Szanowni Państwo,

informujemy, że Spółka Dom Development Kredyty Sp. z o.o. padła ofiarą zaawansowanego cyberataku wymierzonego w jej infrastrukturę IT. Doszło również do nieuprawnionego pobrania danych z systemów. Analiza przeprowadzona przez Spółkę prowadzi do wniosku, iż atak mógł dotyczyć również Państwa danych.

W trosce o Państwa bezpieczeństwo przygotowaliśmy dla Państwa najważniejsze informacje, realizując tym samym wymogi obowiązujących przepisów prawa.

Zgodnie z rozporządzeniem 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 (ogólne rozporządzenie o ochronie danych; dalej jako: „RODO"), informujemy, że:

Administratorem Państwa danych osobowych jest Dom Development Kredyty Sp. z o.o. z siedzibą w Warszawie, Plac Piłsudskiego 3, 00-078 Warszawa (zwany dalej „Administratorem").

Administrator wyznaczył Inspektora Ochrony Danych. Z Administratorem mogą się Państwo skontaktować we wszelkich sprawach związanych z ochroną danych osobowych w następujący sposób:

a) za pośrednictwem poczty elektronicznej: iodo@domd.pl w temacie wskazując „dane osobowe Dom Development Kredyty Sp. z o.o.",

b) listownie: Dom Development Kredyty Sp. z o.o., Plac Piłsudskiego 3, 00-078 Warszawa, z dopiskiem „IODO".

Zgodnie ze stanem analizy na moment publikacji niniejszego zawiadomienia w bazie dotkniętej naruszeniem znajdują się następujące dane, przy czym ich indywidualny zakres zależy od przekazanych przez Państwa informacji:

jeśli są Państwo:	**incydent dotyczy następujących danych osobowych:**
klientami, byłymi klientami lub potencjalnymi klientami	bank, całkowita kwota do spłaty, imię, koszty ubezpieczenia, kwota proponowanego kredytu, minimalna wartość rynkowa nieruchomości jako wartość zabezpieczenia, nazwisko, okres kredytowania, podpis, rodzaj kredytu, rodzaj oprocentowania, typ kredytu, waluta, wysokość oprocentowania, wysokość raty, adres zamieszkania, całkowite koszty inwestycji i kredytu, cel kredytowania, data urodzenia, data uruchomienia kredytu, data ważności decyzji, adres mailowy, harmonogram spłat, informacje o hipotece, informacje o karcie kredytowej, kwota przyznanego kredytu, lokal, LTV, marża, metraż, nazwa towarzystwa ubezpieczeniowego, numer dokumentu tożsamości, numer umowy, numer księgi wieczystej, numer rachunku bankowego, opłaty i koszty udzielonego kredytu, PESEL, prognozowany adres nieruchomości, ubezpieczenie nażycie oraz ubezpieczenie nieruchomości - numery i suma ubezpieczenia, ustrój majątkowy, wartość zabezpieczenia, warunki cenowe kredytu, wkład własny, numer telefonu, RRSO
kontrahentem lub byłym kontrahentem	imię, nazwisko, funkcja, dane dotyczące postępowań i roszczeń, stanowisko, numer uprawnień zawodowych, imiona rodziców, miejsce pracy, PESEL/NIP, wskazany adres, numer i rodzaj dokumentu tożsamości, data ważności i

	organ wydający dokument tożsamości, informacje dotyczące realizowanych transakcji.
członkiem zarządu lub byłym członkiem zarządu	imię, nazwisko, adresy mailowe, numery telefonu, adres korespondencyjny, numer PESEL, data urodzenia
osobami działającymi w charakterze pełnomocnika	imię, nazwisko, adres mailowy, wskazany adres, numer telefonu, numer i rodzaj dokumentu tożsamości, data ważności i organ wydający dokument tożsamości, PESEL/NIP, informacje dotyczące realizowanych transakcji.

Państwa dane osobowe będą przetwarzane w celu zarządzania incydentem bezpieczeństwa w postaci naruszenia ochrony danych osobowych, w tym dokonania analizy zdarzenia, zgłoszenia naruszenia organowi nadzorczemu i poinformowania osób, których dane dotyczą, podjęcia działań zaradczych i ograniczenia skutków incydentu oraz udokumentowania zdarzenia zgodnie z obowiązującymi przepisami prawa. Przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. c RODO (wypełnienie obowiązku prawnego ciążącego na administratorze) oraz art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes administratora polegający na zapewnieniu bezpieczeństwa danych i systemów informatycznych).

Państwa dane osobowe będą przetwarzane przez okres niezbędny do realizacji celów, w których dane są przetwarzane bądź do czasu wniesienia sprzeciwu (jeśli podstawą przetwarzania jest prawnie uzasadniony interes Administratora) – w zależności, które ze zdarzeń wystąpi wcześniej.

Później Administrator będzie je przechowywać do momentu przedawnienia ewentualnych roszczeń lub do momentu wygaśnięcia obowiązku przechowywania danych wynikającego z przepisów prawa (np. prawa podatkowego) – w zależności, które ze zdarzeń nastąpi później.

Przysługuje Państwu prawo dostępu do swoich danych osobowych oraz prawo żądania ich sprostowania, ich usunięcia lub ograniczenia ich przetwarzania.

Przysługuje Państwu prawo do przenoszenia danych osobowych, tj. do otrzymania od Administratora Państwa danych osobowych, które Państwo dostarczyli Administratorowi, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Mogą Państwo żądać od Administratora przesłania tych danych innemu administratorowi.

W zakresie, w jakim podstawą przetwarzania Państwa danych osobowych jest przesłanka prawnie uzasadnionego interesu Administratora, przysługuje Państwu prawo wniesienia sprzeciwu wobec przetwarzania swoich danych osobowych.

W celu skorzystania z powyższych praw należy skontaktować się z Administratorem, korzystając ze wskazanych wyżej danych kontaktowych.

Nadto, przysługuje Państwu prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych (Prezesa Urzędu Ochrony Danych Osobowych), jeśli sądzą Państwo, że przetwarzanie danych narusza RODO.

Niniejsza informacja czyni zadość obowiązkom wynikającym z art. 34 Rozporządzenie 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).

Negatywnym skutkiem cyberataku może być:

- uzyskanie dostępu do Państwa ww. danych osobowych i ograniczenie przez Państwa kontroli nad tymi danymi osobowymi,
- usiłowanie uzyskania przez osoby trzecie, na Państwa szkodę, kredytów w instytucjach poza bankowych,
- usiłowanie kradzieży lub sfałszowania tożsamości,
- usiłowanie wyłudzenia ubezpieczenia,
- usiłowanie skorzystania z praw obywatelskich osoby, której dane naruszono, np. wykorzystanie danych do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego.

W celu uniknięcia ewentualnych negatywnych następstw tego zdarzenia oraz zabezpieczenia się przed negatywnymi skutkami naruszenia, Spółka zaleca Państwu stosowanie powszechnie zalecanych zasad ostrożności – podobnych do tych, które obowiązują w sytuacjach wzmożonej aktywności phishingowej:

- zastrzeżenie numeru PESEL w aplikacji mObywatel,
- założenie konta w systemie informacji kredytowej i gospodarczej celem monitorowania swojej aktywności kredytowej,
- zachowanie szczególnej ostrożności przy podawaniu danych osobowych innym osobom, w tym w szczególności numeru dokumentu tożsamości i numeru PESEL,
- zachowanie szczególnej czujności, gdyby telefonicznie zostali Państwo poproszeni o weryfikacje tożsamości, dokumentu tożsamości lub czynności, w których Państwo nie uczestniczyli,
- zachowanie ostrożności wobec wiadomości lub telefonów od nieznanych nadawców,
- niewchodzenie w linki z podejrzanych lub niespodziewanych wiadomości,
- nieotwieranie załączników, których pochodzenia nie są Państwo pewni,
- weryfikowanie tożsamości nadawców i instytucji, które proszą o podanie danych,
- rozważenie możliwości zastrzeżenia lub wymiany dowodu osobistego,
- śledzenie informacji na portalach https://bezpiecznedane.gov.pl/ oraz https://cyber.gov.pl/.

Jeśli mają Państwo wątpliwości, czy dana wiadomość jest autentyczna, najlepiej jej nie otwierać i nie odpowiadać na nią. W razie potrzeby mogą się Państwo skontaktować z nami- chętnie pomożemy zweryfikować sytuację.

Jakie działania podjęliśmy jako administrator danych?

Od momentu wykrycia incydentu:

- wdrożyliśmy działania techniczne zabezpieczające systemy (system EDR, SIEM, AV, systemy anty phishingowe),
- prowadzimy szczegółową analizę zdarzenia,
- zabezpieczyliśmy dostępność i integralność danych poprzez kopie zapasowe,
- współpracujemy ze specjalistami ds. cyberbezpieczeństwa,
- podjęliśmy działania mające na celu ograniczenie skutków incydentu i zapobieganie podobnym zdarzeniom w przyszłości.

Jednocześnie informujemy, ze spółki z grupy Dom Development S.A. prowadzą działalność operacyjną bez zakłóceń, a o zdarzeniu niezwłocznie poinformowaliśmy odpowiednie organy państwowe, w tym Prezesa Urzędu Ochrony Danych Osobowych i Prokuraturę.

W razie jakichkolwiek pytań lub wątpliwości Spółka pozostaje do Państwa dyspozycji i prosi o kontakt za pośrednictwem adresu e-mail: iodo@domd.pl lub pocztą tradycyjną na ww. adres korespondencyjny. W przypadku jakichkolwiek nowych ustaleń związanych z analizą naruszenia będziemy Państwa niezwłocznie informować.