O efektywnym wdrożeniu domyślnej ochrony danych osobowych w systemach informatycznych

*prof. ALK dr hab. Przemysław Polański**

Privacy by Design to bardziej pewna filozofia postępowania niż precyzyjnie sformułowane obowiązki. Przy jej wdrażaniu pomocne powinny okazać się 7 zasad PbD sformułowanych przez dr *Ann Cavoukian* w pracy „Privacy by Design: The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices", a następnie odzwierciedlone w rezolucji w sprawie prywatności w fazie projektowania przyjętej przez 32 Międzynarodową Konferencję Rzeczników Ochrony Danych i Prywatności w 2010 r.[1].

Privacy by Design to nakaz projektowania systemów informatycznych w taki sposób, aby wszystkie zasady przetwarzania danych osobowych zostały odzwierciedlone w programie komputerowym w jak najszerszym zakresie. *Privacy by Default* stanowi dopełnienie tego obowiązku i zakłada zaprojektowanie systemu w taki sposób, aby domyślnie uruchomione były te opcje programu, które chronią prywatność użytkownika w stopniu najszerszym. Wobec braku orzecznictwa TSUE w tej materii, istotną rolę odgrywać będą Wytyczne nr 4/2019 sformułowane przez Europejską Radę Ochrony Danych Osobowych[2].

Wprowadzenie

Wyciek danych osobowych i ich publikacja w Internecie to jedna z najgorszych rzeczy, jaka może się przytrafić organizacjom w dzisiejszych czasach. Tego typu zdarzenia nie ominęły też kancelarii prawnych, które stały się ofiarami szantaży z jednej strony, a ich klienci – osobami zagrożonymi ujawnieniem sensytywnych danych osobowych znajdujących się w posiadaniu kancelarii. Publikacja tego typu danych narusza prywatność osób fizycznych, a jednocześnie stanowi ujawnienie treści, które są bezprawne i stanowi druzgocące uderzenie w wizerunek kancelarii adwokackiej.

Odpowiedzią prawodawcy unijnego na rosnące zagrożenia w związku z przetwarzaniem danych osobowych w systemach informatycznych miało być uchwalenie ogólnego rozporządzenia dotyczącego ochrony danych osobowych[3]. Choć akt ten stanowił w dużej mierze kontynuację wcześniejszej dyrektywy 95/46/WE[4], której implementację stanowiła rodzima ustawa z 29.8.1997 r. o ochronie danych osobowych[5], zawierał on jednak szereg nowości. Jednym z nich był **obowiązek uwzględniania ochrony danych osobowych w fazie projektowania** w art. 25 RODO (ang. *Privacy by Design*), który miał stanowić jedną z najważniejszych odpowiedzi na rosnące cyberzagrożenia.

Koncentracja na działaniu prewencyjnym, która ma zapewnić ochronę dóbr osób fizycznych, jest jedną z cech charakteryzujących podejście prawodawcy unijnego do regulacji technologii informatycznych przynajmniej od 2016 r. Obok danych osobowych, podobne obowiązki obserwujemy w obszarze ochrony dostępu do interfejsu graficznego serwisów internetowych w stosunku do osób, które przez wzgląd na stałe lub czasowe trudności nie mogą korzystać z myszki czy klawiatury komputera. Przykładowo, niewidzący prawnicy mają obecnie prawo do dostępności cyfrowej internetowych stron publicznych zagwarantowane ustawą o dostępności cyfrowej[6], która wymusza zaprojektowanie internetowych stron publicznych w sposób zgodny z odpowiednimi standardami technicznymi, takimi jak WCAG opracowane oddolnie przez społeczność internetową[7]. Co więcej, od września tego roku, obowiązek ten dotyczy także projek-

* Autor jest prawnikiem i informatykiem; ORCID: 0000-0001-9708-5335. Artykuł powstał w ramach grantu NCN nr DEC- 2014/15/B/HS5/03138 „Model zwalczania bezprawnych treści w Internecie" oraz grantu NCN nr 2016/22/E/HS5/00434 „Model udostępniania treści w Internecie osobom z niepełnosprawnościami zgodnie z obowiązującym prawem krajowym i międzynarodowym oraz zasadami WCAG 2.0.". Artykuł stanowi rozszerzoną wersję publikacji *P. Polański*, Privacy by Design (PbD) – czyli o uwzględnianiu ochrony danych w fazie projektowania systemu teleinformatycznego kancelarii prawnej, s. 107–120, zawartej w monografii pod red. prof. *D. Szostka*, Bezpieczeństwo danych i IT, Warszawa 2020.

[1] Rezolucja w sprawie prywatności w fazie projektowania przyjęta przez 32. Międzynarodową Konferencję Rzeczników Ochrony Danych i Prywatności, która obradowała w Jerozolimie w dniach 27–29.10.2010 r.

