnętrzne procedury regulujące organizację monitoringu wizyjnego, w tym zasady i termin przechowywania nagrań, który zgodnie z art. 22^2 §3 Kodeksu pracy nie powinien przekraczać trzech miesięcy.

Nieprawidłowości w prowadzeniu monitoringu wizyjnego stwierdzono jedynie w **Urzędzie Miasta Kutno**, gdzie zapisy z monitoringu wizyjnego prowadzonego w Urzędzie przechowywano przez okres dłuższy niż określony w procedurach wewnętrznych (w Polityce bezpieczeństwa), tj. ponad 30 dni. Najstarszy, stwierdzony w wyniku kontroli, zapis nagrania z monitoringu pochodził sprzed 46 dni od daty nagrania. Zdaniem Zastępcy Prezydenta Miasta spowodowane jest to techniką nagrywania. Kamery załączane są za pomocą detektora ruchu i im mniej osób porusza się w zasięgu kamery, tym mniej jest zapisu na dysku rejestratora i czas zapisu się wydłuża.

Infografika nr 8
Monitoring wizyjny



Źródło: opracowanie własne NIK.

Ochrona systemów informatycznych

Wszystkie kontrolowane jednostki opracowały procedury wewnętrzne dotyczące ochrony fizycznej i technicznej budynków oraz infrastruktury informatycznej[24]. Procedury te określały m.in. mechanizmy zapewniające ciągłość działania zasobów informatycznych, bezpieczeństwo fizyczne i śro-

[24] Zgodnie z art. 32 ust. 1 RODO, administratorzy i podmioty przetwarzające są zobowiązani do wdrożenia odpowiednich środków technicznych i organizacyjnych, które powinny zapewnić jednostce zdolność do utrzymania poufności, integralności i odporności systemów informatycznych i usług przetwarzania danych osobowych. Ponadto zgodnie z art. 32 ust. 1 pkt c) RODO, administrator i podmiot przetwarzający są zobowiązani do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

dowiskowe, zasady zarządzania kopiami bezpieczeństwa, ochronę przed szkodliwym oprogramowaniem, systemy wydawania kluczy, systemy kontroli wejść do serwerowni i centrali telefonicznej, systemy przeciwpożarowe, systemy sygnalizacji włamania i napadu.

Nieprawidłowości dotyczące fizycznego zabezpieczenia systemów polegały przede wszystkim na utrzymywaniu serwerowni w niewłaściwym stanie technicznym w następujących jednostkach:

Przykłady

W **Urzędzie Miasta i Gminy Wieliczka** w pomieszczeniu serwerowni znajdowały się urządzenia komputerowe wycofane z użytku oraz materiały łatwopalne (meble, papierowe/tekturowe opakowania, papier do drukarek). Ponadto, poza kamerą rejestrującą obraz zamontowaną wewnątrz pomieszczenia, nie było systemu kontroli dostępu do serwerowni. Było to niezgodne z art. 32 ust. 1 lit. b) w związku z art. 24 ust. 1 RODO oraz § 20 ust. 2 pkt 7 i 9 rozporządzenia w sprawie KRI[25]. Przepisy te nakładają na kierownictwo podmiotu publicznego/administratora zapewnienie ochrony przetwarzanych informacji m.in. przed ich kradzieżą, nieuprawnionym dostępem, usunięciem lub zniszczeniem. W wyniku kontroli (przed jej zakończeniem) zainstalowano i uruchomiono system kontroli dostępu dla osób upoważnionych, wyniesiono z pomieszczenia wszystkie zbędne przedmioty, a także umieszczono w serwerowni dwie gaśnice wolnostojące.

W **Urzędzie Miasta Kutno** w pomieszczeniu serwerowni nie zainstalowano urządzeń systemu alarmowego służącego ochronie przeciwpożarowej. Stanowiło to naruszenie § 13 pkt 9 Polityki bezpieczeństwa obowiązującej w Urzędzie, zgodnie z którym pomieszczenia, w których przetwarzane są zbiory danych osobowych, powinny być zabezpieczane przed skutkami pożaru za pomocą systemu alarmowego. Zastępca Prezydenta Miasta wyjaśnił, że bezpieczeństwo serwerowni zostało zapewnione, ponieważ w korytarzu przy tym pomieszczeniu zainstalowana jest kamera i system czujek przeciwpożarowych, a kilkadziesiąt metrów od serwerowni (na tym samym poziomie) znajduje się dyżurka ochrony. Ponadto dodał, że trwają prace przygotowawcze do przeniesienia serwerowni. W ocenie NIK, stwierdzony w toku kontroli sposób zabezpieczenia serwerowni nie spełniał jednak wymogów określonych w Polityce bezpieczeństwa.

W **Urzędzie Miejskim w Stargardzie** pomieszczenie serwerowni usytuowane było w holu wejściowym Urzędu użytkowanym m.in. przez petentów. Wejście do serwerowni nie było zabezpieczone alarmami przeciwwłamaniowymi, nie było też monitoringu wizyjnego ani elektronicznej weryfikacji dostępu. Drzwi do serwerowni nie miały atestu antywłamaniowego. Wyposażenie pomieszczenia serwerowni nie miało atestu przeciwpożarowego (drzwi drewniane, wykładzina podłogowa), a także nie było odpowiedniego dla sprzętu informatycznego systemu gaszenia. Stwarzało to zarówno możliwość nieautoryzowanego dostępu do serwerowni przez osoby postronne, jak i niedostatecznie minimalizowało ryzyko zagrożenia pożarowego.
Prezydent Miasta wyjaśnił, że właściwe zabezpieczenie serwerowni zostało rozłożone w czasie z uwagi na możliwości finansowe budżetu miasta i będzie kontynuowane w 2020 r.

