RODO w praktyce

1. Wstęp

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO lub ogólne rozporządzenie o ochronie danych) określa ochronę osób fizycznych w związku z przetwarzaniem danych osobowych oraz stanowi o swobodnym przepływie danych osobowych. Oznacza to nałożenie na przetwarzających dane większej odpowiedzialności. To oni będą musieli wykazać, że zastosowane metody ochrony danych są skuteczne.

Kiedy 8 czerwca 2018 r. pod Nowym Targiem doszło do wypadku drogowego, w którym uczestniczył autokar wiozący dzieci wracające z wycieczki szkolnej, część poszkodowanych uczniów została niezwłocznie rozwieziona do okolicznych szpitali. Jak się jednak okazało, ich rodzice mieli olbrzymie problemy z ustaleniem, gdzie przebywają ranne dzieci. Odnalezienie małego pacjenta w konkretnym szpitalu lub otrzymanie choćby podstawowych informacji przez telefon było bardzo trudne albo w ogóle niemożliwe. Jak się okazało, powodem takiej wstrzemięźliwości pracowników służby zdrowia było unijne rozporządzenie o ochronie danych osobowych, które 25 maja tego roku, a więc niecały miesiąc wcześniej, weszło w życie także w Polsce. Niebezpieczną sytuację bardzo szybko skomentował Maciej Kawecki, dyrektor departamentu zarządzania danymi w Ministerstwie Cyfryzacji. Zapewnił on, że jego urząd uczuli jednostki zdrowia, by bardziej racjonalnie podchodziły do tematu ochrony danych osobowych.

Najważniejszym słowem w powyższej wypowiedzi urzędnika jest racjonalność, która jest kluczem do zrozumienia i zastosowania w życiu nowych regulacji prawnych. Racjonalne dostosowanie, elastyczność środków oraz otwarty katalog stosowanych metod, technik i regulacji wewnętrznych stanowią o innowacyjności i atrakcyjności nowych przepisów. Z tych samych powodów stanowią one jednak wyzwanie i zmuszają do zupełnie nowego spojrzenia na ochronę danych osobowych, tak by dostosowując się do nowych mechanizmów prawnych nie narazić się na odpowiedzialność prawną i finansową. Ci, którzy myślą, że doświadczenia nabyte w trakcie praktyki pod rządami wcześniejszych przepisów (w tym między innymi ustawy o ochronie danych osobowych) są wystarczające, by stawić czoła nowym przepisom, są w poważnym błędzie.

Należy przypomnieć, że na podstawie poprzednio obowiązującej ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (dalej: OchrDanychU) konieczne i zarazem wystarczające było sporządzenie dokumentacji w postaci Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemami Informatycznymi, których forma i treść były uregulowane rozporządzeniem wykonawczym. Ich sporządzenie było zatem wyłącznie niezbyt uciążliwą formalnością. Co więcej, kary finansowe przewidziane ustawą, niezależnie od ich niewielkiej wysokości, miały charakter wyłącznie przymuszający. Stosowane były dopiero wtedy, gdy kontrolowany podmiot nie dostosował się do zaleceń pokontrolnych organu. Te przyczyny spowodowały, że ochrona danych osobowych była jednym z tych zagadnień, o których przedsiębiorca pamiętał w ostatniej kolejności.

UWAGA
Doświadczenia nabyte w czasie obowiązywania OchrDanychU są istotne, jednak niewystarczające, by sprostać wymaganiom RODO.

O ochronie tych jakże wrażliwych danych pamiętał jednak europejski prawodawca. Zauważył on, że zmieniający się świat wymaga dostosowania do niego mechanizmów prawnych. Coraz powszechniejsze aplikacje mobilne, galopujący rozwój branży e-commerce, nowe technologie oraz postępująca wirtualizacja i digitalizacja