Rozdział I. Opis metodyki przeprowadzenia kontroli zgodności z RODO

1. Uwagi ogólne

Zgodność z RODO jest procesem ciągłym trwającym przez cały czas przetwarzania danych osobowych przez administratora. Przez zgodność z RODO należy rozumieć przyjęte w organizacji zasady realizacji poszczególnych obowiązków oraz poziomy bezpieczeństwa danych osobowych, bowiem niektóre obszary będą przewidywały działanie na zasadzie ryzyka, jego minimalizacji i zarządzania nim, ale nie jego pełne wyeliminowanie. Nie można osiągnąć zgodności z RODO raz i uznać, że wypełniliśmy już swoje obowiązki w tym zakresie. Ciągłość procesów związanych ze zgodnością z RODO występuje na kilku płaszczyznach:

1) **skuteczności wdrożenia** – weryfikacji, czy ustanowione w organizacji zasady realizacji obowiązków RODO oraz procedury wewnętrzne są przestrzegane przez pracowników;
2) **uzupełniania procedur RODO** – weryfikacji nowych przypadków dotyczących przetwarzania danych osobowych pod względem zgodności z RODO i w razie potrzeby wprowadzania nowych zasad w celu zapewnienia zgodności z RODO;
3) **kontroli skuteczności stosowanych rozwiązań** – weryfikacji, czy wprowadzone zasady i procedury zapewniają w praktyce zgodność z RODO, czyli czy są właściwe, wystarczające oraz ergonomiczne dla tej organizacji.

Niezgodność z RODO, pomimo przeprowadzonego procesu wdrożenia, może wynikać z różnych przyczyn, z których najczęściej spotykanymi są:

1) **nieprzeprowadzenie wdrożenia przyjętych zasad i procedur przez pracowników**, tj. sytuacja, w której organizacja zapewniła opracowanie i przyjęcie do stosowania niezbędne zasady przetwarzania danych osobowych oraz procedury postępowania, ale nie zostały one skutecznie przekazane pracownikom do stosowania;
2) **niedopasowanie przyjętych procedur postępowania do organizacji**, przez co pracownicy, pomimo nakazu ich stosowania, nie przestrzegają ich;

3) **niekompletność projektu wdrożeniowego**, tj. niepełne przeprowadzenie inwentaryzacji zasobów zawierających dane osobowe, co powoduje, że pomimo wdrożenia RODO nadal są w organizacji obszary niezweryfikowane lub niedostosowane do wymogów RODO;
4) **brak procedur zapewniających weryfikację nowych przypadków związanych z przetwarzaniem danych osobowych i uzupełnianie wdrożonych zasad i procedur zgodnie z potrzebami**, co powoduje, że zgodność z RODO jest zapewniana wyłącznie w zakresie objętym projektem wdrożeniowym, a wszystkie nowe przypadki, niezweryfikowane podczas wdrożenia, nie są weryfikowane pod względem zgodności z RODO i powodują występowanie nowych niezgodności;
5) **niekompletność wdrożonych zasad i procedur**, tj. pozostawienie niektórych obszarów nieuregulowanych, co powoduje, że obszary te są niezgodne z RODO.

Ważne

Aby uniknąć występowania niezgodności, niezbędne jest przeprowadzenie kontroli wdrożenia RODO, a następnie przeprowadzanie cyklicznych kontroli zgodności. W przeciwnym razie zgodność z RODO w organizacji będzie trwała krótko, a czasami w ogóle nie nastąpi, pomimo przeprowadzenia pełnego projektu wdrożeniowego.

Pierwszym krokiem do kontroli zgodności z RODO – jak w każdym innym przypadku – powinno być odpowiednie przygotowanie projektu przeprowadzenia kontroli wdrożenia lub zgodności RODO w organizacji. W ramach przygotowania należy:

1) określić ogólny zakres prac projektowych;
2) określić wykaz komórek wewnętrznych organizacji (dla uproszczenia komórki wewnętrzne będziemy określać jako działy, ale w zależności od wielkości organizacji i stosowanej terminologii mogą to być poszczególne obszary obowiązków realizowane przez poszczególnych pracowników, działy, wydziały, departamenty, piony itd.), które będą objęte projektem;
3) określić osoby, które będą uczestniczyły w realizacji projektu, reprezentując poszczególne działy;
4) podjąć decyzję, kto będzie koordynował projekt;
5) rozważyć, czy organizacja jest w stanie przeprowadzić wdrożenie w ramach własnych zasobów, czy będzie potrzebowała wsparcia zewnętrznego;
6) opracować ogólny harmonogram projektu;
7) opracować techniczne zasady realizacji projektu;
8) oszacować budżet projektu;
9) pozyskać odpowiednie wsparcie kierownictwa organizacji.

2. Ogólny zakres prac projektowych

Ponieważ celem do osiągnięcia jest kontrola wdrożenia RODO, zakres prac projektowych będzie obejmował wszystkie obowiązki, jakie RODO nakłada na podmioty, które przetwarzają dane osobowe. Jeżeli natomiast przeprowadzamy kontrolę zgodności z RODO w ramach cyklicznych działań bieżących, możemy zdecydować się na przeprowadzanie

rzadszych, lecz kompleksowych kontroli lub kontroli bieżących obejmujących wybrane obszary, np. wybrane obowiązki RODO lub wybrane działy organizacji.

Znaczna większość obowiązków RODO to obowiązki formalne, które mogą być realizowane organizacyjnie, za pomocą środków technicznych, jakie już posiadamy lub z użyciem nowych technologii, np. dedykowanych narzędzi IT wspierających realizację niektórych obowiązków RODO i pozwalających zaoszczędzić czas specjalisty RODO. W zależności od tego, jak liczebna jest organizacja oraz jakie usługi świadczy, będziemy dobierać odpowiednie dla nas i dla naszej organizacji rozwiązania, które mogą, ale nie muszą pociągać za sobą konieczność poczynienia inwestycji finansowych. Jeżeli organizacja jest niewielka, a świadczone usługi nie opierają się na skomplikowanych procesach przetwarzania danych osobowych, można realizować zgodność z RODO z nakładem finansowym jednego etatu lub nawet mniejszym. Im większa organizacja oraz im bardziej złożone procesy przetwarzania danych osobowych, tym nakłady czasowe będą większe, może też pojawić się potrzeba poniesienia inwestycji finansowych.

W ramach przygotowania organizacji do rozpoczęcia projektu kontroli wdrożenia RODO należy określić, czy obszar IT i bezpieczeństwo teleinformatyczne sieci i systemów będzie objęte zakresem jednego projektu, czy temu obszarowi zostanie poświęcony oddzielny projekt. Jeżeli organizacja ma własną sieć teleinformatyczną i na bieżąco dba o bezpieczeństwo teleinformatyczne, tj. ma wdrożone odpowiednie zabezpieczenia teleinformatyczne oraz specjalistę ds. bezpieczeństwa teleinformatycznego, lub jeżeli nie ma własnej sieci teleinformatycznej, tj.:

1) korzysta z outsourcingu IT w pełnym zakresie, tj. u siebie posiada wyłącznie stacje robocze (komputery, laptopy), lecz dane przechowuje na hostowanych serwerach lub w chmurze,
2) nie posiada serwerów, a w firmie działa kilka – kilkanaście niepołączonych ze sobą komputerów,
3) nie posiada żadnych dedykowanych programów do przetwarzania danych osobowych, a korzysta wyłącznie z programów typu Word, Excel, poczta elektroniczna

– wówczas obszar IT powinien w całości wchodzić w zakres projektów z obszaru RODO.

Jeżeli jednak organizacja posiada własną sieć teleinformatyczną, lecz do tej pory nie korzystała ze specjalistów ds. bezpieczeństwa teleinformatycznego, np.:

1) posiada własną serwerownię,
2) komputery posiadane przez organizację są ze sobą połączone,
3) posiada więcej niż jedną lokalizację fizyczną firmy i te lokalizacje są ze sobą połączone,
4) korzysta z dedykowanych programów, w których przetwarzane są dane osobowe,
5) posiada własne bazy danych

– warto przeprowadzać projekty RODO dwutorowo, rozdzielić kwestie związane z RODO oraz kwestie wynikające z bezpieczeństwa teleinformatycznego i połączyć te dwa projekty dopiero po otrzymaniu wyników kontroli z obszaru IT i bezpieczeństwa teleinformatycznego przeprowadzonej przez podmiot profesjonalny w tych obszarach. Specjalista RODO nie będzie bowiem posiadał wystarczającej wiedzy technicznej, aby skutecznie zadbać również o obszar bezpieczeństwa teleinformatycznego.

Ważne

Do najczęściej popełnianych błędów należy mylenie obsługi IT z bezpieczeństwem teleinformatycznym i zakładanie, że skoro został zatrudniony informatyk lub organizacja korzysta z zewnętrznej firmy informatycznej, to tym samym ma zapewnioną obsługę w obszarze bezpieczeństwa teleinformatycznego. Jest to duży błąd. Owszem, każdy informatyk obsługujący nasz sprzęt teleinformatyczny zna i wprowadza elementy bezpieczeństwa teleinformatycznego, lecz bezpieczeństwo teleinformatyczne to pewna odrębna całość, której najczęściej nasza obsługa informatyczna nie świadczy nam kompleksowo, a jeżeli tak się dzieje, to nadal pozostaje kwestia nadzoru. Mówiąc obrazowo: IT dba o to, żeby działało, a BTI o to, żeby nikt z zewnątrz ani z wewnątrz nie robił niczego, do czego nie jest lub nie powinien być uprawniony. A więc, jeżeli korzystamy z obsługi IT, sprawdźmy umowę, zapytajmy informatyka, poprośmy o dokumentację bezpieczeństwa teleinformatycznego i upewnijmy się, czy na pewno mamy zapewnione bezpieczeństwo w tym obszarze.