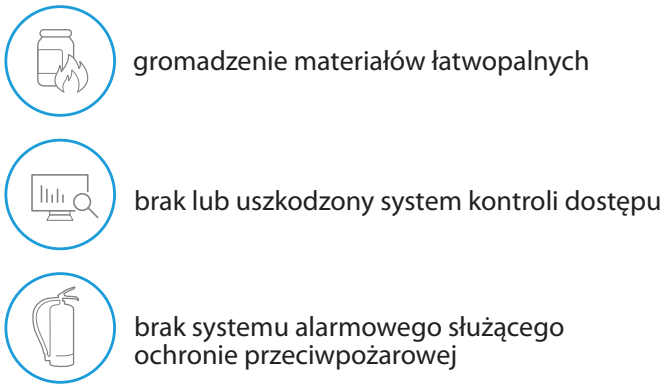
[25] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247).

Ponadto w Urzędzie tym ustalono, że zgodnie z wewnętrzną Instrukcją Zarządzania Systemami Informatycznymi powinny być utworzone dwie serwerownie w dwóch różnych lokalizacjach, a utworzona była tylko jedna. Wiązało się to też z niezgodnym z tą Instrukcją sposobem przechowywania kopii bezpieczeństwa baz danych, tj. przechowywaniem ich tylko w jednej lokalizacji, a nie w dwóch. Jak wyjaśnił Prezydent, utworzenie dodatkowej serwerowni zaplanowano na IV kw. 2019 r.

W **Urzędzie Miasta Ciechanów** w pomieszczeniach serwerowni magazynowane były materiały łatwopalne. Uszkodzone były również zamki elektroniczne w drzwiach wejściowych do serwerowni. W trakcie kontroli NIK usunięto wymienione nieprawidłowości.

NIK zwraca uwagę, że dane gromadzone w serwerowni stanowią informacje dotyczące najważniejszych sfer działalności urzędu, a ich utrata lub brak dostępności może doprowadzić do sytuacji kryzysowej.

Infografika nr 9
Nieprawidłowości w fizycznym zabezpieczeniu serwerowni



Źródło: opracowanie własne NIK.

Istotnym problemem dla prawidłowego zabezpieczenia danych osobowych przed nieuprawnionym dostępem, kradzieżą lub utratą jest ograniczenie dostępu do sieci lokalnych, w których te dane są przetwarzane. W skontrolowanych jednostkach najczęstszym rozwiązaniem zabezpieczenia danych osobowych była konieczność uwierzytelnienia dostępu do sieci lokalnych przy użyciu identyfikatora (login) i hasła. Było to opisane w procedurach wewnętrznych, gdzie określano m.in. zasady tworzenia hasła, w tym wymaganą liczbę znaków. Ustalono jednak, że w trzech jednostkach system nie wymuszał stosowania haseł o przewidzianej w procedurze liczbie znaków, tj. dopuszczał stosowanie mniejszej ich liczby. Sytuacja taka wystąpiła w Urzędach Miast w Ciechanowie, Kutnie i Sieradzu. W wyniku ustaleń kontroli NIK w jednostkach tych jeszcze w trakcie kontroli wprowadzono odpowiednie zmiany gwarantujące wymuszanie przez systemy wprowadzania haseł dostępu zgodnych z wymaganiami procedur wewnętrznych.

5.3. Zarządzanie danymi osobowymi przetwarzanymi, w tym gromadzonymi w jednostce

Postępowanie w przypadku naruszenia ochrony danych osobowych

We wszystkich kontrolowanych jednostkach administratorzy opracowali regulacje dotyczące postępowania w związku z naruszeniem ochrony danych osobowych. Ustalono sposób postępowania, osoby odpowiedzialne za konkretne działania oraz sposoby wyliczania wagi naruszenia[26].

Przykład

W **Urzędzie Miasta Stołecznego Warszawy** wdrożono narzędzie informatyczne w sieci intranetowej do celów zgłaszania przypadków naruszenia ochrony danych osobowych, które umożliwia zgłaszanie takich incydentów przez urzędników. Wprowadzono także metodykę oceny wagi naruszenia oraz zautomatyzowano sposób wyliczania wagi naruszenia. Wdrożone rozwiązanie standaryzuje klasyfikacje incydentów i ocenę wagi naruszenia w całej strukturze Urzędu. Opracowywano także kwartalne i roczne raporty dotyczące incydentów, które zawierały analizy pod względem liczb, miejsca stwierdzenia oraz najczęstszych przyczyn ich powstania.

Najwięcej stwierdzonych naruszeń ochrony danych osobowych w okresie objętym kontrolą, wystąpiło w dużych urzędach miast np. w Urzędzie Miasta Stołecznego Warszawy do 18 grudnia 2019 r. do Prezesa UODO zostały zgłoszone 134 naruszenia ochrony danych osobowych. W Urzędzie Miasta Łodzi zidentyfikowano 15 przypadków naruszenia ochrony danych osobowych, z czego po przeprowadzeniu analizy w 14 przypadkach stwierdzono brak przesłanek do przekazania informacji do Prezesa UODO, a w jednym przypadku, z zachowaniem odpowiedniego terminu, zawiadomiono Prezesa UODO. W pozostałych jednostkach liczba zidentyfikowanych naruszeń wahała się pomiędzy jednym (Urząd Miejski w Stargardzie, nie zgłaszano tego zdarzenia do UODO) a siedmioma przypadkami (Mazowiecki Urząd Wojewódzki, z których jeden przypadek zgłoszono do Prezesa UODO, a w pozostałych przypadkach, zdaniem jednostki, nie było takiej potrzeby). Natomiast w pięciu jednostkach, tj. Urzędach Miast Chrzanowa, Polic, Siedlec, Sieradza i Wieliczki nie odnotowano żadnych przypadków naruszenia ochrony danych osobowych.
Kontrola wykazała dwa przypadki nieprawidłowego postępowania w razie stwierdzenia naruszenia ochrony danych osobowych.

