**Daria Worgut-Jagnieża, Agnieszka Świerczyńska,
Agnieszka Szalińska, Ewa Boboli, Joanna Noga–Bogomilska,
Milena Kraszewska, Michał Madecki,
Jan Kurowski, Kacper Szułkowski**

MONITOROWANIE I TESTOWANIE ZGODNOŚCI Z RODO Z PERSPEKTYWY PRAWNIKA I INFORMATYKA

Stan prawny na dzień 1 czerwca 2021 r.

Warszawa 2021

Spis treści

1. Metody monitorowania zgodności z regulacjami w zakresie ochrony danych. Jak zachować zgodność z RODO?

Każda organizacja, która gromadzi, przechowuje i przetwarza dane osób z Unii Europejskiej, musi wykazać zgodność z RODO. Nie ma przy tym znaczenia jej forma prawna, cel, sektor czy też lokalizacja. Organizacja może znajdować się w dowolnym miejscu na świecie, ale tak długo, jak ma do czynienia z danymi osobowymi Europejczyków, jest zobowiązana przestrzegać RODO. Dotyczy to zarówno podmiotów, będących administratorami danych, jak i podmiotów przetwarzających.

Jaka jest różnica pomiędzy administratorem a podmiotem przetwarzającym?

Status administratora oznacza uprawnienie do decydowania o tym, jakie dane będą przetwarzane, jak długo, kto będzie miał do nich dostęp oraz jakie środki bezpieczeństwa należy podjąć w celu ich ochrony (art. 4 pkt 7 RODO).

Podmiot przetwarzający natomiast przetwarza dane osobowe w imieniu administratora i zgodnie z jego wskazówkami (art. 4 pkt 8 RODO). Istnienie podmiotu przetwarzającego zależy od decyzji podjętej przez administratora, który może przetwarzać dane w ramach swojej organizacji (np. za pośrednictwem własnych pracowników) lub przekazać całość lub część działań związanych z przetwarzaniem danych zewnętrznemu podmiotowi.

Zgodnie z opinią Grupy Roboczej art. 29 1/2010 w sprawie pojęć" administrator danych" i „przetwarzający" (WP 169) – klasyfikowanie podmiotów odpowiednio jako administrator i podmiot przetwarzający ma charakter obiektywny i następuje w związku z konkretnymi okolicznościami, podejmowanymi decyzjami gospodarczymi, ocenia kto w tych okolicznościach podejmuje decyzje co do celu przetwarzania danych osobowych oraz sposobów, jakimi się ono odbywa.

Oznacza to, że strony nie mogą umówić się w jakich rolach występują. Jest to stan faktyczny, który występuje obiektywnie i niezależnie od ich woli.

Pierwszym krokiem do osiągnięcia przez organizacje zgodności z RODO jest zrozumienie jej obowiązków, poznanie aktualnych procesów i zidentyfikowanie wszelkich luk.

Istotne jest by nie traktować zapewnienia zgodności z RODO jako kwestii czysto prawnej lub informatycznej – będzie ona musiała być prowadzona, wdrażana i wzmacniana w całej organizacji, przy ciągłym i wspólnym zaangażowaniu zespołów prawnych, informatycznych, zgodności, ryzyka i audytu wewnętrznego.

Dlaczego zapewnienie zgodności z RODO jest ważne dla organizacji?

Nieprzestrzeganie przepisów może oznaczać karę finansową w wysokości do 20 mln EUR lub 4% rocznego obrotu – w zależności od tego, która z tych kwot jest wyższa. Większość organizacji przestraszy się – i słusznie – skali ryzyka finansowego związanego z podwyższonymi karami. Koszty finansowe niezgodności z przepisami są znaczące, na skalę, która może doprowadzić do bankructwa mniejsze lub bardziej finansowo zagrożone organizacje.

Inne zagrożenia finansowe związane z nieprzestrzeganiem przepisów, to koszty prawne i ewentualne odszkodowania wypłacane stronom postępowania, jeśli ludzie zdecydują się pozwać organizację za niewłaściwe obchodzenie się z ich danymi osobowymi.

Udowodniona niezgodność z przepisami, zwłaszcza jeśli towarzyszy jej wysoka kara finansowa jest wiadomością z pierwszych stron gazet w kraju, a być może i na świecie. Utrata dobrego wizerunku organizacji może być trudniejsza do odbudowy niż koszty związane z obowiązkiem zapłaty kary.

Na co należy zwrócić uwagę w pierwszej kolejności?

