

PRZYGOTUJ SIĘ NA

RODO



**WAR WSP
DYN OLN
SKI+ ICY.**

krok po kroku

1

Przeanalizuj proces przetwarzania danych w swojej organizacji

Sprawdź, jakie dane osobowe przetwarzasz i na jakiej podstawie. Ustal, skąd pochodzą dane i do kogo je przekazujesz. Jeżeli przetwarzasz dane w oparciu o zgodę, sprawdź, czy dane nadal są przetwarzane w celu, dla którego zgoda została udzielona i czy zgoda spełnia wymogi RODO. Zweryfikuj, jak zabezpieczasz dane i kto ma do nich dostęp.

Zidentyfikuj wszystkie dane, które przetwarzasz

Sprawdź, czy obok oczywistych danych osobowych, jak imię i nazwisko czy PESEL, uwzględniłeś także nieoczywiste dane, jak np. stałe lub dynamiczne adresy IP, komunikację M2M, adresy poczty elektronicznej, podpisy, nagrania CCTV. Czy dbasz o to, by przetwarzać tylko niezbędne dane i aby były one poprawne i aktualne?

2

Ustal, wobec których danych działasz jako administrator, a które zostały ci powierzone do przetwarzania

Ustal, czy sam decydujesz o celach i środkach przetwarzania danych (czyli jesteś administratorem danych), czy też przetwarzasz dane na zlecenie innego podmiotu, np. w ramach realizacji usługi na rzecz tego podmiotu. RODO pozwala na współadministrowanie danymi. Zastanów się, czy warto rozważyć korzyści, jakie daje to rozwiązanie.

3

Zweryfikuj, czy prawidłowo powierzasz przetwarzanie danych innym podmiotom

Ustal, na jakiej podstawie powierzasz przetwarzanie danych innym podmiotom lub przetwarzasz dane pochodzące od innych podmiotów. Zweryfikuj, czy podmiot przetwarzający zapewnia środki techniczne i organizacyjne odpowiednie do zagrożeń i kategorii przetwarzanych danych. Sprawdź, czy podmiot przetwarzający podpowierza przetwarzanie danych dalszym podmiotom. Zastanów się, w jaki sposób weryfikujesz wtedy bezpieczeństwo danych. Czy wiesz, że RODO precyzuje warunki, jakie musi spełniać powierzenie przetwarzania danych? Sprawdź, czy umowy, które zawierasz, odpowiadają tym warunkom.

4

Jeżeli przetwarzasz dane osobowe na podstawie zgody osoby, której dane dotyczą, sprawdź, czy zgoda ta stanowi prawidłową podstawę przetwarzania

5

Sprawdź, czy prawidłową podstawą przetwarzania danych jest właśnie zgoda (a nie np. realizacja obowiązku wynikającego z prawa). Czy wiesz, że RODO przewiduje szczególne wymagania dotyczące warunków skutecznego wyrażenia zgody na przetwarzanie danych? Sprawdź, czy formularze zgody, które stosujesz, odpowiadają tym wymaganiom.

Jeżeli oferujesz usługi tzw. społeczeństwa informacyjnego, zweryfikuj, czy przetwarzasz dane osobowe dzieci na podstawie ich zgody

W Polsce dzieci, które ukończyły 13 lat, będą mogły wyrażać zgodę na usługi społeczeństwa informacyjnego. Zastanów się, w jaki sposób będziesz sprawdzał wiek dziecka od 25 maja 2018 r. Sprawdź, czy informacje przekazywane osobom, których dane przetwarzasz, są dostosowane do ich wieku.

6

Ustal, czy prowadzisz rejestr czynności przetwarzania danych

7

Ustal, czy prowadzisz rejestr czynności przetwarzania danych osobowych i czy spełnia on wymagania wynikające z RODO. Sprawdź, czy zgodnie z RODO będziesz miał obowiązek prowadzić rejestr. Czy pamiętasz, że rejestr prowadzić będą także podmioty, którym powierzono przetwarzanie danych? Zastanów się, czy prowadzić taki rejestr, nawet jeżeli nie będziesz mieć takiego obowiązku.

Upewnij się, że wiesz, jakie informacje trzeba przekazać osobom, których dane przetwarzasz

RODO przewiduje szersze obowiązki informacyjne — przygotuj się na uzupełnienie dotychczas udzielonych informacji oraz przygotuj wzór nowej informacji. Ustal, w jaki sposób przekażesz zaktualizowane informacje. Upewnij się, że osoby, których dane przetwarzasz, otrzymają uzupełnione informacje na czas.

8

Sprawdź, czy wewnętrzne procedury i rozwiązania techniczne pozwolą na realizację rozszerzonych praw osób, których dane są przetwarzane, oraz realizacji nowych obowiązków wobec regulatora

9

Ustal, czy jesteś przygotowany organizacyjnie i technicznie do obsługi i realizacji nowych praw. Sprawdź, czy stosowane w organizacji systemy pozwalają odszukać i usunąć dane osobowe osoby, która chce skorzystać z prawa do bycia zapomnianym, oraz czy umożliwiają przekazanie danych osobowych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Sprawdź, czy wewnętrzne procedury przewidują sposób realizacji wniosków osób o dostęp do danych, o sprostowanie danych, o ograniczenia przetwarzania, a także sposób działania w razie wniesienia sprzeciwu wobec przetwarzania danych oraz konieczności zgłoszenia naruszeń ochrony organowi nadzorczemu. Zastanów się nad wyznaczeniem osób odpowiedzialnych za realizację takich zadań.

