POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

Pracodawca, który nieprawidłowo gromadzi i przetwarza dane osobowe swoich pracowników i osób ubiegających się o zatrudnienie, naraża się na odpowiedzialność cywilną i karną.

Rozmowa z **Michałem Serzyckim, Generalnym Inspektorem Ochrony Danych Osobowych.**

Czy dane osobowe, a w zasadzie ich zbiór powinien być przechowywany w specjalnych warunkach, np. w sejfie lub specjalnie do tego przeznaczonych pomieszczeniach? Czy są jakieś szczególne wymagania co do zabezpieczeń komputerów, w których pamięci znajdują się dane osobowe w formie elektronicznej?

– Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych stanowi, że administrator danych osobowych powinien zadbać o należyte zabezpieczenie danych osobowych, tak aby nie mogły być one ukradzione lub wyniesione. Na administratorze ciąży również obowiązek takiego zabezpieczenia danych, aby nie miały do nich dostępu żadne osoby nieuprawnione, nawet z tej samej instytucji.

Nie ma natomiast przepisów mówiących wprost, jakie konkretnie środki techniczne (np. kasy pancerne) zastosować, żeby ten cel osiągnąć.

Ustawa o ochronie danych osobowych przesądza jedynie, że zastosowane zabezpieczenia muszą być adekwatne do występujących zagrożeń. W związku z tym rodzaj zastosowanych zabezpieczeń zależy od konkretnego przypadku. Mogą to być kasy pancerne, specjalne zamki w drzwiach, odpowiednie hasła dostępu do komputerów budowane na podstawie szerokiego zestawu znaków, w tym znaków specjalnych i cyfr.

Bardzo często inspektorzy w czasie kontroli dokonują ocen, czy zastosowane środki bezpieczeństwa są adekwatne do zagrożeń. Jako przykład najprostszego sposobu zabezpieczenia danych można podać odpowiednie ustawienie monitora, na którym widoczne są dane osobowe, tak aby osoba nieuprawniona nie mogła przeczytać, co się na nim znajduje.

Jakie warunki muszą spełniać osoby mające dostęp do baz danych osobowych?

– Regulacja dotycząca tego zagadnienia została zawarta w ustawie o ochronie danych osobowych. Przepis art. 39 ustawy wskazuje, że osoba dopuszczona do przetwarzania danych osobowych musi posiadać upoważnienie wydane przez administratora danych osobowych. Upoważnienie takie musi zawierać imię i nazwisko osoby upoważnionej, zakres, datę nadania i ustania upoważnienia oraz identyfikator osoby upoważnionej, jeżeli dane są przetwarzane w systemie informatycznym. W treści upoważnienia powinna również znaleźć się klauzula zobowiązująca do zachowania w tajemnicy danych osobowych oraz sposobu ich zabezpieczenia. Dodatkowo administrator danych osobowych musi prowadzić ewidencję wydanych upoważnień.

Pracodawca będący administratorem danych zawsze musi mieć kontrolę nad tym, kto i w jaki sposób zajmuje się przetwarzaniem danych osobowych w firmie.

Oprócz tego jest jeszcze kwestia powołania administratora bezpieczeństwa informacji, która jest często pomijana. W ustawie został zamieszczony przepis, nakładający na administratora danych osobowych obowiązek powołania administratora bezpieczeństwa informacji, chyba że administrator danych osobowych sam pełni tę funkcję.

Ustawa nie nakłada na taką osobę wymogu posiadania specjalnych kwalifikacji. Na pewno powinna ona mieć wiedzę na temat nowych technologii, znać przepisy dotyczące ochrony danych osobowych oraz potrafić odpowiednio je zastosować.

Czy pracodawca może zlecić przetwarzanie danych osobowych firmie zewnętrznej? Kto może kontrolować sposób przechowywania jak też inne formy przetwarzania

danych osobowych? Czy pracodawca może kontrolować swoich podwładnych lub pracowników firmy zewnętrznej, której zostały powierzone dane osobowe?

