1. Co ma norma ISO/IEC 27701 do przetwarzania danych w sieci i kto powinien ją stosować

„Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane" – tak brzmi art. 24 RODO. Z przepisu tego wynika, że administrator danych jest zobowiązany samodzielnie ocenić, czy i jakie środki powinien podjąć w odniesieniu do danych osobowych, w szczególności znając specyfikę swojego środowiska pracy i warunki, w jakich dane osobowe mogą być przetwarzane. Samo RODO nie wymusza stosowania żadnych konkretnych metod zabezpieczenia, takich jak kraty w oknach, szafki z określonymi zamkami, szyfrowanie czy dostęp do systemu IT z wykorzystaniem loginu i hasła.

Ogólnie o zabezpieczeniach

Zabezpieczenie danych osobowych może mieć charakter:

- **prawny** – regulacje obowiązujące u administratora danych osobowych, np. polityka prywatności, instrukcja zarządzania systemem informatycznym;
- **organizacyjny** – takie rozwiązania administracyjne (techniczne) jak polityka kluczy, zmiany haseł, udzielania i cofania upoważnień do przetwarzania danych;

- **informatyczny** – środki elektroniczne służące zachowaniu bezpieczeństwa i integralności przetwarzanych danych, takie jak firewalle, oprogramowanie antywirusowe, infrastruktura sieciowa, system wykrywania naruszeń;
- **fizyczny**.

Normy ISO – co to takiego

Normy ISO/IEC to międzynarodowe kodeksy praktyk służące wsparciu w określonym zakresie funkcjonowania przedsiębiorstwa, np. w odniesieniu do zarządzania danymi osobowymi czy bezpieczeństwem informacji.

PRZYKŁAD

Wybierając środki ochrony fizycznej, należy brać pod uwagę także potrzeby biznesowe oraz tzw. najlepsze praktyki. Wśród nich można wskazać normę ISO 27002 (następcę od 2007 roku normy ISO 17799). Określa ona wytyczne co do treści i stosowania systemu zarządzania bezpieczeństwem informacji w danej jednostce. Norma, począwszy od strony 41 (ISO Second Edition 2005-06-15), wskazuje na najistotniejsze zagadnienia związane z bezpieczeństwem fizycznym i środowiskowym, takie jak m.in.:

- wyznaczanie bezpiecznych obszarów firmy;
- kontrolowany dostęp dla osób z zewnątrz;
- ochrona infrastruktury kablowej;
- wycofywanie urządzeń z eksploatacji.

Wprowadzenie konkretnych środków zawsze musi być **poprzedzone przeprowadzeniem analizy ryzyka**. To od poziomu ryzyka zależy to, jaki stopień zabezpieczeń ochrony fizycznej będzie skuteczny. Dobrze przeprowadzona analiza daje odpowiedź na pytania: co, przed czym, w jaki sposób i z jakim skutkiem chronimy. Wyniki analizy mogą posłużyć do sklasyfikowania kategorii zagrożonych wartości, wyboru poziomu bezpieczeństwa, klasy środków ochrony oraz klasy systemu alarmowego zgodnie z polską normą PN-93 E-08390/14 oraz normą europejską EN 50131-6:2008.

Rodzina norm 27000

Wskazany przykład to naturalnie tylko wycinek zagadnień jednej normy – ISO IEC 27702, wspomagającej w odniesieniu do wymogów RODO. Ale przecież napisaliśmy, że norma ta odnosi się do systemu zarządzania bezpieczeństwem informacji. Jak rozumieć tę kwestię i czy to oznacza, że można wdrażać normy ISO i być wówczas pewnym, że spełniamy automatycznie wymogi RODO? Absolutnie nie. Ale aby to zrozumieć, musimy przyjrzeć się bliżej **rodzinie norm 27000** oraz zagadnieniu cyberbezpieczeństwa i jego relacji do kwestii ochrony danych osobowych.