Każda organizacja, która przetwarza dane obywateli UE, musi zapoznać się z podstawowymi zasadami zawartymi w art. 5 RODO. Zasady te należy traktować jako przewodnie reguły postępowania administratorów i podmiotów przetwarzających, określające jednocześnie ich podstawowe powinności[1].

[1] Arleta Nerka, Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, Warszawa 2018 pod red. M. Sakowska – Baryła str. 142

I. Zasada zgodności z prawem, rzetelności i przejrzystości

Przetwarzanie danych jest legalne, jeżeli znajduje podstawy w art. 6 ust. 1 oraz art. 9 ust. 2 RODO, następuje z uwzględnieniem zasad współżycia społecznego. Osoby fizyczne muszą mieć możliwość zrozumienia, co dzieje się z ich danymi osobowymi, aby była zapewniona przejrzystość przetwarzania (patrz art. 13–14 RODO).

II. Zasada ograniczenia celu

Oznacza, że uzasadniony lub konkretny cel gromadzenia danych, o którym należy poinformować podmiot danych. Zasada wyklucza zbieranie danych na zapas, bo może w przyszłości te dane będą administratorowi do czegoś potrzebne.

III. Zasada minimalizacji danych

Minimalizacja danych ma na celu ograniczenie zbierania danych do możliwie najniższego poziomu, umożliwiającego realizację celów przetwarzania.

IV. Zasada prawidłowości

Dane osobowe muszą być prawidłowe, a także aktualizowane. W związku z tym należy przewidzieć możliwość sprostowania, a jeśli to możliwe, usunięcia wszelkich niedokładnych danych osobowych.

V. Zasada poufności i integralności

Dane osobowe powinny być przetwarzane w sposób gwarantujący bezpieczeństwo danych osobowych osób fizycznych. Obejmuje to ochronę danych przed nieuprawnionym, bezprawnym przetwarzaniem, a także przed przypadkową utratą lub uszkodzeniem.

VI. Zasada ograniczenia przechowywania

Dane osobowe mogą być przechowywane tylko tak długo, jak długo istnieje jeszcze potrzeba ich przechowywania. Okres przechowywania może wynikać bezpośrednio z przepisów prawa – wtedy sprawa jest prosta – po upływie terminów ustawowych dane należy usunąć. W przypadku gdy brak jest takich przepisów administrator sam musi ustalić okres przechowywania danych pamiętając, że

jest on zdeterminowany celem przetwarzania – brak celu oznacza brak możliwości przechowywania danych.

VII. Zasada rozliczalności

Królową wszystkich wymienionych powyżej zasad jest zasada rozliczalności zgodnie, z którą organizacja ma obowiązek wykazać przestrzeganie wszystkich wskazanych powyżej zasad oraz udokumentować podjęte działania oraz decyzje w sprawie wyboru konkretnych rozwiązań.

Podkreślenia wymaga fakt, że RODO w ramach neutralności technologicznej nie wskazuje administratorowi środków, które mają zapewnić zgodność. Wskazuje jedynie, że mają to być odpowiednie środki techniczne i organizacyjne, które w razie potrzeby należy przeglądać i uaktualniać. Polityki ochrony danych są wskazane jako jedne z tych środków (art. 24 RODO). Adekwatność wdrożonych środków administrator powinien udowodnić przeprowadzoną analizą ryzyka.

Dokumentacja systemu ochrony danych osobowych

Dokumentacja stanowi istotną część systemu mającego zapewnić zgodność z RODO. RODO wprost reguluje kwestie związane z prowadzeniem rejestru czynności przetwarzania danych (rejestr ten prowadzi administrator) oraz rejestru kategorii czynności (ten z kolei prowadzi podmiot przetwarzający), zasady obowiązku powołania inspektora ochrony danych i przeprowadzenia DPIA. Jednak by zapewnić sprawne funkcjonowanie zasad ochrony danych w organizacji powinny funkcjonować procedury, które wyjaśniają m. in. jakie w konkretnym przypadku należy podjąć działania, do kogo zgłosić podejrzenia naruszenia, jakie są zasady przeprowadzenia analizy ryzyka w organizacji.

Zaproponowana poniżej lista polityk/procedur jest punktem wyjścia do stworzenia przez organizację własnej dokumentacji, która zapewni sprawne zarzadzanie ochroną danych osobowych oraz w przypadku kontroli organu nadzorczego będzie stanowiła jeden z dowodów zapewnienia przez organizację zgodności z RODO.

