Warszawa, dn. 16.02.2023 r.

Retencja w rekrutacji, czyli o usuwaniu danych kandydatów do pracy

W grudniowym wpisie Katarzyna Ułasiuk-Delamare opracowała obszerne podsumowanie zagadnień związanych z ochroną danych osobowych w procesach rekrutacyjnych. Dzisiaj rozszerzę wątek, któremu poświęcony został ostatni akapit tego opracowania, mianowicie: usuwanie danych osobowych w procesach rekrutacyjnych.

Obowiązek ograniczonego przetwarzania danych osobowych wynika wprost z przepisów RODO, tj. artykułu 5 oraz motywu 39, których fragmenty brzmią jak poniżej:

Art. 5 ust. 1: *„Dane osobowe muszą być: (…) e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; (…)"*

Motyw 39: *„(…) Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu. (…)"*

Temat wydaje się prozaiczny, jednak nie jest oczywisty dla wielu organizacji. Pracownicy spoza struktur jednostek odpowiedzialnych za sprawy pracownicze są angażowani w procesy rekrutacyjne (np. dyrektorzy, kierownicy, menadżerowie) i z tego powodu nie powinni zostać pomijani w procesie usuwania danych.

Pozyskiwanie danych kandydatów do pracy

Obecnie pracodawcy dysponują szeregiem możliwości w rekrutowaniu pracowników. Procesy rekrutacyjne mogą być prowadzone zarówno przez zatrudnionych specjalistów do spraw rekrutacji w strukturze firmy bądź zlecane firmom zewnętrznym, które profesjonalnie świadczą usługi związane z rekrutacją kandydatów do pracy (outsourcing). Jest wiele możliwych rozwiązań dotyczących pozyskiwania danych kandydatów do pracy. Mogą to być m.in.:

- własna strona internetowa z zakładką „Oferty pracy". Popularnym rozwiązaniem zaszytym w taką funkcjonalność jest przesyłanie aplikacji kandydatów na skrzynkę e-mail, funkcyjną np. rekrutacje@nazwafirmy.pl lub imienną - osoby odpowiedzialnej za procesy rekrutacyjne;
- korzystanie z rozwiązania dostarczanego przez firmę zewnętrzną, oferującą zarządzanie ofertami pracy na dedykowanej platformie internetowej. Najbardziej popularnymi rozwiązaniami są: udostępnienie ogłoszenia, które przekierowuje do aplikowania za pośrednictwem strony internetowej pracodawcy (jak opisano w pierwszym przykładzie) lub zarządzanie dokumentami aplikacyjnymi za pośrednictwem serwisu, do którego pracodawca ma dostęp;
- system poleceń pracowników – osoba zatrudniona w firmie poleca kandydata do pracy i może przesłać CV osoby do działu kadr lub bezpośrednio do osoby rekrutującej do swojego zespołu. W takiej sytuacji, obrót dokumentami zazwyczaj odbywa się na wymianie e-maili;
- osobiste złożenie dokumentów aplikacyjnych przez kandydata w tradycyjnej formie papierowej;
- zlecenie procesów rekrutacyjnych na zewnątrz firmy (outsourcing).

Niezależnie od przyjętego rozwiązania, niezmienne pozostają zasady przetwarzania danych osobowych określone w RODO. Na potrzeby niniejszego opracowania załóżmy, iż spełniliśmy przesłanki:

a. zgodności z prawem, rzetelności, przejrzystości,
b. ograniczonego celu przetwarzania,
c. minimalizacji danych,
d. prawidłowości danych,
e. zapewnienia integralności i poufności.

W ramach realizacji zasady przejrzystości, spełniliśmy wobec kandydata obowiązek informacyjny. Co do zasady, klauzula powinna zawierać informację, iż dane kandydata do pracy usuwamy niezwłocznie po zakończeniu procesu rekrutacyjnego.

„Dane zgromadzone w procesie rekrutacyjnym usuniemy niezwłocznie po zakończeniu rekrutacji."

Jeżeli korzystamy z rozwiązań technologicznych dostarczanych przez firmę zewnętrzną, która ma zaszyty mechanizm retencji tj. automatycznego usuwania danych po konkretnym okresie – na przykład trzech miesięcy – możemy taką informację zawrzeć w obowiązku informacyjnym:

„Dane zgromadzone w procesach rekrutacyjnych będziemy przetwarzać przez okres nie dłuższy niż 3 miesiące od dnia zakończenia procesu rekrutacji."

Faktycznie usunięcie danych

Wydaje się, iż zlecając czynności rekrutacyjne na zewnątrz organizacji lub korzystając z gotowych rozwiązań technologicznych, kwestię retencji danych, czyli ich usuwania mamy zabezpieczoną. Jednak **należy pamiętać o tych zasobach, z których dane nie są automatycznie usuwane,** czyli m.in.:

- dokumenty przechowywane na skrzynkach pocztowych. Należy pamiętać o każdej skrzynce mailowej, tj. funkcyjnej i imiennej, o skrzynkach odbiorczej (jeżeli otrzymaliśmy CV), nadawczej (jeżeli przesłaliśmy aplikację kandydata do innej osoby) i elementach usuniętych;
- zasoby sieciowe – lokalne i współdzielone:
  - foldery: „Pobrane", „Dokumenty" oraz wszelkie pozostałe, w których zapisywaliśmy dane kandydatów,
  - „Kosz",
  - dane na serwerze firmowym.

Jeżeli analizujemy dane z CV w odrębnym arkuszu, wprowadzając zbiorczo informacje w celu porównania doświadczenia i kwalifikacji kandydatów, również w tej sytuacji należy przeanalizować zakres zapisywanych danych pod kątem ewentualnego usunięcia.

Przechowywanie danych kandydata w celu przyszłych rekrutacji powinno również być zabezpieczone posiadaniem odpowiedniej zgody na przetwarzanie danych osobowych w tym celu. Należy zweryfikować, czy kandydat udzielił nam takiej zgody lub o takową poprosić.

Właściciel biznesowy czynności

Zazwyczaj czynności związane z procesami rekrutacyjnymi przypisywane są pracownikom działów HR. W zakresie usuwania danych należy weryfikować, czy zobowiązanie do usuwania danych znajduje się w postanowieniach umownych w związku ze współpracą z innym podmiotem lub czy rozwiązania systemowe, z których korzystamy, uwzględniają automatyczne usuwanie danych lub pozwalają usuwać dane ręcznie. Jeżeli w organizacji praktykuje się przesyłanie aplikacji kandydatów w e-mailach, dobrym rozwiązaniem jest dodanie do wiadomości zdania:

Pamiętaj o usunięciu wiadomości wraz z załącznikiem po zakończeniu procesu rekrutacyjnego.

Takie przypomnienie może być realizowane cyklicznie przez pracownika działu HR do kadry kierowniczej lub do wszystkich pracowników, jeżeli w organizacji funkcjonuje program poleceń. Jeżeli klauzula na potrzeby rekrutacji zawiera informację o okresie trzech miesięcy przetwarzania danych osobowych, taki monit również może być realizowany kwartalnie.

Agnieszka Dominiak – specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.