Volume 21, Issue 2
December 2023

ISSN 1731-8297, e-ISSN 6969-9696
http://czasopisma.uni.opole.pl/index.php/osap

ORIGINAL ARTICLE
received 2023-08-22
accepted 2023-12-03

Zagrożenia w obszarze bezpieczeństwa informacji i ochrony danych osobowych a rola Inspektora Ochrony Danych w tym zakresie

Threats in the area of security information and personal data protection and the role of Data Protection Officer in this regard

MARCIN JANIK

Wydział Prawa i Administracji, Uniwersytet Śląski w Katowicach
ORCID: 0000-0002-6197-2722, e-mail: kontakt@janikadwokat.pl

STANISŁAW HADY-GŁOWIAK

Katedra Prawa Gospodarczego, Uniwersytet Ekonomiczny w Katowicach
ORCID: 0000-0002-1060-6984, e-mail: stanislawhg@gmail.com

Citation: Janik, Marcin. Hady-Głowiak, Stanisław. 2023. Zagrożenia w obszarze bezpieczeństwa informacji i ochrony danych osobowych a rola Inspektora Ochrony Danych w tym zakresie. *Opolskie Studia Administracyjno-Prawne* 21(2): 119–140. DOI: 10.25167/osap.5205.

Abstract: The article presents issues related to current threats in the area of security information and personal data protection as well as preventive measures in this area. With the above in mind, the article discusses the current system and legal solutions as well as the advisory and monitoring role of Data Protection Officer in the institution in this respect.

Keywords: Information security, cyber security, Data Protection Officer, personal data protection, incident

Abstrakt: W artykule przedstawiono zagadnienia dotyczące aktualnych zagrożeń w obszarze bezpieczeństwa informacji i ochrony danych osobowych oraz działań zapobiegawczych w tym zakresie. Mając powyższe na uwadze, w artykule omówiono aktualne rozwiązania

systemowe i prawne oraz rolę doradczą i monitorującą Inspektora Ochrony Danych w instytucji w przedmiotowym zakresie.

Słowa kluczowe: bezpieczeństwo informacji, cyberbezpieczeństwo, Inspektor Ochrony Danych, ochrona danych osobowych, incydent

Niniejszy artykuł ma na celu przedstawienie aktualnych zagrożeń w obszarze bezpieczeństwa informacji i ochrony danych osobowych oraz działań zapobiegawczych w tym zakresie. Mając powyższe na uwadze, w artykule omówiono aktualne rozwiązania systemowe i prawne oraz rolę doradczą i monitorującą Inspektora Ochrony Danych (zwanego dalej IOD) w instytucji w przedmiotowym zakresie.

1. Wprowadzenie do tematyki związanej z zagrożeniami w obszarze bezpieczeństwa informacji i ochrony danych oraz przepisów prawnych w przedmiotowym zakresie

Ochrona cyberprzestrzeni stała się jednym z najczęściej podejmowanych tematów dotyczących bezpieczeństwa, ponieważ stabilność funkcjonowania i rozwój globalnego społeczeństwa informacyjnego są uzależnione od otwartej, niezawodnej i – przede wszystkim – bezpiecznej cyberprzestrzeni. Podnoszenie świadomości w tym zakresie oraz konstrukcja odpowiednich narzędzi prawnych i karnych w zwalczaniu cyberprzestępczości nie idą w parze z gwałtownym wzrostem liczby cyberincydentów i nowych rodzajów cyberzagrożeń. Obecnie istnieje problem braku spójnych międzynarodowych rozwiązań systemowych i prawnych, co ogranicza rządy państw, instytucje oraz inne podmioty, których celem jest zapewnienie bezpiecznego działania globalnej sieci. Klasycznym przykładem międzynarodowej problematyki dotyczącej cyberbezpieczeństwa są zmasowane cyberataki na infrastrukturę teleinformatyczną Estonii w 2007 r. oraz Gruzji w 2008 r. Cyberataki na te państwa doprowadziły do funkcjonalnego paraliżu m.in. poprzez: blokowanie czy podmienianie rządowych portali; ataki DDoS poprzez sfałszowane komunikaty BBC i CNN, które w rzeczywistości infekowały komputery; cyberataki na strony internetowe banków czy ambasad państw wspierających zaatakowaną Gruzję i Estonię (Gwoździewicz 2019: 3).

W środowisku praktyków panuje pogląd, że administracja lokalna jest atrakcyjnym celem dla cyberprzestępców. Jedną z przyczyn takiego stanu rzeczy jest możliwość łatwego uzyskania informacji o kontrahentach urzędów publicznych. Ponadto pracownicy urzędów nie mają wystarczającej wiedzy pozwalającej na identyfikację wszelkich prób cyberataków. Podkreślić należy również, że bardzo często budżet małych jednostek samorządu terytorialnego nie pozwala na zaangażowanie specjalistów odpowiedzialnych za zapewnienie odpowiedniego poziomu ochrony posiadanych zasobów jednostki przed cyberatakami oraz

za monitorowanie i aktualizowanie systemów informatycznych. W pandemii wzrosła liczba ataków hakerskich na serwery jednostek samorządu terytorialnego, a ich praca została sparaliżowana na wiele dni. Według Barracuda Networks (światowy lider w zakresie IT) ofiarami ponad 44% ataków *ransomware* są właśnie władze lokalne. Należy podkreślić, że w bazach samorządowych przechowywane są praktycznie wszystkie dane osobowe obywateli, które przestępcy mogą wykorzystać do kradzieży tożsamości (Horbaczewski 2022).

Jeżeli chodzi o przepisy prawne regulujące przedmiotowe zagadnienie, to jako kluczowe należy wskazać unijne ramy cyberbezpieczeństwa, takie jak: Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U.UE.L.2016.119.89, zwana dalej dyrektywą 2016/680), 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 (Dz.U.UE.L.2016.119.1, zwane dalej RODO) oraz Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U.UE.L.2016.194.1, zwana dalej dyrektywą NIS). Dyrektywa NIS określiła obowiązki z zakresu cyberbezpieczeństwa, którym podlegają: 1) operatorzy usług kluczowych – co najmniej 7 sektorów krytycznych – energetyka (energia elektryczna, ropa naftowa, gaz), transport (transport lotniczy, transport kolejowy, transport wodny, transport drogowy), bankowość, infrastruktura rynków finansowych, służba zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja, infrastruktura cyfrowa, oraz 2) dostawcy usług cyfrowych (internetowe platformy handlowe, wyszukiwarki, usługi przetwarzania w chmurze). Dyrektywa 2016/1148 ustanawia obowiązki dla wszystkich państw członkowskich dotyczące: przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, tworzenia grupy współpracy w celu wspierania i ułatwiania strategicznej współpracy i wymiany informacji między państwami członkowskimi oraz tworzenia sieci zespołów reagowania na cyberincydenty CSIRT. Ponadto ustanawia wymogi dotyczące bezpieczeństwa i zgłaszania incydentów dla operatorów usług kluczowych i dostawców usług cyfrowych oraz wymogi dotyczące wyznaczania właściwych organów krajowych, pojedynczych punktów kontaktowych oraz CSIRT mających zadania związane z bezpieczeństwem sieci i systemów informatycznych. Bardzo

ważnym elementem dyrektywy 2016/1148 są także definicje legalne m.in. takich pojęć jak: „sieci i systemy informatyczne", „bezpieczeństwo sieci i systemów informatycznych", „krajowa strategia w zakresie bezpieczeństwa sieci i systemów informatycznych", „operator usług kluczowych", „usługa cyfrowa" i „dostawca usług cyfrowych", „incydent" i „postępowanie w przypadku incydentu" czy też „usługa przetwarzania w chmurze".

Dzięki dyrektywie 2016/1148 państwa członkowskie UE podjęły działania w celu dostosowania wewnętrznych przepisów prawnych (Gwoździewicz 2019: 4–5).