Przykłady

W **Urzędzie Miasta Ciechanów** cztery osoby zgłosiły fakt naruszenia ochrony ich danych osobowych. Wszystkie związane były z nieprawidłowościami dotyczącymi głosowania w ramach budżetu obywatelskiego na 2020 r. IOD został zawiadomiony o zaistniałej sytuacji, a administrator, stosownie do art. 34 i 12 RODO, poinformował wszystkich zgłaszających o podejrzeniu naruszenia ich danych i wskazał na konieczność zgłoszenia sprawy Policji. Równocześnie samodzielnie wystosował w tej sprawie pismo do KP Policji w Ciechanowie z prośbą o podjęcie czynności przewidzianych prawem. Nie przekazano jednakże do Prezesa UODO zgłoszenia naruszenia ochrony danych osobowych, co było niezgodne z art. 33 RODO.

[26] Zgodnie z art. 33 ust. 1 RODO w przypadku naruszenia ochrony danych osobowych administrator zgłasza je organowi nadzorczemu, tj. UODO. Administrator powinien wykonać to bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

W **Łódzkim Urzędzie Wojewódzkim** do Prezesa UODO wystosowano trzy zgłoszenia o naruszeniu ochrony danych osobowych. Dwa z nich przekazano w terminie określonym w art. 33 ust. 1 RODO, tj. do 72 godzin, natomiast jedno zgłoszenie przekazano z przekroczeniem wymaganego terminu, tj. osiem dni od stwierdzenia naruszenia. Wynikało to z błędu w systemie EZD, po jego naprawieniu zgłoszenie przesłano ze stosownym wyjaśnieniem przyczyn opóźnienia.

Infografika nr 10
Zidentyfikowane przez jednostki przypadki naruszenia ochrony danych osobowych

Źródło: opracowanie własne NIK.

Postępowanie w przypadku żądań usunięcia lub sprostowania danych osobowych

W większości urzędów kontrola nie stwierdziła nieprzestrzegania procedur dotyczących postępowania w sprawie żądania przez osoby od administratora usunięcia jej danych osobowych[27]. W kontrolowanych

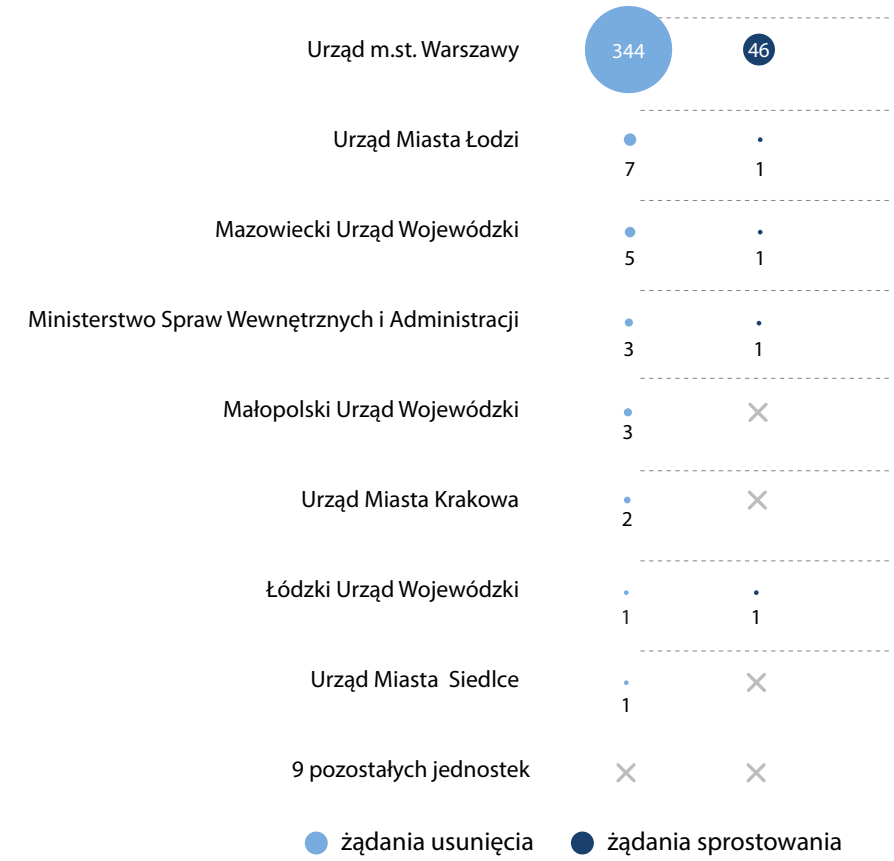
[27] Zgodnie z art. 17 ust. 1 RODO osoba, której dane dotyczą, ma prawo żądania od administratora usunięcia jej danych osobowych.

jednostkach składano takie żądania i poza jednym przypadkiem (Urząd Miasta Siedlce) postępowanie w przypadku żądania usunięcia danych było prawidłowe, tj. informowano osoby bez zbędnej zwłoki o podjętych działaniach w związku z żądaniem. Natomiast w Urzędzie Miasta Siedlce doszło do sytuacji, w której niezgodnie z art. 12 ust. 4 RODO, administrator przesyłając wnioskodawcy informację o niepodjęciu działań nie poinformował go o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem. Uzupełnienie przekazanej odpowiedzi zostało przekazane wnioskodawcy dopiero w trakcie kontroli NIK.

Liczba zgłaszania żądań usunięcia danych osobowych wynosiła od jednego (Łódzki Urząd Wojewódzki, Urząd Miasta Siedlce) do siedmiu (Urząd Miasta Łodzi). Żadnych żądań usunięcia danych nie zgłoszono w dziewięciu jednostkach. Jedynie w przypadku Urzędu Miasta Stołecznego Warszawy zgłoszono 344 żądania usunięcia danych osobowych.

