Gdańsk, dnia 29.05.2024 r.

UCK Uniwersyteckie Centrum Kliniczne

Zawiadomienie o naruszeniu ochrony danych osobowych

W trybie art. 34 pkt 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO) Uniwersyteckie Centrum Kliniczne, Samodzielny Publiczny Zakład Opieki Zdrowotnej z siedzibą przy ul. Dębinki 7, 80-952 Gdańsk, zarejestrowany w VII Wydziale Gospodarczym Krajowego Rejestru Sądowego Sądu Rejonowego Gdańsk – Północ w Gdańsku pod numerem KRS 0000122150, NIP 957-07-30-409, REGON 000288640 (dalej jako UCK) informuje **o stwierdzeniu naruszenia ochrony Pani/Pana danych osobowych.**

Poniżej przekazujemy informacje dotyczące ww. naruszenia, podjętych przez nas i przez naszego podwykonawcę – Selly Sp. z o.o. działań, a także działań, które Pani/Pan może podjąć w związku z ww. naruszeniem. Prosimy o uważną lekturę niniejszego zawiadomienia.

Sposób wykrycia naruszenia oraz inne istotne informacje

27.05.2024 r. UCK otrzymało od Selly Sp. z o.o. zgłoszenie o naruszeniu ochrony danych osobowych polegającym na nieuprawnionym dostępie do znajdujących się na serwerze ww. podmiotu danych dotyczących klientów sklepu internetowego, których Administratorem Danych jest UCK.

Naruszenie zauważone zostało przez Selly Sp. z o.o. w 26.05.2024 o godz. 22:37, kiedy to administrator serwerów - podczas przeglądania logów – wykrył nieautoryzowany dostęp do serwera. Pracownik przeglądający logi zauważył, iż miał miejsce nieautoryzowany dostęp do serwera. Niezwłocznie podjęte przez Selly Sp. z o.o. działania skutkowały zabezpieczeniem dostępu do infrastruktury ww. podmiotu (infrastruktura zabezpieczona została po ok. 20 minutach od wykrycia ww. nieautoryzowanego dostępu do serwera, tj. – zgodnie z oświadczeniem Selly Sp. z o.o. – w dniu 26.05.2024 r., o godz. 23:00.

Charakter naruszenia

Szczegółowy opis naruszenia:

Do naruszenia poufności Pani/Pana danych osobowych doszło na skutek ataku, jaki został przeprowadzony w dniach 24.05.2024 r. – 26.05.2024 r. na serwery Selly Sp. z o.o., który jest dostawcą oprogramowania dla sklepów internetowych różnych podmiotów, w tym między innymi dla UCK.

W wyniku niniejszego ataku – zgodnie z informacją przekazaną przez Selly Sp. z o.o. – osoba trzecia uzyskała dostęp do znajdujących się na serwerach ww. podmiotu plików (w tym pobrała te pliki). Jednym z tych plików jest zaszyfrowana kopia bezpieczeństwa, w której znajdują się dane klientów sklepu internetowego służącego do zlecania wykonania przez UCK płatnych badań laboratoryjnych, w tym Pani/Pana dane.

Wymaga przy tym doprecyzowania, iż:

a) UCK korzysta z usług Selly Sp. z o.o. w celu prowadzenia sklepu internetowego, za pośrednictwem którego możliwe jest zlecanie przez klientów ww. sklepu wykonania przez UCK płatnych badań laboratoryjnych (ww.

sklep internetowy stanowi jedną z opcji zlecania wykonania ww. badań; za jego pośrednictwem realizowanych jest część zleconych płatnych badań laboratoryjnych),

b) pozyskane na skutek ww. ataku dane dotyczą – w odniesieniu do danych, których Administratorem Danych jest UCK – oprócz danych z pliku konfiguracyjnego sklepu, wyłącznie klientów ww. sklepu internetowego, którzy założyli konto w ww. sklepie od momentu uruchomienia sklepu do dnia 24.05.2024 r.,

c) ww. atak rozpoczęto w dniu 24.05.2024 r., ok. godz. 17:00 i trwał do dnia 26.05.2024 r. (w tym okresie doszło do pobrania pliku konfiguracyjnego sklepu oraz zaszyfrowanej kopii bezpieczeństwa - zabezpieczonych hasłem archiwum.zip) (nie jest możliwe ustalenie dokładnej daty i godziny),