Unijne przepisy dotyczące cyberbezpieczeństwa wprowadzone w 2016 r. zostały zaktualizowane Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dz.U.UE.L.2022.333.80, zwaną dalej dyrektywą NIS 2). W ramach NIS2 zmodernizowano istniejące ramy prawne, aby nadążyć za rosnącą cyfryzacją i zmieniającym się krajobrazem zagrożeń dla cyberbezpieczeństwa. Rozszerzono zakres przepisów dotyczących cyberbezpieczeństwa na nowe sektory i podmioty, dodatkowo zwiększona została odporność i zdolność reagowania na incydenty podmiotów publicznych i prywatnych, właściwych organów i całej UE (Komisja Europejska).

W celu dostosowania wewnętrznych przepisów prawnych w Polsce uchwalona została ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2023, poz. 913, t.j., zwana dalej KSC). Projekt nowelizacji wskazanej ustawy został skierowany do prac sejmowych na początku lipca 2023 roku. Zgodnie z art. 1 ust. 1 ustawa KSC określa:

1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;

2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;

3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Ustawa ta wskazuje legalną definicję incydentu, czyli zdarzenia, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo, wyróżniając jednocześnie 3 rodzaje incydentów: krytyczny, poważny i istotny. W ustawie wyróżniono również Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego, tj. CSIRT GOV (prowadzone przez Szefa Agencji Bezpieczeństwa Wewnętrznego), CSIRT MON (prowadzone przez Ministra Obrony Narodowej) oraz CSIRT NASK (prowadzone przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy). Wskazano również podmioty zobowiązane do zgłaszania incydentów niezwłocznie, nie później niż w ciągu 24 godzin od momentu

ich wykrycia, do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego przez operatorów usług kluczowych, dostawców usług cyfrowych czy podmioty publiczne. Ponadto, gdy jednostki sektora finansów publicznych realizują zadania publiczne zależne od systemu informacyjnego, to zgodnie z art. 21 ust. 1 KSC są zobowiązane do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami KSC. Wskazane zespoły zajmują się obsługą incydentu, a więc podejmują czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, ustalenie priorytetów oraz podejmowanie działań naprawczych i ograniczenie skutków incydentu w celu umożliwienia użytkownikom wznowienia normalnej działalności po ich usunięciu. Incydenty zgłasza się poprzez wypełnienie formularza interaktywnego na stronie CERT (Zespołu Reagowania na Incydenty Bezpieczeństwa) dostępnego pod adresem: https://incydent.cert.pl/#!/lang=pl,entityType=publicInstitution,publicEssentialService=false,publicInstitutionIncident=true.

Mając powyższe na uwadze, każdy podmiot – nie tylko publiczny – powinien niezwłocznie zgłaszać incydenty, co daje możliwość uzyskania profesjonalnego wsparcia i opracowania mechanizmów obronnych, np. w postaci deskryptorów oraz ostrzeżenia innych podmiotów przed incydentem.

2. Incydent bezpieczeństwa informacji i naruszenie przepisów o ochronie danych osobowych oraz rola i zadania osób odpowiedzialnych i działania zapobiegawcze

Identyfikacja incydentu bezpieczeństwa informacyjnego zobowiązuje administratora danych do podjęcia wszelkich środków po to, aby ten incydent we właściwy sposób sklasyfikować oraz wdrożyć właściwe kroki w celu wyeliminowania jego negatywnych następstw. Pojęcie incydentu bezpieczeństwa informacji nie zostało uregulowane w przepisach prawnych, ale należy je kwalifikować jako pojęcie szersze niż pojęcie naruszenia ochrony danych osobowych. Norma ISO 27000 w pkt 2.36 definiuje incydent związany z bezpieczeństwem informacji jako pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. Natomiast naruszenie ochrony danych osobowych, w myśl art. 4 pkt 12 RODO, zostało zdefiniowane jako 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 (Siemieniak 2020).

Oznacza to, że nie każde naruszenie przepisów o ochronie danych stanowi naruszenie ochrony danych w rozumieniu przepisów unijnych, a jedynie takie naruszenie, które spełnia wymogi wskazane w definicji, a więc: stanowi naruszenie bezpieczeństwa (wymogów dotyczących zabezpieczenia danych) i skutkiem naruszenia bezpieczeństwa jest zniszczenie, utrata, modyfikacja, nieuprawnione ujawnienie lub nieuprawniony dostęp do przetwarzanych danych (Fajgielski 2019: 176).

Wstępna klasyfikacja zdarzenia polega przede wszystkim na ocenie tego, czy dane zdarzenie należy uznać za naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO. W pierwszej kolejności niezbędne jest ustalenie, czy dane zdarzenie dotyczyło danych osobowych w rozumieniu art. 4 pkt 1 RODO (np. imion i nazwisk, numerów PESEL, adresów e-mail czy danych dotyczących zdrowia). Następnie administrator danych musi ocenić, czy dane zdarzenie spełnia dodatkowe przesłanki, które wynikają z definicji naruszenia ochrony danych osobowych, czyli czy doszło do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu. Wskazane przesłanki stanowią punkt wyjścia dla administratora w odniesieniu do głębszej oceny naruszenia ochrony danych w kontekście obowiązków zgłoszeniowych wynikających z art. 33 oraz 34 RODO (Siemieniak 2020). I tutaj kluczowa jest rola IOD w obszarze zarówno wdrożenia, jak i weryfikacji obowiązujących zasad i procedur w tym zakresie.

Przykładowe naruszenia ochrony danych to: kradzież nośnika (w postaci zarówno papierowej, jak i elektronicznej) zawierającego dane osobowe czy też uzyskanie dostępu do systemu informatycznego zawierającego dane osobowe przez osobę do tego nieuprawnioną. Nie stanowi naruszenia ochrony danych osobowych w rozumieniu nadanym temu pojęciu przez prawodawcę unijnego naruszenie innych przepisów o ochronie danych niż przepisy dotyczące zabezpieczenia danych, np. niedopełnienie obowiązku informowania osób o przetwarzaniu danych, czy też niespełnienie żądania podmiotu danych dotyczącego skorygowania jego danych (Fajgielski 2019: 196).

Na podstawie art. 33 RODO administrator danych jest zobowiązany do zgłoszenia naruszenia ochrony danych osobowych organowi ochrony danych. Warunkiem zwalniającym z obowiązku zgłoszeniowego jest wystąpienie małego prawdopodobieństwa, by naruszenie ochrony danych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Zgłoszenie naruszenia ochrony danych osobowych w przypadku powstania obowiązku zgłoszeniowego musi zostać zrealizowane niezwłocznie, w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. W przypadku gdy do zgłoszenia dojdzie po upływie 72 godzin, niezbędne jest dołączenie organowi ochrony danych wyjaśnienia dotyczącego przyczyn opóźnienia. Regulacja dotycząca pod-

miotów przetwarzających dane osobowe została ujęta w art. 33 ust. 2 RODO, który stanowi, że podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych jest zobowiązany do zgłoszenia naruszenia administratorowi. W przypadku podmiotów przetwarzających procedura notyfikowania zgłoszenia naruszenia ochrony danych administratorowi powinna zostać odpowiednio uregulowana w umowie dotyczącej powierzenia przetwarzania danych osobowych (Siemieniak 2020).

Za datę stwierdzenia naruszenia należy przyjąć dzień, w którym uznano, że zdarzenie stanowi naruszenie bezpieczeństwa, co niekoniecznie będzie tożsame z dniem, w którym zdarzenie nastąpiło. Jako przykład można wskazać sytuację, w której zniszczeniu uległo urządzenie służące jako nośnik, na którym zapisane były dane osobowe. Tego rodzaju zdarzenie może, ale nie musi być kwalifikowane jako naruszenie ochrony danych, a ocena w tym zakresie uzależniona może być od wielu różnych okoliczności, np. od tego, czy dane osobowe były zgromadzone jedynie na tym nośniku (np. dysku twardym komputera), czy też na innych nośnikach (np. dysku sieciowym) – w sytuacji gdy urządzenie uległo uszkodzeniu lub zniszczeniu, jednak dane nie zostały utracone, gdyż były przechowywane także na innym nośniku, mimo że zdarzenie nastąpiło, jego ustalenie nie jest równoznaczne ze stwierdzeniem naruszenia ochrony danych, a osoba, która zgłasza tego rodzaju zdarzenie, może nie być w stanie samodzielnie określić, czy zdarzenie stanowi naruszenie ochrony danych osobowych (Fajgielski 2019: 178).