Przede wszystkim skupmy się na tej grupie norm, które mają znaczenie także co do aspektu ochrony danych osobowych. Chodzi tu o tzw. rodzinę norm ISO 27000. Te normy, różniące się końcówkami numerów, jako „rodzina norm", dotyczą tych samych kwestii. I tak, norma:

- **ISO 27000** – wprowadza w temat bezpieczeństwa informacji;
- **ISO 27001** – określa wymagania w zakresie certyfikacji;
- **ISO 27002** – rozwija normę ISO 27001;
- **ISO 27701** – precyzuje techniki bezpieczeństwa i stanowi rozszerzenie norm ISO 27001 oraz ISO 27002 w zakresie zarządzania informacjami o prywatności; dotyczy osobistych danych osobowych (Personally Identifiable Information, PII) w ramach systemów zarządzania informacjami (SZBI);
- **ISO 27702** – wspomniana wyżej jako przykładowa norma tej rodziny.

Cyberbezpieczeństwo w polskich przepisach

Ustawa o krajowym systemie cyberbezpieczeństwa to akt prawny implementujący do krajowego porządku prawnego dyrektywę NIS. Nie dotyczy ona ochrony danych osobowych (przynajmniej nie bezpośrednio – jak RODO), ale bezpieczeństwa systemów informatycznych. I tu pojawia się łącznik między obydwiema regulacjami: do systemów informatycznych, w których dochodzi do przetwarzania danych osobowych, będzie się stosowało zarówno wymogi RODO, jak i ustawy o krajowym systemie cyberbezpieczeństwa. W przeciwieństwie jednak do RODO dyrektywę NIS w kształcie prezentowa-

nym przez ustawę o krajowym systemie cyberbezpieczeństwa stosuje się do zdecydowanie mniejszej liczby podmiotów.

O ile RODO stosuje się praktycznie do wszystkich podmiotów przetwarzających dane osobowe, o tyle ustawa o krajowym systemie cyberbezpieczeństwa obowiązuje jedynie określone w niej podmioty. Są nimi wyszczególnione w art. 4 urzędy, instytuty, spółki wykonujące zadania o charakterze użyteczności publicznej czy podmioty świadczące usługi z zakresu cyberbezpieczeństwa. Oprócz nich krajowy system cyberbezpieczeństwa obejmuje dwie nieco większe grupy.

Pierwszą z nich są tzw. **operatorzy usług kluczowych** – podmioty, wobec których organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Decyzję tę można zaś wydać wyłącznie w stosunku do podmiotów działających w określonych dziedzinach, wyliczonych w załączniku nr 1 do ustawy o krajowym systemie cyberbezpieczeństwa. Chodzi tu dokładnie o wydobycie kopalin, energię elektryczną oraz ciepło (np. wytwarzanie, dystrybucja). Drugą grupę stanowią dostawcy usług cyfrowych, np. chmury, usług dla przeglądarek czy platform handlowych – chodzi generalnie o usługi cyfrowe wyliczone w załączniku nr 2 do ustawy.

WAŻNE

Jeżeli więc dany podmiot należy do jednej z kategorii wyliczonych powyżej, to musi wypełniać obowiązki z ustawy o krajowym systemie cyberbezpieczeństwa, a jeżeli dodatkowo przetwarza dane osobowe – to także obowiązki w ramach RODO.

W motywie 49 RODO czytamy, że przetwarzanie danych osobowych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji jest **prawnie uzasadnionym interesem administratora**, którego sprawa dotyczy.

Może to obejmować na przykład zapobieganie nieuprawnionemu dostępowi do sieci łączności elektronicznej i rozprowadzaniu złośliwych kodów, przerywanie ataków typu „odmowa usługi", a także przeciwdziałanie uszko-

dzeniu systemów komputerowych i systemów łączności elektronicznej. Na gruncie RODO administrator danych osobowych ma także wybierać takie podmioty przetwarzające, które gwarantują prawidłowe przetwarzanie danych osobowych. W przypadku danych osobowych mamy więc do czynienia ze swoistym pilnowaniem czy audytowaniem dostawców usług, które to czynności wprowadza obecnie ustawa o krajowym systemie cyberbezpieczeństwa w odniesieniu do cyberbezpieczeństwa.