d) podkreślenia wymaga, iż:
   - zgodnie z informacją przekazaną przez Selly Sp. z o.o. doszło wyłącznie do pobrania ww. pliku konfiguracyjnego sklepu oraz ww. kopii bezpieczeństwa i nie znaleziono śladów ingerencji w zawartość ww. plików (w tym w zawartość ww. kopii bezpieczeństwa) oraz bazy produkcyjnej,
   - ww. plik zawierający kopię bezpieczeństwa był zaszyfrowany, ale należy oczywiście przyjąć, iż hasło mogło zostać złamane, a w konsekwencji mógł nastąpić dostęp do znajdujących się w ww. pliku danych; należy przy tym podkreślić – co istotne – iż, z informacji przekazanej przez Selly Sp. z o.o. wynika, że:
     - konstrukcja hasła do ww. pliku jest silna, tj. hasło składa się z 16 znaków,
     - hasło do ww. kopii bezpieczeństwa było przez Selly Sp. z o.o. przechowywane na serwerze, na którym znajdowała się ww. kopia bezpieczeństwa, ale w innym miejscu oprogramowania (zgodnie z oświadczeniem Selly Sp. z o.o. nie można z całą pewnością stwierdzić czy osoba trzecia złamała ww. hasło oraz należy przyjąć, iż mając dostęp do konta „root" osoba trzecia mogła pozyskać również to hasło),
   - UCK oraz Selly Sp. z o.o. do chwili przekazania niniejszego zgłoszenia nie otrzymały żadnych informacji wskazujących, iż ww. dane zostały ujawnione czy wykorzystane w inny sposób oraz nie zgłoszono żadnych żądań finansowych dotyczących ww. zdarzenia,

e) ww. sklep nie jest częścią infrastruktury informatycznej UCK,

f) za pośrednictwem ww. sklepu nie jest możliwe uzyskanie dostępu do wyników zleconych za pośrednictwem ww. sklepu badań laboratoryjnych (mianowicie, na podstawie pobranych ww. danych nie jest możliwe uzyskanie dostępu do wyników zleconych badań laboratoryjnych, gdyż dostęp ten możliwy jest po wpisaniu dodatkowych informacji, jakimi są kod PIN oraz numer zlecenia generowane z systemu laboratoryjnego należącego do infrastruktury teleinformatycznej UCK).

Przyczyna naruszenia:

Do naruszenia doszło na skutek wykorzystania podatności w oprogramowaniu ww. sklepu internetowego.

Dane osobowe, których dotyczy naruszenie

Naruszenie dotyczy niżej wskazanych Pani/Pana danych osobowych:

a) nazwa użytkownika i/lub hasło,
b) imię i nazwisko,
c) numer ewidencyjny PESEL
d) seria i numer dowodu osobistego (dotyczy wyłącznie 6 użytkowników – obcokrajowców, którzy nie posiadali numeru ewidencyjnego PESEL),
e) adres,
f) adres e-mail,
g) numer telefonu,
h) kraj pochodzenia (narodowość),
i) data urodzenia,
j) płeć,

k) historia zamówień, w tym daty i rodzaje zleconych badań oraz zaplanowane terminy ich wykonania (należy przy tym podkreślić, iż – z uwagi na fakt, iż są to badania płatne – w historii zamówień brak jest informacji na temat przyczyny zlecenia danego badania).

Podjęte działania w celu zminimalizowania jego skutków oraz zapobieżenia wystąpieniu podobnych zdarzeń

Na skutek otrzymanej informacji, wszczęto postępowanie wyjaśniające i stwierdzono naruszenie ochrony danych osobowych, a także podjęto działania mające na celu zminimalizowanie jego skutków oraz zapobieżenie wystąpienia podobnych zdarzeń w przyszłości.

W celu zaradzenia naruszeniu i zminimalizowania negatywnych dla Pani/Pana skutków UCK oraz Selly Sp. z o.o. podjęły następujące działania:

a) odebranie nieautoryzowanego dostępu nieupoważnionej osobie trzeciej do serwera, na którym znajduje się ww. sklep internetowy (zrealizowane przez Selly Sp. z o.o.),
b) niezwłoczne po wykryciu podatności usunięcie możliwości ponownego jej wykorzystania (usunięto podatność) (tj. uniemożliwienie dostępu do serwera, na którym znajduje się ww. sklep internetowy) (podatność została usunięta po ok. 20 minutach od jej wykrycia) (zrealizowane przez Selly Sp. z o.o.),
c) zabezpieczenie dowodów z działań osoby trzeciej w celu dalszej analizy oraz dokonanie przeglądu całej infrastruktury technicznej Selly Sp. z o.o. pod kątem spełnienia wymogów bezpieczeństwa, w tym zwłaszcza przeskanowanie systemu operacyjnego (zrealizowane przez Selly Sp. z o.o.).