W przypadku gdy w wyniku procesu klasyfikacji naruszenia ochrony danych osobowych administrator danych uzna, że dane naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, wówczas administrator musi niezwłocznie poinformować osoby, których dane dotyczą, o naruszeniu. Zakres notyfikacji wynikający z art. 34 ust. 2 RODO w związku z naruszeniem jest nieznacznie zawężony w stosunku do zakresu wynikającego z treści art. 33 ust. 3 RODO. Nie obejmuje on informacji na temat specyfiki naruszenia ochrony danych z art. 33 ust. 3 lit. a RODO. Administrator danych jest zobowiązany do poinformowania podmiotów danych w zakresie: wskazania możliwych konsekwencji naruszenia ochrony danych osobowych; wskazania odpowiedniego punktu kontaktowego oraz danych inspektora ochrony danych, od którego można uzyskać więcej informacji, a także wskazania zastosowanych lub proponowanych środków w celu zaradzenia naruszeniu (Siemieniak 2020).

Zgłoszenia można dokonać za pomocą formularza dostępnego na stronie uodo.gov.pl na 4 sposoby: elektronicznie poprzez wypełnienie dedykowanego formularza dostępnego bezpośrednio na platformie biznes.gov.pl; elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: UODO/SkrytkaESP; za pomocą pisma ogólnego dostępnego na

platformie biznes.gov.pl; możliwe jest również przesłanie zgłoszenia tradycyjną pocztą – wysyłanie wypełnionego formularza na adres Urzędu (Urząd Ochrony Danych Osobowych 2019).

Administrator danych nie musi realizować obowiązku notyfikacyjnego w przypadku, gdy zostały zastosowane odpowiednie środki techniczne i organizacyjne, jak np. szyfrowanie, które uniemożliwią odczyt danych osobowych osobom do tego nieuprawnionym (art. 34 ust. 3 lit. a RODO). Zwolnienie z obowiązku notyfikacji podmiotu danych przysługuje również w przypadku, gdy administrator danych zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób fizycznych (art. 34 ust. 3 lit. b RODO). Administrator danych musi zatem dokonać przeglądu stosowanych środków technicznych, jak np. szyfrowanie, pseudonimizacja czy minimalizacja, oraz szczegółów dotyczących zakresu naruszenia po to, aby przeprowadzić ocenę możliwości zastosowania zwolnienia z art. 34 ust. 3 lit. b RODO. Ostatnim zwolnieniem z obowiązku notyfikacji podmiotu danych jest przesłanka niewspółmiernie dużego wysiłku (art. 34 ust. 3 lit. c RODO) w realizacji tego obowiązku. Administrator danych stosuje wówczas alternatywne środki notyfikacji o naruszeniu w postaci wydania publicznego komunikatu lub stosuje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób (Siemieniak 2020). Należy zwrócić uwagę na to, że argument związany z wysokimi kosztami notyfikacji jako niewspółmiernie dużym wysiłkiem nie jest wystarczający, aby administrator mógł uznać możliwość zastosowania omawianego przepisu (Hady-Głowiak 2022).

Wśród najważniejszych problemów, będących konsekwencją cyberataków, są:

1) straty finansowe, które wynikają m.in. z kradzieży informacji poufnych czy stanowiących tajemnicę przedsiębiorstwa, kradzieży informacji finansowych, kradzieży pieniędzy, zakłóceń operacji biznesowych (np. niemożność wykonywania transakcji online), a często również utrata ważnych umów czy dokumentów; środki zaradcze wykonywane po naruszeniu bezpieczeństwa powodują zaś dalsze straty finansowe;

2) zakłócenia w infrastrukturze krytycznej, spowodowane faktem, iż funkcjonowanie najważniejszych z punktu widzenia bezpieczeństwa państwa obiektów, instalacji, usług oraz urządzeń jest coraz bardziej uzależnione od rozwiązań teleinformatycznych; zakłócenia mogą mieć poważne konsekwencje społeczne, gdyż cyberprzestępcy coraz częściej atakują nie tylko instytucje finansowe, ale i instytucje służby zdrowia, firmy transportowe, firmy energetyczne;

3) utrata, ujawnienie lub modyfikacja danych; w przypadku sektora energetycznego nieuprawniona zmiana wartości sterujących czy celowa modyfikacja wartości obserwowanych może spowodować poważne zakłócenie procesu sterowania; z uwagi na złożoność i wielkość systemu elektroenergetycznego już

nawet jedna awaria kluczowego systemu może spowodować destabilizację całości i wywołać dalsze zniszczenia;

4) dewaluacja reputacji firmy; szkody wywołane atakami hakerów mogą negatywnie wpłynąć na wizerunek firmy oraz obniżyć zaufanie klientów i partnerów biznesowych (Gwoździewicz 2019: 4).

Dobrym podejściem jest podawanie przykładów odnoszących się do konkretnego interesu danej osoby. W przypadku procesu zatrudnienia warto uzmysłowić pracownikowi, jakie mogą być konsekwencje dla niego samego w momencie wycieku danych, co pozwoli mu lepiej zrozumieć zasadność ochrony danych. Raczej nikt nie chciałby usłyszeć przez telefon, że w wyniku incydentu bezpieczeństwa jego dane wyciekły i mogą zostać wykorzystane w działaniach przestępczych polegających na wyłudzaniu pieniędzy. Dlatego w celu ochrony przed tego typu działaniami dobrym rozwiązaniem jest w takiej sytuacji niezwłoczne zastrzeżenie swoich dokumentów, czy kart płatniczych. Władcza postawa IOD, imperatywny sposób przekazywania informacji i zaleceń nie pomogą w powstrzymywaniu niekorzystnego zjawiska, jakim jest niechęć do ochrony danych osobowych w organizacji. Dobry IOD pokazuje ryzyko, jakie wiąże się z określonymi działaniami; uświadamia, jakie mogą być konsekwencje nieprawidłowości; podejmuje próbę uświadomienia pracowników, dlaczego metody, działania i narzędzia, jakimi posługiwali się wcześniej, nie mogą być dalej akceptowane i dlaczego pozostają one w sprzeczności z przepisami. Warto wskazać pracownikom, jakie zagrożenia wiążą się z przetwarzaniem danych i jakie konsekwencje może nieść dla podmiotów danych (a więc także ich samych) brak odpowiedniego zabezpieczenia (Kołodziej 2020: 39).

IOD powinien uczulić pracowników, że najpopularniejszym sposobem zabezpieczenia jest program antywirusowy, dość skuteczny w wykrywaniu oprogramowania *malware*. Kolejnym ważnym elementem jest *firewall*, który filtruje ruch, jaki jest „wpuszczany" do naszego komputera. Te zabezpieczenia jednak nie są wystarczające dlatego warto zwracać uwagę na rankingi i zestawienia przed wyborem odpowiedniego oprogramowania tego typu. Nic nie zastąpi jednak rozwagi użytkownika. Przede wszystkim trzeba zwracać uwagę na zagrożenia płynące z poczty elektronicznej czy przeglądanych witryn internetowych (Jakubik, Wojciechowski 2020).

