

Szanowni Państwo!

Drukpak Spółka z ograniczoną odpowiedzialnością, z siedzibą w Aleksandrowie Kujawskim wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w Toruniu, VII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: 0000550346, NIP: 891 1000492, REGON 910170574, na podstawie art. 34 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO), niniejszym zawiadamia o możliwym naruszeniu ochrony danych osobowych, które jest wynikiem ataku hakerskiego na serwery spółki, który został stwierdzony w dniu 20 czerwca 2025 roku.

I. Charakter naruszenia ochrony danych osobowych.

Do naruszenia ochrony danych osobowych doszło w wyniku ataku złośliwego oprogramowania szyfrującego pliki znajdujące się na serwerze Drukpak Sp. z o.o. Po stwierdzeniu incydentu natychmiast podjęto działania zaradcze. Spółka prowadzi intensywne prace mające na celu odzyskanie dostępu do danych.

Spółka na podstawie przeprowadzonej wewnętrznej weryfikacji ustaliła, że poza skutkiem ataku w postaci zaszyfrowania danych istnieje wysokie ryzyko, że sprawcy bezprawnie pobrali przynajmniej część danych i ewentualnie mogą je upubliczniać. Na chwilę obecną nie zostało ustalone czy na pewno oraz ewentualnie jaki zakres danych mógł zostać pobrany przez sprawców, ale kierując się szczególną troską wobec pracowników, osób na umowach cywilnoprawnych i pracowników młodocianych Spółka podjęła decyzję o zawiadomieniu o tym ryzyku, możliwych zagrożeniach, a także rekomendacjach w jaki sposób można zabezpieczyć się przed skutkami utraty poufności danych.

INFORMACJA DLA PRACOWNIKÓW, OSÓB WSPÓŁPRACUJĄCYCH NA UMOWACH CYWILNOPRAWNYCH

II. Kategorie osób, których incydent dotyczy.

Incydent dotyczy wszystkich kategorii danych pracowników obecnych i byłych, w tym pracowników młodocianych oraz osób zatrudnionych na podstawie umów cywilnoprawnych, w tym PESEL, imię nazwisko, adres zamieszkania, numer rachunku bankowego, numer i seria dowodu osobistego, adres e-mail, dane o wynagrodzeniach, , dane o stanie zdrowia (np. przebywaniu na L4) – w stosunku do pracowników, zleceniobiorców, pracowników młodocianych), dane o przynależności do związków zawodowych (tylko w stosunku do pracowników);

III. Możliwe konsekwencje naruszenia ochrony danych osobowych.

Następstwem naruszenia Państwa danych osobowych może być:

- przetwarzanie danych osobowych w celach marketingowych bez uprzedniego uzyskania zgody (w przypadku prowadzenia marketingu drogą elektroniczną na adres e-mail lub numer telefonu),

- publikacja lub ujawnienie danych osobowych co może naruszać Państwa dobra osobiste,
- zagrożenie nękaniami lub szantażem przy wykorzystaniu ujawnionych danych,
- narażenie na wzmożone ataki phishingowe, zmierzające do wyłudzenia danych osobowych,
- założenie konta internetowego przy wykorzystaniu danych osobowych (np. w serwisach społecznościowych),
- podjęcie przez osobę trzecią próby uzyskania na Państwa szkodę pożyczek w instytucjach poza bankowych, np. przez internet lub telefonicznie, bez konieczności okazywania dokumentu tożsamości,
- podjęcie przez osobę trzecią próby uzyskania dostępu do systemów obsługujących udzielanie świadczeń medycznych i uzyskania wglądu do danych o Państwa stanie zdrowia (często dostęp do systemów rejestracji pacjenta można uzyskać, potwierdzając swoją tożsamość za pomocą numeru PESEL),
- wykorzystanie danych osobowych celem korzystania z praw obywatelskich np. poprzez oddanie głosu w głosowaniu nad środkami budżetu obywatelskiego,
- wykorzystanie przez osobę trzecią danych osobowych do próby wyłudzenia ubezpieczenia lub środków z ubezpieczenia,
- wykorzystanie przez osobę trzecią danych osobowych do próby zawarcia umów cywilno-prawnych,
- wykorzystanie danych osobowych przez osoby trzecie do ukrycia swojej tożsamości (np. przy otrzymywaniu mandatów),
- zarejestrowanie przedpłaconej karty telefonicznej (pre-paid), która może służyć do celów przestępczych.