– Pracodawca może powierzyć przetwarzanie danych osobowych firmie zewnętrznej, musi jednak pamiętać, że samo powierzenie przetwarzania danych osobowych firmie zewnętrznej nie zwalnia go z obowiązków administratora, co wynika z art. 31 ustawy o ochronie danych osobowych. W takiej sytuacji za zabezpieczenie powierzonych danych osobowych wspólną odpowiedzialność ponoszą powierzający dane i osoba, firma, której powierzono przetwarzanie danych osobowych. Pracodawca pełniący cały czas funkcję administratora powinien mieć kontrolę nad tym, aby nawet wówczas, kiedy dane podlegają przetwarzaniu nawet przez firmę zewnętrzną specjalizującą się w tego typu zadaniach, powierzone dane osobowe były w należyty sposób zabezpieczone. W przepisach karnych ustawy o ochronie danych osobowych mówi się wyraźnie o odpowiedzialności karnej administratora i administrującego.

Jednak biorąc pod uwagę odpowiedzialność, jaką administrator ponosi za przetwarzanie powierzonych danych, wszystkie szczegóły dotyczące powierzenia powinny być określone w pisemnej umowie. Dodatkowo dla własnego bezpieczeństwa administrator powinien nadzorować rzetelność wykonywania umowy.

Ponadto powierzenie przetwarzania danych osobowych warto zlecić starannie dobranej, profesjonalnej firmie. Należy przy tym zaznaczyć, że pracodawca będący administratorem danych przy jej wyborze powinien zwrócić szczególną uwagę na to, czy w firmie powołany jest administrator bezpieczeństwa informacji, czy jest odpowiedni poziom zabezpieczeń oraz czy są wydane upoważnienia do przetwarzania danych osobowych. Trzeba też pamiętać, że w tej chwili nie są wydawane żadne certyfikaty, które potwierdzałyby rzetelność bądź dobre zabezpieczenia danych osobowych przez firmy, które zajmują się przetwarzaniem danych osobowych.

Co powinien zrobić pracodawca w przypadku, gdy dysponuje danymi osobowymi kandydatów do pracy, którzy nie zostali przyjęci?

– W sytuacji gdy rekrutacja została zakończona, zgromadzonych danych osobowych osób niezatrudnionych nie można dalej przetwarzać. Pracodawca, aby móc je wykorzystać np. w celu przyszłej rekrutacji, musi uzyskać zgodę osoby składającej aplikację. Taka zgoda może zostać wyrażona przez zamieszczenie w życiorysie odpowiedniej klauzuli, np. „Wyrażam zgodę na przetwarzanie danych osobowych na potrzeby przyszłej rekrutacji". Natomiast jeśli takiej klauzuli nie ma, to takie aplikacje po zakończonej rekrutacji powinny być albo odesłane, albo zniszczone.

Jakie przepisy z zakresu ochrony danych osobowych pracodawcy naruszają najczęściej?

– Najczęściej spotykane naruszenia ustawy dotyczą właśnie art. 221 Kodeksu pracy. Bardzo często kandydaci do pracy chcą napisać więcej o sobie, aby zwiększyć swoje szanse na zdobycie dobrej pracy. Natomiast pracodawcy, zbierając takie dane bez odpowiednich klauzul, naruszają przepisy, gdyż bez podstawy prawnej zbierają dane osobowe, w których posiadaniu nie powinni być. Uważam, że to trochę nieżyciowe regulacje prawne. Obecnie bardzo często zdarza się również, że pracodawca chce wiedzieć więcej o rekrutowanym pracowniku, szuka więc potrzebnych informacji, np. na portalach społecznościowych, czemu trudno się dziwić.

Zauważając ten problem, wystąpiłem do organizacji pracodawców i pracowników, instytucji zajmujących się ochroną praw człowieka, a także reprezentantów świata nauki z prośbą o konsultacje w sprawie zmiany nieżyciowych przepisów. Zwróciłem uwagę na potrzebę wprowadzenia takich uregulowań prawnych, które wyważą interesy obu stron stosunku pracy – pracodawcom umożliwią lepsze poznanie umiejętności i predyspozycji kandydatów do pracy i pracowników, a pracownikom zagwarantują prawo do ochrony ich prywatności.

Dziękuję za rozmowę.

Rozmawiał Paweł Łukaszuk