Konkretna lista zagrożeń w większości przypadków działa na wyobraźnię i pozwala lepiej uświadomić sobie wagę zagrożenia. Przykładami wskazanych działań mogą być: zakładanie i prowadzenie fałszywej działalności, której celem są wyłudzenia VAT, wyłudzanie kredytów gotówkowych i hipotecznych, fałszerstwa dowodów osobistych, paszportów, podszywanie się pod osobę za pomocą fałszywego konta e-mail lub profilu społecznościowego w celu wyłudzania pieniędzy. Wśród pozostałych zagrożeń można wymienić wynajmowanie

mieszkań, pokojów hotelowych, samochodów, przyjmowanie mandatów lub punktów karnych na fałszywe dane, czy zawieranie umów z operatorami telekomunikacyjnymi na fałszywe dane. W trakcie szkoleń można przytoczyć także przykłady wycieków danych i ich częstotliwość. Warto uświadomić uczestnikom szkolenia, że takie przypadki są codziennością – podejście „nas to nie dotyczy" może być zgubne dla organizacji i podmiotów danych (a także pracowników). Za przykład może służyć lista wycieków z okresu od czerwca 2018 r. do lutego 2019 r., które omówiono w mediach branżowych: MyHeritage.com – w czerwcu 2018 r. wyciek dotyczący 92 mln rekordów danych czy Urzędu Skarbowego we Wrocławiu – w czerwcu 2018 r., gdzie udostępniono dla petentów komputer z dostępem do Internetu i drukarki, na którym w folderze „pobrane" znajdowały się wypełnione druki PIT oraz potwierdzenia zapłat, a na biurkach dla petentów – ich wydruki. Kolejne wycieki: we wrześniu 2018 r. – Facebook, gdzie wyciekło 50 mln rekordów danych, następnie wyciek danych osobowych ponad 533 milionów użytkowników Facebooka, w tym dane ponad 2,5 mln Polaków w kwietniu 2019 r. (Prezes Urzędu Ochrony Danych Osobowych, zwany dalej UODO wystąpił do władz Facebook Poland o podjęcie działań w celu ograniczenia ryzyka wykorzystania danych osobowych objętych naruszeniem poprzez zaoferowanie usługi umożliwiającej wszystkim polskim użytkownikom sprawdzenie, czy to naruszenie ich dotyczy; https://uodo.gov.pl/pl/138/2022, dostęp: 06.06.2021), a w październiku 2018 r. – Google, gdzie w wyniku zatajonej luki systemu uzyskano dostęp do 500 tys. rekordów. Nie sposób nie wspomnieć o Wietnamwiza.pl, z której w styczniu 2019 r. wyciekło ponad 3000 skanów polskich paszportów. Powyższe przykłady pokazują, że dane osobowe nie zawsze są bezpieczne – nawet w tak dużych podmiotach jak Google, co do których powinna być pewność w zakresie stosowania najwyższego poziomu bezpieczeństwa. Budowanie świadomości ryzyka pracowników organizacji można dodatkowo poprzeć przykładami, takimi jak sytuacja dotycząca dostępu do danych wystawionych na sprzedaż w Internecie w formie zbiorczej bazy, określonej jako Collection #1. Jest ona sprzedawana nielegalnie w tzw. deepweb lub darknet, będących obszarem sieci Internet, do którego dostęp uzyskuje się za pomocą TOR (ang. The Onion Router) – anonimowej wirtualnej sieci komputerowej. W bazie tej znajduje się 773 mln adresów e-mail i 21 mln haseł pochodzących z ponad 2000 serwisów (także polskich). Wieczysty dostęp do rzeczonej bazy wraz z regularnymi aktualizacjami kosztuje jedynie 45 dolarów. Pracownikom warto też zwrócić uwagę na problem używania przez nich takich samych danych dostępowych (loginy i hasła lub same hasła) w sferze zarówno zawodowej, jak i prywatnej (Kołodziej 2020: 40). Jeżeli przestępca uzyska dane logowania do konta w jednym z tego typu serwisów, to z dużym prawdopodobieństwem

będzie mógł uzyskać dostęp do służbowych zasobów pracownika (Hady-Głowiak 2022).

Z danych przedstawionych w Rezolucji Parlamentu Europejskiego z dnia 3 października 2017 r. w sprawie walki z cyberprzestępczością (2017/2068(INI) Dz. Urz. UE C Nr 346, s. 29) wynika, że 80% europejskich przedsiębiorstw doświadczyło przynajmniej jednego incydentu w zakresie bezpieczeństwa cybernetycznego i że ataki cybernetyczne wymierzone w przedsiębiorstwa często pozostają niewykryte lub nie są zgłaszane. Z różnych badań wynika, że roczny koszt ataków cybernetycznych dla gospodarki światowej jest bardzo wysoki. Obecnie obowiązek ujawniania przypadków naruszenia bezpieczeństwa oraz wymiany informacji o ryzyku, wprowadzony na mocy RODO oraz dyrektywy 2016/1148, przyczyni się do rozwiązania tego problemu poprzez zapewnienie wsparcia dla przedsiębiorstw, w szczególności mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Gwoździewicz 2019: 4).

Zadaniem IOD powinno być uświadomienie konieczności wdrożenia w organizacji lub aktualizacji planu ciągłości działania. Plan ciągłości działania jest niezbędny nie tylko do właściwego oszacowania ryzyka, ale również zaplanowania działań na wypadek cyberataku, na skutek którego może zostać utracona dostępność danych czy też usługa może stać się niedostępna. Dokument ten największe znaczenie powinien mieć dla obszaru IT, gdyż uświadamia, bez jakich danych czy też usług biznes nie może działać i które z nich są kluczowe do tego, by móc nadal funkcjonować. Dobrze przygotowany plan ciągłości działania ukazuje, jakie systemy czy dane, w tym dane osobowe, należy uznać za krytyczne dla działania organizacji (Jakubik, Wojciechowski 2020).

Globalne ataki oprogramowaniem typu *ransomware* zainfekowały dziesiątki tysięcy komputerów w niemal 100 państwach i licznych organizacjach, m.in. w państwowej służbie zdrowia (National Health Service) w Zjednoczonym Królestwie (gdzie wdrożono plan zapobiegania tym cyberatakom w ramach inicjatywy „No More Ransom", który zapewnił ponad 40 darmowych narzędzi do deszyfrowania, umożliwiający ofiarom ataków oprogramowania typu *ransomware* na całym świecie odszyfrowanie zainfekowanych urządzeń) (Gwoździewicz 2019: 6–7).

Nie sposób tu nie wspomnieć o ataku, jaki nastąpił na Urząd Marszałkowski w Krakowie 8 lutego 2021 r., gdzie systemy instytucji zostały zaszyfrowane za pomocą złośliwego oprogramowania, a hakerzy zażądali okupu za ich odblokowanie. Na skutek działania wirusa doszło do „utraty dostępności danych osobowych", w tym m.in. klientów Urzędu (https://www.cyberdefence24.pl/atak-na-urzad-marszalkowski-w-krakowie-nadal-nie-dziala-system-informatyczny, dostęp: 28.03.2021). Podobna sytuacja wystąpiła w Starostwie Powiatowym w Oświęcimiu, które zapłaciło ponad 600 tys. zł za odzyskanie danych po tym,

jak 13 października 2020 r. hakerzy zaatakowali serwer z bazami danych Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej w Oświęcimiu. Starosta oświęcimski o ataku hakerskim powiadomił policję, CERT Polska, czyli zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w Internecie, oraz Urząd Ochrony Danych Osobowych (https://naszkrakow.com. pl/2021/03/10/czy-mamy-do-czynienia-z-seria-atakow-hakerskich/, dostęp: 16.03.2021).

Zatem najczęstszym rodzajem cyberataku, w którym pojawia się żądanie okupu, jest atak z wykorzystaniem *ransomware*, polegający na zainfekowaniu komputera ofiary złośliwym oprogramowaniem przejmującym kontrolę nad jej zasobami i żądaniu okupu w zamian za przywrócenie dostępności i poufności tych zasobów. Jego kluczowym elementem jest szantaż wymuszający za pomocą gróźb określone zachowanie ofiary. Zasadniczym dylematem osoby zaatakowanej jest to, czy spełnić żądanie atakującego i zapłacić okup, nie ma jednak żadnych gwarancji, że integralność i poufność przejętych danych i zasobów nie zostały naruszone, a atakujący przywróci ofierze dostęp do zasobów (Wachta, Troć).

Warto również zwrócić uwagę na fakt, że czas na wykup jest ograniczony, ponieważ podjęcie decyzji o zapłacie staje się utrudnione wraz z upływem czasu, mając na uwadze fakt, że domeny informacyjne są wpisywane na tzw. czarne listy i blokowane. Nie sposób nie zauważyć również faktu, że im później podejmiemy decyzję o zapłacie to cena będzie wzrastać. Z kolei pliki są szyfrowane silnym algorytmem, co nie daje gwarancji, że integralność i poufność przejętych danych i zasobów nie zostały naruszone. Oczywistym faktem jest, że przestępcy nie wystawiają faktur VAT, a zapłata okupu trafia do anonimowego odbiorcy, ponieważ zwykle żądanie okupu wymaga zapłaty w kryptowalucie.