VI. Zalecenia dla pracowników oraz osób współpracujących na umowach cywilnoprawnych.

W celu zminimalizowania ewentualnych negatywnych skutków zdarzenia zalecamy:

- zastrzec swój numer PESEL (zastrzeżenie numeru PESEL jest możliwe przez internet – kliknij przycisk [Zastrzeż PESEL](#) i zaloguj się, system przeniesie cię do gov.pl, można też w [aplikacji mObywatel](#) (Usługi – Zastrzeż PESEL) lub pobierz i wypełnij wniosek w domu albo zrób to w swoim urzędzie gminy) – od 1 czerwca 2024 r. instytucje finansowe (np. banki) mają obowiązek weryfikować, czy numer PESEL jest zastrzeżony przy zawieraniu np. umowy kredytu lub pożyczki;
- założyć konto 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. strona <https://krd.pl>, Serwis CHRONPESEL strona <https://www.chronpesel.pl>);
- zmienić login lub hasło do systemów, w których loginem lub hasłem był numer PESEL;
- włączyć dodatkowe zabezpieczenie w serwisach, które umożliwiają weryfikację dwuetapową;
- zwracać szczególną uwagę na próby logowania na konta i sprawdzania alertów przesyłanych na adres e-mail;

- zachować ostrożność **wobec podejrzanych wiadomości e-mail, połączeń i wiadomości SMS** – przede wszystkim unikać odpowiadania na nieznane adresy e-mail i numery telefonów, szczególnie te pochodzące z nieznanych lokalizacji lub krajów. Nie należy klikać w linki ani otwierać załączników oraz nie podawać żadnych danych osobowych, jeśli wiadomość e-mail lub SMS wydaje się nietypowa lub pochodzi od nieznanego nadawcy;
- zachować ostrożność w kontakcie ze strony banków lub innych instytucji finansowych, firm telekomunikacyjnych lub innych organizacji w szczególności gdy rozmówca chce, powołując się na numer PESEL, uzyskać dane takie jak nr dowodu osobistego, nr konta bankowego, hasła, dane karty kredytowej itp.;
- zachować ostrożność przy korzystaniu z mediów społecznościowych, w szczególności przy odbieraniu wiadomości prywatnych zawierających linki;
- w razie stwierdzenia podszywania się pod Państwa – zawiadomić organy ścigania o możliwości popełnienia przestępstwa;
- w razie stwierdzenia naruszenia Państwa dóbr osobistych przez wykorzystanie danych osobowych, które zostały objęte niniejszym naruszeniem, rekomendujemy wykorzystanie środków ochrony dóbr osobistych określonych w przepisach Kodeksu cywilnego;
- **zgłoszenie podejrzanych aktywności lub oszustwa** na Policję lub do CERT Polska (<https://incydent.cert.pl/>) w przypadku otrzymania podejrzanej wiadomości lub połączeń telefonicznych

INFORMACJA DLA PRZEDSTAWICIELI KLIENTÓW I KONTRAHENTÓW

III. Zakres danych przedstawicieli klientów lub kontrahentów

Incydent dotyczy następujących danych osobowych przedstawicieli klientów i kontrahentów: imię, nazwisko, służbowy adres email, służbowy numer telefonu, miejsce zatrudnienia, stanowisko.

III. Możliwe konsekwencje naruszenia dla przedstawicieli klientów lub kontrahentów

Potencjalne skutki obejmują:

- przetwarzanie danych osobowych w celach marketingowych bez uprzedniego uzyskania zgody (w przypadku prowadzenia marketingu drogą elektroniczną na adres e-mail lub numer telefonu),
- utrata kontroli nad danymi;
- kradzież tożsamości lub oszustwo dotyczące tożsamości np. poszywanie się pod Państwa
- narażenie na wzmożone ataki phishingowe, zmierzające do wyłudzenia danych osobowych,
- założenie konta internetowego przy wykorzystaniu danych osobowych (np. w serwisach społecznościowych),

VI. Zalecenia dla przedstawicieli klientów lub kontrahentów

W celu zminimalizowania ewentualnych negatywnych skutków zdarzenia zalecamy:

- włączyć dodatkowe zabezpieczenie w serwisach, które umożliwiają weryfikację dwuetapową;
- zwracać szczególną uwagę na próby logowania na konta i sprawdzania alertów przesyłanych na adres e-mail;
- zachować ostrożność **wobec podejrzanych wiadomości e-mail, połączeń i wiadomości SMS** – przede wszystkim unikać odpowiadania na nieznane adresy e-mail i numery telefonów, szczególnie te pochodzące z nieznanymi lokalizacji lub krajów. Nie należy klikać w linki ani otwierać załączników oraz nie podawać żadnych danych osobowych, jeśli wiadomość e-mail lub SMS wydaje się nietypowa lub pochodzi od nieznanego nadawcy;
- zachować ostrożność przy korzystaniu z mediów społecznościowych, w szczególności przy odbieraniu wiadomości prywatnych zawierających linki;
- w razie stwierdzenia podszywania się pod Państwa – zawiadomić organy ścigania o możliwości popełnienia przestępstwa;
- w razie stwierdzenia naruszenia Państwa dóbr osobistych przez wykorzystanie danych osobowych, które zostały objęte niniejszym naruszeniem, rekomendujemy wykorzystanie środków ochrony dóbr osobistych określonych w przepisach Kodeksu cywilnego;
- **zgłoszenie podejrzanych aktywności lub oszustwa** na Policję lub do CERT Polska (<https://incydent.cert.pl/>) w przypadku otrzymania podejrzanej wiadomości lub połączeń telefonicznych

