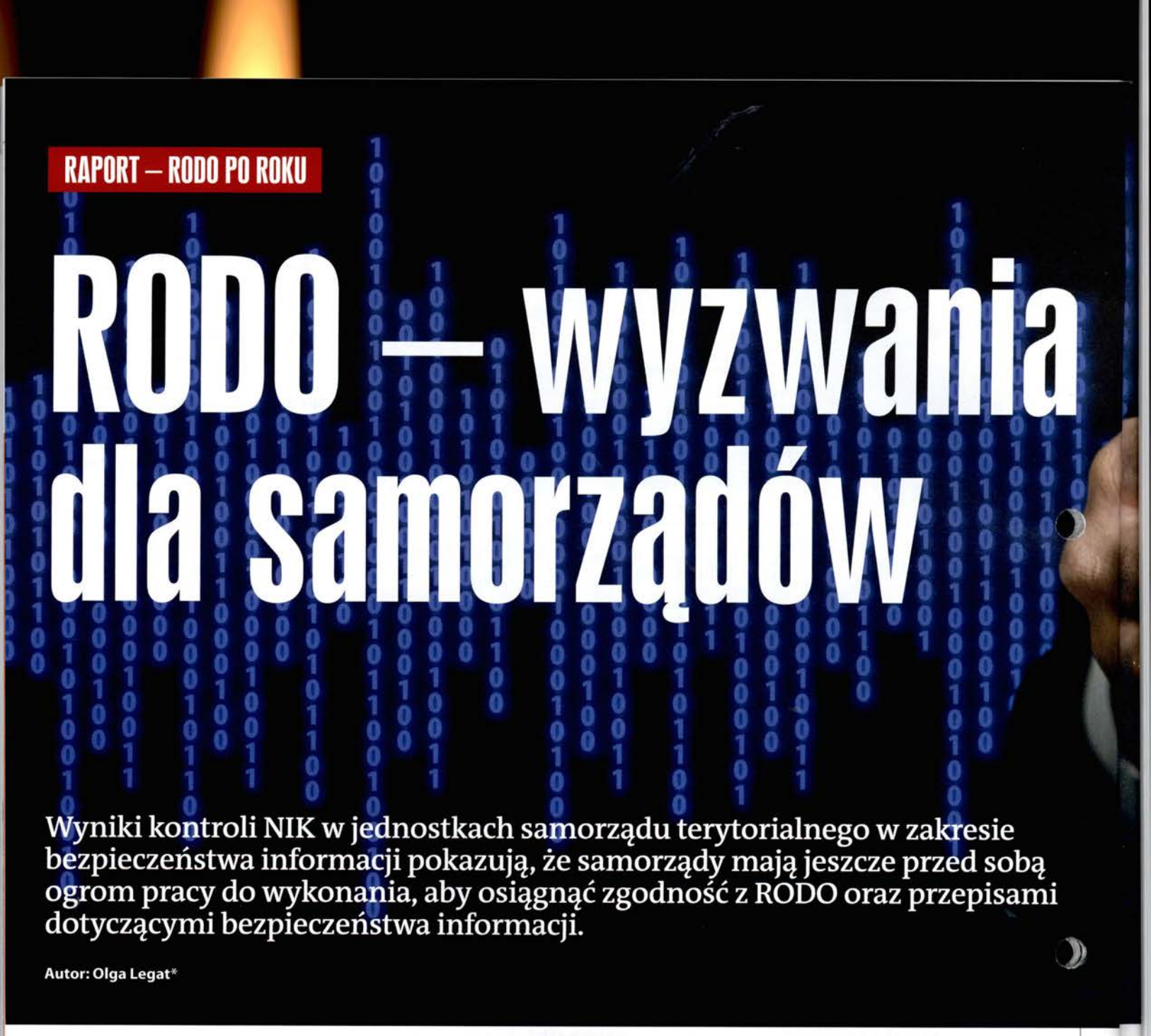
RAPORT – RODO PO ROKU

RODO – wyzwania dla samorządów



Wyniki kontroli NIK w jednostkach samorządu terytorialnego w zakresie bezpieczeństwa informacji pokazują, że samorządy mają jeszcze przed sobą ogrom pracy do wykonania, aby osiągnąć zgodność z RODO oraz przepisami dotyczącymi bezpieczeństwa informacji.