Nie sposób nie wspomnieć tutaj o częstym procederze wykorzystywanym przez firmy oferujące „odzyskanie plików", które w istocie negocjują niższy okup z przestępcami, płacą ten okup, ale same żądają opłaty w wysokości obejmującej okup oraz marżę. Za przykład może tutaj posłużyć rosyjska firma Dr. Shifro, przed którą w grudniu 2018 r. ostrzegała firma Checkpoint. Wskazana firma oferowała odzyskanie plików zaszyfrowanych przez *ransomware* Dharma/Crisis (Maj). Pozostali usługodawcy zwykle w takiej sytuacji nie dają żadnej gwarancji powodzenia, podczas gdy Dr. Shifro gwarantował odblokowanie plików zaszyfrowanych przez *ransomware*, dla którego nigdy nie udostępniono publicznych kluczy. W wyniku przeprowadzonego śledztwa szybko się okazało, że Dr. Shifro w rzeczywistości kontaktował się z twórcą *ransomware*, umawiając się na odszyfrowanie plików ofiary w zamian za płatność okupu (1300 $). Dr. Shifro następnie obciążał ofiarę tym kosztem wraz z dodatkową własną prowizją (za kolejne 1000 $). Pojawienie się w ostatnich latach usług typu Ransomware-as-a-Service pokazuje, że cyberprzestępcy cały czas mają

nowe pomysły na rozwój. Model biznesowy stworzony przez Dr. Shifro jest bardzo atrakcyjny i może z łatwością zostać powielony przez kolejne firmy współpracujące z hakerami, więc zarówno organizacje, jak i osoby prywatne powinny mieć się na baczności (Ścibór).

W związku z powyższym nie zaleca się płacenia okupu, natomiast niezwłocznie zaleca się zgłoszenie incydentu do właściwego CSIRT; warto również zweryfikować na stronie https://www.nomoreransom.org/pl/index.html, prowadzonej z inicjatywy Europolu, czy nie istnieje klucz pozwalający odzyskać zaszyfrowane dane. Jednak najbardziej istotne w przypadku wskazanego ataku jest to, czy administrator dysponuje odpowiednią kopią zapasową, powinien bowiem wykonywać kopie zapasowe w regularnych odstępach czasu, oraz czy aktualizuje oprogramowanie i korzysta z firewalla i programu antywirusowego. Ponadto zapłata okupu w przypadku jednostek sektora finansów publicznych jest mało realna z uwagi na dyscyplinę budżetową.

Powyższe działania mają swoje konsekwencje prawne zarówno dla ofiary, jak i dla poszkodowanego, który ulegnie działaniom przestępców. Działania podejmowane przez hakerów, tj. bezprawne uzyskanie informacji, niszczenie, uszkadzanie, usuwanie lub utrudnianie dostępu do danych informatycznych, zakłócanie prac systemów komputerowych, wytwarzanie określonych programów komputerowych, w tym przystosowanych do popełniania przestępstw hakerskich, a także sprzedaż haseł komputerowych i kodów dostępu umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym – stanowią przestępstwa uregulowane w Kodeksie karnym. W zależności od rodzaju podjętych czynności i ich skutków za ataki hakerskie grozi – jak stanowi Kodeks karny – do trzech lat więzienia. Jeśli w wyniku takiego ataku wyrządzi się „znaczną szkodę majątkową", kara wzrasta do pięciu lat pozbawienia wolności. W przypadku gdy atak dotyczy instytucji państwowych, kara może wzrosnąć nawet do ośmiu lat pozbawienia wolności. Oznacza to, że w przypadku ataku hakerskiego w firmie można rozważyć złożenie do prokuratury zawiadomienia o podejrzeniu popełnienia przestępstwa. Niektóre przestępstwa tego typu są ścigane na wniosek pokrzywdzonego, co oznacza, że prokuratura rozpocznie dochodzenie tylko w przypadku złożenia stosownego wniosku przez pokrzywdzonego. Jeśli haker swoimi działaniami, np. niszcząc dane, wyrządził firmie szkodę, poszkodowana spółka może żądać odszkodowania. W przypadku ataków hakerskich często niemożliwe jest naprawienie szkody poprzez przywrócenie stanu poprzedniego (istniejącego przed atakiem), dlatego najczęściej w takich okolicznościach jedynym racjonalnym żądaniem będzie żądanie zapłaty odszkodowania pieniężnego za poniesione szkody lub utracone korzyści, np. gdy wskutek podjętych działań haker uzyskał korzyść majątkową (np. sprzedał wykradzione dane podmiotowi trzeciemu). W takim przypadku

poszkodowana firma może domagać się zwrotu wartości uzyskanych korzyści (tj. kwoty uzyskanej z tytułu sprzedaży nielegalnie pozyskanych informacji) (Zwierzyńska, Zielepucha).

Jeżeli chodzi o konsekwencje prawne dla poszkodowanego podmiotu związane z podjęciem ewentualnej decyzji o zapłacie okupu za odszyfrowanie danych, to należałoby tutaj przywołać treść art. 296 § 1 Ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 2022, poz. 1138 z późn. zm.), który wskazuje, że kto, będąc obowiązany na podstawie przepisu ustawy, decyzji właściwego organu lub umowy do zajmowania się sprawami majątkowymi lub działalnością gospodarczą osoby fizycznej, prawnej albo jednostki organizacyjnej niemającej osobowości prawnej, przez nadużycie udzielonych mu uprawnień lub niedopełnienie ciążącego na nim obowiązku wyrządza jej znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Z kolei § 3 precyzuje, że jeżeli sprawca przestępstwa określonego w § 1 wyrządza szkodę majątkową w wielkich rozmiarach, podlega karze pozbawienia wolności od roku do lat 10. W świetle powyższego jasne wydaje się, że zapłata okupu generuje ryzyko odpowiedzialności karnej z art. 296 Kodeksu karnego dla szerokiego grona osób decyzyjnych w różnego rodzaju podmiotach. Inaczej niż szkody poniesione bezpośrednio na skutek cyberataku, które są niezależne od woli jakiejkolwiek osoby decyzyjnej, w przypadku zapłaty okupu mamy do czynienia ze świadomą decyzją osób zarządzających zaatakowanym podmiotem. Odpowiedzialność z art. 296 Kodeksu karnego może zmaterializować się w szczególności w sytuacji, gdy zapłata okupu nie przyniesie oczekiwanego rezultatu, tj. atakujący nie przywróci dostępu do przejętych zasobów i danych podmiotu płacącego okup. Jednak nawet jeśli dostęp zostanie przywrócony, taka odpowiedzialność nie jest wykluczona. Jak się bowiem wskazuje, okup płacony jest w najlepszym razie za „czasowy dostęp do swoich danych w nieznanym stanie". W takiej sytuacji niewykluczone jest uznanie, że kwota zapłacona za odzyskanie dostępu do zasobów i danych jest niewspółmierna do uzyskanych w ten sposób korzyści (Wachta, Troć). W przypadku podmiotów jednostek sektora finansów publicznych należy mieć również na uwadze art. 11 ustawy z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych (Dz.U. z 2021, poz. 289 z późn. zm.), zgodnie z którym naruszeniem dyscypliny finansów publicznych jest dokonanie wydatku ze środków publicznych bez upoważnienia określonego ustawą budżetową, uchwałą budżetową lub planem finansowym albo z przekroczeniem zakresu tego upoważnienia lub z naruszeniem przepisów dotyczących dokonywania poszczególnych rodzajów wydatków. Zatem musi istnieć konkretna podstawa prawna do dokonania wydatku.

