

Cykl GIODO radzi...;)



GIODO

Generalny Inspektor
Ochrony Danych Osobowych

**Jak chronić dane osobowe
podczas wakacji?**

GIODO radzi ;)

Jak chronić dane osobowe w czasie wakacji? Tylko znajomość tematu pozwoli nam

się uchronić od najczęściej popełnianych błędów.

W INTERNECIE

Nie zamieszczajmy w Internecie informacji, dokąd i na jak długo wyjechaliśmy, i że nie ma nas w domu. Taka wiadomość to sygnał dla złodziei. Zanim więc podzielimy się ze znajomymi jakąkolwiek informacją, umieszczając ją np. na portalu społecznościowym, zastanówmy się, czy nie narażamy się przez to na niebezpieczeństwo. Dotyczyć to może również zamieszczania zdjęć. Ich publikacja w zależności od tego, w jaki sposób widniejąca na nich osoba wygląda - czy jest np. skąpo ubrana czy wręcz roznegliżowana - może być uznana za zachętę do kontaktu w celach, których by tego nie chciała.

Również osoby trzecie mogą nie życzyć sobie, by ich wizerunek znalazł się w sieci. Pamiętajmy, że publikując informację o innych osobach, możemy nieświadomie narazić je na szkody osobiste, nawet nie zdając sobie z tego sprawy. Może się bowiem okazać, że nie życzą sobie one informowania innych o miejscu i czasie ich pobytu, a zdjęcie może takie informacje zdradzać. Zatem przed jego udostępnieniem w Internecie, lepiej zapytać o zgodę widoczne na nim osoby, nawet gdy są to osoby nam bliskie. W przeciwnym przypadku narażamy się nie tylko na pretensje z ich strony, ale też na proces sądowy z powodu naruszenia ich dóbr osobistych.

Rozważnie musimy także podchodzić do umieszczania zdjęć swoich dzieci w Internecie, ponieważ może to dla nich stanowić zagrożenie. Trzeba pamiętać, że treści, które udostępniamy w Internecie, pozostają w nim na zawsze. Dlatego przed zamieszczeniem zdjęcia dzieci, zawsze warto pomyśleć o konsekwencjach takiego działania, zarówno teraz, jak i w przyszłości. Kradzież, powielenie fotografii i wykorzystanie wizerunku dziecka w negatywnym kontekście, modyfikacja zdjęcia i udostępnienie go w postaci mema, a w skrajnych przypadkach kradzież tożsamości lub pożywka dla osób o pedofilskich skłonnościach - to tylko przykładowe zagrożenia, na jakie rodzice bez namysłu publikujący zdjęcia w Internecie, narażają swoje dzieci. Dziecko, tak jak dorosły, ma prawo do prywatności i prawo ochrony dóbr osobistych. Co więcej, fakt, że samo nie umie jeszcze nimi zarządzać, tym bardziej powinien skłaniać rodziców do tego, by robili to w jego imieniu rozważnie.

Pamiętajmy także o potencjalnych zagrożeniach, z jakimi wiąże się korzystanie z publicznych sieci wi-fi. Jesteśmy wówczas narażeni m.in. na przechwytywanie wysyłanych przez nas informacji, co może umożliwić np. zdobycie loginu oraz hasła

do naszego konta bankowego lub innych serwisów, z których korzystamy. W tym kontekście warto wskazać, że używając cudzego sprzętu, zawsze należy wylogować się z danego portalu lub usługi w Internecie po zakończeniu korzystania z niej. Jeżeli zaś przez przypadek użyjemy opcji „zapisz/zapamiętaj hasło”, pomocne okaże się wyczyszczenie plików cookies z pamięci przeglądarki. Jednocześnie dobrze jest regularnie kontrolować stan naszego konta bankowego, by w razie potrzeby móc szybko zareagować na ewentualne włamanie się do niego, a także dokładnie sprawdzać wydruk po przeprowadzonej transakcji przy użyciu karty płatniczej. W przypadku korzystania z własnego sprzętu, np. laptopa, zadbajmy o zabezpieczenie znajdujących się na nim danych, stosując szyfrowanie dysku. Jeśli go stracimy, złodziej lub znalazca nie będzie miał dostępu do przechowywanych na nim danych.

PRZY REKRUTACJI DO PRACY SEZONOWEJ

Okres wakacyjny to wzmożona liczba ofert dotyczących pracy sezonowej, co sprzyja oszustom, wyłudzającym dane osobowe. Ubiegający się o pracę np. przy zbieraniu owoców i warzyw czy też w turystyce i gastronomii, są przez to narażeni na ryzyko utraty zawartych w CV informacji. Często bowiem zamieszczane ogłoszenia o rekrutacji służą jedynie pozyskaniu danych osobowych osób ubiegających się o pracę, a nie ich zatrudnieniu. Czasami dane pozyskiwane są na potrzeby budowy osobnej bazy danych, a czasami wręcz w celach przestępczych.

Dlatego, przy udostępnianiu danych należy być ostrożnym i zwracać uwagę m.in. na to, czy prowadzący rekrutację potencjalny pracodawca podaje informacje, w tym nazwę i adres i inne dane kontaktowe, które pozwolą zweryfikować jego wiarygodność. Warto też przeanalizować, czy nie żąda zbyt wielu naszych danych, pamiętając, że ich zakres dokładnie określa art. 221 Kodeksu pracy, i że żadnych dodatkowych informacji wykraczających poza ten katalog nie musimy mu udostępniać. Są to: imię (imiona) i nazwisko, imiona rodziców, data urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie oraz przebieg dotychczasowego zatrudnienia. Ponadto pracodawca ma prawo żądać od osoby ubiegającej się o pracę podania także innych danych osobowych, jeżeli obowiązek taki wynika z odrębnych przepisów, np. zaświadczenie o niekaralności, specjalistyczne uprawnienia.

Biorąc zaś pod uwagę przepisy ustawy o ochronie danych osobowych, należy pamiętać, że każdy podmiot pozyskujący dane od osób, których one dotyczą, jest

zobowiązany do poinformowania ich m.in. o swojej pełnej nazwie i adresie swojej siedziby, celu zbierania danych, prawie dostępu do swoich danych oraz prawie ich poprawiania, a także o dobrowolności albo o obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej. Nasz niepokój powinny zatem wzbudzać takie sytuacje, w których firma prowadząca rekrutację nie podaje na swój temat wystarczającej ilości informacji (a zgodnie z ustawą o ochronie danych osobowych powinna to zrobić), lub prosi nas o podanie zbyt wielu danych osobowych, tj. w zakresie wykraczającym poza przepisy Kodeksu pracy.

28-06-2016

- [Udostępnij](#)
- [Drukuj](#)
- [PDF](#)

[Wszystkie aktualności](#)