W RODO przewidziano także możliwość żądania sprostowania bądź uzupełnienia niekompletnych danych. Żądania takie złożono tylko w pięciu kontrolowanych jednostkach. W czterech (MSWiA, Mazowiecki Urząd Wojewódzki, Łódzki Urząd Wojewódzki i Urząd Miasta Łodzi) złożono po jednym, a w Urzędzie Miasta Stołecznego Warszawy 46 wniosków o sprostowanie danych. We wszystkich jednostkach postępowania w związku z takim żądaniem były prawidłowe.

Infografika nr 11
Zgłaszane do jednostek żądania usunięcia lub sprostowania danych



Źródło: opracowanie własne NIK.

Przestrzeganie ochrony danych osobowych w miejscach ogólnodostępnych

Badaniem kontrolnym objęto w urzędach miejsca ogólnodostępne, jak również prowadzone przez nie strony internetowe, pod względem stosowania zasady „minimalizacji danych", tj. nieupubliczniania zbędnych i nieadekwatnych danych w stosunku do celu. W żadnej z kontrolowanych jednostek nie doszło do sytuacji, w której w ogólnodostępnych miejscach, jak również na stronach internetowych jednostek znajdowały się informacje, które mogłyby naruszać ochronę danych osobowych. Stwierdzono też, że zgodnie z art. 13 RODO informowano gości i petentów wchodzących do urzędów o przetwarzaniu ich danych osobowych, a w przypadku monitoringu wizyjnego, również o przetwarzaniu ich wizerunku. W miejscach ogólnodostępnych były zamieszczane informacje o przetwarzaniu danych osobowych wchodzących, a także o objęciu pomieszczeń monitoringiem (jeśli był w jednostce stosowany).

Prawidłowość działań związanych z usuwaniem zbędnej dokumentacji

W kontrolowanych jednostkach stosowano różne rozwiązania niszczenia zbędnej dokumentacji i zbędnych nośników danych. Właściwa ochrona danych osobowych wiąże się także z usuwaniem dokumentacji przeznaczonej do zniszczenia, w taki sposób, by nie doszło do sytuacji, że dane osobowe zostałyby ujawnione w wyniku niedbałego wyrzucenia dokumentów lub przekazane podmiotom, które mogłyby je niewłaściwie wykorzystać bez żadnych konsekwencji. Jeżeli dokumentacja zawierająca dane osobowe niszczona jest przez podmiot zewnętrzny, to również w takiej sytuacji powinno nastąpić powierzenie przetwarzania danych osobowych. W obszarze tym stwierdzono nieprawidłowości tylko w jednym urzędzie.

W **Urzędzie Miasta Szczecin** zawarto trzy umowy na usługę niszczenia dokumentacji. Do jednej z tych umów nie zawarto umowy powierzenia przetwarzania danych osobowych, co było niezgodne z art. 28 ust. 3 RODO. Dyrektor Biura Obsługi Urzędu wyjaśniła, że sytuacja ta była wynikiem niedopatrzenia.

W 10 jednostkach likwidacja takiej dokumentacji odbywała się we własnym zakresie. Natomiast w siedmiu jednostkach objętych badaniem niszczenie zbędnej dokumentacji powierzane było wyspecjalizowanym firmom, z którymi zawierano odpowiednie umowy i jednocześnie zawierano umowy powierzenia przetwarzania danych.

Niszczenie zbędnej dokumentacji było uregulowane w wewnętrznych przepisach jednostek. Procedury określały przede wszystkim, że niepotrzebne wydruki zawierające dane chronione należy niszczyć wyłącznie przy pomocy niszczarek, a uszkodzone lub wymontowane z likwidowanego sprzętu dyski twarde i inne równoważne nośniki danych mają być niszczone mechanicznie, w taki sposób, by nie nadawały się do odczytu. Oprócz niszczenia przez pracowników samodzielnie dokumentacji w niszczarkach, stosowano specjalnie do tego przystosowane, oznakowane, zamykane pojemniki „wrzutnie", w których pracownicy byli zobowiązani umieścić dokumenty przeznaczone do zniszczenia. Dokumenty z tych pojemników były następnie niszczone w centralnej niszczarce urzędu (np. Zachodniopomorski Urząd Wojewódzki).

W przypadku przekazywania dokumentacji do zniszczenia podmiotowi zewnętrznemu sporządzane były dokumenty potwierdzające ten proces, tj. dokument potwierdzający odbiór oraz certyfikat zniszczenia dokumentów, który zawierał m.in. datę zniszczenia, ilość zniszczonych metrów bieżących dokumentacji, numery pojemników, w których odebrano dokumentację.

W razie, gdy niszczenie dokumentów lub nośników danych odbywało się we własnym zakresie, sporządzane były protokoły z komisyjnego niszczenia dokumentacji lub elektronicznych nośników danych.

Wywiązywanie się z obowiązku informowania pracowników o przetwarzaniu ich danych osobowych

Wszystkie jednostki objęte kontrolą informowały pracowników o przetwarzaniu ich danych osobowych, zgodnie z art. 13 RODO[28]. Informacje te były podawane zarówno poprzez przekazywanie takich informacji drogą mailową, na obowiązkowych szkoleniach wewnętrznych, a także poprzez zamieszczenie informacji na stronach intranetowych urzędów oraz w siedzibach urzędów w odpowiednich miejscach ogólnodostępnych. Pracownicy w 13 jednostkach zostali zobowiązani do pisemnego potwierdzenia zapoznania się z przekazanymi informacjami. Jak ustalono podczas kontroli, w jednym przypadku nie zrealizowano polecenia przekazania pracownikom informacji o przetwarzaniu ich danych za potwierdzeniem odbioru oraz w trzech przypadkach NIK zwróciła uwagę, że niedołączanie do umów zleceń informacji o przetwarzaniu danych osobowych może rodzić w przyszłości problem dla administratora z rozliczeniem się z tego obowiązku.