Jeżeli okaże się, że nasza organizacja potrzebuje wdrożenia bezpieczeństwa teleinformatycznego, ten obszar może okazać się dla nas kosztowny ze względu na konieczność poczynienia inwestycji finansowych w odpowiednie zabezpieczenia teleinformatyczne, których naszej organizacji brakuje, a i specjaliści od bezpieczeństwa teleinformatycznego nie są tani. O tym, na ile RODO wymusi od nas zajęcie się tematem BTI, zadecydują zasoby danych osobowych, jakie przetwarzamy. Może się bowiem okazać, że mimo iż ten temat jest u nas zupełnie zaniedbany, ze względu na niewielki zakres przetwarzania danych osobowych (np. tylko dane kontaktowe, korespondencja mailowa oraz bieżące projekty pism) wystarczą podstawowe zabezpieczenia. Zazwyczaj jednak przetwarzamy znacznie obszerniejsze zasoby danych osobowych i nasze zabezpieczenia powinny zapewniać skuteczną ochronę poufności danych osobowych. Pamiętajmy o tym, że **bezpieczeństwo informacji oraz bezpieczeństwo teleinformatyczne to odrębny od RODO obszar i nie dotyczy wyłącznie danych osobowych, lecz także bezpieczeństwa informacji, tajemnicy przedsiębiorstwa, bezpieczeństwa naszych finansów**. Wdrożenie bezpieczeństwa informacji i bezpieczeństwa teleinformatycznego w organizacji jest konieczne nie tylko ze względu na RODO i ochronę danych osobowych, a koszty wdrożenia i utrzymania odpowiedniego stanu bezpieczeństwa można podzielić na kilka wewnętrznych źródeł budżetowania organizacji.

Podobnie będzie przy kontroli bezpieczeństwa danych osobowych w systemach informatycznych. Niektóre obszary mogą być kontrolowane przez IOD, lecz kompleksowa weryfikacja poprawności wdrożenia RODO oraz cykliczne kontrole bezpieczeństwa teleinformatycznego powinny być przeprowadzane przez specjalistów w swojej dziedzinie.

Następnie możemy przystąpić do opracowania ogólnego zakresu projektu. Przykładowy zakres projektu wygląda następująco:

1) inwentaryzacja zasobów zawierających dane osobowe;
2) określenie celów przetwarzania danych osobowych oraz zakresów danych osobowych przetwarzanych do tych celów;
3) prowadzenie rejestru czynności przetwarzania danych osobowych;
4) legalność danych osobowych;
5) ocena zasady minimalizacji danych osobowych;
6) retencja danych osobowych;
7) obowiązki informacyjne;

8) realizacja praw osób, których dane osobowe dotyczą;
9) powierzanie przetwarzania danych osobowych;
10) udostępnianie danych osobowych innym podmiotom;
11) upoważnienia do przetwarzania danych osobowych;
12) obowiązek zachowania w tajemnicy;
13) procedury regulujące realizację obowiązków RODO:
    a) zasada rozliczalności,
    b) certyfikacje,
    c) bezpieczeństwo techniczne i organizacyjne;
14) ocena skutków dla ochrony danych;
15) informowanie o naruszeniach;
16) obowiązek powołania IOD;
17) transfer danych osobowych do państw trzecich.

3. Działy organizacji, które będą objęte projektem

Ustalenie działów organizacji, które będą objęte projektem kontrolnym wdrożenia RODO, nie będzie stanowiło dla nas żadnego wyzwania, bowiem udział w projekcie powinna wziąć cała organizacja, tj. każdy obszar jej działalności. W toku projektu będziemy bowiem weryfikować kompletność i poprawność identyfikacji czynności przetwarzania danych osobowych oraz dokonywać kontroli zgodności z RODO realizacji poszczególnych obowiązków, w których określone obszary będą brały udział lub nie. Nawet jeżeli w toku projektu okaże się, że określony dział nie przetwarza żadnych danych osobowych, może on uczestniczyć w obowiązkach związanych z bezpieczeństwem, np. z bezpieczeństwem fizycznym budynków czy z bezpieczeństwem teleinformatycznym. W związku z tym nawet pewność, że określony dział jest wyłączony spod przetwarzania danych osobowych, nie determinuje tego, że nie będzie on realizował żadnych obowiązków RODO.

Ważne

Do często popełnianych błędów należy wyłączenie z projektu wdrożeniowego RODO niektórych działów lub obszarów działalności organizacji, zakładając, że nie uczestniczą one w realizacji żadnych obowiązków RODO, ponieważ albo w ogóle nie przetwarzają danych osobowych, albo przetwarzają dane osobowe w bardzo niewielkim zakresie, a więc są nieważne z punktu widzenia projektu. Jeżeli tak postąpimy, narażamy się na ryzyko pozostawienia niezweryfikowanych niektórych obszarów, które mogą okazać się ważnym ogniwem przetwarzania danych osobowych lub bezpieczeństwa tych danych. Często okazuje się, że obszary, w których wydawałoby się, że nie są przetwarzane dane osobowe, w rzeczywistości przetwarzają je, a błędne założenie wynika z nieprawidłowej interpretacji definicji danych osobowych lub przetwarzania danych osobowych. Ponadto, nawet jeśli określony obszar faktycznie nie jest związany z samymi danymi osobowymi, może być ważnym elementem bezpieczeństwa i wyłączenie go z projektu może spowodować znaczącą lukę w systemie zabezpieczeń, która narazi organizację na podwyższone ryzyko błędów niezgodności z RODO.

W toku realizacji projektu bardzo szybko okaże się, które działy będą zaangażowane w pełni w kontrolę wdrożenia RODO, a które będą jedynie towarzyszyły pozostałym działom.