Rejestr czynności przetwarzania danych osobowych/rejestr kategorii czynności

Administratorzy danych oraz podmioty przetwarzające mają obowiązek prowadzenia odpowiednio rejestru czynności lub rejestru kategorii czynności. Art. 30 RODO wskazuje ich obligatoryjne elementy:

- nazwa i dane kontaktowe administratora danych oraz, w stosownych przypadkach, wspólnego administratora danych, przedstawiciela administratora danych i inspektora ochrony danych;
- cele przetwarzania;
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
- w stosownych przypadkach, międzynarodowe przekazywanie danych osobowych oraz dokumentacja odpowiednich zabezpieczeń;
- jeśli to możliwe, przewidywane terminy usunięcia różnych kategorii danych;
- jeśli to możliwe, ogólny opis wdrożonych technicznych i organizacyjnych środków bezpieczeństwa.

Obowiązek dotyczący prowadzenia rejestrów nie ma zastosowania do organizacji, które zatrudniają mniej niż 250 osób, chyba że:

- przetwarzanie może powodować ryzyko dla praw i wolności osób, których dane dotyczą;
- przetwarzanie nie ma charakteru sporadycznego lub
- przetwarzanie obejmuje dane szczególnych kategorii lub dane dotyczące wyroków skazujących i przestępstw.

Z doświadczenia zalecamy prowadzenie rejestrów nawet w sytuacji, gdy nie jest to obligatoryjnie.

Rejestr jest jednym z narzędzi, które zapewnia realizacje zasady rozliczalności i przejrzystości. Nawet jeśli organizacja zatrudnia mniej niż 250 pracowników, prowadzenie dokumentacji jest istotną częścią ułatwiania osobom, których dane dotyczą, korzystania z ich praw, a prawidłowo prowadzony rejestr to ułatwia. Dodatkowo wskazany w art. 30 zakres rejestru nie stanowi katalogu zamkniętego co umożliwia dodanie innych elementów, które ułatwiają realizacje zasady rozliczalności. Do takich elementów można zaliczyć podstawy przetwarzania danych w danym procesie, sposób realizacji obowiązku informacyjnego, czy też wskazanie czy dany proces wymaga przeprowadzenia DPIA.

Procedura reakcji na incydenty i zgłaszania naruszeń ochrony danych

Art. 33 RODO nakłada na wszystkich administratorów danych obowiązek zgłaszania organowi nadzorczemu, niektórych (nie wszystkich) naruszeń danych osobowych, w ciągu 72 godzin od uzyskania informacji o naruszeniu. W przypadku, gdy naruszenie może spowodować wysokie ryzyko niekorzystnego wpływu

na prawa i wolności osób fizycznych, należy również bez zbędnej zwłoki poinformować te osoby.

Aby cały proces przeszedł sprawnie dobrze jest mieć opisane w sposób przejrzysty procedury, dotyczące wykrywania naruszeń, ich zgłoszeń w ramach organizacji, podejmowanych środków zaradczych.

ICO przygotował tzw. listę kontrolą, która może służyć jako punkt wyjścia do opracowania stosownej procedury. Lista jest dostępna pod linkiem https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ dostęp z dnia 26.04.2021 r.

Lista kontrolna składa się z dwóch części:

Przygotowanie na naruszenie	Reagowanie na naruszenia
– wiemy, jak rozpoznać naruszenie danych osobowych; – rozumiemy, że naruszenie danych osobowych to nie tylko utrata lub kradzież danych osobowych; – przygotowaliśmy plan reagowania na wszelkie naruszenia ochrony danych osobowych; – przydzieliliśmy odpowiedzialność za zarządzanie naruszeniami dedykowanej osobie lub zespołowi; – nasi pracownicy wiedzą, jak przekazać incydent bezpieczeństwa do odpowiedniej osoby lub zespołu w naszej organizacji, aby ustalić, czy doszło do naruszenia.	– wdrożyliśmy proces oceny prawdopodobnego ryzyka dla osób fizycznych w wyniku naruszenia; – dysponujemy procesem informowania poszkodowanych osób o naruszeniu, gdy ich prawa i wolności są zagrożone; – wiemy, że musimy bez zbędnej zwłoki informować poszkodowanych; – wiemy, kto jest właściwym organem nadzorczym dla naszych działań związanych z przetwarzaniem; – posiadamy proces powiadamiania organu o naruszeniu w ciągu 72 godzin od uzyskania informacji, nawet jeśli nie znamy jeszcze wszystkich szczegółów; – wiemy, jakie informacje musimy przekazać organowi o naruszeniu; – wiemy, jakie informacje o naruszeniu musimy przekazać osobom fizycznym i że powinniśmy udzielać porad, aby pomóc im chronić się przed jego skutkami; – dokumentujemy wszystkie naruszenia, nawet jeśli nie wszystkie muszą być zgłaszane.

