

Warszawa, dnia 28 listopada 2025 r.

Herkules S.A.

Ul. Annopol 5

03-236 Warszawa

KRS 261094

ZAWIADOMIENIE O MOŻLIWYM NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Szanowni Państwo,

Działając w imieniu spółki Herkules S.A. z siedzibą w Warszawie przy ul. Annopol 5 (kod pocztowy: 03-236 Warszawa), wpisanej do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIV Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000261094, posiadającej NIP: 9512032166 oraz numer REGON: 017433674 (dalej jako „Spółka”), dopełniając swoich obowiązków jako administratora danych w rozumieniu art. 4 ust. 7 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 (ogólne rozporządzenie o ochronie danych) (dalej jako „**RODO**”), niniejszym informujemy, że w dniu 26.11.2025 r. został stwierdzony atak hackerski, który doprowadził do naruszenia ochrony danych osobowych. Naruszenie mogło dotyczyć Państwa danych osobowych lub danych osobowych Państwa pracowników. W związku z tym **prosimy o dokładne zapoznanie się z treścią poniższego komunikatu.**

W dniu 26.11.2025 r. nieustalone osoby uzyskały nielegalnie dostęp do skrzynki poczty elektronicznej i zawartej w niej korespondencji co najmniej trzech zaatakowanych użytkowników: jacek.mrozik@herkules-polska.pl, grzegorz.sycz@herkules-polska.pl oraz marcin.bernaciak@herkules-polska.pl. W następnym etapie ataku rozesłane zostały wiadomości poczty elektronicznej podszywające się pod zaatakowanych użytkowników, zawierające potencjalnie niebezpieczne treści w postaci linku do strony internetowej zawierającej plik do pobrania. Cele ataku ani dalsze zamiary nie są znane.

Niezwłocznie po stwierdzonym incydencie rozpoczęto prace w trybie reakcji na zdarzenie, a także w miarę ustalania skutków zdarzenia podejmowano kolejne działania mające na celu próbę ograniczenia skutków tego ataku, jak również kroki w celu wyeliminowania takich zdarzeń w przyszłości.

Zostały wycofane autoryzacje dla wszystkich urządzeń, na których byli zalogowani pracownicy, także konta wszystkich użytkowników zostały zablokowane i wymuszono zmianę haseł z autoryzacją przez sms lub Microsoft Authenticator. Przeskanowano komputery oprogramowaniem antywirusowym i anty-malware. Dokonano wstępnego przeglądu infrastruktury pod kątem zmian podnoszących poziom bezpieczeństwa. Niezwłocznie zostanie przeprowadzony audyt pod kątem cyberbezpieczeństwa i wprowadzone zostaną zalecenia audytu. Zostanie złożone zawiadomienie o popełnieniu przestępstwa do Prokuratury Rejonowej Warszawa Praga Północ w Warszawie oraz zgłoszony zostanie incydent do CERT Polska a także zgłoszenie naruszenia ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych.

Nasza spółka poinformowała pracowników o incydencie. Zwrócono im uwagę na konieczność zachowania szczególnej ostrożności przy otwieraniu podejrzanych wiadomości email. Planowane jest szkolenie przypominające zasady bezpieczeństwa.

Z daleko idącej ostrożności, informujemy, że atakiem hackerskim mogły być objęte Państwa dane osobowe lub dane osobowe Państwa pracowników, o ile takie dane były przekazywane w takim zakresie do Spółki lub występowało w roli klienta, przedstawiciela/pełnomocnika/reprezentanta klienta Spółki.

Poniżej wskazujemy zakres danych **jaki mógł być** objęty naruszeniem ochrony danych osobowych: nazwa prowadzonej działalności gospodarczej, adres siedziby, nr KRS, REGON, NIP, nr rachunku bankowego, dane osób reprezentujących i właścicieli prowadzonych działalności (JDG oraz spółki prawa cywilnego), dane osoby upoważnionej do składania dyspozycji w imieniu firmy/ wskazanej do kontaktu w sprawie realizacji umowy: imię, nazwisko, stanowisko, pełniona funkcja, e-mail, telefon kontaktowy, dane z zawartych umów, wynagrodzenie i przedmiot umowy, numer PESEL lub seria i numer dokumentu tożsamości jeśli były podane przy okazji zawarcia umowy, wysokość i rodzaj wierzytelności, numer ID.

Pomimo natychmiastowych działań podjętych przez Spółkę w związku z zaistniałym naruszeniem, istnieje pewne ryzyko, że ktoś może wykorzystać ww. dane niezgodnie z Państwa wolą. W związku z tym, podajemy informacje o krokach, które mogą Państwo podjąć w związku z zaistniałym incydentem.

W przypadku otrzymania drogą elektroniczną (mailową) wiadomości od użytkowników: jacek.mrozik@herkules-polska.pl, grzegorz.sycz@herkules-polska.pl lub marcin.bernaciak@herkules-polska.pl lub innego adresu pochodzącego z domeny herkules-polska.pl o podejrzanym charakterze, należy zwracać szczególną uwagę na:

- podejrzone załączniki w wiadomościach mailowych – załączniki nie powinny być przesyłane w postaci archiwum typu ZIP lub RAR,
- podejrzone linki znajdujące się w treści wiadomości,
- prośby podania swoich dodatkowych danych osobowych (np. w celu potwierdzenia swojej tożsamości).

Tego typu maile mogą zawierać złośliwe oprogramowanie (np. wirusy, trojany), a także służyć do prób wyłudzenia kolejnych danych osobowych, np. numerów kont bankowych, numerów kart kredytowych czy też danych wykorzystywanych do logowania (np. loginy i hasła). Z tego też względu zalecamy szczególną ostrożność przy otwieraniu tego typu wiadomości. Zalecamy również korzystanie z oprogramowania antywirusowego z zawsze aktualną bazą sygnatur wirusów.

W przypadku podejrzenia wykorzystania Państwa danych osobowych w sposób nieuprawniony, prosimy o kontakt z odpowiednimi organami państwowymi, np. Policją. Wskazujemy, że istnieje również możliwość zastrzeżenia swojego numeru PESEL.

Ze względu na zamieszczony powyżej szczegółowy opis prosimy również nie ujawniać treści niniejszego pisma osobom niezaufanym. W takim bowiem wypadku może to ułatwić osobom nieuprawnionym działania mające na celu wykorzystanie Państwa danych osobowych.

Po przeprowadzeniu audytu cyberbezpieczeństwa poinformujemy Państwa o rzeczywistym zakresie naruszenia danych osobowych.

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 Herkules S.A. – Katarzyną Kądzelską na adres e-mail: iod@herkules-polska.pl lub pocztą tradycyjną na adres siedziby Spółki z dopiskiem „IOD”.