WYŁUDZANIE DANYCH

PRZEKAZYWANIE DOKUMENTÓW TOŻSAMOŚCI PRZEZ INTERNET, PRZEKAZYWANIE DANYCH OSOBOWYCH, METODY WYŁUDZANIA DANYCH

PORADNIK

Suwałki 2024

Każdy kolejny rok przynosi społeczeństwu wiele nowinek technologicznych, a tym samym więcej możliwości, które generują wiele niebezpieczeństw i zagrożeń. Rozwój Internetu powoduje, iż coraz więcej spraw ludzie mogą załatwić bez wychodzenia z domu, zarówno tych urzędowych (np. możliwość złożenia dokumentu w formie elektronicznym w urzędzie czy instytucji, uczestnictwo w rozprawie sądowej w formie zdalnej, etc.), ale również tych prywatnych (komunikacja elektroniczna, uzyskanie pożyczki za pomocą środków porozumiewania się na odległość, etc.). Niewątpliwie powyższy proces przyśpieszyła pandemia koronawirusa Sars-Cov-2, która wymusiła na państwach, instytucjach, a także podmiotach prywatnych, rewolucję teleinformatyczną. Aktualnie bez problemu każdy z nas może kupić towar prawie z całego świata, zawrzeć skutecznie umowę przez Internet czy załatwić większość spraw.

Internet stał się nośnikiem informacji i źródłem komunikacji. Za pomocą Internetu podmioty publiczne i prywatne weryfikują nasze dane osobowe, w tym wymagają przesyłania dokumentów tożsamości, najczęściej dowodów osobistych, w postaci elektronicznej, tj. w formie skanów, kserokopii, zdjęć, etc. Czy takie działania są legalne i czy ta kwestia została uregulowana prawnie? Częściowo na pewno tak, ale nie w sposób kompleksowy, o czym będzie poniżej. Jednocześnie zostanie przedstawiony krótki rys dotyczący niebezpieczeństw i ryzyk z tym związanych.

Skan dowodu osobistego jest zazwyczaj potrzebny przy zawieraniu umów na odległość w zakresie usług finansowych, bankowych czy telekomunikacyjnych. Przykładowo o przesłanie tego skanu proszą banki, np. przy zakładaniu rachunku bankowego czy podczas zawierania umowy o inne usługi finansowe, ale również parabanki, które umożliwiają zawarcie pożyczki na dowód przez Internet. Czy takie działania są legalne? Czy przepisy prawne wymuszają na tych podmiotach takie działania? Komentatorzy przedmiotowej problematyki nie są zgodni i z jednej strony wskazują na stanowisko Prezesa Urzędu Ochrony Danych Osobowych, zgodnie z którym takie działania, jak chociażby kserowanie dowodów osobistych (czytaj udostępnianie dokumentów tożsamości) nie jest uzasadnione w każdym przypadku, ponieważ obowiązuje zasada minimalizacji danych i celowości ich przetwarzania, a z drugiej strony cytowane są przepisy prawa, które nakazują lub wymuszają takie działania. Sztampowymi normami prawnym, które odnoszą się do tej kwestii są chociażby art. 112b ustawy prawo bankowe (banki mogą przetwarzać dla celów prowadzonej działalności bankowej informacje zawarte w dokumentach tożsamości osób fizycznych) czy art. 34 ust. 4 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (kinstytucje obowiązane na potrzeby stosowania środków bezpieczeństwa finansowego mogą przetwarzać informacje zawarte w dokumentach tożsamości klienta i osoby upoważnionej do działania w jego imieniu oraz sporządzać ich kopie).

Jak widać z powyższej refleksji, polski ustawodawca nie uregulował kwestii udostępniania dokumentów tożsamości, w tym w Internecie, w sposób kompleksowy, a dotychczasowe przepisy niejednokrotnie budzą wiele kontrowersji i dyskusji, zarówno na poziomie prawniczym, ale i obywatela. Co więcej, działania wielu instytucji wymuszają na nas określony sposób zachowania, co niekiedy stanowić może nadużycie

prawa. Czy wobec braku jednoznacznej odpowiedzi mamy jakiekolwiek wyjście z sytuacji, w której podmiot żąda od nas przesłania dokumentu tożsamości?

Po pierwsze, pośpiech jest wówczas najgorszym doradcą, a tym samym zadajmy sobie proste pytanie, czy w danej konkretnej sytuacji niezbędnym do dokonania określonej czynności jest udostępnienie naszych danych osobowych, w tym przesłanie dokumentu tożsamości. Przykładowo, nieuzasadnionym jest ww. wymóg podczas np. rejestracji w sklepie internetowym czy serwisie społecznościowych. Nawet jeśli okaże się, że podmiot uzależnia dokonanie danej czynności od przesłania przez nas dokumentu tożsamości, to zastanówmy się czy nie jest wystarczającym podanie (bez konieczności przesyłania dokumentu) danych niezbędnych do dokonania tej czynności. W tym miejscu wskazać trzeba, iż na rynku działa wiele podmiotów, które oferują podobne produkty lub usługi, przy czym procedura ich udostępniania może różna, w tym jeden podmiot w tej samej sytuacji może żądać od na przesłania dokumentu tożsamości, a inny nie. Warto wówczas się zastanowić czy w takiej sytuacji nie skorzystać z oferty konkurencyjnego podmiotu celem zapewnienia sobie bezpieczeństwa oraz wyeliminowania potencjalnego zagrożenia.

Niezależnie od powyższego, nawet jeśli podjęliśmy decyzję o udostępnieniu naszego dokumentu tożsamości innemu podmiotowi zweryfikujmy tożsamość tego podmiotu, np. w ogólnie dostępnych rejestrach publicznych (KRS, CEiDG, etc.), na stronach internetowych i innych, a także sprawdźmy czy adres poczty elektronicznej czy strona internetowa, na której przykładowo znajduje się formularz umożliwiający przesłanie dokumentu, należy do podmiotu, któremu rzeczywiście chcemy udostępnić nasz np. dowód osobisty. Poza tym, można ograniczyć ryzyko niekontrolowanego wycieku naszych danych wrażliwych poprzez zastosowanie metody anonimizacji częściowej danych, które znajdują się na danym dokumencie. Przykładowo, udostępniając nasz dowód osobisty, możemy ujawnić takie dane jak: imię, nazwisko, numer PESEL, numer dowodu osobistego, data ważności dowodu osobistego, a możemy zakryć pozostałe dane, jak: wszystkie zdjęcia, nazwisko rodowe oraz imiona rodziców, data i miejsce urodzenia oraz płeć, data wydania dowodu osobistego, adres (w starszych dowodach).

Powyższe przykładowe formy ostrożności niewątpliwie zmniejszą ryzyko i poprawią Twoje bezpieczeństwo, ale na pewno nie wyeliminują wszystkich zagrożeń, w tym kradzieży tożsamości czy bezprawnego wykorzystania naszych danych osobowych przez osoby trzecie, co może skutkować stratami finansowymi i długotrwałymi postępowaniami cywilnymi lub karnymi, które nie zawsze muszą zakończyć się na naszą korzyść, np. z uwagi na niewykrycie sprawcy przestępstwa czy brakiem dowodów na obronę przed roszczeniami innych podmiotów. Pamiętajmy, iż rozwój Internetu daje wiele możliwości, ale również jest źródłem wielu niebezpieczeństw.

Powyższe rady niewątpliwie nie wyeliminują wszystkich problemów, ale pomogą wielu ich uniknąć. Nie zapominajmy, iż nasze dokumenty tożsamości są źródłem wielu informacji o nas, w tym zawierają dane wrażliwe. Zadbajmy o to, że nawet jeśli jesteśmy zobligowani do ich udostępnienia lub dobrowolnie je udostępniamy stosując w/w metody i inne, w szczególności stosujmy oprogramowanie antywirusowe, zapory ogniowe, zachowujmy ostrożność w korzystaniu ze stron

internetowych, zabezpieczajmy przesyłane pliki hasłem, aktualizujmy posiadane przez siebie oprogramowanie.

Kończąc powyższy temat, nie sposób nie wspomnieć o tzw. zjawisku Phising, czyli wyłudzaniu i kradzieży danych osobowych. W dobie społeczeństwa internetowego oraz wykorzystania urządzeń mobilnych, pomysłowość przestępców nie zna granic i niejednokrotnie organy ścigania nie nadążają za ich przestępczymi działaniami lub ich działania tych organów podejmowane są po fakcie z różnym skutkiem. Wskazać trzeba, iż przestępcy wyłudzają nasze dane na różne sposoby – przez telefon, SMS, e-mail, chat internetowy czy portale społecznościowe. Oszuści podszywają się pod banki, firmy energetyczne, operatorów sieci telefonicznych, firmy kurierskie, sklepy internetowe i inne.

Pamiętajmy, iż większość z tych podmiotów nie korzysta z form porozumiewania się na odległość, co potwierdzają liczne komunikaty prasowe i w środkach masowego przekazu. Najważniejszym środkiem obrony przed takim szkodliwymi działaniami jest zdrowy rozsądek, brak pośpiechu, stosowna weryfikacja kontrahenta czy inne środki ostrożności, które zostały przedstawione przykładowo w niniejszym artykule, ale które nie wyczerpują wszystkich możliwości. Pogłębiajmy i poszerzajmy wiedzę w tym zakresie, gdyż świadomość oraz środki zaradcze są najlepszą metodą obrony przed działaniami przestępczymi, a także pozwalają na eliminację ryzyk i niebezpieczeństw.

Poradnik wydany przez Centrum Aktywności Społecznej PRYZMAT
ul. Noniewicza 91, 16 – 400 Suwałki, tel./fax 87 565 02 58
e-mail: pryzmat@pryzmat.org.pl www.pryzmat.org.pl

Zadanie z zakresu administracji rządowej, finansowane ze środków budżetu państwa przekazanych przez Miasto Suwałki.