W imieniu Administratora danych osobowych, którym jest: Naftor spółka z ograniczoną odpowiedzialnością z siedzibą w Rasztowie, adres: ul. Napoleońska 1 Rasztów, 05-205 Klembów, numer KRS: 223173 (Biuro Centrali: ul. Wał Miedzeszyński 630, 03-994 Warszawa),

zgodnie z 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) zawiadamiamy o możliwości naruszenia ochrony Państwa danych osobowych, wskutek incydentu cyberbezpieczeństwa, do którego doszło w dniu 10 listopada 2023 r., około godziny: 19:00.

Incydent polegał na wykryciu w systemie informatycznym Administratora złośliwego oprogramowania typu ransomware, którego działanie naruszyło infrastrukturę informatyczną Administratora i doprowadziło do zaszyfrowania danych znajdujących się w zasobach informatycznych.

Ponadto informujemy, iż cyberatak może wskazywać na naruszenie poufności ochrony danych osobowych i w związku z tym istnieje ryzyko ujawnienia danych osobowych w internecie przez cyberprzestępców.

Wśród informacji, będących przedmiotem naruszenia mogły być dane osobowe byłych i obecnych pracowników oraz współpracowników Administratora (imię, nazwisko, stanowisko, data urodzenia, numer PESEL, adres zamieszkania, wizerunek, dane dotyczące wynagrodzenia, numer rachunku bankowego, dane zawarte w paszporcie) oraz dane osobowe członków rodzin pracowników, byłych pracowników i współpracowników Administratora (imię, nazwisko, pesel, data urodzenia, stopień pokrewieństwa, deklarowany dochód w związku z ubieganiem się o dofinansowanie z Zakładowego Funduszu Świadczeń Socjalnych).

Informujemy, że niezwłocznie po wykryciu incydentu odłączono systemy NAFTOR od sieci oraz rozpoczęto proces przywracania funkcjonalności systemów IT.

Jednocześnie informujemy, iż współpracujemy z ekspertami zewnętrznymi w dziedzinie cyberbezpieczeństwa, celem zidentyfikowania metod i źródeł naruszenia infrastruktury informatycznej oraz zabezpieczenia środowiska IT.

Naruszenie może skutkować ryzykiem wykorzystania Pani/Pana danych osobowych, m.in. w formie:

- zaciągnięcia przez osoby trzecie kredytów lub pożyczek w instytucjach pozabankowych, ponieważ wiele takich instytucji umożliwia ich uzyskanie w łatwy i szybki sposób, np. przez internet lub telefonicznie bez konieczności okazywania dokumentu tożsamości;
- uzyskania 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;
- korzystania z praw obywatelskich osoby, której dane naruszono, np.: do głosowania nad środkami budżetu obywatelskiego - uniemożliwiałoby to właściwej osobie skorzystanie z przysługującego jej prawa;
- 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;
- bezprawnego publikowania danych osobowych w internecie lub w innej formie,
- podszycia się pod inną osobę lub instytucję w celu bezprawnego uzyskania od Pani/Pana dodatkowych określonych informacji;

- założenie na Panią/Pana dane osobowe konta internetowego np. w serwisach społecznościowych.

Zalecamy rozważenie następujących działań redukujących ryzyko nieuprawnionego wykorzystania danych osobowych:

- zastrzeżenie dokumentów tożsamości w Systemie DOKUMENTY ZASTRZEŻONE – w swoim banku lub w dowolnym banku przyjmującym zastrzeżenia także od osób niebędących jego klientami (wystarczy zgłosić zastrzeżenie tylko w jednym banku, a dane zostaną automatycznie przekazane do wszystkich pozostałych uczestników Systemu DOKUMENTY ZASTRZEŻON – więcej informacji na stronie: https://dokumentyzastrzezone.pl/;
- 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 takiej aktywności). 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).;
- założenie bezpłatnego konta na stronie e-Sądu w Lublinie (strona https://www.e-sad.gov.pl/), co pozwoli na uzyskanie natychmiastowej informacji o prowadzonych postępowaniach komorniczych, związanych z bezprawnym wykorzystaniem danych osobowych do zaciągania zobowiązań;
- zachowanie ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu;
- w przypadku upublicznienia w/w danych w jakiejkolwiek formie w internecie lub w inny sposób, niezwłoczne poinformowanie o tym fakcie Administratora, który udzieli Państwu niezbędnej pomocy;
- dokonanie samodzielnego zgłoszenia faktu naruszenia danych osobowych właściwym organom w celu zapobieżenia tzw. „kradzieży tożsamości".

Jednocześnie informujemy, iż od dnia 17 listopada 2023 r. każdy obywatel może bezpłatnie skorzystać z usługi **Zastrzeż numer PESEL**. Jest to możliwe np. przy użyciu aplikacji mObywatel 2.0, za pośrednictwem portalu mObywatel.gov.pl lub osobiście w swoim urzędzie gminy. Instytucje finansowe (np. banki) od 1 czerwca 2024 r. będą miały obowiązek weryfikować, czy numer PESEL jest zastrzeżony przy zawieraniu np. umowy kredytu lub pożyczki. Każdy z obywateli będzie miał możliwość weryfikacji kto sprawdzał jego numer PESEL za pośrednictwem konta na portalu mObywatel. Więcej informacji o tej usłudze można znaleźć na stronie: https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie.
Zalecamy skorzystanie z rejestru w celu wyeliminowania zagrożeń związanych z nieuprawnionym użyciem numeru PESEL.

Podjęcie tych działań ma na celu zabezpieczenie Państwa danych osobowych przed ich niewłaściwym wykorzystaniem. Administrator danych zapewnia, iż zostaną podjęte niezbędne działania, aby podobna sytuacja nie miała miejsca w przyszłości. W szczególności przeprowadzona zostanie analiza przyczyn i przebiegu incydentu oraz wdrożone działania naprawcze mające na celu eliminację lub co najmniej redukcję ryzyka jego powtórnego wystąpienia.

W razie dodatkowych pytań lub wątpliwości prosimy o kontakt z p. Pawłem Kowalczykiem (tel. 501 097 378) lub Inspektorem Ochrony Danych – Marcinem Stryszko – marcin.stryszko@isecure.pl