Wprowadzenie

Każdego, kto przetwarza dane osobowe, niezależnie od tego, czy jest spółką prawa handlowego, osobą fizyczną prowadzącą działalność gospodarczą, czy nawet osobą fizyczną, obowiązuje RODO. Wprowadza ono tylko jeden wyjątek podmiotowy: jeżeli osoba fizyczna przetwarza dane osobowe w ramach czynności o czysto osobistym lub domowym charakterze, do tego przetwarzania nie stosuje się RODO. Oznacza to, że jeżeli osoba fizyczna przetwarza dane innych osób fizycznych wyłącznie w celach prywatnych, np. kontakty do swoich znajomych, rodziny lub dane kontaktowe przedstawicieli przedsiębiorców, ale wyłącznie we własnych, prywatnych celach (np. doradcy w banku, z którego korzysta prywatnie), w tym zakresie RODO nie obowiązuje takiej osoby. Jednak, gdyby osoba fizyczna rozpoczęła przetwarzać nawet te same dane osobowe, lecz w celach zawodowych, społecznych, zarobkowych lub innych celach przekraczających cele wyłącznie prywatne, wówczas RODO zaczyna ją obowiązywać. Każdego zatem, niezależnie od formy działalności, może obowiązywać RODO.

W praktyce niemal każdy podmiot, również przedsiębiorca jednoosobowy prowadzący działalność, z którą mogłoby się wydawać, że nie wiąże się przetwarzanie danych osobowych innych osób, przetwarza dane osobowe w celach zawodowych, zarobkowych, społecznych lub gospodarczych, a więc podlega RODO. Najczęściej przetwarzane kategorie danych osobowych to:

1) dane osobowe pracowników, niezależnie od rodzaju umowy: umowy o pracę, umowy zlecenia, wolontariatu, jak również dane stażystów i praktykantów;
2) dane osobowe kontrahentów będących osobami fizycznymi lub osobami fizycznymi prowadzącymi działalność gospodarczą;
3) dane osobowe klientów (osób fizycznych, w tym prowadzących działalność gospodarczą) zawarte na wystawianych fakturach;
4) dane zawarte w składanych reklamacjach, skargach, korespondencji tradycyjnej oraz elektronicznej;
5) dane potencjalnych klientów;
6) dane zawarte w adresach e-mail zostawianych przedsiębiorcy w celu wysyłki newslettera;
7) dane zawarte w plikach cookies i innych podobnych technologiach stosowanych na stronie internetowej przedsiębiorcy, w tym informacje pozyskiwane z Google Analytics;
8) dane osób śledzących fanpage przedsiębiorcy na profilach społecznościowych, np. na Facebooku.

Jednocześnie dla wielu podmiotów przeprowadzenie wdrożenia RODO stanowi wyzwanie nie tylko organizacyjne, ale także finansowe, a podmioty, w szczególności te niewielkie, o prostej strukturze działania i prostej strukturze organizacyjnej, nie wiedzą, jak takie wdrożenie przeprowadzić.

Aby ułatwić Państwu wdrożenie RODO i zapewnić dobrą bazę wyjściową, niniejszym składam w Państwa ręce kolejną publikację zawierającą opis proponowanej i stosowanej przeze mnie od lat

metodyki kontroli zgodności działania organizacji z przepisami dotyczącymi ochrony danych osobowych oraz opis polityk i procedur RODO, które każdy administrator powinien opracować i wdrożyć, wraz z przykładowym wzorem. Informacje praktyczne zamieszczone w opisie proponowanej metodyki oraz zawartości każdej procedury umożliwią Państwu szybkie i efektywne dostosowanie prezentowanych wzorów do indywidualnych potrzeb organizacji.

Nie da się bowiem opracować jednej uniwersalnej metodyki ani wzoru procedur wewnętrznych, które będą jednocześnie tak samo dobrze dostosowane do potrzeb każdego podmiotu, niezależnie od jego charakterystyki działania i struktury organizacyjnej. Cel, jaki przyświeca niniejszej publikacji, to praktyczny opis przykładowej metodyki przeprowadzania kontroli zgodności z RODO w organizacji oraz procedur wewnętrznych administratora na poziomie na tyle ogólnym, aby były one dobrym punktem wyjścia dla każdego małego lub średniego podmiotu, ale jednocześnie na poziomie na tyle szczegółowym, aby wzory były procedurami postępowania, czyli by dawały Państwu konkretne wytyczne dotyczące działań, jakie krok po kroku powinny zostać podjęte w określonych przypadkach, a nie były tylko ogólnymi informacjami czy politykami przedstawiającymi założenia i cele, do których nadal nie wiadomo, jaką ścieżką dotrzeć.

Punktem wyjścia dla opisywanej metodyki oraz opisu procedur zawartych w niniejszej publikacji jest średniej wielkości podmiot na poziomie zatrudnienia ok. 50–100 osób, z wydzielonymi komórkami wewnętrznymi zarządzanymi przez odpowiednich kierowników lub managerów. W konsekwencji:

1) zdecydowanie mniejsze podmioty z zatrudnieniem na poziomie kilku – kilkunastu pracowników mogą znacząco uprościć niniejszą metodykę i procedury, jak również usunąć regulacje dotyczące kwestii, które zapewne nie znajdą zastosowania w tym podmiocie;
2) większe podmioty ze znacząco większym zatrudnieniem, rozproszeniem strukturalnym na różne siedziby lub o zdecydowanie bardziej złożonej strukturze organizacyjnej zapewne będą potrzebować bardziej rozbudowanej metodyki, większego zaangażowania poszczególnych działów oraz dodania kilku szczebli osób decyzyjnych w procedurach postępowania;
3) w przypadku zdecydowanie większych podmiotów niniejsza metodyka i opis procedur również będą stanowić dobrą bazę wyjściową do wdrożenia, ale z pewnością będą takie obszary, w których poszczególne procedury powinny zostać opracowane przez profesjonalistów w dziedzinie innej niż RODO, w szczególności kwestie bezpieczeństwa informacji, bezpieczeństwa teleinformatycznego powinny zostać rozważone przez specjalistów BTI na poziomie zdecydowanie bardziej złożonym.

Wprawdzie RODO wprowadza obowiązek posiadania odpowiednich procedur, lecz, co do zasady, nie wskazuje sposobów organizacyjnej realizacji poszczególnych obowiązków z niego wynikających. Oznacza to, że wszędzie tam, gdzie nie ma określonego obowiązku wprost wyrażonego w RODO, a w praktyce również w preambule lub wytycznych Grupy Roboczej Art. 29 (obecnie – Europejskiej Rady Ochrony Danych), tam podmiot ma pełną dowolność w kształtowaniu sposobów realizacji tych obowiązków.

Wzory przedstawiane w niniejszej publikacji zostały opracowane na bazie RODO, wytycznych Grupy Roboczej Art. 29, materiałów dostarczanych przez organy nadzoru oraz standardowych rozwiązań rynkowych. Niektóre wzory raportów czy wykazów pochodzą właśnie z tych źródeł, zgodnie z założeniem, że jeżeli określony dokument jest publikowany przez organ nadzoru, z założenia spełnia on wymogi RODO, a od strony praktycznej zazwyczaj jest absolutnie wystarczający dla większości administratorów danych. W każdym przypadku do wzoru raportu została opracowana odpowiednia procedura lub instrukcja, aby podmiot wiedział nie tylko to, co musi osiągnąć, ale także, jak to osiągnąć.

Agnieszka Sagan-Jeżowska