Najłatwiej określić wykaz działów uczestniczących w projekcie, wykorzystując do tego wewnętrzną dokumentację organizacji: schemat i regulamin organizacyjny. Jeżeli w naszej organizacji te dokumenty nie zostały jeszcze opracowane, powinniśmy to zrobić – przy okazji projektu RODO lub w ramach oddzielnego działania. Te dwa dokumenty pozwalają bowiem skutecznie zarządzać organizacją oraz przypisać określonym pracownikom odpowiedzialność za poszczególne obszary.

Zarówno **schemat organizacyjny**, jak i **regulamin organizacyjny** powinny określać nie tylko nazwy poszczególnych pionów czy działów organizacji, ale obejmować wykaz wszystkich stanowisk pracy: od szefostwa organizacji, przez wyższą i średnią kadrę menadżerską aż po szeregowe stanowiska pracy. Schemat organizacyjny nie musi zawierać imion i nazwisk aktualnych pracowników, ale powinien przewidywać wszystkie aktualnie funkcjonujące stanowiska pracy wraz z określeniem ich nazw lub funkcji. Imiona i nazwiska powinny znaleźć się co najmniej przy stanowiskach szczebla menadżerskiego, aby nie pozostawiało wątpliwości, kto imiennie jest odpowiedzialny za poszczególne obszary działalności organizacji. Regulamin organizacyjny powinien natomiast określać główne zadania poszczególnych wewnętrznych komórek organizacyjnych. W regulaminie organizacyjnym powinny znaleźć się zakresy kompetencji poszczególnych stanowisk wewnątrz danej komórki organizacyjnej, przy czym każde zadanie komórki organizacyjnej powinno zostać przypisane do któregoś ze stanowisk pracy tak, aby nie pozostawały obszary odpowiedzialności komórki organizacyjnej nieprzypisane do żadnego stanowiska pracy.

Najłatwiejszym sposobem jest skorzystanie ze schematu organizacyjnego, poddanie analizie wszystkich stanowisk i stworzenie listy wszystkich obszarów działalności organizacji, zarówno tych stanowiących główną jej działalność (*core* działalności organizacji), jak i obszarów wspomagających, administracyjnych (*back office* organizacji).

4. Osoby, które będą uczestniczyły w realizacji projektu, reprezentując poszczególne obszary

Jak już zostało powiedziane, w projekcie powinny wziąć udział wszystkie działy organizacji. Następnym krokiem jest zatem wskazanie reprezentantów poszczególnych działów, bowiem to ci reprezentanci będą zarówno reprezentować interesy swojego działu, jak i wykonywać lub koordynować wykonywanie poszczególnych zadań przez te działy w ramach projektu. Reprezentantami powinni być członkowie kadry menadżerskiej, bowiem tylko oni będą mieli realną możliwość koordynacji prac wewnątrz obszaru, który reprezentują, a gdy zajdzie taka potrzeba, również dyscyplinowania wyznaczonych pracowników do rzetelnej i terminowej realizacji zadań w ramach projektu.

Ważne

Często popełnianym błędem jest niewłaściwe umocowanie członków zespołu projektowego do działania. Jeżeli członkami zespołu będą osoby niemające możliwości skutecznego zobowiązywania pracowników do rzetelnej realizacji zadań obszaru w ramach projektu oraz do dotrzymywania ustalonych terminów projektowych, część zadań nie zostanie wykonana, a więc projekt będzie

obarczony ryzykiem niepełności, ponadto będzie występowało podwyższone ryzyko nieterminowości, co może negatywnie wpływać na realizację całego projektu, a w skrajnym przypadku uniemożliwić jego zakończenie.

W ten sposób zostanie utworzony zespół projektowy. Liczebność tego zespołu będzie zależała od liczby działów i obszarów w organizacji, stopnia skomplikowania procesów przetwarzania danych osobowych oraz od liczby pracowników. Jeżeli organizacja ma niewielu pracowników, może okazać się, że tworzenie zespołu projektowego jest niecelowe, a jedna osoba jest w stanie sama zagłębić się we wszystkie obszary działalności firmy i wykonać całość projektu, a osoby odpowiedzialne za poszczególne obszary będą jedynie odpowiedzialne za udzielanie niezbędnych informacji.

Jeżeli natomiast organizacja ma dużą liczbę pracowników lub procesy przetwarzania danych osobowych są skomplikowane, w zespole projektowym powinny znaleźć się nie tylko osoby należące do szczebla menadżerskiego, ale także – albo zamiast – osoby bezpośrednio odpowiedzialne za poszczególne obszary zadań, bowiem to one będą miały pełną i bezpośrednią wiedzę o wszystkich aspektach dotyczących danych osobowych przetwarzanych w organizacji.

Ważne

Z doświadczenia autorki wynika, że w każdym przypadku zespół projektowy nie powinien przekraczać 20–25 osób. Większa liczba osób w zespole może utrudnić skuteczną komunikację w zespole, zbyt rozproszyć odpowiedzialność za poszczególne zadania i tym samym powodować ryzyko niepowodzenia projektu. Jeżeli projekt wymaga uczestnictwa zdecydowanie większej liczby osób, należy zastanowić się nad zasadnością utworzenia piramidy zarządzania projektem, wówczas członkowie zespołu projektowego szczebla menadżerskiego są pośrednikami pomiędzy koordynatorem projektu i pracownikami.

Ogólna lista członków zespołu projektowego powinna obejmować następujące osoby:

1) przedstawiciela głównego kierownictwa, np. jednego z członków zarządu, asystenta zarządu,
2) kierownika sprzedaży,
3) kierownika produktu lub produktów,
4) kierownika obsługi posprzedażnej,
5) kierownika *call center*,
6) kierownika działu skarg i reklamacji,
7) kierownika działu marketingu,
8) kierownika PR,
9) kierownika HR,
10) przedstawiciela BHP,
11) głównego księgowego,
12) kierownika IT,
13) przedstawiciela działu prawnego,
14) przedstawiciela zespołu audytu wewnętrznego, *compliance*,
15) kierownika pionu administracyjnego,
16) osobę odpowiedzialną za flotę samochodową,
17) osobę odpowiedzialną za zarządzanie pocztą przychodzącą i wychodzącą,

18) kierownika ochrony,
19) po jednym przedstawicielu związków zawodowych działających w organizacji,
20) przedstawiciela pracowniczej kasy zapomogowo-pożyczkowej.

5. Wyznaczenie project managera i koordynatora projektu

Kolejnym ważnym, a czasami wręcz kluczowym krokiem jest podjęcie decyzji o tym, kto będzie koordynował projekt, czyli powołanie project managera. W zależności od tego, jak duża i zasobna jest organizacja, można zdecydować się na:
1) koordynatora zewnętrznego lub wewnętrznego,
2) koordynatora merytorycznego lub organizacyjnego.

Ważne

W przypadku przeprowadzania kontroli wdrożenia RODO osobą, która będzie koordynatorem merytorycznym, nie może być osoba, która prowadziła projekt wdrożeniowy. Jeżeli bowiem osoba będzie kontrolowała swoją własną, dopiero co wykonaną pracę, jest oczywiste, że nie dostrzeże swoich własnych błędów, uchybień czy alternatywnych rozwiązań.

Bieżące kontrole zgodności z RODO mogą, a wręcz powinny być przeprowadzane przez naszego specjalistę RODO/IOD, lecz wówczas również warto zapewnić raz na kilka lat kompleksową kontrolę przeprowadzaną przez specjalistę niezależnego od specjalisty RODO/IOD, jako wsparcie jego działań. O to, by takie kontrole zewnętrzne były przeprowadzane, a budżet na nie zapewniony przez organizację, powinien zadbać sam specjalista RODO/IOD w ramach zapewniania weryfikacji stosowanych rozwiązań. Z uwagi na zapewnioną przez RODO merytoryczną niezależność IOD w wykonywaniu swoich zadań podejmowanie decyzji o kontroli zewnętrznej przez organizację może zostać uznane za próbę ingerencji w tę niezależność. Zdaniem autorki przyznanie IOD niezależności w wykonywaniu swoich zadań nie oznacza jednak, że organizacja nie ma żadnych możliwości weryfikacji merytorycznej stanu ochrony danych osobowych przez osoby niezależne od IOD. Przeciwna interpretacja stanowiłaby bowiem zagrożenie zarówno dla organizacji, jak i dla osób, których dane dotyczą ze strony nierzetelnych IOD. Jeżeli zatem weryfikacja jest przeprowadzana profesjonalnie, przez specjalistów w zakresie RODO, jest wcześniej planowana i nie jest skutkiem określonej decyzji podjętej przez IOD w celu wywarcia nacisku na IOD na zmianę tej decyzji, a celem tej weryfikacji jest wsparcie IOD w wykonywaniu jego zadań, a nie szukaniem powodów do jego odwołania, ani IOD, ani organ nadzoru nie powinni kwestionować takich działań organizacji. Jest bowiem sprawą oczywistą, że każdy popełnia błędy, a ich podłoże może być różne i nie musi wynikać ze złej woli IOD. Ważnym czynnikiem generującym uchybienia jest rutyna, w szczególności, jeżeli osoba wykonuje te same obowiązki od dłuższego czasu w jednej organizacji, błędy mogą być też skutkiem niezapewnienia IOD odpowiedniego wsparcia merytorycznego: szkoleń materiałów edukacyjnych, konsultacji zewnętrznych.

Ponieważ niniejsza publikacja ma na celu przedstawienie projektu kontrolnego krok po kroku w sposób umożliwiający jego samodzielne przeprowadzenie przez organizację –

małe lub średnie przedsiębiorstwo. Dla jej potrzeb zdecydujemy się na koordynatorów wewnętrznych: jednego koordynatora merytorycznego i jednego organizacyjnego, który będzie project managerem. Takie rozwiązanie ma w ocenie autorki najwięcej zalet, jednak wymaga pełnego zaangażowania koordynatora merytorycznego, w większości wyłączając go z ewentualnych innych zadań na czas trwania projektu.

Zadaniem koordynatora merytorycznego będzie merytoryczne przeprowadzenie projektu, czyli dokonywanie wszystkich spraw dotyczących RODO:

1) ustalanie zakresu potrzebnych informacji, materiałów i dokumentów,
2) opracowywanie dokumentów wykorzystywanych w ramach projektu (np. formularzy),
3) analiza pozyskanych materiałów, ich ocena pod kątem zgodności z RODO,
4) analiza możliwych sposobów realizacji obowiązków RODO,
5) ocena materiałów przygotowywanych przez poszczególne obszary,
6) podejmowanie decyzji merytorycznych,
7) dokonywanie konsultacji w właściwymi obszarami.