Informujemy, iż UCK oraz Selly Sp. z o.o. zainicjowały natychmiastowe niezbędne działania, aby podobna sytuacja nie miała miejsca w przyszłości, w tym zrealizowano lub zaplanowało nw. działania:

a) niezwłoczne po wykryciu podatności usunięcie możliwości ponownego jej wykorzystania (usunięto podatność) (tj. uniemożliwienie dostępu do serwera, na którym znajduje się ww. sklep internetowy) (podatność została usunięta po ok. 20 minutach od jej wykrycia) (zrealizowane przez Selly Sp. z o.o.),
b) zmiana hasła do konta SMPT służącego do wysyłki powiadomień ze sklepu internetowego UCK przez Administratora Systemu UCK (zrealizowane przez UCK),
c) wprowadzenie dodatkowego zabezpieczenia polegającego na ograniczeniu do powłoki serwerowej (zrealizowane przez Selly Sp. z o.o.),
d) ponowny przegląd bezpieczeństwa systemu sklepów i powiązanej infrastruktury informatycznej (zrealizowane przez Selly Sp. z o.o.),
e) dokonanie ponownej instalacji wszystkich systemów okołosklepowych współpracujących z oprogramowaniem sklepu w celu zapewnienia, iż ww. systemy są wolne od luk i zaktualizowane do najnowszej wersji oprogramowania (zrealizowane przez Selly Sp. z o.o.),
f) przeniesienie infrastruktury sklepu internetowego UCK na nowy serwer (zaplanowane przez Selly Sp. z o.o.),
g) odseparowanie lokalnej kopii bezpieczeństwa od serwera sklepu (zaplanowane przez Selly Sp. z o.o.),
h) odseparowanie miejsca przechowywania hasła oraz pliku, którego hasło dotyczy (zaplanowane przez Selly Sp. z o.o.).

Możliwe konsekwencje naruszenia i inne istotne informacje

Podkreślenia wymaga, iż wskutek wystąpienia ww. zdarzenia doszło do sytuacji, w której dostęp do danych, o których mowa powyżej, uzyskała w sposób celowy osoba nieupoważniona o nieznanej nam tożsamości (pobranie zaszyfrowanego pliku oraz możliwe zapoznanie się z jego treścią z uwagi na informacje, o których mowa powyżej). **Na chwilę obecną nie mamy żadnych sygnałów, że wskazane powyżej dane zostały gdzieś upublicznione lub są wykorzystywane przez osobę niepowołaną.**

UCK informuje przy tym, iż:

a) biorąc pod uwagę kontekst i okoliczności niniejszego naruszenia – dokonaliśmy jego oceny, podczas której uwzględniliśmy, w szczególności:

- prawdopodobieństwo wystąpienia dla Pani/Pana różnego rodzaju negatywnych zdarzeń (konsekwencji) będących skutkiem tego naruszenia (tj. materialnych lub niematerialnych szkód),
- powagę ww. zdarzeń, tj. wielkość potencjalnych szkód jakie ww. zdarzenia mogą spowodować w odniesieniu do Pani/Pana osoby,

b) w przypadku wystąpienia tego typu naruszenia ochrony danych osobowych istnieje **tzw. wysokie ryzyko** naruszenia praw lub wolności osób fizycznych (tj. **istnieje wysokie ryzyko, że dane osobowe zostaną wykorzystane w celach, o których mowa poniżej**),

c) **podjęliśmy wskazane powyżej w niniejszym zawiadomieniu działania mające na celu zminimalizowanie skutków niniejszego naruszenia, w tym zminimalizowanie ryzyka wystąpienia ww. ewentualnych jego konsekwencji, o których mowa w tabeli poniżej**.

Ewentualne konsekwencje naruszenia <u>mogą stanowić:</u>

1. Utrata kontroli nad własnymi danymi osobowymi, w tym np.:
   - dane będące przedmiotem niniejszego naruszenia, w tym dane kontaktowe, mogą trafić do wielu baz, z których korzystają spamerzy,
   - osoby trzecie mogą założyć na Pani/Pana dane osobowe konto internetowe (np. w serwisie społecznościowym),
   - osoby trzecie mogą podszyć się pod inną osobę lub instytucję w celu wyłudzenia od Pani/Pana dodatkowych określonych informacji (np. danych do logowania, szczegółów karty kredytowej), co może skutkować uzyskaniem dostępu do środków finansowych zgromadzonych na Pani/Pana kontach bankowych (osoby, które uzyskały dostęp do Pani/Pana danych, mogą podejmować próby wyłudzenia środków finansowych zgromadzonych na Pani/Pana kontach bankowych podszywając się pod instytucje finansowe np. za pomocą wiadomości SMS).

