PROCEDURY

Pięć obszarów, o których powinien pamiętać pracodawca podczas przeglądu danych osobowych

Początek roku to dobry moment na weryfikację podstaw do ich przetwarzania. **Niektóre przepisy wprost zobowiązują administratora do usunięcia tych danych, które nie są już niezbędne do celu, w jakim zostały zgromadzone**

Agata Majewska
radca prawny,
Ślązak, Zapiór i Partnerzy

Rozliczalność to jednocześnie jedna z podstawowych zasad przetwarzania danych osobowych, jakie wymienia 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 (ogólne rozporządzenie o ochronie danych – dalej: RODO), jak i jeden z kluczowych obowiązków każdego administratora. Jak jest ona ważna, pokazują kolejne decyzje prezesa UODO. Kładą one coraz większy nacisk na transparentność procesów przetwarzania zarówno pod kątem zakresu gromadzonych danych, jak i czasu ich przetwarzania.

Dodatkowo istotnym i zachęcającym argumentem za cykliczną weryfikacją danych osobowych w organizacji jest to, że im mniej mamy ich w posiadaniu, tym mniej wysiłku i nakładów wymaga ich fizyczne zabezpieczenie, co oszczędza czas i środki firmy.

Początek roku to dobry moment na przegląd tego, jakie dane osobowe przetwarza nasza organizacja, pod kątem ich aktualności i istnienia aktualnej podstawy przetwarzania.

Oto najważniejsze obszary, nad którymi powinien się pochylić każdy administrator w tym zakresie.

1. Ustal okresy retencji i ich przestrzegaj

RODO wyraźnie określa, że przetwarzanie danych osobowych ponad dopuszczalny przyjęty okres jest przetwarzaniem bez podstawy prawnej, a więc rodzi ryzyko odpowiedzialności za naruszenie przepisów rozporządzenia.

Częściowo okres retencji danych zebranych w konkretnym celu określają właściwe przepisy (np. w przypadku monitoringu pracowniczego, dokumentacji pracowniczej, dokumentów księgowych itp.). W pozostałym zakresie ustalenie tego okresu to zadanie administratora. Tymczasem wskazanie, jak długo konkretne dane osobowe będą niezbędne dla celu, dla którego są gromadzone, sprawia administratorom spore problemy. Z pewnością przydatne jest tu więc wsparcie specjalisty w obszarze ochrony danych osobowych.

Przy czym warto regularnie weryfikować, czy w każdym przypadku gromadzenia danych na potrzeby danego przedsięwzięcia okres ich przechowywania został wyraźnie ustalony i jest obiektywnie uzasadniony, a w razie potrzeby – trzeba dokonać niezbędnych korekt w tym zakresie.

Kolejnym krokiem powinna być dokładna weryfikacja, jak w praktyce wygląda przestrzeganie przyjętego okresu retencji. A więc tego, czy po jego upływie zbędne dane osobowe – zgromadzone chociażby w bazie CV, bazie klientów, liście subskrybentów newsletter itd. – są faktycznie w całości usuwane, czy też część z nich w jakiejkolwiek postaci pozostaje w obiegu.

Warto w tym miejscu przypomnieć, co często umyka uwadze administratorów, że przetwarzaniem danych osobowych jest również samo ich przechowywanie (np. w skrzynce e-mail, na pulpicie, serwerze lub nawet w archiwum), nawet jeśli nie wiąże się ono np. z ich przeglądaniem, przesyłaniem między działami ani innym aktywnym działaniem.

Dobrym rozwiązaniem jest też opracowanie i stosowanie procedury określającej proces usuwania lub niszczenia danych. Pozwoli to nie tylko na jego ujednolicenie, lecz takze na zapewnienie realizacji zasady rozliczalności.

2. Zwróć uwagę na przepisy wymuszające przegląd danych

Warto pamiętać, że niektóre przepisy wprost zobowiązują administratora do cyklicznego przeglądu danych i usunięcia tych, które nie są już niezbędne do celu, w jakim zostały zgromadzone. Przykładem są tu przepisy ustawy z 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych (t.j. Dz.U. z 2023 r. poz. 998; ost.zm. Dz.U. z 2023 r. poz. 1586), które wymuszają co najmniej coroczny przegląd danych osobowych zgromadzonych w celu przyznania ulgowej usługi i świadczenia oraz dopłaty z funduszu i ustalenia ich wysokości, zebranych przez pracodawcę. Celem takiego przeglądu jest ustalenie niezbędności ich dalszego przechowywania. Obowiązek analogicznego przeglądu przepisy nakładają na zarząd kasy zapomogowo-pożyczkowej w odniesieniu do danych osobowych członków kasy.