Na koordynatora merytorycznego wybieramy osobę, która będzie pełniła w organizacji funkcję specjalisty RODO, a jeżeli zdecydujemy się na powołanie IOD wewnętrznego, to właśnie ta osoba nim zostanie. W ten sposób zapewnimy, że:

1) podczas realizacji projektu specjalista RODO pozna dobrze organizację, co znacząco ułatwi mu wykonywanie swoich zadań w przyszłości,
2) projekt będzie zarządzany przez osobę, która ma największą wiedzę dotyczącą RODO w organizacji, a tym samym koordynator na bieżąco będzie mógł modyfikować zakres projektu, a w razie potrzeby także jego harmonogram, podejmując decyzje korzystne z merytorycznego punktu widzenia, a nie tylko organizacyjnego,
3) przy okazji przeprowadzania projektu specjalista RODO nabierze nowej wiedzy i doświadczenia w zakresie merytorycznym RODO, samodzielnie mierząc się z wszystkimi ważnymi do analizy i rozstrzygania zagadnieniami.

Minusem takiego rozwiązania jest brak wsparcia merytorycznego specjalisty RODO z zewnątrz – specjalista RODO jest pozostawiony samemu sobie, chyba że zapewnimy mu częściowe wsparcie zewnętrzne w zakresie, w jakim będzie tego potrzebował.

Jeżeli zdecydujemy się na wyznaczenie osobnego project managera, jego zadaniem będzie wyłącznie zarządzanie realizacją projektu, czyli wszystkimi sprawami organizacyjnymi:

1) organizacją spotkań zespołu,
2) ustalaniem terminów realizacji poszczególnych zadań,
3) egzekwowaniem dotrzymywania terminów,
4) zbieraniem prac poszczególnych obszarów, w razie potrzeby ich kompilowaniem, obróbką niemerytoryczną (np. powielanie, umieszczanie w jednym, wyznaczonym folderze sieciowym),
5) opracowywaniem dokumentacji projektowej,
6) zarządzaniem budżetem projektu,
7) składaniem sprawozdań z realizacji projektu,
8) rozliczaniem realizacji projektu.

Dzięki powołaniu osobnego project managera:

1) uwolnimy koordynatora merytorycznego od obowiązków administracyjno-technicznych, oszczędzając mu dużo czasu i tym samym wpływając na przyspieszenie realizacji projektu,
2) zapewnimy nadzór organizacyjny nad realizacją projektu,
3) zapewnimy ciągłość działania na stanowiskach project managera oraz specjalisty RODO.

Aby to osiągnąć, powinniśmy tak wybrać project managera projektu, aby uczestniczył we wszystkich działaniach organizacji i w razie nagłej potrzeby był w stanie zastąpić w projekcie, choćby czasowo, specjalistę RODO.

Ważne

Częstym błędem jest niepowołanie odrębnego project managera, którego zadaniem będzie zarządzanie organizacyjne projektem. Brak nadzoru nad przestrzeganiem harmonogramu powoduje ryzyko utraty kontroli nad realizacją harmonogramu projektu, co w skrajnym przypadku może spowodować niepowodzenie całego projektu – jego nieukończenie. Można uniknąć tego ryzyka poprzez zobowiązanie koordynatora merytorycznego projektu do cyklicznego raportowania realizacji harmonogramu najwyższemu kierownictwu.

Jeżeli natomiast zdecydujemy się na zewnętrznego koordynatora merytorycznego, to każdy specjalista ma własny, wypracowany sposób przeprowadzania wdrożeń, będący sumą wcześniejszych doświadczeń eksperta i jeżeli zdecydowaliśmy się podjąć współpracę z tym specjalistą, powinniśmy mu zaufać i pozwolić pracować zgodnie z jego własnymi założeniami. Nie oznacza to, że nie mamy prawa do weryfikacji stosowanych lub planowanych do stosowania rozwiązań czy podejmowania prób dostosowania ich do własnych potrzeb, bowiem każda organizacja różni się specyfiką działalności organizacyjnej, branżowej i stosowane rozwiązania, mimo że oparte na pewnym wypracowanym już schemacie, powinny zostać każdorazowo zmodyfikowane z uwzględnieniem indywidualnych potrzeb organizacji. Jeżeli chcemy wprowadzić określone zmiany w projekcie, przedstawmy ekspertowi problem, który pojawił się po naszej stronie (nawet, jeśli to jest „tylko" duże niezadowolenie naszego kierownictwa czy jednego z działów), pomysł na rozwiązanie tego projektu i poddajmy go dyskusji z ekspertem, ale nie naciskajmy w obliczu rzetelnych argumentów eksperta wykluczających wprowadzenie proponowanej zmiany. Dobry ekspert ma wiedzę i doświadczenie pozwalające na zaproponowanie kilku alternatywnych sposobów realizacji projektu w danym obszarze i sam również powinien wyjść naprzeciw naszym oczekiwaniom i znaleźć rozwiązanie pozwalające przeprowadzić projekt skutecznie, lecz chociaż częściowo wyeliminować powstały w organizacji problem. Jednak nie spodziewajmy się zbyt wiele – w ciągu 11 lat osobistego doświadczenia autorka nie spotkała organizacji, w której projekt dotyczący ochrony danych osobowych byłby witany z radością, nie powodował dodatkowej ilości pracy w organizacji i nie wprowadzał zmian.