W przypadku udanego ataku hakerskiego, na skutek którego nastąpił wyciek danych osobowych, każda osoba, która poniosła szkodę majątkową lub niema-

jątkową (np. pracownik firmy), ma prawo żądać od administratora odszkodowania za poniesioną szkodę. Administrator (czyli poszkodowana firma) może jednak uwolnić się od odpowiedzialności poprzez wykazanie, że nie ponosi winy za zdarzenie skutkujące powstaniem szkody, np. udowadniając, że sprostał swoim obowiązkom w zakresie zapewnienia bezpieczeństwa i ochrony przetwarzania danych osobowych (Zwierzyńska, Zielepucha).

Mając powyższe na uwadze, nie sposób nie odnieść się do kontroli Najwyższej Izby Kontroli (zwanej dalej NIK) dotyczącej wprowadzania RODO, jaką przeprowadzono w urzędach dużych miast. We wszystkich kontrolowanych urzędach przed wejściem w życie przepisów RODO opracowano regulacje dotyczące niezbędnych działań, które powinny zostać podjęte w przypadku ewentualnego naruszenia ochrony danych osobowych. Kontrola wykazała natomiast dwa przypadki nieprawidłowego postępowania już po stwierdzeniu naruszenia ochrony danych osobowych, m.in. w Urzędzie Miasta Ciechanów. Cztery osoby zgłosiły tam takie nieprawidłowości w związku z głosowaniem w ramach budżetu obywatelskiego na 2020 r. Prezydent miasta złożył w tej sprawie doniesienie w Komendzie Policji, nie przekazał jednak informacji o naruszeniu danych osobowych Prezesowi UODO, co – według NIK – było niezgodne z RODO. NIK oceniła, że w większości skontrolowanych przypadków działania w reakcji na stwierdzone naruszenia ochrony danych osobowych oraz żądania ich usunięcia lub sprostowania były prowadzone prawidłowo https://samorzad.pap.pl/kategoria/aktualnosci/nik-o-wprowadzaniu-rodo-w-urzedach-duzych-miast-pojedyncze-potkniecia, dostęp: 16.03.2021).

W związku z wszelkimi cyberatakami może dojść do kradzieży czy też braku dostępności danych, w tym danych osobowych. Dlatego tak ważny jest udział IOD w analizie zdarzeń wpływających na cyberbezpieczeństwo oraz zgłaszanie incydentów do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego. Udział IOD pozwala nie tylko na właściwe rozpoznanie, czy doszło do naruszenia danych osobowych, ale również na podjęcie odpowiednich działań. Dodatkowo udział IOD pozwala w przypadku, gdy będzie taka potrzeba, przygotować odpowiednie zgłoszenie do UODO (Jakubik, Wojciechowski 2020).

W przepisie art. 33 RODO, nakładającym na administratorów wymóg zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych, zawarty został ust. 5, w którym przewidziano obowiązek polegający na dokumentowaniu naruszeń oraz wskazano główny cel tego obowiązku. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania niniejszego artykułu. Dla prawidłowego wypełniania obowiązku zgłaszania naruszeń organowi nadzorczemu oraz dokumentowania naruszeń przez administratora istotne jest określenie odpowiedniej procedury postępowania przez osoby przetwarzające

dane (pracowników, osoby wykonujące prace zlecone), które uzyskają informację o podejrzeniu lub zaistnieniu naruszenia ochrony danych osobowych. Osoby takie powinny być obowiązane do zgłoszenia zaistnienia tych okoliczności IOD (bądź innej wskazanej osobie, jeżeli w danej jednostce organizacyjnej inspektor ochrony danych nie został wyznaczony). Nałożenie tego rodzaju obowiązku może znaleźć się w instrukcji postępowania w przypadku podejrzenia lub stwierdzenia naruszenia ochrony danych, która to instrukcja nadal funkcjonuje w wielu jednostkach organizacyjnych (Fajgielski 2019: 176–177).

Nie sposób nie wspomnieć tutaj o karze pieniężnej nałożonej przez Prezesa UODO w wysokości ponad 1,1 mln zł z powodu zbyt później identyfikacji incydentów i powiadamiania o nich osób, których dane dotyczą, oraz zgłaszania naruszeń organowi nadzorczemu. Brak wdrożonych odpowiednich środków organizacyjnych i technicznych pozwalających szybko identyfikować naruszenia powodował, że osoby, których dane dotyczą, przez długi czas nie wiedziały o ryzyku wykorzystania ich danych przez osoby nieuprawnione, np. do tzw. kradzieży ich tożsamości. Nie mogły też przez ten czas podjąć działań, które ograniczyłyby takie niebezpieczeństwo. Nie ma tu znaczenia fakt, że naruszenia związane były z nieprawidłowościami po stronie firmy kurierskiej, ponieważ to właśnie ukarany administrator danych nieprawidłowo realizował nadzór nad egzekwowaniem postanowień umownych, wskutek czego dochodziło do późnej identyfikacji naruszeń (https://uodo.gov.pl/pl/138/2048, dostęp: 06.06.2021).

W ramach ustalania zasad postępowania w sytuacji naruszenia ochrony danych administrator danych powinien określić w nich udział IOD. Zazwyczaj IOD wchodzi w skład zespołu wyznaczanego do wyjaśniania sytuacji związanych z naruszeniami ochrony danych lub podejrzeniami zajścia takich sytuacji. Zdarzają się też rozwiązania, w których powoływany jest zespół ds. wyjaśniania incydentów związanych z bezpieczeństwem informacji, który konsultuje się z IOD jedynie w sytuacjach związanych z podejrzeniem naruszenia ochrony danych, na potrzeby potwierdzenia właściwego stwierdzenia zajścia takiego zdarzenia. Zespół, w którego skład zwykle wchodzi IOD, ma takie zadania, jak analiza zgłoszonych sytuacji podejrzenia naruszenia ochrony danych, stwierdzenie naruszenia ochrony danych, ocena poziomu ryzyka naruszenia praw osób, których dane dotyczą, określenie konieczności zgłaszania zawiadomienia o naruszeniu ochrony danych do Prezesa UODO. Należy tu również wyróżnić pozostałe zadania dotyczące określenia konieczności poinformowania osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych, podejmowania działań zaradczych czy dokumentowania naruszeń ochrony danych osobowych. Podczas zgłoszenia naruszenia IOD jest zazwyczaj wskazywany jako punkt kontaktowy dla organu nadzorczego. W związku z tym przedstawiciele Prezesa UODO prowadzący daną sprawę kontaktują się z IOD w sprawach dotyczących

złożonego wniosku. Zazwyczaj chodzi o doprecyzowanie informacji, np. czy zostały poinformowane osoby, których danych dotyczyło zdarzenie, w sytuacji gdy we wniosku podano przyszłą datę wykonania tej czynności. Zadaniem IOD jest bardzo często również dokumentowanie sytuacji naruszenia ochrony danych (Kołodziej 2020: 13).

Kluczowa jest współpraca oraz nić porozumienia na linii IOD – obszar IT. Inspektor ochrony danych powinien być poinformowany o każdorazowym cyberataku, który nastąpił i na skutek którego mogło dojść do wycieku czy też kradzieży danych, które były danymi osobowymi. IOD powinien być poinformowany nie tylko o konkretnej kradzieży danych, ale również o każdej próbie dostępu do danych. Powinien on po uzyskaniu informacji z obszaru IT sporządzić raport dla administratora danych osobowych o zaistniałej sytuacji, ze szczególnym uwzględnieniem tego, czy działanie miało znamiona naruszenia oraz czy miało wpływ na integralność, poufność i dostępność danych osobowych. Po uzyskaniu informacji IOD powinien w swojej rekomendacji nie tylko zawrzeć faktyczny opis zaistniałej sytuacji, ale również określić, czy działanie miało znamiona naruszenia ochrony danych osobowych, czy też mogło mieć wpływ na wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczyły. Informacje czysto techniczne powinny zostać przedstawione IOD w sposób zrozumiały i zwięzły, gdyż nie jest on zobligowany do posiadania wiedzy w zakresie cyberbezpieczeństwa. Inspektor ochrony danych powinien w organizacji wypracować konkretną ścieżkę zgłaszania tego typu naruszeń/incydentów, gdyż powinien być świadomy występujących zdarzeń oraz ryzyka, które się z tym wiąże. W przypadku gdy IOD oceni, że konkretne zdarzenie nosi znamiona naruszenia danych osobowych, powinien on w terminie 72 godzin od powzięcia informacji poinformować organ nadzorczy o zaistniałym fakcie. W przypadku gdy posiada szczątkowe informacje, zgłoszenie do UODO powinno wpłynąć w takim zakresie, w jakim IOD posiada wiedzę, a następnie powinno być sukcesywnie uzupełniane, by ostatecznie było kompletne (Jakubik, Wojciechowski 2020).