Autor: Olga Legat*

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, Dz.Urz.UE, seria L, 119, s. 1) (w skrócie „RODO") zostało przez ustawodawcę unijnego przyjęte w 2016 r. Przewidziano dwuletni okres dostosowawczy dla administratorów – zarówno z sektora prywatnego, jak i publicznego – RODO weszło bowiem w życie 25 maja 2018 r. Polski ustawodawca podjął także wysiłek dostosowania polskiego prawa do wymogów RODO, wprowadzając ustawę z 10 maja 2018 r. o ochronie danych osobowych (DzU z 2018 r., poz. 1000), a także ustawę z 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO (DzU z 2019 r., poz. 730). Pomimo dwuletniego okresu dostosowawczego przewidzianego przez ustawodawcę unijnego wielu administratorów podjęło wysiłki w zakresie wdrożenia RODO dopiero w 2018 r. lub też nadal prowadzi działania wdrażające. Ogólny obraz dostosowania jednostek samorządu terytorialnego do RODO daje „Informacja o wynikach kontroli. Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego" opublikowana przez Najwyższą Izbę Kontroli (znak KAP.430.020.2018, Nr ewid. 187/2018/P/18/006/KAP). Kontrola przeprowadzona przez NIK w 2018 r. objęła dziewięć starostw powiatowych, 14 urzędów miast oraz gmin, łącznie 23 jednostki samorządu terytorialnego zlokalizowane w pięciu województwach. NIK pochyliła się nad stosowaniem w tych jednostkach zarówno zasad RODO, jak i krajowych zasad interoperacyjności. Niestety, kontrola NIK wykazała sporo nieprawidłowości, z których wiele wydaje się mieć swoją przyczynę czy to w braku traktowania ochrony danych osobowych jako kwestii priory-

tetowej dla jednostek samorządu terytorialnego, czy to w wadliwej interpretacji przepisów RODO, czy wreszcie w braku środków w budżetach jednostek samorządu terytorialnego, które pozwoliłyby na prawidłowe wdrożenie rozwiązań zgodnych z RODO.

Tymczasem ochrona danych osobowych powinna być traktowana jako jedno z najważniejszych zadań jednostek samorządu terytorialnego. Samorządy przetwarzają bardzo szeroki zakres danych dotyczących obywateli i korzystają z centralnych baz danych osobowych, które potencjalnie dają możliwość dostępu do informacji o każdym obywatelu Polski (np. baza PESEL czy baza dowodów osobistych).

Nie bez znaczenia pozostaje także, że w kontekście RODO niebagatelne ryzyko niesie ze sobą niezadowolenie – czy to klienta urzędu, czy pracownika – który może swoje rozczarowanie wyrazić w skardze do Prezesa Urzędu Ochrony Danych Osobowych. Czy skarga taka będzie zasadna i czy może w dalszej perspektywie doprowadzić do nałożenia na urząd administracyjnej kary pieniężnej będzie zaś zależało od tego, czy określony urząd wdrożył RODO i czy zrobił to prawidłowo.

Analiza wcześniej powołanej informacji o wynikach kontroli NIK w jednostkach samorządu terytorialnego pozwala na wskazanie następujących głównych problemów, z jakimi borykają się samorządy terytorialne w świetle RODO:

- Prawidłowa polityka nadawania i odbierania uprawnień do systemów informatycznych, także tych, w których przetwarzane są dane osobowe – aż 80 proc. skontrolowanych jednostek postępowało nieprawidłowo w tym zakresie;
- Prawidłowa inwentaryzacja zasobów służących do przetwarzania informacji, w tym danych osobowych – w tym zakresie aż 74 proc. skontrolowanych przez NIK jednostek nie miało kompletnego rejestru takich zasobów;
- Zawieranie umów powierzenia w sytuacji przekazywania danych

osobowych podmiotowi zewnętrznemu – 52 proc. skontrolowanych jednostek nie uwzględniło w umowach o zakup czy serwis sprzętu komputerowego postanowień dotyczących powierzenia danych osobowych do przetwarzania;
- Prowadzenie oceny skutków dla ochrony danych (tzw. DPIA) w odpowiednich przypadkach – z którym to problemem borykało się aż 30 proc. kontrolowanych jednostek;
- Tworzenie kopii zapasowych, które zapobiegają naruszeniu ochrony danych polegającemu na utracie danych czy ich nieprawidłowej modyfikacji – 48 proc. skontrolowanych urzędów nie mogło wykazać prawidłowego sporządzania kopii zapasowych;
- Wprowadzenie prawidłowych dokumentów wewnętrznych regulujących ochronę danych osobowych – w tym zakresie 26 proc. skontrolowanych jednostek nie uzyskało zgodności z RODO;
- Zapewnienie niezależności powołanych inspektorów ochrony danych – aż w 22 proc. skontrolowanych jednostek IOD miał także obowiązki, które mogą powodować konflikt interesów;
- Prowadzenie rejestru czynności przetwarzania danych osobowych – 22 proc. kontrolowanych jednostek w ogóle nie prowadziło tego rejestru.

Warto także zwrócić szczególną uwagę na ocenę NIK, że „nie jest możliwe zapewnienie wysokiego poziomu ochrony danych osobowych bez zachowania właściwego bezpieczeństwa informacji" (Informacja o wynikach kontroli..., s. 7).

Dodatkowo, w ocenie autorki także poniższe kwestie będą w przyszłości nastręczały jednostkom samorządu terytorialnego wielu problemów:
- Prawidłowa interpretacja przesłanek legalności przetwarzania danych, w szczególności przesłanki obowiązku prawnego przetwarzania danych osobowych (art. 6 ust. 1 lit. a RODO) oraz przesłanki niezbędności przetwarzania danych do wykonania zadania w interesie publicznym lub w ramach władzy publicznej powierzonej administratorowi;
- Prawidłowe wyważenie kwestii dostępu do informacji publicznej oraz prawa do ochrony danych osobowych – jako że te dwie wartości pozostają często w konflikcie.