2. Kradzież lub oszustwo dotyczące tożsamości (sfałszowanie tożsamości), a także nadużycia finansowe lub straty finansowe. Może to spowodować dla Pani/Pana negatywne konsekwencje w postaci problemów związanych z próbą przypisania Pani/Panu odpowiedzialności za dokonanie takiego oszustwa. W szczególności:
   - osoby trzecie mogą podjąć próbę uzyskania na Pani/Pana szkodę pożyczek w instytucjach pozabankowych np. przez Internet lub telefonicznie, bez konieczności okazywania dokumentu tożsamości (może to wynikać z faktu, że instytucje pozabankowe umożliwiają realizację procedury uzyskania pożyczki przez Internet lub telefonicznie bez należytej weryfikacji i po podaniu podstawowych danych identyfikacyjnych, w tym numeru PESEL, nie wymagają przy tym okazywania dokumentu tożsamości),
   - osoby trzecie mogą podjąć próbę wykorzystania Pani/Pana danych osobowych w celu wyłudzenia ubezpieczenia lub środków z ubezpieczenia, co może skutkować próbą przypisania Pani/Panu oszustwa w postaci ww. wyłudzenia (może to wynikać z faktu, iż niektóre firmy ubezpieczeniowe wydają polisy ubezpieczeniowe, a także wypłacają odszkodowania z ubezpieczenia bez dokonania weryfikacji oryginalnych dokumentów tożsamości ubezpieczonego),
   - osoby trzecie mogą wykorzystać Pani/Pana dane osobowe do zarejestrowania przedpłaconej karty telefonicznej typu prepaid, która może posłużyć do celów przestępczych, co może skutkować próbą przypisania Pani/Panu odpowiedzialności za przestępstwo, do popełnienia którego posłużono się ww. kartą zarejestrowaną na Pani/Pana dane,
   - osoby trzecie mogą wykorzystać Pani/Pana dane osobowe do przejęcia Pani/Pana karty SIM. Przejęcie karty SIM z kolei może skutkować uzyskaniem dostępu do Pani/Pana konta bankowego bądź innych usług powiązanych z numerem telefonu (poczty e-mail, serwisów społecznościowych) (odzyskiwanie haseł do kont bardzo często opiera się na kodach/hasłach przesyłanych na numer telefonu komórkowego).
   - osoby trzecie mogą podjąć próbę zawarcia na Pani/Pana szkodę umów cywilnoprawnych, np. najmu nieruchomości lub sprzedaży nieruchomości, a także umów na dostawę usługi (np. telewizji kablowej lub usług telekomunikacyjnych), co może skutkować powstaniem w stosunku do Pani/Pana zadłużenia, np. w przypadku nieopłacania nabytych usług przez te osoby (może to wynikać z faktu, iż strony ww. umów, w tym również niektórzy dostawcy usług, dopuszczają skuteczne zawarcie umowy

bez konieczności okazania dokumentu tożsamości, a jedynie po podaniu podstawowych danych identyfikacyjnych).
- osoby trzecie mogą podjąć próbę wykorzystania Pani/Pana danych osobowych do ukrycia swojej tożsamości, np. przy otrzymaniu mandatu.
- osoby trzecie mogą – przy wykorzystaniu pozyskanych danych - podjąć próbę uzyskania dostępu do Pani/Pana kont (np. w serwisach społecznościowych, poczty e-mail).

3. Ograniczenie możliwości realizowania innych praw, w tym np.:
   - osoby trzecie mogą wykorzystać Pani/Pana dane osobowe w celu skorzystania z Pani/Pana praw obywatelskich, np. do zagłosowania nad środkami budżetu obywatelskiego, co uniemożliwiłoby Pani/Panu skorzystanie z przysługującego prawa (należy przy tym zaznaczyć, iż samorządy lub inne instytucje administracji publicznej udostępniają niektóre swoje usługi w oparciu o identyfikację użytkownika za pomocą numeru ewidencyjnego PESEL).