Zarówno zgłoszenie naruszenia ochrony danych, jak i wewnętrzna dokumentacja dotycząca naruszenia ochrony danych muszą spełnić określone wymagania formalne. Na podstawie art. 33 ust. 3 RODO dokumentacja zgłoszenia naruszenia ochrony danych osobowych musi zawierać elementy dotyczące specyfiki naruszenia ochrony danych, danych kontaktowych właściwego punktu kontaktowego, ocenę konsekwencji naruszenia ochrony danych osobowych oraz charakterystykę podjętych lub proponowanych działań w celu uniknięcia podobnych naruszeń ochrony danych w przyszłości. Opis charakteru naruszenia ochrony danych, w myśl art. 33 ust. 3 lit. a RODO, musi zawierać szczegółowe informacje dotyczące kategorii danych osobowych (np. klienci sklepu internetowego), przybliżoną liczbę osób objętych naruszeniem oraz kategorie

i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie (Siemieniak 2020).

Dokumentacja powinna pozwolić organowi nadzorczemu na weryfikowanie przestrzegania przepisu dotyczącego zgłaszania naruszeń; można uznać, że dokumentacja powinna zawierać jeszcze co najmniej jeden element: informację, czy naruszenie zostało zgłoszone do organu nadzorczego, a jeżeli nie, to wskazanie powodów braku zgłoszenia. Wskazany powyżej zakres jest minimalny i może być rozszerzany o inne kategorie informacji, jeżeli administrator uzna to za potrzebne (Fajgielski 2019: 177).

Na podstawie art. 33 ust. 5 RODO administrator danych jest zobowiązany do dokumentowania naruszeń ochrony danych osobowych. Dokumentacja zawarta w rejestrze naruszeń ochrony danych osobowych powinna uwzględniać okoliczności naruszenia, jego skutki oraz wykaz podjętych działań zaradczych. Dokumentacja powinna być na tyle szczegółowa, aby było możliwe prawidłowe zweryfikowanie przestrzegania art. 33 RODO (Siemieniak 2020).

W ramach prowadzenia dokumentacji związanej z naruszeniami ochrony danych osobowych zdaniem Macieja Kołodzieja powinny się tam znaleźć następujące rodzaje dokumentów:

1) zgłoszenia incydentów skutkujących naruszeniem ochrony danych od pracowników poszczególnych działów, od działu IT oraz od podmiotu przetwarzającego;

2) raport z postępowania wyjaśniającego dotyczącego wystąpienia incydentu skutkującego naruszeniem ochrony danych osobowych, w tym ocena poziomu ryzyka naruszenia praw osób, których dane dotyczą, oraz wykaz zaleceń lub działań zaradczych w celu zminimalizowania wystąpienia incydentu w przyszłości;

3) kopia zgłoszenia naruszenia ochrony danych do Prezesa UODO;

4) kopie listów z zawiadomieniami osób, których dane dotyczą, o naruszeniu ich danych osobowych;

5) ewidencja naruszeń ochrony danych osobowych;

6) raport z wykonania zaleceń lub podjęcia działań zaradczych przez poszczególne komórki organizacyjne administratora danych; w ramach przeprowadzania działań zaradczych związanych z naruszeniem IOD powinien przygotowywać materiały informacyjne lub szkoleniowe dla pracowników, dotyczące zaistniałych sytuacji naruszenia, w celu zminimalizowania ryzyka ich wystąpienia w przyszłości (Kołodziej 2020: 14).

Określenie użyte w art. 33 ust. 5 RODO w brzmieniu „administrator dokumentuje wszelkie naruszenia" może być także różnie rozumiane. Pomimo że przepis wyraźnie nie wymaga prowadzenia rejestru naruszeń, to jednak wydaje się, że dokumentowanie naruszeń może być efektywnie realizowane właśnie

w tej postaci, tzn. przez odnotowywanie wszystkich naruszeń w stworzonym specjalnie w tym celu rejestrze (ewidencji). Jednak można uznać, że określenie „dokumentuje" oznacza coś więcej niż tylko odnotowanie informacji i wymaga gromadzenia dokumentów, które mają istotne znaczenie dla oceny zaistniałego naruszenia i dalszego postępowania administratora. Wśród tych dokumentów znaleźć się powinny materiały potwierdzające informacje wskazane w rejestrze naruszeń, w tym m.in. zawiadomienia o podejrzeniu naruszenia składane przez pracowników – jeżeli zostały złożone na piśmie, zgłoszenia pochodzące od podmiotów przetwarzających, jak również kopie zgłoszeń kierowanych do organu nadzorczego. Sformułowanie „wszelkie naruszenia" oznacza, że obowiązek dokumentacyjny jest zakreślony szeroko i obejmuje nie tylko naruszenia, które podlegają zgłoszeniu do organu nadzorczego, ale także naruszenia, z którymi nie wiąże się obowiązek zgłoszeniowy, tzn. naruszenia, w przypadku których administrator uzna, że jest mało prawdopodobne, by naruszenia te skutkowały ryzykiem naruszenia praw lub wolności osób fizycznych (Fajgielski 2019: 178).

Zgodnie z wytycznymi Grupy Roboczej Art. 29 (obecnie Europejskiej Rady Ochrony Danych) dotyczącymi zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 przyjętymi w dniu 3 października 2017 r., IOD powinien odgrywać kluczową rolę we wspieraniu administratora danych w zapobieganiu naruszeniom, przygotowaniu się na wypadek ich wystąpienia oraz w sytuacji wystąpienia takiego naruszenia (Kołodziej 2020: 13). Zalecane jest, aby niezwłocznie informować IOD o wystąpieniu naruszenia oraz włączać go do procesu zarządzania taką sytuacją, w tym do zgłaszania informacji o naruszeniu do organu nadzorczego (Hady-Głowiak 2022).

CERT Polska każdego roku udostępnia raporty dotyczące zagrożeń dla pols 483 incydentów cyberbezpieczeństwa, podczas gdy w 2022 roku liczba ta wynosiła 39 683, co stanowi ponad 30 procentowy ich wzrost w stosunku do roku poprzedniego. Głównym rodzajem zagrożenia pozostaje phishing, który stanowił 25 625 przypadków spośród zarejestrowanych incydentów w 2022 roku. Należy podkreślić, że to administrator danych musi wdrożyć odpowiednie procedury prowadzące do identyfikacji, klasyfikacji, priorytetyzacji, notyfikacji (nie później niż w terminie 24 godzin do właściwego CSIRT) oraz wyeliminowania negatywnych następstw incydentu bezpieczeństwa informacyjnego. Nie sposób nie wspomnieć tutaj o weryfikacji, czy incydent nie stanowi jednocześnie naruszenia przepisów o ochronie danych osobowych w rozumieniu art. 4 pkt 12 RODO. W tym wypadku powstaje również obowiązek powiadomienia osób fizycznych o naruszeniu ich danych „bez zbędnej zwłoki" (ze wskazaniem możliwych konsekwencji naruszenia ich danych osobowych, danych IOD oraz zastosowanych lub proponowanych środków w celu zaradzenia naruszeniu) oraz organu nadzorczego nie później jednak niż w terminie 72 godzin od jego

