RODO-ADVISOR

Adrian Gajzler
Prawnik w RODO-ADVISOR Sp. z o.o.

Zasady bezpiecznego przetwarzania danych osobowych za pośrednictwem skrzynki e-mail

Korzystanie z poczty elektronicznej jest niewątpliwie nieodłącznym elementem naszej codziennej pracy. W dzisiejszych czasach nie wyobrażamy już sobie prowadzenia własnego biznesu bez poczty elektronicznej. Firmy przetwarzające dane osobowe powinny zatem zadbać o to, aby osoby działające w ich strukturach zostały odpowiednio przeszkolone w zakresie zasad prawidłowego korzystania ze skrzynki e-mail. Co istotne, stosowane przez nie środki techniczne już nie wystarczają, bowiem to właśnie działania pracownika coraz częściej stają się bezpośrednią przyczyną wszelkich naruszeń w obszarze danych osobowych.

Każda z zatrudnionych przez firmę osób w ramach swoich zadań codziennie przetwarza szereg danych osobowych. Poczta e-mail to jedno z największych skupisk danych osobowych gromadzonych przez przedsiębiorcę w formie elektronicznej.

Prowadząc korespondencję mailową wymieniamy się rozmaitymi plikami, w tym obszernymi bazami danych osobowych konstruowanych w formie plików excel lub też skanami ważnej dla nas dokumentacji. Coraz częściej dostarczamy sobie materiały w formie elektronicznej aniżeli w formie papierowej, do której zdążyliśmy się już przyzwyczaić.

Znakomita większość z nich opiewa w ważne dla nas dane osobowe, które powinny być chronione przed ich ewentualnym przechwyceniem przez nieuprawnioną osobę. Zapominamy także o bardzo ważnej zasadzie bezpiecznego obrotu danymi. Dane osobowe mają być nie tylko chronione przed intruzami z zewnątrz. Istotne jest bowiem, by uwzględniać także ryzyka czyhające na nas wewnątrz instytucji. Tak też konieczna staje się także ochrona danych osobowych przed tymi pracownikami, których pracodawca mógł nie upoważnić do ich przetwarzania.

Na które wiadomości e-mail powinniśmy zwrócić uwagę?

Obowiązki związane z ochroną RODO powinny objąć wszelkie wiadomości e-mail zawierające dane osobowe, a zatem takie informacje, które pozwalają nam na bezpośrednią lub przynajmniej na pośrednią identyfikację konkretnej osoby. Najczęściej będą to imię i nazwisko, adres korespondencyjny, numer pesel lub telefon kontaktowy, nieco rzadziej wizerunek tychże osób.

Warto także zauważyć, że sam adres e-mail może być już uznany za daną osobową. Należy przy tym zwrócić uwagę, że w niektórych sytuacjach dane te przesyłane samodzielnie nie będą stanowić danych osobowych. Nie pozwalają one bowiem na ustalenie, której osoby one dotyczą. Nie oznacza to jednak, że tych danych nie trzeba chronić. Wręcz przeciwnie, co do zasady rekomenduję wprowadze-

nie do procedur zapisów ustanawiających jednolite zasady korzystania ze skrzynki mailowej. W mojej ocenie pewne rozwiązania powinny być stosowane bez względu na fakt, czy przesyłany plik zawiera dane osobowe w rozumieniu RODO.

Wszak należy uwzględnić te sytuacje, w których przechwycona korespondencja może zawierać poufne informacje na temat naszej firmy lub realizowanego przez nas przedsięwzięcia. Dodatkowo trzeba uwzględnić fakt, iż mimo przeprowadzanych w instytucji szkoleń personelu nie jesteśmy w stanie uniknąć tych sytuacji, w których pracownik mógłby błędnie uznać, iż treść przesyłanej przez niego wiadomości e-mail jest pozbawiona jakichkolwiek danych osobowych. Rezygnacja chociażby z zabezpieczania w postaci nadania hasła dostępu może doprowadzić do naruszeń RODO.

Czy służbowa skrzynka e-mail może służyć nam do celów prywatnych?

Wiele kontrowersji budzi zagadnienie korzystania ze skrzynki służbowej do celów innych niż prywatnych. Spotkałem się zarówno z argumentacją za jak i przeciw tej koncepcji. Mimo tego, iż takie rozwiązanie w wielu przypadkach stosunkowo mogłyby wprowadzić szereg ułatwień w zakresie prowadzenia bieżących spraw życia codziennego, to należy pamiętać, iż pociąga ono za sobą poważne ryzyka. Na co dzień zdecydowanie odradzam wprowadzanie takich rozwiązań swoim klientom.

Co ważne, trzeba zwrócić uwagę na to, iż pracodawca może samodzielnie ustalić zasady korzystania z poczty służbowej. I tu polecam skorzystać z możliwości wprowadzenia zakazu wykorzystywania poczty elektronicznej do celów prywatnych. Pozwoli to nam uniknąć wątpliwości chociażby co do ewentualnej możliwości monitorowania korespondencji prowadzonej przez pracowników.

Co istotne, informacja o zakazie prowadzenia korespondencji prywatnej za pośrednictwem służbowej skrzynki, jak i o jej monitorowaniu przez pracodawcę powinna zostać przekazana pracownikowi w sposób jednoznaczny, czytelny, a także zgodny z przepisami prawa. Wiąże się to z faktem, iż pracownik powinien posiadać całkowitą świadomość tego, że taki zakaz został przez pracodawcę wprowadzony, a za jego nieprzestrzeganie grożą mu odpowiednie konsekwencje.

W jaki sposób pracownik powinien korzystać ze skrzynki e-mail?