W obydwu ww. przypadkach mogą to być informacje dotyczące zdrowia, sytuacji rodzinnej, materialnej i socjalnej, więc ścisłe przestrzeganie cyklicznego przeglądu i redukowania ich do niezbędnego zakresu jest tym bardziej uzasadnione.

Początek roku to dobry moment na audyt tego, czy w ramach poszczególnych procesów przetwarzania danych osobowych w naszej organizacji nie istnieją przepisy, które nakładają obowiązek regularnych przeglądów, i ustalenie ich dat – w zależności od zakresu gromadzonych danych – raz w roku lub częściej.

By zrealizować zasadę przejrzystości, z takiego przeglądu powinien zostać sporządzony raport określający zakres i datę brakowania danych, które nie są już niezbędne dla przyjętych celów.

3. Minimalizuj dane i ich nośniki

W CV, kwestionariuszu osobowym kandydata, kwestionariuszu osobowym pracownika, osobnych arkuszach dotyczących korzystania z poszczególnych uprawnień lub ulg związanych z zatrudnieniem powielają się te same dane osobowe. Mimo rozwijających się rozwiązań paperless i tego, że przepisy nie wymuszają obecnie na pracodawcach prowadzenia tak obszernej dokumentacji pracowniczej, w wielu organizacjach można zauważyć (wynikającą często z zaszłości i przyzwyczajeń) słabość do mnożenia dokumentów.

Dotyczy to zresztą nie tylko obszaru HR, lecz także działań marketingowych, kontaktów z klientami, kontrahentami itp. Jak dużym problemem dla zachowania poufności i integralności danych może się okazać nadmiar papierowych dokumentów, przekonał się każdy, kto w gąszczu akt próbował odnaleźć jeden zagubiony dokument.

Nie mniejszym kłopotem może się okazać aktualizacja danych osobowych konkretnej osoby w sytuacji, gdy nie jesteśmy w stanie określić, w ilu miejscach i na ilu nośnikach je zgromadziliśmy, w szczególności zaś, czy w obiegu nie pozostają dokumenty z nieaktualnymi danymi takiej osoby.

Dobrym krokiem, ułatwiającym zachowanie integralności danych, jest wdrożenie rozwiązań paperless, które pozwalają na cyfryzację zasobów firmy. Na odchodzenie od papieru pozwalają też coraz częściej przepisy, które stopniowo dopuszczają alternatywne postacie (papierową i elektroniczną), m.in. dokumentów pracowniczych.

Zastąpienie papierowego obiegu dokumentów komunikacją elektroniczną pozwala z jednej strony na sprostanie zasadom przetwarzania danych określonym w RODO, a z drugiej na ułatwienie pracy (zwłaszcza zdalnej) i na oszczędności, zarówno finansowe (mniejsze zużycie papieru/tuszu/urządzeń drukujących), jak i przestrzenne – ze względu na brak konieczności wygospodarowania odpowiednio zabezpieczonych przed dostępem osób niepowołanych pomieszczeń na przechowywanie dokumentów.

Co ważne, rozwiązania paperless nie wymagają zakupu specjalistycznego oprogramowania. Często może je zastąpić komunikacja mailowa lub za pośrednictwem stosowanych już w firmie do innych celów komunikatorów lub podobnych narzędzi.

Cykliczna kontrola spełniania wymogu minimalizacji danych powinna się więc sprowadzać przede wszystkim do weryfikacji tego, czy liczba dokumentów lub innych nośników i gromadzonych w nich danych osobowych w naszej organizacji jest niezbędna i adekwatna do przyjętego celu oraz czy korzystniejszym rozwiązaniem dla zachowania odpowiedniego poziomu bezpieczeństwa nie będzie ich ograniczenie do koniecznego minimum.