Przykłady

W **Urzędzie Miasta Stołecznego Warszawy** burmistrzowie dzielnic zostali zobowiązani, by pracownikom, którzy nie mają konta służbowego e-mail, klauzule informacyjne o przetwarzaniu danych osobowych dla pracowników Urzędu zostały przekazane w formie papierowej za potwierdzeniem odbioru. W Urzędzie Dzielnicy Ochota nie zostało wykonane to zalecenie. Burmistrz dzielnicy wyjaśniła, że nie wykonała tego polecenia ze względu na to, że informacje te były wywieszone w sekretariacie Wydziału Administracyjno-Gospodarczego Urzędu oraz w pokojach pracowników.

W przypadku Urzędów Miast w: **Warszawie**, **Ciechanowie** i **Siedlcach** oraz Ministerstwa Spraw Wewnętrznych i Administracji do umów zleceń nie we wszystkich przypadkach były dołączane klauzule o przetwarzaniu danych osobowych. W jednostkach tych podkreślano, że obowiązek ten został wykonany poprzez zamieszczenie takiej informacji np. na stronie internetowej i w związku z tym osoby miały możliwość zapoznania się z takimi informacjami. Zdaniem NIK chociaż przepisy RODO nie narzucają konkretnej formy spełnienia obowiązku informacyjnego, przyjęcie domniemania, że osoby zapoznały się z informacją dostępną np. w jednostce lub na stronie internetowej jednostki, może rodzić w przyszłości problem w przypadku ewentualnego sporu dotyczącego przekazania informacji, gdzie ciężar wykazania, że obowiązek informacyjny został zrealizowany spoczywa na administratorze.

[28] Oprócz obowiązku informowania o przetwarzaniu danych osobowych osób, które korzystają z usług urzędu lub które z nim współpracują, istnieje także obowiązek powiadomienia przez administratora pracowników o przetwarzaniu ich danych osobowych. Dotyczy to zarówno pracowników zatrudnionych w jednostce na podstawie umowy o pracę, jak również na podstawie umów cywilnoprawnych.

Informowanie o przetwarzaniu danych osobowych podczas prowadzenia rekrutacji

Spośród 17 kontrolowanych jednostek tylko w jednej stwierdzono nieprawidłowość związaną z publikowaniem ogłoszeń o pracę[29]. W większości jednostek kandydaci do pracy byli informowani o przetwarzaniu ich danych osobowych. W informacjach tych zawierano konieczne elementy wskazujące na to m.in. kto jest administratorem danych, w jakim celu zbierane są dane osobowe, podstawę prawną przetwarzania danych, a także prawa przysługujące kandydatowi związane z przekazanymi danymi np. do dostępu, sprostowania, ograniczenia przetwarzania, wniesienia sprzeciwu wobec ich przetwarzania. Informowano także kandydatów o prawie wniesienia skargi do Prezesa UODO. Jednostki wybierały różny sposób informowania kandydatów o przetwarzaniu ich danych. Było to np. zamieszczanie na stronach internetowych urzędu w zakładce, gdzie znajdowały się ogłoszenia o pracę, informacji administratora o przetwarzaniu danych (np. Urząd Miasta Krakowa), zamieszczanie takich informacji bezpośrednio w ogłoszeniach o pracę (np. Mazowiecki Urząd Wojewódzki, Urząd Miasta Kutno), ale także, gdy rekrutacja wymagała złożenia formularza elektronicznego, kandydat musiał elektronicznie potwierdzić (poprzez kliknięcie w odpowiednie okienko) zapoznanie się z informacjami o przetwarzaniu danych osobowych (np. Urząd Miasta Stołecznego Warszawy).

Nieprawidłowość dotycząca informowania kandydatów o przetwarzaniu danych osobowych została stwierdzona w **Urzędzie Miasta Ciechanów**. Ustalono, że obowiązujący Regulamin naboru na wolne stanowiska urzędnicze, na podstawie którego prowadzono postępowania rekrutacyjne, nie zawierał informacji związanych z ochroną danych osobowych w związku z wejściem w życie przepisów RODO (nie został zaktualizowany od 2009 r.). W związku z tym ogłoszenia o naborze na wolne stanowiska nie zawierały wszystkich informacji określonych w art. 13 ust. 2 lit. b) i f) RODO.

Okres przechowywania dokumentacji aplikacyjnej kandydatów także podlegał uregulowaniu w kontrolowanych jednostkach. Termin ten wahał się od trzech miesięcy do pięciu lat.

Oferty kandydatów, którzy nie zostali wyłonieni w drodze naboru, przechowywane były przez okres trzech miesięcy od zakończenia procesu rekrutacji (np. Mazowiecki Urząd Wojewódzki, Urząd Miejski w Chrzanowie, MSWiA, Urząd Miasta Szczecin).

Dokumenty aplikacyjne kandydata, który został wyłoniony w procesie rekrutacji, były dołączane do jego akt osobowych. Okres przechowywania wynosił np. dwa lata (Urząd Miasta Ciechanów) lub pięć lat (MSWiA, Łódzki Urząd Wojewódzki, Urząd Miasta Sieradza, Urząd Miasta Krakowa). Po upływie tego okresu dokumenty miały być przekazywane do archiwum.

[29] Obwiązek informowania o przetwarzaniu danych osobowych, zgodnie z art. 13 RODO, spoczywa na administratorze również w odniesieniu do osób ubiegających się o zatrudnienie w danej instytucji. Osoby odpowiadające na ogłoszenie o pracę są zobowiązane do przekazania szeregu informacji oraz dokumentów je potwierdzających do potencjalnego pracodawcy. Dlatego osoby takie również powinny być świadome tego, że ich dane będą przetwarzane przez pracodawcę oraz wiedzieć, jakie prawa im przysługują w związku z tym.

6. ZAŁĄCZNIKI

6.1. Metodyka kontroli i informacje dodatkowe

Cel główny kontroli

Czy organy administracji publicznej wdrożyły w wymaganym zakresie i czasie przepisy dotyczące ochrony danych osobowych po wejściu w życie RODO?