4. Dalsza utrata ochrony danych chronionych tajemnicą zawodową, w tym np.:
   - osoby trzecie mogą podjąć próbę uzyskania dostępu do systemów obsługujących udzielanie świadczeń medycznych (tj. do korzystania ze świadczeń opieki zdrowotnej Pani/Panu przysługujących) oraz uzyskać wgląd do danych o stanie Pani/Pana zdrowia, ponieważ czasem dostęp do systemów rejestracji pacjenta można uzyskać potwierdzając (np. telefonicznie) swoją tożsamość za pomocą numeru PESEL.

5. Naruszenie prawa do prywatności i/lub innych dóbr osobistych.

6. Uszczerbek fizyczny lub psychiczny, w tym np.:
   - informacja o wystąpieniu ww. naruszenia może wywoływać stres lub inne negatywne odczucia,
   - stres wywołany naruszeniem, w tym np. świadomość możliwego upublicznienia Pani/Pana danych osobowych, w skrajnych przypadkach może wpłynąć na stan Pani/Pana zdrowia.

Zgodnie z wytycznymi Urzędu Ochrony Danych Osobowych, zaleca się <u>ewentualne podjęcie następujących działań</u> w celu zminimalizowania ewentualnych negatywnych skutków naruszenia:

1. Należy zachować ostrożność przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu, które mogą mieć na celu wyłudzenie od Pani/Pana dodatkowych danych, w tym zwłaszcza:
   - zaleca się zachować ostrożność i zachować czujność podczas połączeń telefonicznych od nieznanych numerów telefonów oraz w komunikacji internetowej,
   - zaleca się ignorowanie nieoczekiwanych wiadomości, w szczególności od nieznanych i podejrzanych nadawców,
   - zwraca się uwagę, iż oszuści mogą być bardzo wiarygodni, skoro posiadają szereg informacji na Pani/Pana temat.

2. Zaleca się skorzystanie z możliwości zastrzeżenia numeru ewidencyjnego PESEL za pośrednictwem strony internetowej https://obywatel.gov.pl albo w dowolnym urzędzie gminy, na poczcie czy w placówce bankowej zgodnie z ustawą z dnia 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczenia niektórych skutków kradzieży tożsamości. Zastrzeżenie numeru PESEL, niezależnie od niniejszego naruszenia, jest zalecane jako dobra praktyka, gdyż ma na celu zapewnienie lepszej Pani/Pana ochrony przed wykorzystaniem Pani/Pana numeru PESEL do nieuprawnionych celów. W przypadku dokonania ww. zastrzeżenia, od dnia 1 czerwca 2024 r. niektóre podmioty przed dokonaniem poszczególnych czynności zobowiązane będą do weryfikacji czy dana osoba zastrzegła swój numer PESEL. Do powyższego zobowiązane będą m.in. banki i firmy pożyczkowe (przed udzieleniem kredytu czy pożyczki), operatorzy telekomunikacyjni (m.in. przed wydaniem duplikatu karty SIM w celu jego wykorzystania do nielegalnego autoryzowania transakcji) i notariusze (m.in. przy sprzedaży lub obciążeniu nieruchomości oraz sporządzeniu pełnomocnictwa do dokonania takich czynności). **Dokonanie zastrzeżenia numeru PESEL jest rekomendowane nawet w przypadku braku wystąpienia zdarzenia, w którym**

doszło do ujawnienia Pani/Pana numeru PESEL, gdyż zabezpieczy Panią/Pana w przypadku wystąpienia takiego zdarzenia w przyszłości (opcja bezpłatna). Informacje na ten temat zawarte są również w przygotowanej przez UCK prezentacji załączonej do komunikatu o niniejszym naruszeniu.

3. Zaleca się ewentualnie dodatkowo, tj. obok zastrzeżenia numeru ewidencyjnego PESEL, skorzystanie z możliwości założenia konta w systemie informacji kredytowej i gospodarczej celem monitorowania swojej aktywności kredytowej (tj. w celu dodatkowego zabezpieczenia swoich danych przed nieuprawnionym wykorzystaniem poprzez monitorowanie prób uzyskania kredytu); w tym:
    - może Pani/Pan skorzystać z możliwości uzyskania informacji na temat Pani/Pana zobowiązań pieniężnych z biur informacji gospodarczej (BIG), w tym Krajowego Rejestru Długów, którego pełna nazwa to Krajowy Rejestr Długów Biuro Informacji Gospodarczej Spółka Akcyjna (KRD BIG S.A.). Na podstawie art. 22b ustawy o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych osoby fizyczne mają prawo dostępu do przechowywanych przez biuro danych osobowych ich dotyczących. Dostęp do ww. danych dla dłużników będących konsumentami jest bezpłatny, jeżeli następuje nie częściej niż raz na 6 miesięcy. Więcej informacji na ten temat, w tym wykaz biur informacji gospodarczych oraz lista stron internetowych, na których może Pani/Pan uzyskać więcej informacji, znajduje się na stronie internetowej: https://www.gov.pl/web/rozwoj/wykaz-biur-wykonujacych-dzialalnosc-gospodarcza, jak również w przygotowanej przez UCK prezentacji załączonej do komunikatu o niniejszym naruszeniu **(ewentualna dodatkowa możliwość, opcja bezpłatna, jeżeli następuje nie częściej niż raz na 6 m-cy),**
    - może Pani/Pan zarejestrować się na stronie Biura Informacji Kredytowej (BIK) i ściągnąć raport na temat swoich zobowiązań kredytowych i finansowych oraz zamówić alerty BIK 24/7, które poinformują Panią/Pana, gdy ktoś złoży np. wniosek o kredyt/pożyczkę na Pani/Pana dane. Więcej informacji na ten temat może Pani/Pan uzyskać na stronie BIK: www.bik.pl oraz w przygotowanej przez UCK prezentacji załączonej do komunikatu o niniejszym naruszeniu **(ewentualna dodatkowa możliwość, opcja płatna).**

4. Jeśli w celu dokonania zakupu badania laboratoryjnego podała/podał Pani/Pan serię i numer dokumentu tożsamości (np. z uwagi na brak numeru ewidencyjnego PESEL): Zaleca się skorzystanie z możliwości zastrzeżenia dokumentu tożsamości w systemie dokumenty zastrzeżone i jego wymiany. Więcej informacji na temat opcji zastrzeżenia dokumentu tożsamości znajduje się na stronie internetowej: https://dokumentyzastrzezone.pl).

5. Jeśli będące przedmiotem niniejszego naruszenia hasło wykorzystuje Pan/Pani również do logowania do innych miejsc / usług internetowych (np. innych sklepów, portali społecznościowych, poczty e-mail) zaleca się jego niezwłoczną zmianę we wszystkich z ww. miejsc. Jednocześnie zaleca się niełączenie wszystkich usług, z których Pani/Pan korzysta z tym samym numerem telefonu lub adresem e-mail oraz prowadzenie ewidencji usług powiązanych z danym numerem telefonu lub adresem e-mail. Rozważyć można ewentualnie zaprzestanie korzystania z numeru telefonu i adresu e-mail, które są przedmiotem niniejszego naruszenia. W przypadku wystąpienia innego naruszenia ochrony danych osobowych u jakiegokolwiek z podmiotów, ww. dane kontaktowe mogą stanowić identyfikator (wspólny mianownik), na podstawie którego osoba trzecia połączy, znajdujące się w różnych miejscach/bazach, różne informacje na Pani/Pana temat.

6. Zaleca się niezwłoczne poinformowanie operatora telefonii komórkowej w przypadku, gdyby Pani/Pana numer telefonu przestał być aktywny, co może świadczyć o próbie wyrobienia duplikatu karty SIM.

7. Zaleca się niezwłoczne poinformowanie UCK lub Inspektora Ochrony Danych UCK o jakichkolwiek próbach wykorzystania Pani/Pana danych osobowych, których naruszenie dotyczy lub ich wykorzystaniu przez nieupoważnioną osobę trzecią.

8. Istnieje możliwość zgłoszenia przez Panią/Pana faktu naruszenia ochrony danych właściwym organom w celu zapobieżenia tzw. „kradzieży tożsamości” (np. policji, prokuraturze, straży granicznej).

9. Istnieje możliwość skorzystania przez Panią/Pana ze środków ochrony dóbr osobistych wskazanych w przepisach ustaw Kodeks cywilny i Kodeks postępowania cywilnego.

Poinformowanie o naruszeniu Urzędu Ochrony Danych Osobowych oraz innych podmiotów

UCK przekazało zawiadomienie o przedmiotowym naruszeniu do Prezesa Urzędu Ochrony Danych Osobowych oraz poinformowała inne uprawnione podmioty (CSIRT NASK, CSIRT Centrum E-Zdrowia).

Kontakt w sprawie naruszenia

W razie dodatkowych pytań lub wątpliwości, prosimy o kontakt z Moniką Golubską, Inspektorem Ochrony Danych UCK pod numerem tel. 58 349 21 73 lub adresem e-mail: iod@uck.gda.pl.