

Retencja danych na poczcie elektronicznej

Poczta elektroniczna dla niemal każdego administratora stanowi pokaźny zbiór informacji, w tym również danych osobowych. Pracownicy na swoich skrzynkach służbowych niejednokrotnie posiadają wiadomości e-mail nawet sprzed kilku latu. Pomimo dużej liczby danych osobowych, przetwarzanych na poczcie elektronicznej, tematyka retencji danych w tym obszarze tj. usuwania przetwarzanych danych po określonym czasie, wciąż wydaje się lekceważona przez administratorów.

Konieczność usuwania danych po określonym czasie wynika bezpośrednio z zasady ograniczenia przechowywania, która została sformułowana w art. 5 ust. 1 lit. e RODO. Zgodnie z tą zasadą, przechowywanie danych w formie umożliwiającej identyfikację osoby, której dane dotyczą, powinno mieć miejsce przez okres nie dłuższy, niż jest to niezbędne do celów, dla których te dane są przetwarzane.

Niemniej konieczność przeglądu przetwarzanych danych oraz ich cyklicznego usuwania, jeśli nie są dłużej administratorowi potrzebne, wynika tak naprawdę pośrednio również z pozostałych zasad wyrażonych w art. 5 RODO, a mianowicie zgodności z prawem, ograniczenia celu, czy też prawidłowości. Administrator bowiem przetwarzając dane osobowe „w nieskończoność” naraża się na:

- brak podstawy prawnej do ich przetwarzania (zasada zgodności z prawem),
- przetwarzanie danych w sposób niezgodny z celami, dla których zostały zebrane,
- przetwarzanie nieprawidłowych, nieaktualnych danych (zasada prawidłowości).

Łatwo więc zauważyć, że opracowanie odpowiednich procedur retencji danych, w tym danych znajdujących się na poczcie elektronicznej, powinno stanowić dla administratora ważny element funkcjonowania systemu ochrony danych w jego organizacji. System ten nie będzie nigdy funkcjonował prawidłowo, jeśli administrator nie będzie działał w zgodzie z każdą z zasad wyrażonych w art. 5 RODO.

Jak zapanować nad tysiącami e-maili, które znajdują się na poczcie?

Po ustaleniu okresów retencji danych administrator powinien zadbać o zbudowanie świadomości swoich pracowników oraz współpracowników w tym zakresie oraz dbać o przestrzeganie ustalonych terminów w codziennej pracy. Jest to niestety najtrudniejsza część i często proces budowania retencji danych w organizacjach kończy się na wspomnianym pierwszym kroku. W opisywanym procesie piętą achillesową administratorów jest zazwyczaj poczta elektroniczna. Nawet jeżeli zostaną dla niej ustalone terminy przechowania danych w procedurze retencji danych, to często nie są potem stosowane w praktyce.

Rekomendacje w zakresie retencji danych w poczcie elektronicznej:

- spróbuj wyrobić w sobie nawyk regularnego przeglądania e-maili,
- usuwaj kopie robocze wiadomości, nieistotne e-maile, wiadomości zawierające nieaktualne informacje,

- jeśli korzystasz z Outlooka, używaj funkcji automatycznego archiwizowania i automatycznego usuwania e-mail, aby zapobiec utracie kontroli nad skrzynką mailową,
- przechowuj wiadomości e-mail w folderach, co automatycznie może przyczynić się również do przechowywania na skrzynce mailowej jedynie potrzebnych maili i tym samym ograniczenia ich do niezbędnego minimum.

Co powinna zawierać procedura retencji danych?

Budowanie świadomości pracowników powinno wiązać się w szczególności z opracowaniem odpowiedniej procedury, z którą każdy w organizacji będzie zapoznawany, i do której mógłby sięgać szukając właściwej drogi postępowania z konkretnymi danymi, w tym przetwarzanymi na poczcie elektronicznej. Taka procedura nie może być jedynie kolejnym dokumentem do kolekcji wskazującym, że dane osobowe należy usuwać i uwzględniającym przy tym kilka przykładowych kategorii danych wraz z terminami ich usunięcia.