Cele szczegółowe

1. Czy organy administracji publicznej prawidłowo przygotowały się do wdrożenia RODO?
2. Czy ochrona danych osobowych jest prowadzona zgodnie z wytycznymi określonymi w RODO oraz efektywnie?

Zakres podmiotowy

Skontrolowano ogółem 17 jednostek, w tym: Ministerstwo Spraw Wewnętrznych i Administracji, cztery urzędy wojewódzkie oraz 12 urzędów gmin.

Kryteria kontroli

Czynności kontrolne prowadzono na podstawie:

- art. 2 ust. 1 ustawy *o NIK*, z uwzględnieniem kryteriów: legalności, rzetelności, celowości i gospodarności w Ministerstwie Spraw Wewnętrznych i Administracji oraz czterech urzędach wojewódzkich;
- art. 2 ust. 2 ustawy *o NIK*, z uwzględnieniem kryteriów: legalności, rzetelności i gospodarności w 12 urzędach gmin.

Okres objęty kontrolą

Kontrolą objęto okres od 25 maja 2018 r. do zakończenia czynności kontrolnych w poszczególnych jednostkach (z uwzględnieniem okresu wcześniejszego, jeżeli zaistniałe zdarzenia miały wpływ na kontrolowaną działalność).
Kontrolę przeprowadzono w okresie od 2 września 2019 r. do 27 stycznia 2020 r.

Działania na podstawie art. 29 ustawy *o NIK*

W ramach przygotowania przedkontrolnego, w trybie art. 29 ust. 1 pkt 1 ustawy *o NIK*, zwrócono się do Urzędu Ochrony Danych Osobowych o udzielenie informacji dotyczących ustanowienia mechanizmów certyfikacji, dokonywania certyfikacji dla jednostek administracji publicznej lub ewentualnie prowadzenia takiego procesu certyfikacji, określonego w art. 42 RODO oraz, w celu właściwego zaplanowania jednostek do kontroli NIK, zwrócono się z pytaniem o jednostki objęte lub planowane do kontroli przez UODO.

Pozostałe informacje

Kontrola została podjęta z własnej inicjatywy Najwyższej Izby Kontroli.

Z uwagi na specyfikę przedmiotu kontroli, oceny ogólne kontrolowanej działalności w poszczególnych jednostkach zostały sformułowane w formie opisowej.

Wyniki kontroli przedstawiono w 17 wystąpieniach pokontrolnych, w których sformułowano ogółem 26 wniosków pokontrolnych. Według stanu na dzień 23 kwietnia 2020 r. zrealizowano 19 wniosków, w trakcie realizacji pozostawało sześć wniosków, natomiast nie zrealizowano jednego wniosku.

Zastrzeżenia pokontrolne zostały zgłoszone do wystąpienia pokontrolnego skierowanego do Prezydenta Miasta Stołecznego Warszawy. Z uwagi na złożenie zastrzeżeń przez osobę nieuprawnioną Dyrektor KAP, na podstawie art. 54 ust. 3 ustawy *o NIK* wydał postanowienie o odmowie ich przyjęcia.

ZAŁĄCZNIKI

Wnioski pokontrolne dotyczyły przede wszystkim:

1) Unieważniania bez zbędnej zwłoki, dostępu do systemów informatycznych pracownikom, z którymi rozwiązano stosunek pracy.
2) Upoważniania pracowników do przetwarzania danych osobowych z chwilą powstania stosownego obowiązku.
3) Zabezpieczania pomieszczenia serwerowni przed utratą danych poprzez zminimalizowanie ryzyka nieautoryzowanego dostępu oraz zagrożenia pożarowego.
4) Zgłaszania naruszeń danych osobowych do UODO, w terminie określonym w art. 33 ust. 1 RODO.
5) Zamieszczania klauzuli dotyczącej obowiązku przestrzegania Polityki Bezpieczeństwa w umowach cywilnoprawnych zawieranych z osobami, których upoważnia się do przetwarzania danych osobowych.
6) Zawierania umów powierzenia przetwarzania danych osobowych i zawieranie w tych umowach wszystkich niezbędnych elementów wymaganych RODO.
7) Zapewnienia w regulacjach wewnętrznych podległości służbowej Inspektora Ochrony Danych jedynie kierownikowi jednostki kontrolowanej.
8) Przechowywania nagrań z monitoringu Urzędu przez okres zgodny z procedurami wewnętrznymi oraz uregulowanie w sposób jednolity zagadnienia dotyczącego miejskiego monitoringu wizyjnego.
9) Dostosowania parametrów haseł dostępu do wymogów systemu bezpieczeństwa informacji.

Wykaz jednostek kontrolowanych

Lp.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
1.	Departament Administracji Publicznej	Ministerstwo Spraw Wewnętrznych i Administracji	Mariusz Kamiński
2.		Mazowiecki Urząd Wojewódzki	Konstanty Radziwiłł
3.		Urząd Miasta Ciechanów	Krzysztof Kosiński
4.		Urząd Miasta Stołecznego Warszawy	Rafał Trzaskowski
5.		Urząd Miasta Siedlce	Andrzej Sitnik
6.	Delegatura NIK w Krakowie	Małopolski Urząd Wojewódzki	Piotr Ćwik
7.		Urząd Miejski w Chrzanowie	Robert Maciaszek
8.		Urząd Miasta Krakowa	Jacek Majchrowski
9.		Urząd Miasta i Gminy Wieliczka	Artur Kozioł
10.	Delegatura NIK w Łodzi	Łódzki Urząd Wojewódzki	Tobiasz Bocheński
11.		Urząd Miasta Kutno	Zbigniew Burzyński
12.		Urząd Miasta Łodzi	Hanna Zdanowska
13.		Urząd Miasta Sieradza	Paweł Osiewała

Lp.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
14.	Delegatura NIK w Szczecinie	Zachodniopomorski Urząd Wojewódzki	Tomasz Hinc
15.		Urząd Miejski w Policach	Władysław Diakun
16.		Urząd Miejski w Stargardzie	Rafał Zając
17.		Urząd Miasta Szczecin	Piotr Krzystek