Jednak jeżeli po analizie zgłoszonych przez nas uwag czy pomysłów ekspert zewnętrzny nadal rekomenduje swoje rozwiązanie i nie mamy obiektywnych wątpliwości co do powodów tej rekomendacji (np. wątpliwość mogłaby pojawić się, gdybyśmy proponowali rozwiązanie bezpłatne, a nasz ekspert usilnie przekonuje nas do rozwiązania płatnego

i nie przedstawia nam powodów, dla których nasze rozwiązanie nie może być zgodne z RODO), powinniśmy zaufać naszemu ekspertowi i pozwolić mu realizować projekt zgodnie z jego założeniami lub poszukajmy innego wsparcia merytorycznego.

W przypadku, gdy nasze zastrzeżenia dotyczą kwestii merytorycznych, a rozmowy z ekspertem nie zadowalają nas, w razie potrzeby warto sięgnąć po opinię innego eksperta, np. poprosić naszą obsługę prawną o weryfikację, porozmawiać ze znajomym IOD, o którym wiemy, że ma wiedzę wystarczającą do udzielenia nam rzetelnej porady, skierować zapytanie o poradę w tym jednym obszarze do innego eksperta czy zewnętrznej kancelarii prawnej specjalizującej się w RODO.

Ważne

Częstym błędem jest nadmierne ingerowanie organizacji w sposób realizacji projektu tworzący jedną, kompleksową całość, wcześniej zaakceptowaną na poziomie koncepcyjnym. Zdarza się, że angażujemy wykonawcę z zewnątrz, który jest ekspertem w dziedzinie RODO i ma odpowiednie doświadczenie w przeprowadzaniu wdrożeń. Sprawdziliśmy posiadaną wiedzę i doświadczenie wykonawcy, jego kompetencje i zasoby ludzkie, zaufaliśmy mu i zawarliśmy stosowną umowę o współpracę. Następnie, na etapie realizacji projektu, notorycznie ingerujemy w sposoby lub metodykę przeprowadzania projektu przez naszego wykonawcę zewnętrznego z powodów niemerytorycznych: ponieważ uważamy, że na coś nie mamy czasu, że coś jest niepotrzebne, na wyrost, z powodu ogólnego niezadowolenia pracowników spowodowanego koniecznością uczestnictwa w projekcie. W ten sposób powodujemy, że efekt końcowy będzie różnił się od tego, na co zawarliśmy umowę. Czasami nie zdajemy sobie sprawy, jak pewne zmiany, które nam wydają się drobne i niewiele znaczące dla całego projektu, łącznie powodują duże różnice. Na przykład odstąpienie od przeprowadzenia działań identyfikacyjnych w jednym obszarze, czasami nawet u jednego pracownika, nam wydaje się nieznaczące, podczas gdy może okazać się, że w ten sposób powodujemy, że cały projekt będzie miał obszar, w którym nie wdrożyliśmy RODO.

6. Analiza czy organizacja jest w stanie przeprowadzić kontrolę w ramach własnych zasobów

Jeżeli zdecydowaliśmy się prowadzić projekt samodzielnie z użyciem zasobów wewnętrznych, musimy przeprowadzić analizę, czy nasz koordynator merytoryczny ma wiedzę i doświadczenie w zakresie ochrony danych osobowych wystarczające do skutecznego i rzetelnego zrealizowania projektu. Jeżeli mamy wśród naszych pracowników specjalistę w dziedzinie ochrony danych osobowych, będzie on odpowiednią osobą do poprowadzenia projektu RODO. Jeżeli jednak nasz koordynator merytoryczny to osoba, która została oddelegowana do zajmowania się tym obszarem mimo nieposiadania odpowiedniego przygotowania merytorycznego, musimy mieć świadomość, że nie będzie ona w stanie samodzielnie zadecydować o niektórych kwestiach merytorycznych w trakcie realizacji projektu, a każdy błąd, pozostawienie kwestii nierozstrzygniętej lub tylko częściowe zajęcie się określonym tematem na etapie wdrożenia będą powracać przez długi czas lub będą wielokrotnie powielane w toku dalszej działalności organizacji, a wdrożenie RODO będzie niepełne. Jeżeli mamy świadomość niepełnego przygotowania specjalisty RODO do pełnienia tej funkcji, zapewnijmy mu wsparcie zewnętrzne na czas realizacji projektu, aby mógł w pełni wywiązać się ze swojego zadania, a przy okazji podwyższyć

swoje kompetencje w obszarze RODO. W zależności od tego, na jakim poziomie zaawansowania merytorycznego znajduje się nasz specjalista RODO oraz od stopnia skomplikowania naszych procesów przetwarzania danych osobowych wsparcie będzie wymagało od nas mniejszej lub większej inwestycji finansowej, lecz inwestycja ta jest nie tylko niezbędna, dla zgodności z RODO, ale także zwróci nam się w postaci wiedzy nabytej specjalisty. Tak zdobyta wiedza będzie bardziej efektywna dla specjalisty niż odbycie kilku szkoleń, bowiem będzie miał eksperta zewnętrznego do swojej własnej dyspozycji oraz będzie nabywał wiedzę w praktyce. W zależności od naszych potrzeb, ale również możliwości finansowych, możemy dobrać ofertę dla nas odpowiednią:

1) **bieżące wsparcie zewnętrzne podczas całego projektu kontrolnego RODO** – opcja kosztowna, lecz zapewni pełne wsparcie naszej organizacji, a specjalista RODO będzie miał możliwość prowadzenia projektu w ścisłej współpracy z ekspertem. Przy podejmowaniu decyzji o skorzystaniu z tej możliwości warto zrobić porównanie ofert, gdyż może okazać się, że pełna asysta będzie nieznacznie tańsza od oferty pełnego przeprowadzenia kontroli RODO przez eksperta zewnętrznego i warto wówczas rozważyć opcję kontroli w miejsce asysty;
2) **cykliczne spotkania warsztatowe** mające na celu weryfikację dokonanych przez specjalistę RODO prac – opcja tańsza, pozwoli na bieżąco weryfikować wynik realizacji projektu, lecz nie obciąży budżetu organizacji kosztami pełnej asysty;
3) **wsparcie godzinowe** – wykorzystywane wyłącznie wówczas, gdy specjalista RODO będzie go potrzebował do bieżących konsultacji. Opcja ta jest optymalna w przypadku, gdy nasz specjalista RODO ma już odpowiednią wiedzę i doświadczenie, lecz będzie potrzebował sporadycznej konsultacji.

Każdy samodzielny specjalista RODO powinien posiadać możliwość sięgnięcia po wsparcie zewnętrzne choćby w minimalnym zakresie, bowiem w praktyce każdy, nawet najlepszy specjalista potrzebuje poddać najtrudniejsze kwestie pod dyskusję z innym specjalistą. W firmach profesjonalnie zajmujących się obsługą w obszarze RODO (np. w firmach consultingowych, kancelariach prawnych) specjaliści podejmują takie dyskusje wewnętrznie, we własnym gronie. Zatem nasz specjalista RODO również nie powinien być pozostawiony samemu sobie.

Ważne

Częstym błędem jest powierzenie realizacji kontroli zgodności z RODO osobie niemającej odpowiedniego przygotowania merytorycznego. Jeżeli nie zapewnimy właściwego wsparcia merytorycznego specjaliście RODO, nie będzie on miał realnej możliwości rzetelnego, pełnego przeprowadzenia kontroli, pozostawiając tym samym obszary, w których nasza organizacja nadal nie będzie zgodna z RODO. Wystarczy zapewnić odpowiednie wsparcie zewnętrzne, aby dać naszemu specjaliście możliwość prawidłowego wdrożenia RODO.

7. Ogólny harmonogram projektu

Dobrą praktyką w ramach przygotowania projektu jest opracowanie harmonogramu i jego przestrzeganie. Pozwoli to nie tylko nadzorować czas realizacji projektu, ale również wykluczy sytuację, w której projekt, z powodu ciągłej nieterminowości, zakończy

się fiaskiem z powodu jego nieukończenia. Opracowanie harmonogramu nie powoduje, że na poszczególnych etapach realizacji nie są możliwe odstępstwa lub przesunięcia czasowe, lecz powinny mieć one realne, ważne podstawy związane z okolicznościami wynikającymi z toku prac projektowych i pozostawać pod kontrolą.

Harmonogram projektu powinien obejmować:
1) **harmonogram ogólny**, ogólne ramy czasowe projektu ze wskazaniem kamieni milowych, czyli najważniejszych etapów projektu,
2) **harmonogram szczegółowy**, czyli wskazanie dat realizacji poszczególnych czynności wszystkich członków zespołu projektowego w ramach projektu.

Przykładowy harmonogram projektu może wyglądać następująco:

Harmonogram ogólny

Lp.	Data rozpoczęcia	Data zakończenia	Czynność
1	1 czerwca	4 czerwca	Etap 0. – powołanie zespołu projektowego
2	4 czerwca	22 czerwca	Etap 1. – inwentaryzacja zasobów zawierających dane osobowe w organizacji
3	22 czerwca		1. kamień milowy – zweryfikowane zbiory danych osobowych
4	22 czerwca	11 lipca	Etap 2. – Kontrola podstaw prawnych przetwarzania oraz realizacji obowiązków informacyjnych
5	11 lipca		2. kamień milowy – zweryfikowana i uzupełniona Księga klauzul
6	12 lipca	26 lipca	Etap 3. – prawa osób, których dane osobowe dotyczą
7	26 lipca		3. kamień milowy – zweryfikowana poprawność realizacji praw osób, których dane osobowe dotyczą
8	27 lipca	27 sierpnia	Etap 4. – bezpieczeństwo danych osobowych
9	27 sierpnia		4. kamień milowy – zweryfikowane bezpieczeństwo danych osobowych oraz wewnętrzna dokumentacja przetwarzania danych osobowych
10	28 sierpnia	21 września	Etap 5. – wdrożenie prac projektowych
11	21 września		5. kamień milowy – wdrożenie prac projektowych, zakończenie projektu

Harmonogram szczegółowy

Lp.	Data rozpoczęcia	Data zakończenia	Czynność	Obszar odpowiedzialny
1	**1 czerwca**	**4 czerwca**	**Etap 0 – powołanie zespołu projektowego**	
2	1 czerwca	1 czerwca	Przekazanie propozycji składu zespołu projektowego wszystkim kierownikom	Specjalista RODO