WAŻNE Przetwarzaniem danych osobowych jest również samo ich przechowywanie (np. w skrzynce e-mail, na pulpicie, serwerze lub nawet w archiwum), nawet jeśli nie wiąże się ono np. z ich przeglądaniem, przesyłaniem między działami ani innym aktywnym działaniem.

4. Śledź na bieżąco zmiany w prawie

Na przestrzeni lat obowiązywania RODO można dostrzec tendencję do ograniczania zakresu przedmiotowego i czasowego danych osobowych personelu, jakie może przetwarzać pracodawca. Mimo nowelizacji kodeksu pracy w 2019 r., która odchudziła art. 22^1, określający dane, których podania od kandydata lub pracownika można żądać, w praktyce część pracodawców nadal oczekuje ujawniania przez nich: imion rodziców, nazwiska rodowego matki, adresu zameldowania itp.

Jednak przechowywanie takich danych w sytuacji, gdy przepisy upoważniające do tego już nie obowiązują, a brak jest innej podstawy prawnej do ich gromadzenia, jest przetwarzaniem niezgodnym z przepisami RODO. Tym samym naraża pracodawcę, jako administratora danych, na odpowiedzialność administracyjną (w tym finansową) wobec prezesa UODO.

Warto więc śledzić nie tylko bieżące zmiany przepisów, lecz także stanowiska polskiego i europejskich organów nadzoru oraz orzecznictwo sądów administracyjnych i TSUE w obszarze danych osobowych, dające wskazówki, jakie dane i w jakiej postaci (np. na podstawie oświadczenia pracownika, a nie przedkładaną przez niego kopię poszczególnych dokumentów) może przetwarzać pracodawca.

Z uwagi na tempo zmian stanu prawnego oraz mnogość stanowisk organów nadzorczych w kraju i na poziomie UE dobrze jest przeprowadzić audyt w zakresie aktualnych podstaw prawnych przetwarzania poszczególnych danych wspólnie z ekspertem mającym merytoryczną wiedzę oraz znajomość aktualnych stanowisk organów administracji, UE oraz sądownictwa w obszarze danych osobowych.

5. Cykliczne audyty

Powoli rodzi się świadomość tego, że zgodność z przepisami RODO jest stałym procesem, a nie jednorazowym działaniem. Zmiana narzędzi, jakimi posługujemy się w pracy, nowe przedsięwzięcia i projekty, podejmowanie współpracy z nowymi kontrahentami, coraz to nowsze zagrożenia związane z cyberbezpieczeństwem, wprowadzenie pracy zdalnej, kontroli trzeźwości itp. – wszystkie te obszary wymagają bieżącej analizy tego, czy przyjęte sposoby przetwarzania i zabezpieczenia danych osobowych są adekwatne do ryzyka naruszenia bezpieczeństwa osób, których dane są przetwarzane.

W praktyce chodzi tu o weryfikację:

- adekwatności przyjętych zabezpieczeń informatycznych pod kątem aktualnych ryzyk związanych m.in. z phishingiem i innymi zagrożeniami cyfrowymi;
- sposobu obiegu dokumentów – zapewniającego ich poufność i integralność.

Bieżące dostosowywanie i aktualizacja środków bezpieczeństwa są jednymi z podstawowych obowiązków każdego administratora. Odnosi się do niego art. 24 RODO, który nakazuje poddawanie przeglądom i uaktualnianie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odbywało się zgodnie z przepisami RODO i by móc to wykazać z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania oraz ryzyka naruszenia praw lub wolności podmiotów danych.

Analogiczny obowiązek dotyczy analizy skutków dla ochrony danych, która wymaga przeglądu przynajmniej tak często, jak zmienia się zagrożenie wynikające z konkretnej operacji przetwarzania, która może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

O tym, jak ważny jest to obowiązek, świadczy chociażby kara w wysokości prawie 2 mln zł nałożona przez prezesa UODO na Virgin Mobile. Jej podstawą były m.in. brak regularnych i kompleksowych testów, pomiarów i oceny skuteczności zastosowanych środków bezpieczeństwa danych oraz podejmowanie działań jedynie przy okazji pojawiających się podejrzeń podatności lub w związku ze zmianami organizacyjnymi, co w ocenie organu nadzoru nie pozwalało na zapewnienie stałego adekwatnego poziomu bezpieczeństwa.