Wyniki kontroli w poszczególnych jednostkach przedstawione są w wystąpieniach pokontrolnych zamieszczanych na stronie internetowej NIK pod adresem: https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/prosta/

6.2. Analiza stanu prawnego i uwarunkowań organizacyjno-ekonomicznych

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), zgodnie z art. 2 ust. 1 ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

Zasady przetwarzania danych osobowych

W art. 5 RODO określono zasady dotyczące przetwarzania danych osobowych. I tak dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą – „zgodność z prawem, rzetelność i przejrzystość" (art. 5 ust. 1 lit. a);
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami – „ograniczenie celu" (art. 5 ust. 1 lit. b);
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane – „minimalizacja danych" (art. 5 ust. 1 lit. c);
d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane – „prawidłowość" (art. 5 ust. 1 lit. d);
e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą – „ograniczenie przechowywania" (art. 5 ust. 1 lit. e);
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych – „integralność i poufność" (art. 5 ust. 1 lit. f).

Zgodnie z art. 5 ust. 2 RODO Administrator jest odpowiedzialny za przestrzeganie przepisów art. 5 ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność").

W art. 6 ust. 1 RODO określono warunki jakie muszą być spełnione aby przetwarzanie było zgodne z prawem, w tym m.in.: osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów; przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy; przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze; przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Uprawnienia osób, których dane osobowe są przetwarzane

Zgodnie z art. 7 ust. 1 RODO jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

Osoba, której dane dotyczą, na podstawie art. 7 ust. 3 RODO, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

Zgodnie z art. 13 ust. 1 RODO jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej m.in. następujące informacje:

a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
d) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją.

Zgodnie z art. 13 ust. 2 RODO poza informacjami, o których mowa w art. 13 ust. 1 RODO, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, m.in. następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:

a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
c) informacje o prawie wniesienia skargi do organu nadzorczego;
d) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.

Osoba, której dane dotyczą, na podstawie art. 16 RODO, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Zgodnie z art. 17 ust. 1 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe. W artykule tym wymieniono enumeratywnie okoliczności, które nakładają na administratora obowiązek usunięcia danych osobowych.

W art. 17 ust. 3 RODO określono w jakiej sytuacji art. 17 ust. 1 i 2 nie mają zastosowania.

Obowiązki administratora

Na podstawie art. 19 RODO administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18 RODO, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Zgodnie z art. 24 ust. 1 RODO, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, 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.

Zgodnie z art. 24 ust. 2 RODO jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w art. 24 ust. 1 RODO, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Na podstawie art. 25 ust. 2 RODO administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Podmiot przetwarzający

Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, to zgodnie z art. 28 ust. 1 RODO korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.

Przetwarzanie przez podmiot przetwarzający, zgodnie z art. 28 ust. 3 RODO odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Zgodnie z art. 28 ust. 9 RODO umowa lub inny akt prawny, o których mowa w art. 28 ust. 3 i 4 RODO, mają formę pisemną, w tym formę elektroniczną.

Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych, zgodnie z art. 29 RODO, przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

Rejestr czynności przetwarzania danych osobowych

Zgodnie z art. 30 ust. 1 RODO każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Rejestr kategorii czynności przetwarzania

Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego, zgodnie z art. 30 ust. 2 RODO, prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;

c) gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 RODO akapit drugi, dokumentacja odpowiednich zabezpieczeń;
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Zgodnie z art. 30 ust. 3 RODO rejestry, o których mowa w art. 30 ust. 1 i 2 RODO, mają formę pisemną, w tym formę elektroniczną.

Bezpieczeństwo przetwarzania danych osobowych

Zgodnie z art. 32 ust. 1 RODO uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

Upoważnienie do przetwarzania danych osobowych

Zgodnie z art. 32 ust. 4 RODO administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

Naruszenie ochrony danych osobowych

Na podstawie art. 33 ust. 1 RODO w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Podmiot przetwarzający, stosownie do art. 33 ust. 2 RODO, po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.

W art. 33 ust. 3 RODO określono minimalny zakres informacji jakie muszą być zawarte w zgłoszeniu o naruszeniu danych osobowych.

Zgodnie z art. 33 ust. 5 RODO administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

Zgodnie z art. 34 ust. 1 RODO, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie to, zgodnie z art. 34 ust. 2 RODO, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO.

W art. 34 ust. 3 RODO wymieniono przypadki, w których powyższe zawiadomienie nie jest wymagane.

Na podstawie art. 34 ust. 4 RODO jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w art. 34 ust. 3 RODO.

Inspektor Ochrony Danych

Zgodnie z art. 37 ust. 1 RODO administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych m.in. wówczas gdy przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości.

Na podstawie art. 37 ust. 3 RODO jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych.

Zgodnie z 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 RODO.

Inspektor ochrony danych, zgodnie z art. 37 ust. 6 RODO może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.

Zgodnie z art. 37 ust. 7 RODO administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.

Stosownie do art. 38 ust. 3 RODO administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

Stosownie do art. 38 ust. 6 RODO inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

Zadania inspektora ochrony danych zostały określone w art. 39 ust. 1 RODO i są to:

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;
c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
d) współpraca z organem nadzorczym;
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Ustawa z dnia 10 maja 2018 r. *o ochronie danych osobowych*

Zgodnie z art. 3 ust. 1 ustawy *o ochronie danych osobowych* administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w art. 13 ust. 3 RODO, jeżeli zmiana celu przetwarzania służy realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa w art. 13 ust. 3 RODO, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 RODO, oraz przekazanie tych informacji:

a) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub
b) naruszy ochronę informacji niejawnych.

Zgodnie z art. 3 ust. 2 ww. ustawy w przypadku, o którym mowa w art. 3 ust. 1 tej ustawy, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą.

