Warszawa, 18.06.2020 r.

**Brak całościowego spojrzenia na wdrożenie, czyli lewa ręka nie wie co przetwarza prawa**

Nigdy za wiele powtarzania, że wdrożenie i utrzymanie zgodności z RODO to nie jednorazowy projekt, tylko ciągły proces. Bezpieczeństwo przetwarzania danych osobowych zazwyczaj dotyczy całokształtu działalności danej organizacji i towarzyszy jej w codziennym działaniu - od sposobu pozyskania danych, przez narzędzia do ich przetwarzania i wykorzystywania, na metodach ich usunięcia kończąc. Z natury rzeczy tak kompleksowe zagadnienie musi być rozpatrywane w ramach pewnej całości, ale niestety praktyka w tym zakresie nie rozpieszcza i nierzadko trzeba zderzyć się wdrożeniowym cherry-pickingiem, czyli wybieraniem sobie przez administratora obszarów gdzie chce wdrożyć RODO (np. w zakresie strony internetowej i polityki prywatności skierowanej na realizację praw podmiotów, których dane dotyczą) przy jednoczesnym ignorowaniu innych obszarów związanych z danymi osobowymi (np. retencji danych czy projektowania procesów z domyślnym uwzględnieniem ochrony danych osobowych). Ostatecznie wybiórcze spojrzenie na wdrożenie RODO powoduje, że tego wdrożenia po prostu nigdy nie będzie, bo ochrona danych osobowych w działaniu organizacji przypomina pod tym względem puzzle, gdzie jeden brakujący element powoduje, że cała układanka jest niekompletna.

W przypadku wybiórczego i nie skoordynowanego wdrażania RODO może dojść do sytuacji, w której np. jeden dział spółki zbiera prawidłowo zgody na przetwarzanie danych w celach marketingu elektronicznego, bo został przeszkolony i wyposażony w prawidłowe procedury, a następnie te dane są nieprawidłowo wykorzystywane przez inny dział organizacji (np. następuje profilowanie lub udostępnianie danych bez wiedzy osób, których dane dotyczą), co powoduje, że w efekcie cały proces nie jest zgodny z RODO. Może być też tak, że dwa lub więcej działy organizacji posługują się np. zupełnie odmiennymi klauzulami informacyjnymi czy wzorami umów powierzenia, przez co dochodzi do chaosu w rejestrach umów pisemnych i utrudnia lub uniemożliwia audyt i kontrolę nad procesorami. Utrzymywanie takiej sytuacji prowadzi do frustracji zarówno osoby pełniącej funkcję Inspektora Ochrony Danych jak i ze strony personelu organizacji, co prowadzi do zniechęcenia przestrzegania zasad ochrony danych i obniża jej standard.

Jak przeciwdziałać temu zjawisku? Przede wszystkim jasno komunikować administratorom danych charakter ich obowiązków wynikających z RODO i potrzebę ciągłego dbania o utrzymanie zgodności z obowiązującym prawem, Po drugie istotne jest, aby do pełnienia funkcji IOD powołać osobę, która posiada doświadczenie pozwalające na kompleksowe zarządzanie wdrożeniem i utrzymaniem zgodności z RODO. Po trzecie należy rozpocząć proces od rzetelnego i dogłębnego audytu. który ujawni wszelkie obszary przetwarzania danych, które należy następnie w sposób skoordynowany dostosowywać do obowiązujących przepisów.

Brak kompleksowego spojrzenia na wdrożenie ma zawsze jeden i ten sam skutek. Prędzej czy później organizacja, w której panuje chaos w obszarze ochrony danych osobowych, potknie się o własne nogi i boleśnie wyłoży narażając się na dotkliwe kary. Pytanie nie brzmi czy, tylko kiedy.

**Bartosz Migas, Specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.**



iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł