ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Szanowna Pani / Szanowny Panie,

Z przykrością informujemy, że doszło do zdarzenia, w wyniku którego osoby nieuprawnione mogły uzyskać dostęp do Państwa danych osobowych. Dane te były przechowywane i wykorzystywane przez firmę Flexidea sp. z o.o. z siedzibą w Łodzi. Firma ta została przejęta przez Contrain Poland sp. z o.o. z siedzibą w Łodzi (dalej: „Administrator"), dlatego to my odpowiadamy obecnie za poinformowanie Państwa o tym zdarzeniu i podjęcie odpowiednich działań.

Problem wystąpił w systemie zewnętrznej firmy, która obsługiwała księgowość Flexidea sp. z o.o. oraz zapewniała system do wystawiania i przechowywania faktur.

W dalszej części pisma wyjaśniamy, co się wydarzyło, jakie mogą być tego skutki, co zrobiliśmy w tej sprawie oraz jak mogą Państwo chronić swoje dane przed ich niewłaściwym wykorzystaniem.

1. **Co się wydarzyło?**
   W dniach 27–28 września 2026 r. doszło do ataku hakerskiego na systemy informatyczne podmiotu świadczącego usługi księgowe i udostępniającego platformę do wystawiania oraz przechowywania faktur, z której korzystała Flexidea sp. z o.o. W wyniku ataku osoba nieuprawniona uzyskała dostęp do systemu i skopiowała część przechowywanych w nim danych, w tym Państwa dane osobowe.
   Zdarzenie spowodowało naruszenie poufności danych osobowych. Nie stwierdzono natomiast, aby w jego wyniku dane zostały zmienione, usunięte lub stały się niedostępne.

2. **Jakie Państwa dane osobowe zostały objęte naruszeniem?**
   Z posiadanych przez nas informacji wynika, że naruszenie mogło dotyczyć następujących Państwa danych osobowych:
   - imię i nazwisko;
   - seria/numer paszportu
   - adres zamieszkania.

3. **Jakie mogą być konsekwencje naruszenia i co mogą Państwo zrobić?**
   Ujawnione dane mogą zostać wykorzystane przez osoby nieuprawnione w szczególności do prób podszywania się pod Państwa tożsamość, wyłudzania dodatkowych danych osobowych lub podejmowania prób oszustw, w tym za pośrednictwem wiadomości elektronicznych, połączeń telefonicznych lub korespondencji kierowanej na Państwa adres zamieszkania. Nie można również całkowicie wykluczyć prób wykorzystania tych danych w procesach weryfikacji tożsamości lub uzyskania usług, jeżeli stosowane przez dany podmiot zabezpieczenia okażą się niewystarczające.

W celu ograniczenia ryzyka rekomendujemy:

- zachowanie szczególnej ostrożności wobec wiadomości, telefonów lub innych prób kontaktu, w szczególności gdy osoba kontaktująca się powołuje się na znajomość Państwa danych osobowych, numeru paszportu lub adresu zamieszkania;
- nieudostępnianie skanu ani zdjęcia paszportu oraz dodatkowych danych osobowych, haseł, kodów jednorazowych czy informacji bankowych bez uprzedniego zweryfikowania tożsamości i wiarygodności odbiorcy;
- zwracanie uwagi na nietypową korespondencję, w szczególności informacje dotyczące nieznanych Państwu umów, zobowiązań, wezwań do zapłaty lub prób potwierdzenia tożsamości;
- w razie wątpliwości – skontaktowanie się z organem, który wydał paszport, lub właściwą placówką konsularną w celu ustalenia, czy zalecane jest podjęcie dodatkowych środków ochrony;
- w przypadku podejrzenia nieuprawnionego wykorzystania danych – niezwłoczny kontakt z instytucją, której dotyczy zdarzenie, a w przypadku podejrzenia popełnienia przestępstwa – zawiadomienie właściwych organów ścigania.

Samo ujawnienie numeru paszportu nie oznacza konieczności wymiany dokumentu. Ewentualne działania w tym zakresie należy ustalić z właściwym organem państwa, które wydało paszport.

Na chwilę obecną nie posiadamy informacji wskazujących, aby Państwa dane zostały wykorzystane przez osoby nieuprawnione. Nie można jednak wykluczyć takiego ryzyka w przyszłości.

4. Jakie działania zostały podjęte w związku z naruszeniem?

Po wykryciu incydentu podmiot obsługujący platformę fakturową podjął działania mające na celu zabezpieczenie systemu i zapobieżenie dalszemu nieuprawnionemu dostępowi, obejmujące w szczególności zablokowanie nieuprawnionego dostępu, usunięcie wykorzystanej luki bezpieczeństwa, zmianę danych dostępowych oraz przeniesienie obsługi platformy do nowego środowiska serwerowego. Luka bezpieczeństwa została usunięta 28 września 2026 r. Zdarzenie zostało również zgłoszone do CERT Polska oraz Policji.

Jako następca prawny Flexidea sp. z o.o. przeanalizowaliśmy zakres danych objętych naruszeniem oraz związane z nim ryzyko, zgłosiliśmy naruszenie Prezesowi Urzędu Ochrony Danych Osobowych oraz podjęliśmy działania w celu poinformowania osób, w przypadku których naruszenie może powodować wysokie ryzyko naruszenia ich praw lub wolności. Pozostajemy również w stałym kontakcie z podmiotem obsługującym platformę fakturową w celu uzyskiwania dalszych informacji dotyczących incydentu oraz ewentualnych dodatkowych zagrożeń związanych z ujawnionymi danymi.

5. Gdzie mogą Państwo uzyskać dodatkowe informacje?

W przypadku pytań dotyczących naruszenia ochrony danych osobowych, jego możliwych konsekwencji lub zalecanych środków ostrożności prosimy o kontakt z Inspektorem Ochrony Danych, panem Adamem Kop, drogą elektroniczną pod adresem e-mail: iod@contrain.pl lub

pisemnie na adres Contrain Poland sp. z o.o., ul. 3 Maja 14a, 93-408 Łódź z dopiskiem „Inspektor Ochrony Danych”.

Przepraszamy za zaistniałą sytuację oraz związane z nią niedogodności. Zapewniamy, że traktujemy ochronę danych osobowych z należytą starannością i podejmujemy działania mające na celu ograniczenie skutków naruszenia.

Z poważaniem,
Contrain Poland sp. z o.o.
ul. 3 Maja 14a
93-408 Łódź