

Kraków, 22.12.2021

Sweco Polska Sp. z o.o.
ul. Franklina Roosevelta 22, 60-829 Poznań
tel.: (61) 864 93 00, e-mail: info.pl@sweco.pl / rodo@sweco.pl
KRS 0000140225, NIP 5220004190, REGON 006744144

INFORMACJA O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Szanowni Państwo,

działając w imieniu własnym (jako podmiot przetwarzający) oraz w imieniu Generalnego Dyrektora Dróg Krajowych i Autostrad (administratora danych osobowych), informuję, że wskutek niewłaściwej anonimizacji danych osobowych doszło do zdarzenia, w wyniku, którego mogły one dostać się w niepowołane ręce. Realizując obowiązek, jaki na administratora danych oraz podmiot przetwarzający nakładają przepisy prawa, przekazujemy poniżej informacje na temat tego zdarzenia, działań, jakie w związku z nim podejmujemy, a także informacje o krokach, które mogą Państwo podjąć, aby zminimalizować ryzyko negatywnych konsekwencji tego zdarzenia.

OPIS ZDARZENIA

6 grudnia 2021 r. na stronie internetowej www.dk7rabkachyzne.pl opublikowaliśmy raport z przeprowadzonych spotkań informacyjnych związanych z zadaniem pn. „Opracowanie studium korytarzowego dla zadania Budowa drogi dwujezdniowej klasy GP (na parametrach klasy S) w ciągu DK7 na odc. Rabka - Chyżne”. W treści tego raportu znalazły się niewłaściwie zanonimizowane listy obecności zawierające imiona, nazwiska, podpisy, a także numery PESEL uczestników spotkań z mieszkańcami. Z danymi tymi można było się zapoznać po zastosowaniu dostępnego na rynku oprogramowania komputerowego (jednak nie jest to oprogramowanie domyślne instalowane na komputerach i standardowo nie jest zainstalowane na nich). Dokumenty zawierające dane osobowe były opublikowane od 6 grudnia 2021 r. (ok. godz. 20:00) do 7 grudnia 2021 r. (do godz. 8:40). Po otrzymaniu informacji o możliwym dostępie do danych niezwłocznie zablokowaliśmy stronę internetową i dokonaliśmy aktualizacji dostępnych na niej materiałów. Dokument, który jest obecnie dostępny, został właściwie zanonimizowany i nie ma technicznych możliwości odsłonięcia zawartych w nim danych osobowych.

MOŻLIWE KONSEKWENCJE

Wskazane wyżej dane osobowe mogły zostać pobrane przez osoby nieupoważnione. Konsekwencją tego może być ich nieuprawnione wykorzystanie w kontaktach z firmami i instytucjami, które zawierają umowy i świadczą usługi na podstawie ograniczonej liczby danych osobowych przekazywanych przez klienta, np. przez Internet lub telefonicznie,

i jednocześnie nie dokonują weryfikacji tych danych z dowodem osobistym lub danymi pozyskiwanymi z innych źródeł.

W związku z powyższym istnieje ryzyko, że Państwa dane osobowe zostaną wykorzystane przez osoby trzecie do:

- próby wyłudzenia pożyczki w instytucjach finansowych;
- próby uzyskania dostępu do systemu świadczeń opieki zdrowotnej i zgromadzonych w nich danych o stanie zdrowia;
- próby udziału w Państwa imieniu w głosowaniu nad środkami budżetu obywatelskiego;
- próby wyłudzenia ubezpieczenia lub środków z ubezpieczenia;
- próby zawarcia w Państwa imieniu umów cywilnoprawnych, np. zakupu towarów i usług;
- próby założenia konta na stronie internetowej, forum dyskusyjnym, w sklepie internetowym lub innym tego rodzaju serwisie;
- próby wyłudzenia w oparciu o już posiadane dane dalszych Państwa danych osobowych.

ZABEZPIECZENIE PRZED NEGATYWNYMI KONSEKWENCJAMI:

Aby zabezpieczyć się przed ryzykiem wystąpienia negatywnych konsekwencji, w tym nieuprawnionego wykorzystania Państwa danych, zalecamy ewentualne rozważenie podjęcia następujących kroków:

- założenie konta w systemie informacji kredytowej i gospodarczej celem monitorowania swojej aktywności kredytowej (na rynku dostępne są systemy, instytucje i przedsiębiorstwa, które oferują usługi pozwalające na monitorowanie swojej aktywności kredytowej, np. Biuro Informacji Kredytowej S.A. (<https://www.bik.pl>), Biuro Informacji Gospodarczej InfoMonitor S.A. (<https://big.pl>), Krajowy Rejestr Długów Biuro Informacji Gospodarczej S.A. (<https://krd.pl>), serwis CHRONPESEL (<https://www.chronpesel.pl>) - część tego typu usług jest płatna;
- w przypadku stwierdzenia jakichkolwiek nieprawidłowości - zgłoszenie tego faktu organom ścigania;
- zachowanie ostrożności przy potwierdzaniu danych osobowych, zwłaszcza za pośrednictwem Internetu czy telefonu;
- dokładną analizę kierowanych do Pani/Pana komunikatów, zawartych np. w wiadomościach SMS lub e-mail, by uniknąć np. ataku phishingowego, którego celem może być wyłudzenie dodatkowych danych czy uzyskanie danych dostępowych do internetowych systemów bankowych bądź innych usług, z których Pani/Pan korzysta.

Należy również zauważyć, że coraz więcej firm i instytucji wprowadza procedury bezpieczeństwa, które mają zapobiegać tego rodzaju próbom podszycia się pod inne osoby. Odbywa się to poprzez żądanie okazania przy zawieraniu umowy dokumentu potwierdzającego tożsamość lub weryfikując podawane dane osobowe z innymi Państwa danymi osobowymi, do których mają dostęp.

GDZIE MOGĄ PAŃSTWO UZYSKAĆ WIĘCEJ INFORMACJI ?

Jeżeli mają Państwo jakiegokolwiek pytania lub chcieliby Państwo uzyskać dodatkowe informacje w związku z zaistniałym zdarzeniem, prosimy o kontakt z:

1) Inspektorem Ochrony Danych wyznaczonym przez Sweco Polska Sp. o.o.:

Imię i nazwisko: Barbara Wojtas
e-mail: barbara.wojtas@sweco.pl
tel.: 603 078 744

2) Inspektorem Ochrony Danych wyznaczonym przez GDDKiA:

imię i nazwisko: Błażej Korczak
e-mail: bkorczak@gddkia.gov.pl
tel.: 22 375 88 80

Niezmiernie nam przykro, że doszło do takiej sytuacji i przepraszamy za wszystkie niedogodności, które mogły albo mogą Państwa spotkać w wyniku zdarzenia. Podjęliśmy starania, aby skutki naruszenia były jak najmniej odczuwalne dla Państwa. Zapewniamy też, że zarówno Sweco Polska Sp. z o.o., jak i GDDKiA podejmują wszelkie kroki, w tym wymagane na gruncie przepisów o ochronie danych osobowych, aby podobne zdarzenia nie powtórzyły się w przyszłości.

Z wyrazami szacunku
KIEROWNIK PROJEKTU


mgr inż. Andrzej Borowski

Załącznik: pełnomocnictwo dla osoby dokonującej powiadomienia w imieniu i na rzecz administratora danych osobowych