Nie wszystko co zamaskowane, jest niewidoczne, czyli co TSUE mówi o pseudonimizacji w wyroku z 4 września 2025 r (C-413/23 P)

Kiedy mówimy o ochronie danych osobowych, często pojawia się słowo „pseudonimizacja". To taki magiczny zabieg, który pozwala zmieniać imiona i nazwiska czy numery telefonów na kod czy losowy identyfikator. Wielu przedsiębiorców myśli: „Świetnie, to już nie są dane osobowe, mogę je bezpiecznie wykorzystać". Nic bardziej mylnego. I właśnie potwierdził to Trybunał Sprawiedliwości UE w wyroku z 4 września 2025 r, sprawa EIOD przeciwko SRB, C-413/23 P.

Czym jest pseudonimizacja?

Pseudonimizacja została zdefiniowana w art. 4 pkt 5 RODO jako „przetwarzanie danych osobowych w taki sposób, że nie można przypisać danych konkretnej osobie bez użycia dodatkowych informacji, które są przechowywane oddzielnie". Jest to metoda techniczna mająca na celu zmniejszenie ryzyka identyfikacji osoby na podstawie danych przetwarzanych przez administratora. Choć pseudonimizacja wspiera realizację zasady minimalizacji danych (art. 5 ust. 1 lit. c RODO) oraz bezpieczeństwa przetwarzania (art. 32 RODO), nie jest to jednak forma anonimizacji – dane po pseudonimizacji wciąż mogą, w określonych warunkach, umożliwiać identyfikację osoby.

Pseudonimizacja od dawna budzi emocje w dyskusjach o ochronie danych osobowych. Z jednej strony jest wskazywana wprost w RODO jako środek bezpieczeństwa i minimalizacji ryzyka, z drugiej nie daje takiego samego efektu jak anonimizacja, która nieodwracalne uniemożliwia zidentyfikowanie określonej osoby.

Charakter danych po pseudonimizacji

Powstaje pytanie: czy dane po pseudonimizacji zawsze zachowują charakter danych osobowych, a jeśli nie, to w jakich sytuacjach mogą być traktowane inaczej?

Odpowiedzi na te pytania udzielił Trybunał Sprawiedliwości UE w wyroku z 4 września 2025 r. w sprawie EIOD przeciwko SRB (C-413/23 P). Spór dotyczył konsultacji prowadzonych przez Jednolitą Radę ds. Restrukturyzacji i Uporządkowanej Likwidacji w związku z planowaną likwidacją banku w Hiszpanii. Uczestnicy konsultacji przekazywali swoje opinie i komentarze, które następnie zostały pseudonimizowane i udostępnione firmie Deloitte. Europejski Inspektor Ochrony Danych uznał, że SRB naruszyła przepisy, ponieważ nie poinformowała uczestników o ujawnieniu ich danych stronie trzeciej. Sąd UE nie zgodził się z tym stanowiskiem, twierdząc, że dla Deloitte dane nie miały charakteru osobowego. Dopiero Trybunał w Luksemburgu ostatecznie rozstrzygnął tę kwestię, uchylając wyrok Sądu i wyznaczając nowe ramy interpretacyjne.

Trybunał wyraźnie odróżnił sytuację administratora od sytuacji odbiorcy danych. Dla SRB, jako administratora, pseudonimizowane komentarze były nadal danymi osobowymi, bo posiadała dodatkowe informacje pozwalające na przypisanie ich konkretnym osobom. Dla Deloitte, które takich informacji nie miało i nie mogło ich w rozsądny sposób zdobyć, dane mogły nie być traktowane jako osobowe. W ten sposób TSUE odrzucił stanowisko EIOD, że pseudonimizowane dane zawsze muszą być uznawane za dane osobowe. Jednocześnie przypomniał, że oceny identyfikowalności dokonuje się w momencie zbierania danych i z perspektywy administratora, a nie podmiotu trzeciego. Trybunał podkreślił też, że pseudonimizacja nie zwalnia administratora z obowiązków wynikających z przepisów. Zgodnie z art. 13 RODO i art. 15 rozporządzenia 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE, administrator musi poinformować osoby, których dane dotyczą, o odbiorcach danych. Nie ma znaczenia, że odbiorca nie jest w stanie powiązać danych z konkretnymi osobami: obowiązek przejrzystości jest zawsze. W praktyce oznacza to, że SRB powinna była wskazać Deloitte jako odbiorcę, nawet jeśli przekazane informacje dla samego Deloitte nie miały osobowego charakteru.

