Szanowni Państwo.
W celu zapewnienia dostępu do wiedzy pozwalającej na zrozumienie obecnych zagrożeń cyberbezpieczeństwa oraz sposobów zabezpieczania się przed tymi zagrożeniami przedstawiamy podstawowe zagadnienia w tej kwestii.

Potencjalne konsekwencje naruszenia ochrony danych osobowych:
a) uzyskanie przez osoby trzecie (na szkodę osoby, której dane osobowe naruszono) kredytów w instytucjach poza bankowych - ponieważ wiele takich instytucji umożliwia uzyskanie pożyczki lub kredytu w łatwy i szybki sposób (np. przez Internet lub telefonicznie) bez konieczności okazywania dokumentu tożsamości;
b) uzyskanie przez osoby trzecie dostępu do korzystania ze świadczeń opieki zdrowotnej przysługujących osobie, której dane naruszono oraz do jej danych o stanie zdrowia, ponieważ często dostęp do systemów rejestracji pacjenta można uzyskać telefonicznie potwierdzając swoją tożsamość za pomocą numeru PESEL;
c) skorzystanie przez osoby trzecie z praw obywatelskich osoby, której dane naruszono (np.: do głosowania nad środkami budżetu obywatelskiego) - uniemożliwiałoby to właściwej osobie skorzystanie z przysługującego jej prawa;
d) podjęcie przez osoby trzecie próby wyłudzenia ubezpieczenia (lub środków z ubezpieczenia), co może spowodować dla osoby, której dane dotyczą, negatywne konsekwencje w postaci problemów związanych z próbą przypisania jej odpowiedzialności za dokonanie takiego czynu;
e) zarejestrowanie przedpłaconej karty telefonicznej (pre-paid), która może posłużyć do celów przestępczych;
f) próby zawarcia przez osoby trzecie umów cywilno-prawnych (np. najmu nieruchomości);
g) wykorzystanie danych przez osoby trzecie do ukrycia swojej tożsamości (np. przy otrzymywaniu mandatów);
h) otrzymywanie niezamówionej informacji handlowej na adres zamieszkania;
i) wykorzystanie pozyskanych danych do założenia kont internetowych na Państwa dane.

Zalecane środki i działania w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków:
W celu zminimalizowania ewentualnych negatywnych skutków naruszenia zalecamy aby osoby których dane osobowe mogły ulec naruszeniu, rozważyły podjęcie kroków minimalizujących ryzyko wystąpienia negatywnych konsekwencji i nieuprawnionego wykorzystania danych m.in. poprzez:
a) 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. Podajemy przykładowe: Biuro Informacji Kredytowej S.A. strona https://www.bik.pl, Biuro Informacji Gospodarczej InfoMonitor S.A. strona https://big.pl, Krajowy Rejestr Długów Biuro Informacji Gospodarczej S.A. stron https://krd.pl, Serwis CHRONPESEL strona https://www.chronpesel.pl).
W przypadku stwierdzenia jakichkolwiek nieprawidłowości – zgłoszenie tego faktu organom ścigania
b) zachowanie ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu, gdyż osoby, które w sposób nieuprawniony mogły wejść w posiadanie danych osobowych, mogą je wykorzystać lub przekazać innym podmiotom;
c) zachowanie ostrożności w przypadku niezamówionych przesyłek, usług;
d) ignorować prośby od nieznanych nadawców o podanie dodatkowych danych;
e) każdorazowo niezwłocznie informować organy ścigania po uzyskaniu informacji o nieuprawnionym wykorzystaniu/próbie wykorzystania Państwa danych.

Administrator Danych Osobowych