INFORMACJA DLA KONTRAHENTÓW - Osób prowadzących jednoosobową działalność gospodarczą

III. Zakres danych kontrahentów

Incydent dotyczy następujących danych osobowych kontrahentów prowadzących jednoosobową działalność gospodarczą: firma, imię, nazwisko, adres email, numer telefonu, adres siedziby firmy, dane z faktur takie jak nr rachunku, kwota zapłaconej faktury, NIP, REGON.

III. Możliwe konsekwencje naruszenia dla kontrahentów

Potencjalne skutki obejmują:

- przetwarzanie danych osobowych w celach marketingowych bez uprzedniego uzyskania zgody (w przypadku prowadzenia marketingu drogą elektroniczną na adres e-mail lub numer telefonu),
- utrata kontroli nad danymi;
- kradzież tożsamości lub oszustwo dotyczące tożsamości np. poszywanie się pod Państwa;
- narażenie na wzmożone ataki phishingowe, zmierzające do wyłudzenia danych osobowych,
- założenie konta internetowego przy wykorzystaniu danych osobowych (np. w serwisach społecznościowych),
- niewielkie opóźnienia w płatności;

VI. Zalecenia dla kontrahentów

W celu zminimalizowania ewentualnych negatywnych skutków zdarzenia zalecamy:

- włączyć dodatkowe zabezpieczenie w serwisach, które umożliwiają weryfikację dwuetapową;
- zwracać szczególną uwagę na próby logowania na konta i sprawdzania alertów przesyłanych na adres e-mail;
- zachować ostrożność **wobec podejrzanych wiadomości e-mail, połączeń i wiadomości SMS** – przede wszystkim unikać odpowiadania na nieznane adresy e-mail i numery telefonów, szczególnie te pochodzące z nieznanymi lokalizacji lub krajów. Nie należy klikać w linki ani otwierać załączników oraz nie podawać żadnych danych osobowych, jeśli wiadomość e-mail lub SMS wydaje się nietypowa lub pochodzi od nieznanego nadawcy;
- zachować ostrożność przy korzystaniu z mediów społecznościowych, w szczególności przy odbieraniu wiadomości prywatnych zawierających linki;
- w razie stwierdzenia podszywania się pod Państwa – zawiadomić organy ścigania o możliwości popełnienia przestępstwa;
- w razie stwierdzenia naruszenia Państwa dóbr osobistych przez wykorzystanie danych osobowych, które zostały objęte niniejszym naruszeniem, rekomendujemy wykorzystanie środków ochrony dóbr osobistych określonych w przepisach Kodeksu cywilnego;
- **zgłoszenie podejrzanych aktywności lub oszustwa** na Policję lub do CERT Polska (<https://incydent.cert.pl/>) w przypadku otrzymania podejrzanej wiadomości lub połączeń telefonicznych

IV. Środki zastosowane w związku z incydem.

1. Natychmiast po ujawnieniu incydentu zostały uruchomione procedury wewnętrzne dotyczące incydentów naruszeń ochrony danych osobowych.
2. Powiadomiono Centralne Biuro Zwalczania Cyberprzestępczości i złożono zawiadomienie o podejrzeniu popełnienia przestępstwa.
3. Powiadomiono CERT Polska o zaistniałym incydencie.
4. Zawiadomiono Prezesa Urzędu Ochrony Danych Osobowych o naruszeniu danych osobowych.
5. Powiadomiono osoby, których dane dotyczą.

V. Środki zastosowane przez administratora w celu zminimalizowania negatywnych skutków.

1. Wydane zostało polecenie wyłączenia serwerów służbowych i nieużywania ich do czasu sprawdzenia i odwołania zakazu.
2. Trwają czynności audytu i zabezpieczenia dalszych naruszeń;
3. Przekazano Państwu niniejszą informację

VII. Kontakt

W przypadku dodatkowych pytań jesteśmy do Państwa pełnej dyspozycji.

Więcej informacji odnośnie wskazanego naruszenia ochrony danych osobowych można uzyskać kontaktując się z Inspektorem Ochrony Danych, którym jest Marek Kruczek, na adres e-mail: m.kruczek@drukpak.pl lub pocztą tradycyjną na adres siedziby spółki Drukpak z dopiskiem „IOD”.