Ważnym elementem orzeczenia było też zakwalifikowanie komentarzy jako danych osobowych. Trybunał uznał, że opinie i poglądy wyrażone przez osoby fizyczne są ściśle związane z ich tożsamością i tym samym muszą być traktowane jako dane osobowe. To przypomnienie, że dane osobowe to nie tylko imiona, adresy czy numery identyfikacyjne, ale także treści wypowiedzi, które mogą być powiązane z konkretną osobą.

Co to oznacza w kontekście AI?

Znaczenie wyroku wykracza poza strony i instytucje unijne. Ma on przełożenie na praktykę biznesową, w szczególności w obszarze sztucznej inteligencji. AI w ogromnej mierze opiera się na danych tekstowych, komentarzach, opiniach czy transkrypcjach rozmów. Firmy, chcąc ograniczyć ryzyka, często sięgają po pseudonimizację. Wyrok pokazuje jednak, że z perspektywy administratora takie dane nadal pozostają danymi osobowymi.

Jeśli przedsiębiorstwo zbiera dane klientów, usuwa identyfikatory i używa ich do trenowania modelu AI, musi nadal spełniać wszystkie wymogi RODO: posiadać podstawę prawną, realizować obowiązek informacyjny oraz umożliwiać korzystanie z praw przez osoby, których dane dotyczą.

Inaczej wygląda sytuacja dostawcy zewnętrznego systemu AI, który otrzymuje od administratora już pseudonimizowane dane i nie ma żadnego dostępu do kluczy lub dodatkowych informacji. Dla niego dane mogą być w praktyce anonimowe i nie podlegać RODO.

Odpowiedzialność wobec osób, których dane dotyczą, zawsze spoczywa na administratorze, czyli podmiocie, który pierwotnie dane zebrał i nadal dysponuje możliwością ich powiązania z konkretnymi osobami.

Wyrok ma również znaczenie dla oceny ryzyka reidentyfikacji. RODO w art. 4 pkt 1 nakazuje, by przy ocenie, czy osoba jest możliwa do zidentyfikowania, brać pod uwagę wszystkie środki, które „z uzasadnionym prawdopodobieństwem mogą zostać użyte". W erze rozwiniętych narzędzi sztucznej inteligencji, zdolnych do analizy ogromnych zbiorów danych i wykrywania powiązań, to ryzyko stale rośnie. To, co teraz wydaje się bezpieczne i wystarczająco pseudonimizowane, jutro może być z łatwością połączone z konkretną osobą. Dlatego administratorzy powinni stale aktualizować swoje oceny ryzyka i nie traktować pseudonimizacji jako rozwiązania raz na zawsze.

Wyrok TSUE z 4 września 2025 r. jest odzwierciedleniem zasad ochrony danych osobowych. Potwierdza, że pseudonimizacja to owszem technika minimalizacji ryzyka, ale nie zwalnia administratorów z obowiązków wynikających z RODO. Z punktu widzenia AI oznacza to, że dane tekstowe czy opinie wykorzystywane w trenowaniu modeli wciąż pozostają danymi osobowymi, a odpowiedzialność za ich zgodne z prawem wykorzystanie spoczywa przede wszystkim na administratorze. Pseudonimizacja nie jest więc furtką do ominięcia przepisów, ale narzędziem, które wspiera ich realizację.

Najważniejsze wnioski

- Pseudonimizacja to dobra technika minimalizacji ryzyka, ale nie zwalnia administratorów z obowiązków wynikających z RODO.
- Odpowiedzialność za zgodne z prawem przetwarzanie tych danych spoczywa przede wszystkim na administratorze danych.
- Administrator musi zawsze informować osoby, których dane dotyczą, o udostępnieniu danych stronom trzecim, dbając o pełną przejrzystość procesów przetwarzania.
- Z punktu widzenia odbiorcy danych, który nie posiada dostępu do dodatkowych informacji pozwalających na identyfikację osób, dane pseudonimizowane mogą nie mieć już charakteru danych osobowych i nie podlegać pełnym rygorom RODO
- W kontekście sztucznej inteligencji dane tekstowe, opinie i inne informacje wykorzystywane do trenowania modeli wciąż są danymi osobowymi.

Warto więc pamiętać, że pseudonimizacja to nie „czarodziejska różdżka", która automatycznie zwalnia z obowiązków wynikających z RODO. 😉

Gabriela Tokarska - młodsza specjalistka ds. ochrony danych osobowych w iSecure Sp. z o.o.