Ustal, czy przetwarzasz dane przy użyciu zautomatyzowanych narzędzi podejmowania decyzji

Sprawdź, czy przetwarzasz dane w sposób zautomatyzowany, w tym czy profilujesz osoby, których dane przetwarzasz. Jeżeli tak, to zweryfikuj, czy informujesz o tym osoby, których dane osobowe w ten sposób przetwarzasz. Czy wiesz, że RODO przewiduje szczególne obowiązki informacyjne i uprawnienia osób zainteresowanych w takich przypadkach?

10

Upewnij się, że prawidłowo przekazujesz dane osobowe poza Polskę

Zweryfikuj, na jakiej podstawie przekazujesz dane w ramach Europejskiego Obszaru Gospodarczego i poza ten obszar. Sprawdź, czy podstawy takiego przekazywania pozostaną aktualne, gdy RODO zacznie obowiązywać. Zastanów się, który organ ochrony danych osobowych będzie tzw. organem wiodącym dla twojej organizacji.

11

Zastanów się, czy powoływać inspektora ochrony danych (obecnie ABI)

Zweryfikuj, czy będziesz miał obowiązek powołać inspektora ochrony danych (obecnie administrator bezpieczeństwa informacji, ABI). Rozważ, czy powołać takiego inspektora, nawet jeżeli nie będziesz miał takiego obowiązku. Zastanów się, czy zasadne byłoby powołanie jednego inspektora dla kilku podmiotów twojej organizacji. Pamiętaj o wymogach w zakresie wyboru inspektora ochrony danych i organizacji jego pracy przewidzianych w RODO.

12

Zweryfikuj, czy prawidłowo zabezpieczasz dane

Pamiętaj, że od 25 maja 2018 r. przestaną obowiązywać obecne wymogi techniczne i organizacyjne dotyczące zabezpieczenia danych. Nadal będziesz jednak odpowiedzialny za zapewnienie odpowiedniego bezpieczeństwa danych. Zastanów się, jakie środki techniczne i organizacyjne zastosujesz. Upewnij się, że zostaną wdrożone przed 25 maja 2018 r.

13

Upewnij się, że twoja organizacja będzie prawidłowo reagować na naruszenia ochrony danych

Pamiętaj, że od 25 maja 2018 r. będziesz miał obowiązek zgłaszania naruszeń ochrony danych organowi nadzorcemu i informowania o tym osób, których dane zostały naruszone. Dostosuj wewnętrzne procedury, żeby przewidywały odpowiednie działanie w razie stwierdzenia naruszeń, z uwzględnieniem 72-godzinnego terminu na zgłoszenie naruszenia organowi nadzoru. Upewnij się, że umowy o powierzenie przetwarzania danych zapewniają współdziałanie ze strony przetwarzającego umożliwiające dokonania zgłoszenia w terminie.

14

Upewnij się, że twoja organizacja umie ocenić skutki przetwarzania danych dla ochrony tych danych

15

Szereg procesów przetwarzania danych będzie podlegać obowiązkowej ocenie ich skutków w sferze ochrony danych osobowych. Zweryfikuj, czy będziesz miał obowiązek dokonywać takiej oceny na gruncie RODO. Zastanów się, jak systemowo wdrożyć w twojej organizacji przeprowadzanie takich ocen.

Upewnij się, że twoja organizacja wie, jak uwzględniać kwestie ochrony danych w fazie projektowania ich przetwarzania (privacy by design) oraz jak stosować rozwiązania domyślnej ochrony danych (privacy by default)

Sprawdź, czy przy określaniu sposobów przetwarzania danych oraz podczas przetwarzania wdrażasz 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. Ustal także, czy wdrożyłeś odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzać wyłącznie te dane, które są niezbędne dla osiągnięcia zamierzonego uprawnionego celu przetwarzania.

16

Upewnij się, że jesteś w stanie wykazać przestrzeganie przepisów o ochronie danych osobowych

17

Zasada rozliczalności zakłada wykazanie realizacji wszystkich zasad dotyczących przetwarzania danych osobowych (zasady zgodności z prawem, rzetelności i przejrzystości, zasady ograniczonego celu, zasady minimalizacji danych, zasady prawidłowości i ograniczonego przechowywania, a także zasady integralności i poufności danych). Ustal, w jaki sposób i jakimi środkami udowodnisz realizację tych zasad. Sprawdź, czy opracowana dokumentacja pozwala na wykazanie przestrzegania zasad.

Upewnij się, że twój personel wie, z czym się wiąże RODO

Rozważ przeszkolenie personelu, w szczególności osób, które przetwarzają dane osobowe. Upewnij się, że osoby te rozumieją potencjalne konsekwencje naruszenia przepisów o ochronie danych osobowych poczynając od 25 maja 2018 r.

18

**WAR WSP
DYN OLN
SKI+ ICY.**