[2] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, (dostęp: 10.10.2021 r.), dalej jako: Wytyczne nr 4/2019.

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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. L Nr 119 z 4.5.2016 r., s. 1; dalej jako: RODO.

[4] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.Urz. L Nr 281 z 23.11.1995 r., s. 31 ze zm.

[5] Dz.U. Nr 133, poz. 883, t. jedn.: Dz.U. z 2016 r. poz. 922 ze zm., która została uchylona w związku z wejściem w życie RODO oraz ustawy z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, Dz.U. z 2019 r. poz. 125.

[6] Ustawa z 4.4.2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, Dz.U. z 2019 r. poz. 848.

[7] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2102 z 26.10.2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego, Dz.Urz. L Nr 327 z 2.12.2016 r., s. 1–15, implementowana w Polsce w ustawie o dostępności cyfrowej, która weszła w życie w połowie 2020 r. Dyrektywa 2016/2102 ustanawia wspólne wymogi dostępności dla stron internetowych i aplikacji mobilnych organów sektora publicznego w oparciu o zasady WCAG 2.0 oraz określa wymogi dotyczące oświadczeń w sprawie dostępności, które muszą być udostępnione przez organy sektora publicznego w odniesieniu do zgodności ich stron internetowych i aplikacji mobilnych z tą dyrektywą.

towania aplikacji mobilnych, które odgrywają pierwszoplanową rolę w życiu osób z niepełnosprawnością wzroku. Zarówno więc RODO, jak i wspomniana dyrektywa łączą ze sobą nie tylko daty uchwalenia, lecz także podejście do nakładania obowiązków zapewnienia zgodności z prawem rozwiązań informatycznych tworzonych przez producentów oprogramowania.

Pomysł na to, aby zapewnić ochronę danych osobowych już na etapie projektowania systemów informatycznych, a więc prewencyjnie, a nie reaktywnie, czyli po skutecznym ataku na systemy informatyczne, jest zarówno logiczny, jak i wyprzedza na długo przyjęcie RODO[8]. Łączy się on też np. z obowiązkami nakładanymi w obszarze cyberbezpieczeństwa, które stanowią immanentną część problematyki ochrony prywatności. ENISA w swoim raporcie z 2014 r. podkreślała wagę tzw. PETs, czyli technologii wspierających prywatność, takich jak szyfrowanie danych, które stały się standardem na długo przed rewolucją w ochronie danych osobowych: *„One important element in this endeavour are technical mechanisms, most prominently so-called Privacy-Enhancing Technologies (PETs), e.g. encryption, protocols for anonymous communications, attribute based credentials and private search of databases. Their effectiveness has been demonstrated by researchers and in pilot implementations. However, apart from a few exceptions, e.g., encryption became widely used, PETs have not become a standard and widely used component in system design"*[9].

Kluczowym aspektem zasady PbD (ang. *Privacy by Design*)[10] jest zdolność do zademonstrowania, czyli udowodnienia owej efektywności. Można to uczynić nie tylko poprzez dowód z np. audytu bezpieczeństwa specjalistycznej firmy, ale także poprzez szereg innych działań wskazujących na stałe i realne dbanie o cyberbezpieczeństwo. Problem jednak w tym, że nie do końca wiadomo, co się kryje pod terminem *Privacy by Design* i *Privacy by Default*. Istota i sposób realizacji tej zasady pozostaje nadal wyzwaniem i to nie tylko dla prawników, pomimo wydania wskazówek w tym zakresie w postaci Wytycznych nr 4/2019 przez Europejską Radę Ochrony Danych Osobowych.

Istota *Privacy by Design*

Obowiązek uwzględnienia ochrony prywatności już na etapie projektowania systemów informatycznych będzie mieć doniosłe znaczenie nie tylko dla producentów oprogramowania w Unii Europejskiej, którzy zapewne będą się starać konkurować na tym polu ze sobą, lecz przede wszystkim dla wszystkich podmiotów, które świadczą usługi na rzecz osób fizycznych zlokalizowanych na terytorium Unii Europejskiej, w tym podmiotów takich jak kancelarie prawne, które korzystają z rozwiązań informatycznych przetwarzających dane osobowe swoich klientów. Wytyczne z 2019 r. podkreślają, że **obowiązki zapewnienia prywatności w fazie projektowania obarczają wszystkich kontrolerów bez względu na ich wielkość oraz poziom skomplikowania przetwarzanych danych**, a nie dotyczą bezpośrednio producentów oprogramowania czy procesorów[11]. Ostatecznie, obowiązki obarczają kontrolerów, a więc podmioty, które korzystają z serwisów IT, a nie bezpośrednio samych producentów.