Poważnym problemem dla samorządów może być także brak odpowiedniej konstrukcji czy zabezpieczeń systemów zapewnianych na poziomie centralnym, takich jak system ePUAP czy system dostępu do danych PESEL. Nie jest tajemnicą, że wiele systemów tak zwanego „e-Państwa" uległo w ostatnim czasie awarii lub spowodowało wyciek danych osobowych. Jako przykłady można podać chociażby luki w systemie ZUS (por. https://e-ochronadanych.pl/luka-systemu-epuap-pozwalala-poznac-posiadane-zus-dane-osobowe/), awarię serwisów gov.pl w czerwcu 2018 r. (por. https://www.spidersweb.pl/2018/06/awaria-systemow-informatycznych-ministerstwo.html) czy przypadki wyświetlania cudzych danych w systemie ePUAP w połowie 2018 r. (por. https://niebezpiecznik.pl/post/od-miesiaca-wyciekaja-dane-z-profilu-zaufanego-byc-moze-ktos-zalogowal-sie-takze-i-na-twoje-konto/) albo nieprawidłowości platformy e-PIT wykryte w tym roku (por. https://uodo.gov.pl/pl/138/736).

Jednostki samorządu terytorialnego mogą być ukarane przez Prezesa Urzędu Ochrony Danych Osobowych karą w maksymalnej wysokości 100 000 zł (art. 102 ustawy o ochronie danych osobowych). Polski ustawodawca skorzystał z możliwości ograniczenia maksymalnej kary administracyjnej możliwej do nałożenia na sektor finansów publicznych, mając na uwadze fakt, że środki z administracyjnych kar pieniężnych stanowią dochód budżetu państwa (por. O. Legat, [w:] B. Marcinkowski (red.), Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018, art. 102, s. 249). Ograniczenie odpowiedzialności administracyjnej nie oznacza jednak, że jednostki sektora finansów publicznych mogą sobie pozwolić na mniejszą dbałość o ochronę danych osobowych niż podmioty, które zagrożone są karą w podstawowej wysokości przewidzianej w art. 83 RODO. Nie należy bowiem zapominać, że prawo do prywatności i ochrony danych osobowych to prawa człowieka. Zgodnie z art. 8 Karty Praw Podstawowych Unii Europejskiej ochrona danych osobowych jest jedną z wolności człowieka o podstawowym znaczeniu. Zasady autonomii informacyjnej oraz ochrony życia prywatnego, z którymi ściśle jest powiązana ochrona danych osobowych, znalazły odzwierciedlenie także w art. 47 i 51 Konstytucji Rzeczypospolitej Polskiej. Zgodnie art. 51 ust. 2 konstytucji: „Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym". Także konstytucja nakłada więc na administratorów będących jednostkami publicznymi konieczność przestrzegania zasady minimalizacji danych i ograniczenia celu przetwarzania.

Prawidłowe nadawanie dostępów

Jedna z pierwszych kar administracyjnych opartych na RODO została nałożona na szpital w Portugalii właśnie za nieprawidłową politykę w zakresie nadawania dostępów do systemów, w których przetwarzane są dane osobowe. Szpital, ukarany karą 400 000 euro, zaniedbał zarówno kwestię usuwania kont byłych pracowników, jak i nadawał pełne dostępy do wrażliwych danych osobowych pracownikom, który nie mieli potrzeby posiadać takiego dostępu, ponieważ nie byli lekarzami. Szpital utrzymywał 985 aktywnych kont, podczas gdy zatrudnionych w nim było jedynie 296 lekarzy (por. https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/). Podobne sytuacje miały miejsce w jednostkach samorządu terytorialnego w trakcie prowadzonej przez NIK kontroli – zgodnie z wynikami kontroli nieprawidłowości w nadawaniu dostępów występowały w 15 z 23 kontrolowanych urzędów, a w jednym przypadku konto pracownika zostało usunięte aż po 11 latach od zakończenia zatrudnienia („Informacja o wynikach kontroli...", s. 19). Dbałość o usuwanie niepotrzebnych kont oraz o maksymalne ograniczanie dostępów spełnia nie tylko wymóg minimalizacji danych, ale także wpływa znacząco na bezpieczeństwo przetwarzanych danych osobowych. Każde konto, które powinno być już nieaktywne powoduje większą podatność systemu informatycznego na naruszenia ochrony danych osobowych.

Kluczową kwestią jest także dbałość o nadawanie upoważnień do przetwa-

rzania danych osobowych, w szczególności w zakresie danych wrażliwych, czemu Prezes Urzędu Ochrony Danych Osobowych dał wyraz w uzasadnieniu decyzji z 19 stycznia 2019 r. (znak: ZSZZS.440.104.2018). Nadawane upoważnienia i dostępy do systemów powinny ściśle odpowiadać zakresowi obowiązków określonego pracownika, co wynika z zasady minimalizacji danych (art. 5 ust. 1 lit. c RODO).

