Warszawa, 21.08.2024 r.

Które kraje zapewniają odpowiedni stopień ochrony danych?

Inspektorzy Ochrony Danych w codziennej pracy są wyczuleni na pewne sytuacje, przy których należy się zatrzymać i zwrócić na nie szczególną uwagę. Alarmujące jest, gdy hasło do załącznika znajduje się w treści tej samej wiadomości lub jest niezwykle proste (np. „987654"). Jesteśmy wyczuleni na klauzule zgody, zwłaszcza w sytuacjach, gdy zgoda nie jest prawidłową podstawą przetwarzania danych (np. wyrażam zgodę na przetwarzanie moich danych adresowych w celu wysyłki zakupionego towaru). Podobnie w sytuacjach, gdy opiniowana umowa zawiera słowa „transfer" oraz „EOG".

Jest to bardzo słuszna reakcja, gdyż każdorazowo należy dokładnie zbadać charakter takiego transferu. Transferowanie danych poza EOG zostało szczegółowo uregulowane w przepisach RODO. Chcąc zapewnić pełną zgodność z przepisami o ochronie danych osobowych, musimy mieć pewność, iż dane osobowe są odpowiednio chronione, niezależnie od kraju, w którym je przetwarzamy. Czyli powinniśmy ocenić, czy kraj, do którego planujemy przekazać dane, gwarantuje odpowiedni stopień ochrony.

Dlaczego i w jakich sytuacjach transferujemy dane?
Rozwój technologii i Internetu sprawił, że dostęp do narzędzi oraz usług stał się niezwykle łatwy. Powszechnie korzystamy z usług oferowanych przez globalne przedsiębiorstwa, które nie muszą mieć siedziby po sąsiedzku, na tej samej ulicy, a znajdują się na drugim końcu świata – co wiąże się z transferem danych osobowych. Administrator danych może przekazywać dane do państwa trzeciego wyłącznie, jeżeli to państwo zapewnia odpowiednie zabezpieczenia i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środku ochrony prawnej. Za państwo trzecie uważa się każdy kraj, który nie jest krajem należącym do EOG (Europejski Obszar Gospodarczy). Często zatem oba pojęcia stosuje się wymiennie: transfer do państwa trzeciego lub w drugą stronę: transfer poza EOG.

W jakich sytuacjach może dochodzić do transferu danych? Najczęściej transferowanie danych dotyczy miejsca ich przechowywania lub miejsc, z których regularnie uzyskuje się do nich dostęp. Dla przykładu, wewnątrz organizacji o rozbudowanej strukturze, gdy spółka matka znajdują się poza EOG, może dochodzić do transferów danych pracowników lub klientów w związku z miejscem przechowywania danych (np. w zakresie dostarczania systemu CRM, kadrowego, niezależnie, czy jest to powierzenie, współadministrowanie, czy odrębne administrowanie danymi). Do transferu danych dochodzi również, jeżeli nasze centra danych znajdują się na terenie EOG, ale np. są one zdalnie administrowane przez wsparcie IT outsourcowane do kraju spoza EOG.

Wielu globalnych dostawców jest świadomych przepisów RODO i chcąc zagwarantować pełną zgodność z tymi przepisami, a przy okazji ułatwić życie administratorom danych. W ramach świadczonych usług oferują przechowywanie danych na terenie EOG (w standardzie lub jako płatna, dodatkowa opcja). Jednakże czasami możemy nie mieć takiej możliwości. Wówczas przepisy art. 44 i następnych RODO wymagają od nas podjęcia mniejszej lub większej ilości dodatkowych działań.

Decyzja o adekwatności.
Zgodnie z art. 45 RODO, Komisja Europejska może przyjąć decyzję o adekwatności w odniesieniu do kraju, terytorium lub określonego sektora w danym kraju poza EOG, który zapewnia odpowiedni stopień ochrony danych osobowych. Decyzja taka oznacza, że dane osobowe mogą być przekazywane do tego kraju bez potrzeby uzyskiwania dodatkowych zezwoleń lub spełniania innych warunków (np. w zakresie stosowania dodatkowych zabezpieczeń). Co za tym idzie, takie przekazywanie danych traktowane jest, jak gdyby odbywało się wewnątrz EOG.

Decyzje o adekwatności, opisane w art. 45 RODO, pomagają nam uniknąć ponownego wykonywania pracy, która została już raz dokonana przez Komisję Europejską. W takiej sytuacji, w przypadku zamiaru dokonania transferu do tych krajów administrator danych nie musi ponownie oceniać między innymi: poziomu praworządności, poszanowania praw człowieka, zasad ochrony danych osobowych, orzecznictwa, egzekwowania przestrzegania przepisów o ochronie danych osobowych czy działania skutecznego i niezależnego organu nadzoru w tym kraju.

Do krajów, wobec których Komisja Europejska wydała decyzję o adekwatności, należą:

1. Andora
2. Argentyna
3. Guernsey
4. Izrael
5. Japonia
6. Jersey
7. Kanada (w odniesieniu do komercyjnych organizacji przetwarzających dane)
8. Korea Południowa
9. Nowa Zelandia
10. Szwajcaria
11. Urugwaj
12. USA (podmioty uczestniczące w programie Data Privacy Framework)
13. Wielka Brytania
14. Wyspy Man
15. Wyspy Owcze

Stan na dzień: 21.08.2024.

Data Privacy Framework – jak korzystać?
Niewątpliwie każdy z nas zwrócił uwagę na wyjątek dotyczący USA. Decyzja o adekwatności nie ma zastosowania do wszystkich podmiotów z USA, a jedynie tych wpisanych na listę Data Privacy Framework (DPF) prowadzoną przez Departament Handlu Stanów Zjednoczonych. Chcąc zrealizować transfer, danych powinniśmy zweryfikować, czy podmiot przystąpił do programu, uzyskując certyfikację i wpis na listę. Możemy tego dokonać, korzystając z wyszukiwarki dostępnej pod adresem: https://www.dataprivacyframework.gov/list.

Należy regularnie weryfikować, czy podmiot z USA, z którym współpracujemy, nie utracił certyfikacji, co powodowałoby usunięcie go z listy DPF. Wyszukując podmiot, po wyświetleniu pełnego profilu (Full Profile) ukaże nam się jego status (EU-U.S. Data Privacy Framework: Active) oraz data kolejnej certyfikacji (Next Certification Due Date). Tutaj protip: pamiętajmy, iż daty zapisywane są w amerykańskim formacie, w którym kolejność zapisu dni i miesięcy jest odwrócona (miesiąc/dzień/rok).

Podsumowanie
Na zakończenie należy przypomnieć, iż raz wydana decyzja o adekwatności nie jest wieczna. Komisja Europejska w każdej chwili może dokonać przeglądu skutkującego jej zmianą lub wycofaniem. Ostatnia taka weryfikacja zakończyła się 15 stycznia 2024 r., kiedy to Komisja poinformowała o weryfikacji 11 wcześniej wydanych decyzji. Szczęśliwie w tym przypadku przegląd został zakończony pomyślnie, jednak musimy zawsze pamiętać o konieczności monitorowania, czy decyzje stwierdzające odpowiedni stopień ochrony nie zostały uchylone lub unieważnione – a takie sytuacje historycznie miały już miejsce (zwłaszcza w odniesieniu do USA).

Marcin Stryszko – specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.