Zasada *privacy by design* to bardziej pewna filozofia działania niż zasada *sensu stricto*. Niemniej, **istotą tej zasady jest wdrożenie efektywnych środków organizacyjnych i technicznych zapewniających ochronę danych osobowych**. Z powyższego wynika szereg obowiązków szczególnych wymienionych w RODO, takich jak obowiązek minimalizacji pozyskiwania danych osobowych, jak najszybszej pseudoanonimizacji danych czy przemyślenia domyślnych ustawień prywatności. Tych obowiązków jest jednak znacznie więcej, co może skłaniać do uznania, że chodzi tu o wykształcenie pewnej postawy przez osoby przetwarzające dane niż o nałożenie jasno określonych obowiązków.

Wytyczne nr 4/2019 koncentrują się nie tylko na technicznych, lecz także organizacyjnych środkach stanowiących jej istotę. **Zapewnienie właściwych szkoleń pracownikom** w zakresie cyberhigieny stanowi jeden ze środków organizacyjnych stanowiących realizację zasady *Privacy by Design*[12]. Innym środkiem będzie zawarcie stosownych umów dotyczących przetwarzania danych osobowych, które wymuszą odpowiednie działania minimalizujące przetwarzanie danych na procesorach. Jeszcze innym środkiem będzie wdrożenie rozwiązań informatycznych zabezpieczających kontrolera przed atakami cybernetycznymi.

Zasada *Privacy by Design* powinna być uwzględniona w szczególności w sytuacji, **gdy planowane są nowe operacje przetwarzania danych**. Obowiązkiem kontrolera danych (np. właściciela kancelarii) jest wdrożenie obowiązku PbD przed rozpoczęciem operacji, jak i monitorowanie wdrażania w trakcie prowadzenia operacji na danych. Zasada zapewnienia ochrony danych osobowych w fazie projektowania zmierza do zapewnienia efektywnej ochrony danych osobowych osób, których dane dotyczą w szczególności poprzez stworzenie gwarancji technologicznych i organizacyjnych, by dane osobowe były domyślnie chronione i nie były udostępniane bez woli danej osoby nieokreślonemu kręgowi osób. Obowiązek ten dotyczy także danych przechowywanych w systemach teleinformatycznych kancelarii prawnych, które muszą być chronione odpowiednio przez cały czas.

Nakaz uwzględniania ochrony danych osobowych w fazie projektowania jest stosunkowo mało wyrazisty. Przez wzgląd na fakt, że stanowi ów nakaz uwzględnienie szeregu obowiąz-

[8] Prace nad koncepcją Privacy by Design trwały co najmniej od połowy lat 90. ubiegłego wieku. Por. *R. Hes, J. Borking*, Privacy-Enhancing Technologies: The Path to Anonymity, 1998; *P. Hustinx*, Privacy by Design: Delivering the Promises, „Identity in the Information Society" Nr 3/2010, s. 253–255 o czym szerzej poniżej.

[9] ENISA, Privacy and Data Protection by Design – from policy to engineering, 2014, s. 3.

[10] Zasada zapewnienia ochrony danych osobowych w fazie projektowania; dalej jako: PbD.

[11] Wytyczne nr 4/2019, s. 4–5. Zob. także motyw 78 RODO, który jedynie zachęca producentów do uwzględnienia zasad ochrony danych podczas projektowania systemów IT: *„When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the »state of the art«, to make sure that controllers and processors are able to fulfil their data protection obligations".*

[12] Wytyczne nr 4/2019, s. 6 *„A technical or organisational measure and safeguard can be anything from the use of advanced technical solutions to the basic training of personnel. Examples that may be suitable, depending on the context and risks associated with the processing in question, includes pseudonymization of personal data4 ; storing personal data available in a structured, commonly machine readable format; enabling data subjects to intervene in the processing; providing information about the storage of personal data; having malware detection systems; training employees about basic »cyber hygiene«; establishing privacy and information security management systems, obligating processors contractually to implement specific data minimisation practices, etc."*

ków szczególnych, a jego zastosowanie w konkretnym przypadku wymaga dodatkowo przeprowadzenia analizy opartej na ryzyku (ang. *risk-based approach*) – wdrożenie PbD z pewnością wywoływać będzie wiele pytań i wątpliwości. Tym bardziej warto, aby jej założenia poznali prawnicy, którzy nie tylko będą musieli doradzać swoim klientom w tym zakresie, ale także samym sobie. Nakaz ten dotyczy bowiem także kancelarii prawnych, które w coraz większym zakresie korzystają z rozwiązań informatycznych przetwarzających duże ilości danych, np. rozwiązań w chmurze obliczeniowej (ang. *cloud computing*), a co za tym idzie wprowadzając własne systemy lub korzystając z ogólnie dostępnych (często darmowych) muszą w pełni stosować *privacy by design*.