KRI i SZBI

Skoro norma ISO 27701 odnosi się do systemów zarządzania bezpieczeństwem informacji, należy zauważyć, że obowiązek wdrożenia SZBI wiąże się bezpośrednio z **zabezpieczaniem danych osobowych**. Paragraf 20 rozporządzenia Rady Ministrów z 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 stanowi, że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Zakres obowiązku wdrożenia SZBI wynika z pojęcia „podmiotów realizujących zadania publiczne". Zarówno rozporządzenie, jak i ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne (na podstawie której rozporządzenie zostało wydane) nie definiuje takiego pojęcia. Ustawa definiuje natomiast tzw. podmiot publiczny, który odnosi się między innymi do:

- jednostek samorządu terytorialnego i ich organów,
- jednostek budżetowych i samorządowych zakładów budżetowych,
- państwowych lub samorządowych osób prawnych utworzonych na podstawie odrębnych ustaw w celu realizacji zadań publicznych.

Jeżeli więc dany **podmiot należy do tej kategorii oraz dodatkowo realizuje zadania publiczne**, to ma obowiązek wdrożyć i przestrzegać SZBI.

W jakich przypadkach wdrażać ISO 27701

Należy mieć na względzie, że norma ISO 27701:

- dotyczy „wszystkich typów i wielkości organizacji, w tym firm publicznych i prywatnych, podmiotów rządowych i organizacji non profit, które są administratorami PII i/lub procesorami PII przetwarzającymi PII w ramach SZBI";
- wskazuje, jak postępować z danymi w ramach kategorii określenia PII;
- rozszerza SZBI oparty na ISO 27001, a więc nie jest przeznaczona do samodzielnego stosowania;
- nie dotyczy zasadniczo ochrony danych osobowych, lecz PII i to w ramach SZBI.

Najlepiej spojrzeć na SZBI jako na **całość dokumentacji dotyczącej ochrony informacji w jednostce** – niezależnie od tego, na jakiej podstawie dany dokument został wydany i czego konkretnie dotyczy (np. danych osobowych, informacji niejawnych, tajemnicy handlowej, tajemnicy zawodowej itd.). W SZBI mamy wszystkie akty wewnętrzne (procedury, polityki, instrukcje czy regulaminy) wdrożone w danym podmiocie. System ochrony danych osobowych jest częścią SZBI.

WAŻNE

Wdrożenie normy ISO 27701:

- ma sens tam, gdzie mamy **SZBI na bazie ISO 27001**;
- w pozostałych przypadkach nie może być postrzegane jako zapewnienie zgodności z RODO, co najwyżej jako dobra praktyka tylko w jednym aspekcie ochrony danych – poufności (zapobiegania wyciekom).

2. Urządzenia mobilne prywatne czy służbowe – które wybrać

Współczesne urządzenia mobilne, wykorzystywane w celach służbowych, pozwalają na bardzo szeroki dostęp do danych osobowych. Nie zmienia to faktu, że administrator takich danych, który upoważnia swojego pracownika do ich przetwarzania, odpowiada za bezpieczeństwo tych danych. Wręcz przeciwnie – udostępnienie pracownikowi urządzenia, za pomocą którego ma on dostęp do danych z właściwie każdego miejsca, skutkuje pojawieniem się nowych zagrożeń dla bezpieczeństwa danych. W konsekwencji administrator powinien więc uwzględnić w procesie wdrażania odpowiednich technicznych i organizacyjnych zabezpieczeń to, że dostęp do danych będzie możliwy również za pośrednictwem urządzeń mobilnych. W jaki sposób uregulować te kwestie tak, aby zapewnić swojej organizacji zgodność z RODO, a jednocześnie nie utrudnić użytkownikom korzystania z poszczególnych funkcjonalności telefonu?