W powyższym kontekście bardzo dużym problemem wydaje się częsta rotacja pracowników na stanowisku informatyka w jednostkach samorządu terytorialnego, na co zwracały uwagę kontrolowane przez NIK jednostki („Informacja o wynikach kontroli...", s. 17).

Prawidłowa inwentaryzacja zasobów

W świetle wydanych do tej pory decyzji Prezesa Urzędu Ochrony Danych Osobowych można wskazać, że wiele problemów nastręcza dokładna identyfikacja odbiorców danych osobowych, o których informacja musi być uwzględniona zarówno w obowiązku informacyjnym, jak i w rejestrze czynności przetwarzania. Kwestia niedostatecznie dokładnego określenia zakresu odbiorców danych pojawiła się w trzech postępowaniach Prezesa Urzędu Ochrony Danych Osobowych wydanych względem jednostek samorządu terytorialnego (decyzja z 25 stycznia 2019 r., znak: ZSPU.421.1.2018, decyzja z 3 kwietnia 2019 r., znak: ZSPU.421.8.2018 oraz decyzja z 6 kwietnia 2019 r., znak: ZSPU.421.2.2018). Na gruncie tych decyzji warto zwrócić uwagę, że strony postępowania administracyjnego także są uznawane za odbiorców danych osobowych w rozumieniu RODO – trzeba ten fakt uwzględnić zarówno w obowiązku informacyjnym, jak i w rejestrze.

Należy również pamiętać, że fakt przetwarzania danych osobowych w oparciu o obowiązek wynikający z przepisów prawa nie zwalnia administratora z uwzględnienia takiego przetwarzania w rejestrze czynności przetwarzania danych.

Przy wypełnianiu rejestru czynności przetwarzania danych administrator musi mieć także dokładną wiedzę o wszelkich narzędziach wykorzystywanych do poszczególnych procesów przetwarzania. Zgodnie bowiem z art. 30 ust. 1 lit. g) RODO, rejestr czynności przetwarzania powinien zawierać informacje o stosowanych zabezpieczeniach. Nie jest zaś możliwe prawidłowe opisanie stosowanych zabezpieczeń, jeżeli brak informacji o tym, jakie systemy i jakie zasoby są wykorzystywane do określonych czynności przetwarzania. Co więcej, niewiedza czy bałagan w tym zakresie znacznie zwiększa ryzyko naruszenia ochrony danych osobowych.

Umowy powierzenia

Zgodnie z art. 28 RODO administrator, który korzysta z podmiotu zewnętrznego przy przetwarzaniu danych osobowych, ma obowiązek zawrzeć z takim podmiotem umowę odpowiednio zabezpieczającą przetwarzanie danych osobowych. Treść takiej umowy jest szczegółowo określona w art. 28 ust. 3 RODO. Jednak określenie, w jakich przypadkach mamy do czynienia z powierzeniem przetwarzania danych, a więc także koniecznością zawarcia umowy powierzenia przetwarzania danych, kiedy zaś ma miejsce udostępnienie danych i umowa nie powinna być zawarta, jest często zadaniem bardzo trudnym. Jako przykład można podać w tym miejscu istniejący wśród administratorów w 2018 r. spór w zakresie konieczności zawarcia umowy powierzenia z podmiotami świadczącymi usługi prywatnej opieki zdrowotnej czy wydającym orzeczenia o zdolności do pracy. Spór ten został rozstrzygnięty po wydaniu przez Prezesa Urzędu Ochrony Danych Osobowych poradnika „Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców" (dostępny pod adresem: https://uodo.gov.pl/pl/138/545). W poradniku (s. 29) prezes wskazał, że w przypadku podmiotów medycznych mamy do czynienia z niezależnym od pracodawcy administratorem i zawarcie umowy powierzenia nie będzie prawidłowe.

Dodatkowo, dane osobowe są przekazywane przez administratorów w kontekście usług czy dostaw, które mogą nie nasuwać wniosku o udostępnianiu danych osobowych. Może mieć to miejsce w przypadku dostaw i utrzymania sprzętu IT. Mimo że może wydawać się to nieoczywiste, w bardzo wielu przypadkach usług polegających na serwisie czy wsparciu w zakresie IT dochodzi do przekazywania danych – informatycy firmy zewnętrznej mają bowiem często pełen dostęp do systemów administratora przy okazji świadczenia swoich usług. Najczęściej więc obowiązkowe będzie zawarcie umowy powierzenia, o czym pisało także Ministerstwo Cyfryzacji w poradniku „RODO dla administracji" (dostępny pod adresem: https://www.gov.pl/web/cyfryzacja/rodo-dla-administracji-odpowiedzi-na-27-pytan).