Każda z osób korzystających ze skrzynki mailowej powinna otrzymać od pracodawcy odpowiednie instrukcje postępowania. W celu zachowania poufności danych osobowych należy wskazać, iż pracownik powinien bezwzględnie przestrzegać zakazu udostępniania komukolwiek własnego hasła do skrzynki mailowej.

Korespondencja mailowa z kolei powinna być prowadzona ze szczególną ostrożnością. I tak w przypadku korespondencji wychodzącej istotne jest ograniczanie dostępu do załączonych plików z danymi poprzez nadawanie im odpowiednich haseł dostępu. Co prawda RODO nie wymusza na nas takiego obowiązku, a zatem jego nieprzestrzeganie nie stanowi niezgodności z przepisami prawa. Szyfrowanie stosuje się jednak w celu zmniejszenia ryzyka wystąpienia wycieku danych.

Mając na celu możliwość powstania ewentualnych naruszeń praw lub wolności osób fizycznych, których dane dotyczą, a co za tym idzie stwierdzenia pewnych nieprawidłowości po stronie przedsiębiorcy, zalecam wprowadzenie obowiązku szyfrowania korespondencji wychodzącej. Ważne jest także to, w jaki sposób przekazujemy odbiorcy hasło do zabezpieczonej dokumentacji. Rekomenduję, aby w miarę możliwości uczynić to za pośrednictwem innego kanału informacji, na przykład kierując do niego wiadomość sms.

Unikałbym także przesyłania danych osobowych w tzw. korespondencji masowej, a zatem kierowanej do szerokiej grupy odbiorców. Jeśli jest to konieczne, szczególnie polecam wówczas skorzystanie z opcji szyfrowania załączników z danymi osobowymi lub innymi poufnymi informacjami.

Co zaś się tyczy korespondencji wewnętrznej to zaleca się, by także ten obszar uwzględnić w ramach konstruowania przez przedsiębiorcę swoich wewnętrznych procedur. Tu ryzyka związane z ewentualnym wyciekiem danych są zdecydowanie niższe niż w przypadku korespondencji wycho-

dzącej. Nadal zaleca się jednak prowadzić niezbędne działania mające na celu zwiększanie bezpieczeństwa danych. Wybór odpowiedniego sposobu wymiany plików wewnątrz instytucji powinien być oczywiście zależny od danego podmiotu oraz rodzaju i ilości danych, które są przez niego przetwarzane. Bardzo częstym mechanizmem, który wykorzystuje się w tym celu jest umieszczanie plików z danymi osobowymi na udostępnionych odpowiednim pracownikom dyskach sieciowych.

Jakie zagrożenia mogą wiązać się z nieprawidłowym korzystaniem ze skrzynki e-mail?

Bardzo ważna jest sama świadomość pracownika korzystającego ze skrzynki, a także jego wiedza odnośnie zagrożeń, które mogą czyhać na niego w sieci. I tak warto zadbać o to, aby pracownik potrafił chociażby rozpoznać, która wiadomość mailowa może stanowić atak phishingowy mający na celu wyłudzenie poufnych danych.

Warto także zauważyć, iż w wielu sytuacjach to od pracownika będzie zależeć, czy dalsze konsekwencje naruszenia będą trwać nadal, czy też uda się szybko ustalić źródło naruszenia, a także zapobiec dalszemu wyciekowi danych. Na uwagę zasługuje także zjawisko korzystania przez pracowników z prywatnych urządzeń mobilnych. Niekiedy w organizacjach pracownicy wykorzystują prywatne nośniki do zadań związanych z obowiązkami służbowymi. Odradzam tego typu działania. Trzeba pamiętać, że taki pracownik z łatwością będzie mógł wykorzystać w niewłaściwy sposób chociażby dane osobowe zgromadzone w wiadomościach e-mail.

Zalecam, aby w miarę możliwość kontrolować korespondencję wychodzącą pracowników. I tak też przekazywanie poufnych wiadomości mailowych na prywatną skrzynkę pocztową zawsze powinno zostać przez nas zweryfikowane. Takie działanie może bowiem prowadzić do naruszenia praw lub wolności osób fizycznych, których dane są przetwarzane.

Czy pracodawca może używać imiennego adresu e-mail byłego pracownika?

W ostatnim czasie na stronie Urzędu Ochrony Danych Osobowych pojawił się komunikat, który rozwiał szereg wątpliwości związanych z korzystaniem przez pracodawcę z imiennych adresów e-mail byłych pracowników.

Dzieje się tak często w sytuacji, gdy pracownik odpowiadał za kontakt z kontrahentem, z którym pracodawca kontynuuje współpracę. W ocenie Prezesa UODO tego rodzaju działanie ma swoją podstawę w postaci prawnie uzasadnionego interes administratora danych. Mając na względzie treść tego stanowiska należy uznać za prawidłową praktykę stosowaną przez pracodawców polegającą na stosowaniu automatycznej odpowiedzi kierowanej do klientów lub kontrahentów.

Ważne jest, by w takiej odpowiedzi zawrzeć informację o tym, że dany pracownik nie jest już zatrudniony w strukturach podmiotu oraz wskazać, pod jakim adresem mailowym można kontaktować się z aktualnymi jego przedstawicielami.

Prezes UODO wyraźnie jednak stwierdził, iż adres mailowy zawierający imię i nazwisko byłego pracownika nie może być aktywnie wykorzystywany przez przedsiębiorcę do pozyskiwania nowych klientów. Należy się z tym całkowicie zgodzić, bowiem takie działanie niewątpliwie wykraczałoby poza przyjętą podstawę przetwarzania, jak i byłoby niezgodne z zasadą minimalizacji przetwarzania danych osobowych.