Zgodnie z art. 3 ust. 3 ustawy *o ochronie danych osobowych* administrator jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie nieprzekazania informacji, o których mowa w art. 13 ust. 3 RODO.

Na podstawie art. 5 ust. 4 ustawy *o ochronie danych osobowych* administrator jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie niewykonania obowiązków, o których mowa w art. 15 ust. 1–3 RODO.

Zgodnie z art. 8 ustawy *o ochronie danych osobowych* administrator i podmiot przetwarzający są obowiązani do wyznaczenia inspektora ochrony danych, w przypadkach i na zasadach określonych w art. 37 RODO.

Zgodnie z art. 9 ww. ustawy przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych, o którym mowa w art. 37 ust 1 lit. a RODO, rozumie się m.in. jednostki sektora finansów publicznych.

Stosownie do art. 10 ustawy *o ochronie danych osobowych*:

- podmiot, który wyznaczył inspektora ochrony danych, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora (art. 10 ust. 1);
- podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o każdej zmianie danych, o których mowa w ust. 1 i 3, oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania (art. 10 ust. 4);
- zawiadomienia, o których mowa w ust. 1 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP (art. 10 ust. 6).

Zgodnie z art. 11 ustawy *o ochronie danych osobowych* podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1 tej ustawy, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Stosownie do art. 11a ust. 1 ustawy *o ochronie danych osobowych*[30] podmiot, który wyznaczył inspektora, może wyznaczyć osobę zastępującą inspektora w czasie jego nieobecności, z uwzględnieniem kryteriów, o których mowa w art. 37 ust. 5 i 6 RODO. W związku z wykonywaniem obowiązków inspektora w czasie jego nieobecności do osoby go zastępującej stosuje się odpowiednio przepisy dotyczące inspektora (art. 11a ust. 2).

Zgodnie z art. 11a ust. 3 ww. ustawy podmiot, który wyznaczył osobę zastępującą inspektora, zawiadamia Prezesa Urzędu o jej wyznaczeniu w trybie określonym w ww. art. 10 oraz udostępnia jej dane zgodnie z ww. art. 11.

Zgodnie z art. 34 ust. 1 i 2 ustawy *o ochronie danych osobowych* Prezes Urzędu Ochrony Danych Osobowych jest organem właściwym w sprawie ochrony danych osobowych oraz organem nadzorczym w rozumieniu RODO.

Na podstawie art. 78 ust. 1 ustawy *o ochronie danych osobowych*, Prezes Urzędu Ochrony Danych Osobowych przeprowadza kontrolę przestrzegania przepisów o ochronie danych osobowych.

Zgodnie z art. 102 ust 1 pkt 1 ustawy *o ochronie danych osobowych* na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[31] Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 złotych. Środki z administracyjnej kary pieniężnej stanowią dochód budżetu państwa (art. 104 ustawy o ochronie danych osobowych).

[30] Artykuł ten obowiązuje od 4 maja 2019 r. Dodany został ustawą zapewniającą stosowanie RODO.

[31] Dz. U. z 2019 r. poz. 869, ze zm.

Na podstawie art. 111 ustawy *o ochronie danych osobowych* w Kodeksie pracy dodano art. 22^2 odnoszący się do zasad monitoringu w zakładzie pracy, w tym m.in. określono, że:

- nagranie obrazu pracodawca przetwarza wyłącznie do celów, dla których zostały zebrane, i przechowuje przez okres nieprzekraczający trzech miesięcy od dnia nagrania (art. 22^2 §3);
- pracodawca informuje pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy, nie później niż 2 tygodnie przed jego uruchomieniem (art. 22^2 §7);
- w przypadku wprowadzenia monitoringu pracodawca oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem (art. 22^2 §9).

Ustawa 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)[32] wprowadziła zmiany w 162 ustawach, w tym m.in.:

Zmiany w Kodeksie pracy

Na podstawie art. 4 ustawy zapewniającej stosowanie RODO**,** wprowadzono zmiany w ustawie – *Kodeks pracy*. Obecnie, zgodnie z Kodeksem pracy:

- monitoring wizyjny w miejscu pracy nie może obejmować pomieszczeń udostępnianych zakładowej organizacji związkowej (art. 22^2 § 1^1);
- monitoring nie obejmuje pomieszczeń sanitarnych, szatni, stołówek oraz palarni, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu określonego w art. 22^2 § 1 Kodeksu pracy i nie naruszy to godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Monitoring pomieszczeń sanitarnych wymaga uzyskania uprzedniej zgody zakładowej organizacji związkowej, a jeżeli u pracodawcy nie działa zakładowa organizacja związkowa, uprzedniej zgody przedstawicieli pracowników wybranych w trybie przyjętym u danego pracodawcy (art. 22^2 § 2).

[32] Dz. U. poz. 730.

6.3. Wykaz aktów prawnych dotyczących kontrolowanej działalności

1. 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 119 z 04.05.2016, str. 1, ze zm.)
2. Ustawa z dnia 10 maja 2018 r. *o ochronie danych osobowych* (Dz. U. z 2019 r. poz. 1781)
3. Ustawa 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).

6.4. Wykaz podmiotów, którym przekazano informację o wynikach kontroli

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów
5. Prezes Trybunału Konstytucyjnego
6. Rzecznik Praw Obywatelskich
7. Minister Cyfryzacji
8. Minister Spraw Wewnętrznych i Administracji
9. Prezes Urzędu Ochrony Danych Osobowych
10. Sejmowa Komisja do Spraw Kontroli Państwowej
11. Sejmowa Komisja Administracji i Spraw Wewnętrznych
12. Sejmowa Komisja Samorządu Terytorialnego i Polityki Regionalnej
13. Sejmowa Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii
14. Senacka Komisja Samorządu Terytorialnego i Administracji Państwowej
15. Senacka Komisja Infrastruktury
16. Prezydenci miast/burmistrzowie/wójtowie