Zgodnie z wynikami kontroli NIK w 52 proc. kontrolowanych urzędów pominięto kwestię ochrony danych osobowych w umowach o zakup lub serwis sprzętu komputerowego czy oprogramowania („Informacja o wynikach kontroli...", s. 22). Brak odpowiednich zapisów wynikających z art. 28 RODO w umowie na asystę i konser-

Dbałość o usuwanie niepotrzebnych kont oraz o maksymalne ograniczanie dostępów spełnia nie tylko wymóg minimalizacji danych, ale także wpływa znacząco na bezpieczeństwo przetwarzanych danych osobowych. Każde konto, które powinno być już nieaktywne powoduje większą podatność systemu informatycznego na naruszenia ochrony danych osobowych.

wację systemu IT stwierdził także Prezes Urzędu Ochrony Danych Osobowych w postępowaniu zakończonym decyzją z 6 kwietnia 2019 r. (znak: ZSPU.421.2.2018).

Każda sytuacja, w której jednostka samorządu terytorialnego przekazuje na zewnątrz dane osobowe, wymaga odrębnej analizy w kontekście ewentualnego zawarcia umowy powierzenia przetwarzania. Najbardziej pomocne przy takiej analizie jest, po pierwsze, zadanie pytania: czy samorząd mógłby wykonać zadanie samodzielnie? Czy druga strona posiada własną podstawę przetwarzania, czy może usunąć dane po wykonaniu usługi? Przede wszystkim jednak ważna jest konsultacja z drugą stroną, która może mieć już ustalone stanowisko w sprawie powierzenia.

Ocena skutków przetwarzania dla ochrony danych

Zgodnie z art. 35 RODO, jeżeli określony rodzaj przetwarzania może z dużym prawdopodobieństwem powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, administrator powinien przeprowadzić tak zwaną ocenę skutków przetwarzania dla ochrony danych. Przy ocenie, czy dany rodzaj przetwarzania faktycznie powoduje wysokie ryzyko naruszeń, bierze się pod uwagę charakter, zakres, kontekst i cele przetwarzania. Jeżeli ocena wykaże, że ryzyko dla osób fizycznych faktycznie jest wysokie, należy dokonać konsultacji z Prezesem Urzędu Ochrony Danych Osobowych, zgodnie z art. 36 RODO. Konieczność oceny stosowanych zabezpieczeń w kontekście ryzyka dla osób fizycznych wynika także z art. 32 RODO.

Zgodnie z ustaleniami NIK w 30 proc. kontrolowanych urzędów zaniechano analizy ryzyka w zakresie stosowanych środków bezpieczeństwa („Informacja o wynikach kontroli...", s. 27).

W praktyce wydaje się, że szczególnej uwagi wymagają wszelkie procesy przetwarzania czy systemy, w których przetwarzane jest bądź bardzo dużo jednego rodzaju danych, bądź całe zestawy danych prowadzące do bardzo dokładnej identyfikacji dane osoby fizycznej (warto wskazać, że w sposób szczególny traktowany jest przez Urząd Ochrony Danych Osobowych numer PESEL), bądź gdy przetwarzanie dotyczy danych wrażliwych.

Przeprowadzenie oceny skutków przetwarzania dla ochrony danych nie jest zadaniem czasochłonnym, o ile administrator ma przed przystąpieniem do oceny świadomość stosowanych zabezpieczeń, w tym zabezpieczeń informatycznych. Większym wyzwaniem jest selekcja systemów i sposobów przetwarzania, które powinny podlegać takiej ocenie. W tym zakresie mogą pomóc komunikaty Prezesa Urzędu Ochrony Danych Osobowych w Monitorze Polskim, które zawierają wykaz operacji, które powinny podlegać ocenie skutków dla ochrony danych. Wykaz opublikowany w 2018 r. można także znaleźć na stronie Urzędu.

Regulacje wewnętrzne w zakresie ochrony danych osobowych

Wśród pytań zadanych przez sektor publiczny Ministerstwu Cyfryzacji znalazło się pytanie o zakres minimalnej dokumentacji wdrażającej RODO. Ministerstwo wskazało, że taka dokumentacja powinna składać się co najmniej z systemu bezpieczeństwa danych, który powinien być zarządzany i udoskonalany. Taki system wymaga wdrożenia skutecznych i realnych procedur, polityk bezpieczeństwa i instrukcji zarządzania systemami informatycznymi („RODO dla administracji", s. 31). Niemniej jednak, zgodnie z ustaleniami NIK, aż 61 proc. badanych przez NIK jednostek samorządu terytorialnego nie wdrożyło systemu zarządzania bezpieczeństwem informacji, zaś w 26 proc. urzędów nie dokonano aktualizacji uregulowań dotyczących przetwarzania danych osobowych w związku z RODO („Informacja o wynikach kontroli...", s. 12 i 8).

Wielu administratorów z sektora prywatnego wprowadza następujące procedury, które mają zapewnić stosowanie RODO: polityka ochrony danych osobowych, procedura postępowania z żądaniami podmiotów danych, procedura współpracy z organem nadzorczym (obejmująca kwestię zgłoszenia naruszenia ochrony danych osobowych oraz postępowanie w przypadku kontroli urzędowej), a także instrukcję w zakresie stosowania zasad privacy by default i privacy by design.