Plusy i minusy każdego rozwiązania

Najkorzystniejszą i jednocześnie najprostszą do uregulowania sytuacją jest ta, gdy do realizowania obowiązków służbowych poszczególni pracownicy mają przydzielone im przez administratora urządzenia służbowe. Mogą oni je wykorzystywać co do zasady wyłącznie do wykonywania zadań związanych z pracą. Osoby takie mogą mieć jednocześnie swoje prywatne telefony komórkowe, które są przez nie wykorzystywane w celach związanych z życiem osobistym. Dzięki temu stosunkowo łatwe jest zachowanie prostej zasa-

dy, mówiącej, że służbowy telefon komórkowy wykorzystywany jest w celach służbowych, a prywatny na potrzeby prywatne.

Tego rodzaju sytuacja zapewnia administratorowi (tj. pracodawcy danej osoby albo innemu podmiotowi, który upoważnia osobę do przetwarzania danych) stosunkowo dużą kontrolę nad tym, w jaki sposób dana osoba będzie wykorzystywała urządzenie mobilne w celach służbowych. Możliwe jest więc szczegółowe uregulowanie tego, jak pracownik może wykorzystywać takie urządzenie bezpośrednio w treści polityk lub procedur dotyczących ochrony danych. Nie ma również przeszkód, aby administrator wdrożył w takiej sytuacji dodatkowe środki umożliwiające mu kontrolę nad sposobem korzystania z urządzenia, np. obejmujące zdalny dostęp do urządzenia czy też ograniczające możliwość instalowania aplikacji niezatwierdzonych przez dział IT administratora. Takie działania spotykają się z reguły ze zrozumieniem pracowników, którzy nie mają nic przeciwko temu, aby administrator miał zdalny dostęp do ich służbowego urządzenia i decydował o tym, co na nim zostanie zainstalowane.

Z drugiej strony w wielu organizacjach coraz popularniejsze staje się umożliwianie osobom pracy **za pomocą ich prywatnych urządzeń**. Z tego typu możliwości chcą korzystać pracownicy, którzy wolą mieć tylko jedno urządzenie (prywatne), a nie dwa. Pod pewnymi względami jest to również korzystne dla pracodawców, gdyż pozwala ograniczyć koszty nabywania nowych urządzeń (pracownicy sami kupują prywatne urządzenia i z nich korzystają). W takim przypadku administrator ma jednak bardzo ograniczone możliwości kontroli tego, jakie działania będą podejmowane w ramach takiego prywatnego urządzenia oraz w jaki sposób zabezpieczone będą dane, które są przetwarzane na takim urządzeniu.

Jak uregulować to w organizacji

W praktyce nie istnieją prawne regulacje, które wyraźnie zabraniałyby korzystania z prywatnych urządzeń w celach służbowych. Tym samym pracodawca może zezwolić swoim pracownikom na takie działania. Warunkiem jest jednak, aby rzetelnie oszacował związane z tym ryzyko i ocenił negatywne konsekwencje z punktu widzenia bezpieczeństwa danych. W rezultacie na pracownika zostają nałożone dodatkowe rygory związane z tym, że wykorzy-

stuje on swoje prywatne urządzenie mobilne. Co ważne, rygory te dotykają z reguły wszystkich kwestii związanych z wykorzystaniem takiego telefonu, również w zakresie, w jakim jest on używany w celach prywatnych.

WAŻNE

Do najczęściej stosowanych ograniczeń należą:

1. Obowiązek zastosowania w ramach urządzenia mobilnego określonych przez administratora **zabezpieczeń**, np. szyfrowanie urządzenia, konieczność każdorazowego odblokowywania go za pomocą kodu PIN.
2. Obowiązek zainstalowania na urządzeniu wskazanego przez administratora **oprogramowania antywirusowego** lub innego oprogramowania służącego do zwiększenia poziomu bezpieczeństwa urządzenia mobilnego, w tym np. do zdalnego usunięcia danych zapisanych w ramach tego urządzenia w sytuacji jego zgubienia lub kradzieży.
3. Skonfigurowanie urządzenia bezpośrednio przez pracownika odpowiedzialnego za **bezpieczeństwo IT** w organizacji.
4. Obowiązek umożliwienia (na żądanie administratora) dostępu do urządzenia mobilnego przez pracownika, np. przyniesienia go i umożliwienia dokonania **weryfikacji poziomu zabezpieczeń** przez osobę odpowiedzialną za bezpieczeństwo informatyczne w organizacji.
5. Zainstalowanie oprogramowania umożliwiającego **zdalny dostęp** pracodawcy do urządzenia mobilnego pracownika.
6. Ograniczenie **uprawnień administratora** w ramach danego urządzenia, konieczność uzyskiwania każdorazowej zgody na zainstalowanie nowego oprogramowania.
7. Ograniczenie możliwości **instalowania oprogramowania** wyłącznie do tego zaakceptowanego uprzednio przez administratora.
8. Ograniczenie możliwości wykonywania określonych, związanych z pracą działań, które mogą być realizowane za pomocą **prywatnego urządzenia** (np. pracownik może dzwonić, lecz nie będzie w stanie wysyłać wiadomości e-mail).
9. Zakaz łączenia się z innymi sieciami **wi-fi** niż te zaakceptowane przez administratora.
10. Zakaz udostępniania danego urządzenia osobom innym niż upoważniony pracownik, również członkom jego rodziny.

Często wdrożenie tych zabezpieczeń następuje w ramach specjalnej, odrębnej procedury. Pracownicy, którzy zgłaszają wolę pracy za pomocą prywatnego urządzenia, muszą podpisywać odrębne deklaracje – te wyraźnie wskazują na obowiązek przestrzegania tych zasad i ewentualną odpowiedzialność związaną z ich naruszeniem.

W praktyce zdarza się tak, że pracownicy, którzy mają zadeklarować przestrzeganie tych reguł, a tym samym dobrowolnie zobowiązać się do tego, że nie będą korzystali z wszystkich funkcjonalności swojego prywatnego telefonu komórkowego, rezygnują z korzystania z prywatnego telefonu i wolą otrzymać od pracodawcy osobne, służbowe urządzenie. Innymi słowy, używanie prywatnych urządzeń w celach służbowych jest jak najbardziej dopuszczalne, ale kwestie związane z zapewnieniem bezpieczeństwa danych powodują powstanie tak licznych obowiązków i ograniczeń, że wiele osób przestaje być zainteresowanych tym rozwiązaniem.

Gdy urządzenia udostępnia administrator

Tak jak wskazałem powyżej, umożliwianie pracownikom wykorzystania służbowych urządzeń mobilnych powoduje o wiele mniejsze komplikacje pod względem prawno-regulacyjnym. Oczywiście, prawidłowym postępowaniem będzie również zabezpieczenie takich urządzeń w sposób adekwatny do ewentualnych rodzajów **ryzyka**. Co do zasady, charakter poszczególnych zabezpieczeń będzie zbliżony do tych, które dotyczą urządzeń prywatnych. Łatwiejsze jest z reguły egzekwowanie przestrzegania tego rodzaju zasad – nie ma bowiem jakichkolwiek przeszkód (w tym również pośród pracowników), aby pracodawca decydował o tym, jakie aplikacje mogą być wykorzystywane na takim urządzeniu, i miał kontrolę nad urządzeniem.

Często bowiem zdarza się, że osobami odpowiedzialnymi za przydzielenie telefonów komórkowych pracownikom (nawet służbowych) są po prostu szefowie zespołów lub pracownicy sekretariatu, którzy nie zawsze mają szczegółową wiedzę na temat kwestii związanych z bezpieczeństwem danych. Dodatkowo, ich zadania w tym zakresie czasem ograniczają się do przekazania telefonu pracownikowi. Tego rodzaju sytuacja jest wysoce niepożądana – trzeba bowiem pamiętać, że używanie telefonu może wiązać się ze znacznym