stwierdzenia. Nie należy również zapomnieć o dokumentowaniu wszelkich incydentów i naruszeń ochrony danych osobowych ze wskazaniem okoliczności wystąpienia incydentu lub naruszenia przepisów o ochronie danych osobowych, jego skutków oraz podjętych działań zaradczych. Kluczowe będzie w tym wypadku wdrożenie odpowiednich zasad i procedur w przypadku wystąpienia incydentu lub naruszenia przepisów o ochronie danych osobowych. Zasadą powinno być, iż każde zdarzenie powinno zostać zgłoszone oraz zarejestrowane. Niezbędnym elementem jest również wdrożenie w każdej organizacji planu ciągłości działania oraz jego bieżąca aktualizacja. Zaangażowanie w ten proces IOD oraz Pełnomocnika ds. cyberbezpieczeństwa, w tym służb IT już na etapie projektowania ww. zasad i procedur w tym zakresie jest niezwykle istotne, podobnie jak odpowiednie działania uświadamiające podejmowane przez wskazane osoby (poprzez wskazywanie na aktualne i bieżące zagrożenia, zasady postępowania w przypadku ich wystąpienia oraz środków zapobiegawczych). Brak odpowiednich zasad i procedur, ich aktualizacji oraz bieżącej analizy ryzyka w tym zakresie może spowodować niepowetowane straty dla Administratora w postaci możliwości utraty posiadanych zasobów, bieżących i przyszłych kontrahentów, straty wizerunkowe oraz ewentualną odpowiedzialność karną, cywilną, czy administracyjną. Ponadto biorąc pod uwagę atak typu *ransomware* warto uwzględnić kilka kluczowych kwestii:

1) zapłata za odszyfrowanie danych nie jest zalecana i może narazić organ zarządzający na odpowiedzialność karną oraz w przypadku jednostek sektora publicznego również w zakresie dyscypliny finansów publicznych z tytułu wydatkowania środków publicznych bez upoważnienia albo z jego przekroczeniem. Ponadto zapłata wspiera działalność przestępczą oraz następuje na rzecz anonimowego odbiorcy, a jej wysokość jest uzależniona od momentu podjęcia decyzji o płatności (im później nastąpi tym opłata jest wyższa);

2) warto zweryfikować, czy nie istnieje metoda odszyfrowania plików na stronie https://www.nomoreransom.org/pl/index.html prowadzonej z inicjatywy Europolu

3) należy zwrócić uwagę na firmy dające „gwarancję" odzyskania zaszyfrowanych plików, bowiem istnieje duże prawdopodobieństwo współpracy z cyberprzestępcami w tym zakresie;

4) należy wdrożyć obowiązek regularnego wykonania kopii zapasowych i weryfikacji ich poprawności oraz aktualizacji oprogramowania;

5) należy obowiązkowo korzystać z systemu antywirusowego i firewalla.

Wspomniana konieczność aktualizacji bieżących zasad i procedur ma również kluczowe znaczenie z uwagi na stale zmieniające się przepisy prawne oraz coraz nowsze zagrożenia w obszarze bezpieczeństwa informacji, tj. Qrshing, czy wykorzystanie do ataków sztucznej inteligencji.

Wykaz skrótów

CSIRT – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego
IOD – Inspektor Ochrony Danych
NIK – Najwyższa Izba Kontroli
UODO – Urząd Ochrony Danych Osobowych

Bibliografia

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.U.UE.L.2016.194.1.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.U.UE.L.2016.119.89.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148, Dz.U.UE.L.2022.333.80.

Rezolucja Parlamentu Europejskiego z dnia 3 października 2017 r. w sprawie walki z cyberprzestępczością (2017/2068(INI)), Dz.Urz. UE C Nr 346.

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, Dz.U.UE.L.2016.119.1.

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz.U. 2022, poz. 1138 z późn. zm.

Ustawa z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych, Dz.U. 2021, poz. 289 z późn. zm.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. Dz.U. 2023, poz. 913.

Opracowania

Fajgielski, Paweł. 2019. Dokumentacja naruszeń ochrony danych osobowych**.** W: *Dokumentacja ochrony danych osobowych ze wzorami*, (red.) Mariusz Jagielski. Warszawa: Wolters Kluwer Polska.

Gwoździewicz, Sylwia. 2019. Problematyka cyberbezpieczeństwa i wzrastającej skali cyberataków a dostęp do Internetu jako wartości dla realizacji praw człowieka. W: *Prawa człowieka i ludzkie bezpieczeństwo. Osiągnięcia i wyzwania. W 70. rocznicę ogłoszenia*

Powszechnej Deklaracji Praw Człowieka, (red.) Daria Bieńkowska, Ryszard Kozłowski. Warszawa: C.H. Beck, legalis.pl. Dostęp: 17.08.2023.

Hady-Głowiak, Stanisław. 2022. *Status prawny Inspektora Ochrony Danych jako audytora w ujęciu administracyjno-prawnym*. Maszynopis. Rozprawa doktorska. Uniwersytet Śląski w Katowicach, https://www.bip.us.edu.pl/pl/doktoraty/mgr-stanislaw-hady-glowiak. Dostęp: 18.08.2023.

Horbaczewski, Robert. 2022. *Gdy urzędnik pracuje w domu, hakerowi łatwiej wejść do urzędu*. Samorząd i Administracja. https://www.prawo.pl/samorzad/ataki-hakerskie-na-serwery-gmin-i-miast,513134.html. Dostęp: 10.08.2023.

Jakubik, Mateusz, Piotr Wojciechowski. 2020. *RODO w IT: atak hakerski a ochrona danych osobowych*. Lex/el. Dostęp: 16.03.2021.

Kołodziej, Maciej. 2020. *Vademecum IOD*. Warszawa: C.H. Beck.

Siemieniak, Piotr. 2020. *RODO w IT*: *atak hakerski i co dalej?* Lex/el. Dostęp: 16.03.2021.

Źródła internetowe

https://digital-strategy.ec.europa.eu/pl/policies/nis2-directive. Dostęp: 10.12.2023.

https://naszkrakow.com.pl/2021/03/10/czy-mamy-do-czynienia-z-seria- atakow-hakerskich/. Dostęp: 16.03.2021.

https://samorzad.pap.pl/kategoria/aktualnosci/nik-o-wprowadzaniu-rodo- w-urzedach-duzych-miast-pojedyncze-potkniecia. Dostęp: 16.03.2021.

https://uodo.gov.pl/pl/138/2022. Dostęp: 06.06.2021.

https://uodo.gov.pl/pl/138/2048. Dostęp: 06.06.2021.

https://www.cyberdefence24.pl/atak-na-urzad-marszalkowski-w-krakowie-nadal-nie-dziala-system-informatyczny. Dostęp: 28.03.2021.

Komisja Europejska. *Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (dyrektywa NIS2).*

Maj, Marcin. Oferowali odszyfrowanie plików, ale tak naprawdę płacili okup i doliczali sobie marżę za usługę, https://niebezpiecznik.pl/post/oferowali-odszyfrowanie-plikow-ale-tak-naprawde-placili-okup-i-doliczali-sobie-marze-za-usluge/. Dostęp: 17.08.2023.

Ścibór, Adrian. Przywracanie plików po ataku ransomware: uwaga na podejrzaną firmę Dr. Shifro, https://avlab.pl/przywracanie-plikow-po-ataku-ransomware-uwaga-na-podejrzana-firme-dr-shifro/. Dostęp: 21.08.2023.

Urząd Ochrony Danych Osobowych. Czerwiec 2019. *Obowiązki administratorów związane z naruszeniami ochrony danych osobowych*. Warszawa. https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjBxJzbtNPvAhWwxIsKHbPpB4sQFjAAegQIBBAD&url=https%3A%2F%2Fuodo.gov.pl%2Fpl%2Ffile%2F2210&usg=AO vVaw1PVnALtheH0KHIb5s325OA. Dostęp: 16.03.2021.

Wachta, Bartłomiej, Maciej Troć. Wybrane ryzyka prawne dotyczące zapłaty okupu w przypadku cyberataku, https://sekurak.pl/wybrane-ryzyka-prawne-dotyczace-zaplaty-okupu-w-przypadku-cyberataku/. Dostęp: 17.08.2023.

Zwierzyńska, Agnieszka, Maciej Zielepucha. Atak hakerski okiem prawnika, https://nowoczesny-przemysl.pl/atak-hakerski-okiem-prawnika/. Dostęp: 21.08.2023.