Jednocześnie, naruszenie zasady uwzględniania ochrony danych w fazie projektowania (PbD) obarczone jest ryzykiem poniesienia bardzo dotkliwych sankcji finansowych. Takie z kolei podejście przeczy przyjmowaniu założenia, że chodzi tutaj jedynie o pewną filozofię działania, a nie o obowiązek podjęcia konkretnych działań. Warto także zauważyć, że obowiązki wynikające z omawianej zasady nie mogą zostać ograniczone aktem prawnym wydanym przez prawodawcę unijnego albo krajowego, tak jak może mieć to miejsce w przypadku innych obowiązków nałożonych rozporządzeniem ogólnym[13].

Dla uzyskania pełni obrazu warto jeszcze sięgnąć do art. 83(4) RODO, który określa wysokość **administracyjnych kar pieniężnych** za niezastosowanie m.in. zasady PbD. Zgodnie z tym przepisem naruszenia przepisów dotyczących obowiązków administratora podlegają administracyjnej karze pieniężnej w wysokości do 10 mln euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. W przypadku zastosowania mechanizmu dobrowolnej certyfikacji same podmioty certyfikujące ryzykują 10 mln euro za naruszenie swoich obowiązków. Brak zatem realizacji w systemach teleinformatycznych kancelarii prawnej PbD może być dosyć kosztowne.

Podstawa prawna

RODO nie zawiera definicji pojęcia *privacy by design*. Nakaz uwzględnienia ochrony danych w fazie projektowania wyrażony natomiast został w trzech ustępach art. 25 oraz w motywie 78 RODO. Artykuł 25 ust. 1 RODO określa **zakres przedmiotowy** stosowania tego obowiązku, który obejmuje nie tylko fazę projektowania (określania sposobów przetwarzania), ale także fazę realizacji procesu (przetwarzanie):

1. „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, **zaprojektowane w celu skutecznej realizacji zasad ochrony danych**, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą".

Przy dokonywaniu wykładni tego przepisu warto sięgnąć do motywu 78 RODO, który precyzuje jakie środki techniczne i organizacyjne oraz wewnętrzne polityki powinien zaprojektować administrator, po przeprowadzeniu analizy ryzyka naruszenia przepisów, a także specyfiki prowadzonej działalności i kosztów inwestycji. Zgodnie z tym motywem takie środki mogą polegać m.in. na:

- minimalizacji przetwarzania danych osobowych;
- jak najszybszej pseudonimizacji danych osobowych;
- przejrzystości co do funkcji i przetwarzania danych osobowych;
- umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych;
- umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń.

Jednocześnie warto wskazać, że zakres obowiązków ulegnie poszerzeniu, bowiem nadal nie znamy ostatecznej wersji rozporządzenia ePrivacy[14], które ma zastąpić dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z 12.7.2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[15], a które stanowi bardzo ważny brakujący komponent w modelu ochrony prywatności w UE obok przepisów wykonawczych, kodeksów postępowania oraz praktyk regulatorów.

Artykuł 25 ust. 2 RODO koncentruje się na jednym z kluczowych aspektów omawianej zasady, a mianowicie **obowiązku domyślnej ochrony danych**:

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

Wskazany ustęp akcentuje ograniczenie się do przetwarzania danych niezbędnych dla określonego celu przetwarzania, co powoduje konieczność rozważenia przez administratorów zakresu pozyskiwanych i przechowywanych danych. Równie istotna staje się konieczność przeanalizowania domyślnych ustawień w wykorzystywanych systemach informatycznych z perspektywy zapewnienia jak najszerszej ochrony prywatności.

Waga omawianej zasady wynika także z konsekwencji, jakie ona wywołuje nie tylko dla administratorów, ale przede wszystkim

[13] Por. art. 23 RODO dotyczący podstaw prawnych umożliwiających ograniczenie zakresu obowiązków i praw przez prawodawcę krajowego lub unijnego przez wzgląd na m.in. ważne cele leżące w ogólnym interesie publicznym czy ochronę postępowania sądowego i niezależności sądów oraz egzekucję roszczeń cywilnoprawnych.

[14] Chodzi o projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), który miał zostać przyjęty wraz z RODO, ale od 5 lat nie udało się wypracować wspólnego stanowiska m.in. w kwestiach bezpieczeństwa, VOIP, cookies, czy marketingu wykorzystującego pocztę elektroniczną. Por. https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52017PC0010&from=EN (dostęp: 28.10.2021 r.).

[15] Dz.Urz. L Nr 201 z 31.7.2002 r., s. 37 ze zm.