Uwzględnienie i rozwinięcie powyższych punktów zapewni organizacji sprawną obsługę ewentualnych incydentów, a tym samym wypełnienie obowiązków nałożonych przez RODO.

Procedura analizy ryzyka

Na administratora został nałożony obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, które zapewnią zgodne z RODO przetwarzanie danych. Decyzja o tym jakie to mają być środki została pozostawiona administratorowi, który przy wyborze konkretnych zabezpieczeń musi wykazać, że uwzględnił charakter, zakres, kontekst i cele przetwarzania danych oraz ryzyko naruszenia praw i wolności podmiotów danych (art. 24 RODO).

RODO nie wskazuje żadnych metodologii analitycznych, które ma zastosować administrator, a ich dobór zależy m.in. od rodzaju przetwarzanych danych (dane szczególnych kategorii wymagają dodatkowych zabezpieczeń), jak również od możliwości organizacyjnych i finansowych administratora.

Niebagatelne znaczenia ma też ogólne podejście zarządu do tematyki ochrony danych w organizacji.

Polski organ nadzorczy przygotował dwuczęściowy poradnik (Jak rozumieć podejście oparte na ryzyku według RODO? oraz Jak stosować podejście oparte na ryzyku?), który ma pomóc organizacjom w przyjęciu odpowiednich rozwiązań. Poradniki dostępne są na stronie Urzędu Ochrony Danych Osobowych pod linkiem https://uodo.gov.pl/pl/123/208.

Procedura weryfikacji i wyboru podmiotu przetwarzającego

Administrator część usług może a czasami musi przekazać podmiotom zewnętrznym – czyli podmiotom przetwarzającym. Decydując się na powyższe administrator danych musi wykazać, że wybrany przez niego podmiot zapewnia należyte gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Procedura weryfikacji i wyboru podmiotu przetwarzającego stanowi dowód na spełnienie tego obowiązku. Procedura ta powinna określać metody weryfikacji podwykonawcy (mogą to być m.in. ankiety, zatwierdzone kodeksy postepowania, mechanizmy certyfikacji, czy też normy ISO), jak często podwykonawca jest weryfikowany.

Procedura privacy by design i privacy be default

Planowanie nowych działań, które wiążą się z przetwarzaniem danych osobowych zgodnie z art. 25 ust.1 RODO powinno uwzględniać ochronę danych osobowych w fazie projektowania – privacy by design, jak również kontynuować tę ochronę danych osobowych – podczas całego cyklu przetwarzania danych osobowych (tj. do chwili ich usunięcia) – privacy by default.

Privacy by design oznacza, że już na etapie planowania nowych działań lub zmian w realizowanym już działaniu (np. wdrożenie nowego systemu

IT, organizacja nowego typu działań marketingowych), zostaną uwzględnione niezbędne wymagania prawne oraz dobre praktyki dotyczące ochrony danych osobowych.

Privacy by default sprowadza się do weryfikacji w danym procesie. Przetwarzane są tylko dane niezbędne dla osiągnięcia konkretnego celu przetwarzania.

Procedura realizacji praw podmiotów danych

Organizacje nie mają obowiązku posiadania powyższej procedury – jednak z uwagi na określone w RODO terminy realizacji żądań warto mieć dokument, który wyjaśni, jak należy postępować z poszczególnymi wnioskami, pomoże w wypracowaniu modelu związanego z weryfikacją tożsamości osoby składającej wniosek, formą udzielania odpowiedzi, wskaże co zrobić, gdy wniosek jest nieprecyzyjny oraz w jakich przypadkach należy odmówić realizacji wniosku. Warto wskazać osoby/ zespoły, do których obowiązków będzie należało udzielenie odpowiedzi oraz sposobu dostarczenia przez inne działy niezbędnych do jej udzielania informacji.

Podnoszenie świadomości i wiedzy pracowników

Wdrożenie ochrony danych osobowych w organizacji, to nie tylko posiadanie polityk i procedur zatwierdzonych przez zarząd, ale przede wszystkim ich stosowanie przez wszystkich pracowników mających dostęp do danych oraz projektujących procesy i rozwiązania technologiczne, które będą wiązały się z przetwarzaniem danych osobowych.

Oznacza to nie tylko odpowiednie przeszkoleniem pracowników, ale przede wszystkim wypracowanie właściwej komunikacji pomiędzy poszczególnymi działami zaangażowanymi w dany proces. W tym miejscu mocny nacisk należy położyć na problem szkolenia pracowników.

Każda organizacja niezależnie od formy prawnej działa poprzez swoich pracowników.