Samo jednak wprowadzenie polityk i procedur nie załatwia sprawy zgodności z RODO. Należy także zapewnić, aby dokumenty te były znane, rozumiane i stosowane przez pracowników urzędów. W tym zakresie bardzo pouczająca jest kara administracyjna nałożona przez brytyjski organ ochrony danych osobowych (Information Commissioner) na lotnisko Heathrow (decyzja dostępna pod adresem: https://ico.org.uk/action-weve-taken/enforcement/heathrow-airport/). Lotnisko, mimo że ma do czynienia z danymi osobowymi w bardzo szerokim zakresie i wprowadziło procedury dotyczące bezpieczeństwa informacji, zdecydowało się przeszkolić jedynie „kluczowych" pracowników, którzy mieli do czynienia z największą ilością danych. Jak się okazało, naruszenia dopuścił się pracownik, który nie został przeszkolony, bowiem nie został uznany z jedną z „kluczowych" osób. Kara wyniosła 120 000 GBP.

Każda sytuacja, w której jednostka samorządu terytorialnego przekazuje na zewnątrz dane osobowe, wymaga odrębnej analizy w kontekście ewentualnego zawarcia umowy powierzenia przetwarzania.

Niezależność Inspektora Ochrony Danych

Wedle ustaleń NIK, mimo że w badanych urzędach osoby wyznaczone na stanowisko IOD legitymowały się dostateczną wiedzą i doświadczeniem, w 22 proc. z nich inne zadania wykonywane przez te osoby mogły powodować konflikt interesów, a więc nie zapewniono gwarancji niezależności IOD, wymaganej przez RODO. RODO w art. 38 ust. 6 dopuszcza wykonywanie przez osobę pełniącą funkcję IOD

także innych obowiązków, jednak nie mogą one powodować konfliktu interesów. IOD podlega bezpośrednio najwyższemu kierownictwu administratora (np. burmistrzowi) i nie może samodzielnie decydować o sposobach ani celach przetwarzania danych osobowych. IOD jest wewnętrznym, niezależnym doradcą i wsparciem administratora w temacie danych osobowych. Nie może on obawiać się, że jego opinie będą skutkowały negatywnymi konsekwencjami.

Zapewnienie niezależności IOD może być dużym wyzwaniem w sytuacji braków kadrowych i ograniczonego budżetu, niepozwalającego na zatrudnienie podmiotu zewnętrznego na tę funkcję lub powierzenie jednemu z pracowników wyłącznie funkcji IOD. Niemniej jednak należy podjąć wysiłek zapewnienia niezależności takiej osoby, bowiem brak niezależności będzie skutkował niezgodnością z RODO i ryzykiem nałożenia administracyjnej kary pieniężnej.

Przesłanki przetwarzania danych osobowych

W większości przypadków jednostki samorządu terytorialnego będą przetwarzały dane osobowe w oparciu o dwie przesłanki przetwarzania danych:

- art. 6 ust. 1 lit. c) RODO – realizacja obowiązku prawnego ciążącego na administratorze lub
- art. 6 ust. 1 lit. e) RODO – niezbędność przetwarzania dla wypełnienia zadania w interesie publicznym.

Oczywiście pozostałe przesłanki przetwarzania wymienione w art. 6 ust. 1 RODO, poza przesłanką uzasadnionego interesu administratora, także będą miały zastosowanie – chociażby w stosunkach pracowniczych – jednak w tym zakresie jednostki samorządu terytorialnego nie będą działały w sposób zasadniczo różny od innych administratorów danych, także z sektora prywatnego.