Jeżeli procedura ma stanowić swego rodzaju przewodnik dla pracownika, administrator powinien postarać się jak najbardziej dostosować ją do swojej organizacji pod względem kategorii przetwarzanych danych i terminów ich usunięcia, uwzględniając przy tym dane przetwarzane na poczcie elektronicznej. Ważne jest, aby pracownicy, którzy używają na co dzień poczty elektronicznej, jako ich nieodłącznego narzędzia pracy, od początku budowali w sobie świadomość dobrych nawyków postępowania z tym narzędziem. Niestety, nadal w większości organizacji poczta elektroniczna „żyje własnym życiem” wraz z tysiącami zbędnych wiadomości, zawierających niemal zawsze dane osobowe.

Warto również uregulować w procedurze retencji danych, w części dotyczącej poczty elektronicznej, kwestie związane z różnego rodzaju dokumentami przesyłanymi w formie załączników poprzez wiadomości e-mail.

Administrator w procedurze retencji powinien oczywiście wskazać, jak długo jego pracownicy powinni przetwarzać poszczególne kategorie danych, w tym dane na poczcie elektronicznej. Jeżeli administrator korzysta lub planuje wprowadzić opcje automatycznego usuwania danych, czas po jakim usunięcie ma nastąpić również powinien wynikać z procedury.

Co z pocztą elektroniczną po zwolnieniu lub odejściu pracownika?

Temat dostępu do poczty elektronicznej pracowników po ustaniu zatrudnienia/współpracy budzi wiele kontrowersji. Zwłaszcza, że w wielu przypadkach dozwolony jest ograniczony użytek prywatny poczty służbowej, co generuje pewne oczekiwania pracowników dotyczące ich prywatności. Temat ten na swojej stronie podnosi również Europejski Inspektor Ochrony Danych (EIOD) wskazując, że pracodawcy nie powinni czytać e-maili swoich pracowników, ponieważ mogą one zawierać również informacje prywatne. EIOD dalej wyjaśnia, że jest to problematyczne wówczas, gdy pracownicy opuszczają organizację lub są nieobecni przez dłuższy czas, gdy informacje przechowywane tylko w ich skrzynkach pocztowych są potrzebne do zapewnienia ciągłości działania. W takiej sytuacji administratorzy powinni pamiętać, aby w posiadanych procedurach dotyczących

wykorzystywania narzędzi służbowych poinstruować pracowników o tym, że poczta co do zasady nie powinna być użytkowana w celach prywatnych, a w przypadku, gdy jakiegokolwiek wiadomości prywatne się pojawiają, należy je przechowywać w odpowiednio oznakowanym folderze, tak aby administrator miał świadomość, których wiadomości nie powinien przeglądać.

Ponadto osobom odchodzącym z organizacji należy jasno określić, czy i jak długo będą przechowywane ich skrzynki pocztowe. EIOD zwraca uwagę, że generalną zasadą dotyczącą okresów przechowywania jest: „przechowuj tak krótko, jak to możliwe oraz tak długo jak to konieczne”. Postanowienia w tym zakresie mogą być częścią procedury retencji danych lub zostać zawarte w procedurze dotyczącej wykorzystania narzędzi służbowych. Ważne, aby pracownik otrzymał wspomniane informacje i był w pełni świadomy tego, co będzie działo się z jego skrzynką oraz jej zawartością po jego odejściu.

Z powyższego płynie istotny wniosek dla administratorów w zakresie okresu przechowywania danych na poczcie służbowej byłych pracowników. Okres ten musi być możliwie najkrótszy, a osoby odchodzące z organizacji muszą mieć pełną świadomość tego, czy i na jak długo będą przechowywane ich skrzynki pocztowe.

Inspektor Ochrony Danych w ZUT-mgr Artur Kurek