To pracownicy są na pierwszej linii przetwarzania danych. Tym samym mogą być albo najsłabszym ogniwem organizacji i przez ich działania może dojść do naruszenia albo jako pierwsi mają możliwość zaalarmowania, że mogło dojść do ataku hackerskiego na systemy informatyczne organizacji. Wszystko zależy od tego na ile organizacja zainwestowała w ich szkolenia z ochrony danych osobowych.

Niestety najczęstszą praktyką jest jedno ogólne szkolenie w ramach szkoleń wstępnych realizowanych podczas zatrudniania pracownika.

To jednak za mało. Zagadnienia związane z danymi osobowymi nie są wcale takie proste i w zależności od specyfiki branży oraz działu, w którym jest

pracownik, ma on do czynienia z różnymi danymi i różnymi problemami związanymi z ich przetwarzaniem.

Dlatego istotne jest prowadzenie cyklicznych szkoleń ukierunkowanych na poszczególne działy. Najbardziej efektywne są interaktywne warsztaty, podczas których pracownicy mają możliwość wyjaśnienia wszystkich wątpliwości oraz rozwiązują kazusy nawiązujące do przypadków, z którymi mogą się spotkać w czasie wykonywania swoich czynności służbowych. Istotne jest również przeprowadzenie szkoleń w przypadku zmiany stanu prawnego, który ma wpływ na zakres przetwarzanych przez nich danych.

Kolejnym krokiem jest przeszkolenie pracowników z wdrożonych w organizacji procedur. Nie chodzi o to by pracownicy znali te procedury na pamięć, ale by mieli świadomość ich funkcjonowania, wiedzieli, gdzie znajdą wyciągi z tych procedur oraz do kogo mają zgłosić ewentualne naruszenie, czy też wątpliwości związane z przetwarzaniem danych.

Zapewnienie zgodności z RODO to proces ciągły, a nie jednorazowa czynność. Organizacja musi przestrzegać zasad określonych w RODO i prowadzić odpowiednią dokumentację potwierdzającą ich przestrzeganie. Skala dokumentacji powinna być dostosowana do wielkości i złożoności organizacji, a system zapewnienia zgodności powinien również obejmować szkolenia i świadomość pracowników.

2. Audyt zgodności z wymogami RODO – od czego zacząć zapewnienie zgodności z RODO i jak ją utrzymać?

Aby zadbać o zgodność organizacji administratora danych z wymogami RODO warto przeprowadzić czy raczej regularnie przeprowadzać audyt, aby sprawdzić, czy mechanizmy kontrolne, polityki i procedury stosowane przez organizację są odpowiednie, a jeśli nie, to gdzie należy je poprawić, a czasami po prostu je stworzyć.

W RODO nie ma wyraźnego obowiązku prawnego przeprowadzania audytów. Zobowiązuje ono jedynie organizacje do przeprowadzania regularnych przeglądów technicznych i organizacyjnych środków bezpieczeństwa (np. poprzez testy penetracyjne) w zależności od ryzyka związanego z przetwarzaniem danych (art. 32 ust. 1 lit. d) RODO).

Kompleksowe audyty mogą jednak ułatwić organizacjom udowodnienie zgodności z RODO. Z jednej strony audyt ocenia wewnętrzne wdrożenie wymogów RODO i odpowiednio je dokumentuje. Dokumentacja ta może służyć jako dowód zgodności organizacji z RODO dla organu nadzorczego np. podczas przeprowadzanej kontroli czy też odpowiedzi na skargę podmiotu danych. Nawet jeśli audyt nie dostarczy pełnego dowodu zgodności, udokumentuje on odpowiednie wysiłki i zasadniczo będzie musiał zostać uwzględniony na korzyść organizacji przy ustalaniu wysokości kary. Z drugiej strony, audyt może ujawnić wewnętrzne błędy i niedociągnięcia we wdrażaniu RODO, a tym samym wskazać organizacjom konieczność dostosowania się w celu zapewnienia pełnej zgodności.

Od wejścia w życie RODO minęły już prawie 3 lata a nadal wielu organizacjom nie udało się w pełni go wdrożyć. Ponadto audyty oferują „sprawdzenie rzeczywistości". Znaczna część organizacji, wdrażając wymagania RODO, działała pod presją czasu. W wielu przypadkach początkowo opracowano procesy i sporządzono wytyczne, ale faktyczne przestrzeganie ich w codziennej pracy organizacji jest często zaniedbywane. Wielokrotnie stworzone standardy nie są praktykowane lub są wdrażane niekonsekwentnie (np. wewnętrzne systemy informatyczne nie są dostosowane do wewnętrznych standardów lub zobowiązania