W kontekście przesłanki wymienionej w art. 6 ust. 1 lit. c) RODO warto wskazać, że ustalenie dokładnego zakresu przetwarzania danych osobowych – koniecznych kategorii przetwarzanych danych, sposobu ich przetwarzania czy terminu retencji – w oparciu o przepisy polskiego prawa i art. 6 ust. 1 lit. c RODO może być zadaniem bardzo trudnym. Motyw 45 RODO stanowi, że nie jest konieczne istnienie szczegółowego uregulowania prawnego dla każdego rodzaju przetwarzania. Wystarczy, aby dana regulacja stanowiła podstawę różnych operacji przetwarzania danych wynikających z obowiązku prawnego, któremu podlega administrator. Oznacza to, że oparcie przetwarzania danych na przesłance wymienionej w art. 6 ust. 1 lit. c RODO jest możliwe wtedy, gdy przepisy prawa krajowego nie wskazują wprost, że przetwarzanie jest konieczne i nie wymieniają zakresu danych czy terminu retencji, ale jednak z samego charakteru obowiązku prawnego wynika konieczność przetwarzania danych. Warto pamiętać, że obowiązki prawne, które wypełnia administrator danych osobowych mogą wynikać nie tylko z aktów prawnych o randze ustawowej, ale także z rozporządzeń czy aktów prawa miejscowego, na co zwraca uwagę Ministerstwo Cyfryzacji („RODO dla administracji", s. 8). W tym kontekście szczególnie widoczna jest zasada ryzyka przewidziana w RODO. To administrator musi bowiem ocenić, jakie prawo będzie miało zastosowanie do określonego przetwarzania i będzie ewentualnie ponosił odpowiedzialność za wadliwą interpretację przepisów. Problem interpretacji przepisów stanowiących podstawę przetwarzania danych był przedmiotem badania w postępowaniu Prezesa Urzędu Ochrony Danych Osobowych, zakończonym decyzją z 29 października 2018 r. (znak: ZSZZ.440.717.2018). W przedmiotowej sprawie Centralna Komisja do Spraw Stopni i Tytułów opublikowała dokumenty związane z postępowaniem o nadanie stopnia doktora habilitowanego razem z podpisem wnioskującego o tytuł. Mimo że przepisy wprost nie wskazują, jaki dokładnie zakres danych osobowych powinien zostać opublikowany, Prezes Urzędu uznał takie postępowanie za zgodne z prawem. Trudności z ustaleniem i dotrzymaniem okresów retencji na podstawie przepisów prawa krajowego widoczne są także na przykładzie postępowania Prezesa Urzędu Ochrony Danych Osobowych zakończonego decyzją z 3 kwietnia 2019 r. (znak: ZSPU.421.8.2018). W postępowaniu tym Prezes stwierdził przetwarzanie danych osobowych w rejestrze mieszkańców przez okres dłuży niż dopuszczalny przepisami, jednak ukarany decyzją burmistrz związany był obowiązkiem uzyskania z Archiwum Państwowego zgody na brakowanie dokumentów, co opóźniło usuwanie danych.

Przesłanka opisana w art. 6 ust. 1 lit. e) RODO jest uzupełnieniem względem przesłanki przewidzianej w art. 6 ust. 1 lit. c) RODO (tak: P. Fajgielski, Komentarz do rozporządzenia nr 2016/679 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), [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018, art. 6). Realizacja uzasadnionego interesu publicznego może znaleźć zastosowanie wtedy, gdy brakuje szczegółowych przepisów, które dopuszczają przetwarzanie danych osobowych (por. P. Fajgielski, art. 6).

Przesłanka niezbędności przetwarzania dla wypełnienia zadania w interesie publicznym legitymizuje przetwarzanie w wypadku, gdy w przepisach nie jest wprost wskazany cel takiego przetwarzania (co jest warunkiem koniecznym w przypadku przetwarzania na podstawie art. 6 ust. 1 lit. c RODO), jednak przetwarzanie musi być niezbędne dla określonego celu w interesie publicznym (art. 6 ust. 3 RODO). Zadanie publiczne, któremu ma służyć przetwarzanie danych, musi być ustalone w przepisach powszechnie obowiązującego prawa, określającego m.in. także w zakresie kompetencji czy właściwości rzeczowej lub miejscowej (tak: M. Sakowska-Baryła (red.), Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, Warszawa 2018, art. 6). Przykładowo omawiana przesłanka może być wykorzystywana w kontekście zadań samorządu terytorialnego, ustalonych w odpowiednich ustawach i powodujących konieczność przetwarzania danych (por. M. Sakowska, art. 6). Jednak także skorzystanie z tej przesłanki przetwarzania nie wyłącza konieczności stosowania zasad przewidzianych w art. 5 RODO, a więc nakłada na administratora danych osobowych konieczność rozważenia chociażby zasady minimalizacji danych. W sprawie Heinz Huber przeciwko Bundesrepublik Deutschland (wyrok z 6 grudnia

2008 r., C-524/06, Zbiór Orzeczeń 2008 I-09705) Trybunał Sprawiedliwości wskazał, że dla skorzystania z przesłanki konieczności przetwarzania danych osobowych w celu realizacji zadania publicznego konieczne jest wykazanie, że przetwarzanie obejmuje dane wyłącznie konieczne do stosowania określonych przepisów przez organy władzy publicznej oraz że przetwarzanie pozwala na skuteczniejsze stosowanie takich przepisów. Podobne stanowisko zajął Wojewódzki Sąd Administracyjny w Warszawie na tle sprawy dotyczącej podawania numeru rejestracyjnego samochodu w parkomatach (wyrok z 13 kwietnia 2017 r., sygn. akt VII SA/Wa 1069/16).

W omawianym kontekście szczególnym wyzwaniem dla samorządów będzie precyzyjne określenie zakresu danych i adekwatnych sposobów ich przetwarzania, które będą dawały się obronić w świetle zasad opisanych w art. 5 RODO, w szczególności zasady minimalizacji danych oraz ograniczenia przechowywania.

RODO a dostęp do informacji publicznej

Jednostki samorządu terytorialnego związane są przepisami o dostępie do informacji publicznej i mają obowiązek publikować wiele informacji w Biuletynie Informacji Publicznej, a także muszą szanować zasadę jawności życia publicznego, transmitując na przykład kolegialne posiedzenia władzy publicznej. Nie należy jednak zapominać, że dane w BIP muszą być przetwarzane z uwzględnieniem podstawowych zasad przetwarzania danych wymienionych w art. 5 RODO, w tym zasady minimalizacji danych oraz ograniczenia przechowywania. Kwestia ta znalazła odzwierciedlenie w postępowaniu prowadzonym przez Prezesa Urzędu Ochrony Danych Osobowych, zakończonym decyzją z 30 stycznia 2019 r. (znak: ZSZZS.440.370.2018). Z problemem ograniczenia zakresu danych osobowych udostępnianych w ramach informacji publicznej zmierzył się zaś burmistrz, wobec którego następnie Prezes Urzędu Ochrony Danych Osobowych wydał decyzję z 16 kwietnia 2019 r. (znak: ZSPU.440.636.2018). Ogólnie rzecz biorąc wydaje się, że należy unikać przekazywania danych osobowych (czyli danych dotyczących określonej osoby) w ramach udzielania informacji publicznej, jeżeli tylko jest to możliwe. Takie postępowanie pozwala zachować zasadę poufności danych i minimalizacji przetwarzania danych.

Jeżeli zaś chodzi o transmisję posiedzeń organów kolegialnych władzy publicznej, Ministerstwo Cyfryzacji wskazuje, że w takim przypadku mamy do czynienia z koniecznością przetwarzania dla wypełnienia obowiązku prawnego nałożonego na administratora, niemniej jednak może zachodzić konieczność anonimizacji danych (np. wizerunku) na etapie publikacji nagrań i tylko w zakresie, w jakim publikacja danych naruszyłaby prywatność osoby, której dane dotyczą („RODO dla administracji", s. 12). Fakt wypełniania obowiązku prawnego nie zwalnia jednak administratora z obowiązku informacyjnego, czyli przekazania osobom, których dane dotyczą, informacji o przetwarzaniu ich danych osobowych (art. 13 i 14 RODO). Ministerstwo Cyfryzacji sugeruje, aby takie klauzule publikować w ogłoszeniu o sesji rady gminy, powiatu czy województwa, a także umieszczać przed wejściem na salę obrad („RODO dla administracji", s. 13).

Podsumowanie

Wyniki kontroli NIK w jednostkach samorządu terytorialnego w zakresie bezpieczeństwa informacji pokazują, że samorządy mają jeszcze przed sobą ogrom pracy do wykonania, aby osiągnąć zgodność z RODO oraz przepisami dotyczącymi bezpieczeństwa informacji. Jak się wydaje, w wielu samorządach dużym problemem w tym zakresie jest brak środków oraz natłok innych obowiązków, które trudno połączyć z pracą na rzecz zwiększenia ochrony danych osobowych. Niemniej jednak praca taka jest konieczna, bowiem każdy incydent naruszenia ochrony danych osobowych czy każde nieprawidłowe załatwienie żądania osoby, której dane dotyczą, będzie prowadzić do obniżenia zaufania obywateli do jednostki samorządu terytorialnego i może powodować niezadowolenie.

Mimo że przepisy RODO, jako aktu prawnego o randze europejskiej, są bardzo ogólne, administratorzy mają do dyspozycji coraz więcej poradników i wskazówek przygotowywanych czy to przez Urząd Ochrony Danych Osobowych, czy przez Ministerstwo Cyfryzacji. Kilka takich poradników zostało przywołanych powyżej, a ich lektura pozwala na rozwianie wielu wątpliwości interpretacyjnych, z którymi mierzą się administratorzy zarówno sektora prywatnego, jak i publicznego.

Trzeba także pamiętać o roli inspektora ochrony danych osobowych. Jego zadaniem jest kompleksowe wsparcie administratora w temacie ochrony danych osobowych, w tym informowanie go o obowiązkach prawnych wynikających z RODO i przepisów krajowych, monitorowanie przestrzegania przepisów wewnątrz organizacji, udzielanie zaleceń w ramach badania skutków przetwarzania dla ochrony danych oraz współpraca z Prezesem Urzędu Ochrony Danych Osobowych (art. 39 ust. 1 RODO). Warto dbać o niezależność IOD oraz zapewniać mu możliwość poszerzania swojej wiedzy i uzupełniania jej chociażby poprzez szkolenia, uczestnictwo w konferencjach dla IOD organizowanych przez organizacje prywatne oraz Urząd Ochrony Danych Osobowych oraz lekturę najnowszych wytycznych i decyzji zarówno polskiego Urzędu, jak i innych unijnych organów ochrony danych osobowych. Inspektor ochrony danych może być nieocenioną pomocą dla administratora, jednak musi być niezależny i musi mieć możliwość utrzymywania swoich kompetencji. Warto także pamiętać, że wykonywanie tej funkcji może być zakontraktowane zewnętrznie, co pozwala na skorzystanie z bogatego doświadczenia ekspertów i rozwiązanie ewentualnego problemu konfliktu interesów na stanowisku IOD.

**kancelaria Domański Zakrzewski Palinka, prawniczka zajmująca się w ramach kancelarii DZP prawem ochrony danych osobowych. Jest współautorką komentarza do ustawy o ochronie danych osobowych z 10 maja 2018 r., pełni także funkcję IOD u Klientów.*