

ZAWIADOMIENIE O POTENCJALNYM NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Szanowna Pani,

Szanowny Panie,

ApartHotel Gostyń z siedzibą **Minicentrum Gostyń Sp. z o.o.**

dalej jako „**Administrator**” 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) niniejszym informuje, że zostało wykryte potencjalne naruszenie ochrony danych osobowych, które mogło dotyczyć Pani/Pana danych osobowych. W związku z tym **prosimy o dokładne zapoznanie się z treścią poniższego komunikatu.**

Opis charakteru potencjalnego naruszenia

W dniu 11.12.2025 r. pracownicy naszego dostawcy usług IT, zawiadomili nas, że prawdopodobnie doszło do włamania na jeden z serwerów, na którym znajdowała się baza z danymi naszych Klientów. W bazie tej znajdowały się także Pani/Pana dane z przyjętych rezerwacji. Dotychczasowa weryfikacja zdarzenia nie wykazała, aby atakujący uzyskali bezpośredni dostęp do bazy danych, nie ma również pewności, że Pani/Pana dane zostały pobrane, na ten moment nie można jednak wykluczyć takiej ewentualności.

Zakres kategorii danych osobowych jakie potencjalnie mogły zostać objęte incydem bezpieczeństwa to:

- dane naszego obiektu,
- daty rezerwacji i kwoty rezerwacji,
- dane naszych gości hotelowych (podane bezpośrednio w rezerwacji, np. imię, nazwisko, adres email, numer telefonu lub inne, które wprowadziliście Państwo w rezerwacji),
- wystawione dokumenty księgowe (faktury, paragony).

Na chwilę obecną nie potwierdzamy, że do Pani/Pana danych osobowych uzyskali dostęp przestępcy, jednakże w celu dochowania należytej staranności oraz przeciwdziałania ewentualnym skutkom stwierdzonego incydentu bezpieczeństwa informujemy o podjętych działaniach, a także możliwych negatywnych dla Pani/Pana skutkach incydentu.

Opis możliwych konsekwencji potencjalnego naruszenia ochrony danych osobowych

Kierując się daleko idącą ostrożnością informujemy o potencjalnych następstwach w sytuacji gdyby stwierdzono, że doszło do pobrania Pani/Pana danych osobowych przez przestępców.

O ewentualnym potwierdzeniu się tych okoliczności będziemy informować Panią/Pana w odrębnym komunikacie (na chwilę obecną według naszej wiedzy taka okoliczność nie wystąpiła).

W przypadku potwierdzenia takiego zdarzenia, potencjalnym następstwem ewentualnego naruszenia ochrony Pani/Pana danych osobowych może być wykorzystanie przez osoby trzecie Pani/Pana danych m.in. w celu uzyskania korzyści majątkowej Pani/Pana kosztem. Wykorzystane dane osobowe mogą także potencjalnie służyć nakłoniению Pani/Pana do zapłaty nieistniejących płatności lub służyć do wyłudzenia dodatkowych Pani/Pana danych, które pierwotnie nie były objęte naruszeniem, co w konsekwencji mogłoby skutkować zaciągnięciem innych zobowiązań, np. dokonywanie zakupów w sieci internet lub wyłudzenie kredytów czy też pożyczek w instytucjach pozabankowych. Potencjalnie

ujawnione dane mogą także posłużyć w celu założenia na Pani/Pana dane osobowe konta internetowego (np. w serwisach społecznościowych, poczty elektronicznej), wypożyczania na Pani/Pana dane określonych przedmiotów, a następnie ich kradzieży przez osoby trzecie.

Proponowane działania jakie może Pani/Pan podjąć w celu przeciwdziałania skutkom potencjalnego naruszenia

W przypadku podejrzenia wykorzystania Pani/Pana danych osobowych w sposób nieuprawniony, prosimy o kontakt z odpowiednimi organami państwowymi, np. Policją.

Prosimy zwracać uwagę na wszelką korespondencję kierowaną do Pani/Pana (z wykorzystaniem Pani/Pana danych osobowych) przez osoby, które podają się za przedstawicieli naszego hotelu – prosimy tego typu sytuacje wyjaśniać z nami na bieżąco kontaktując się pod adresem wskazanym na końcu niniejszego pisma. **W szczególności prosimy zwracać szczególną uwagę na ewentualne próby wyłudzeń poprzez podszywanie się pod naszą tożsamość oraz powoływanie na dane z rezerwacji, wysyłane drogą e-mail lub komunikatorami internetowymi (np. WhatsApp) – gdzie jesteście Państwo proszeni o uregulowanie należności za pobyt w naszym hotelu lub podanie danych osobowych klikając w linki znajdujące się w treści wiadomości. Nie należy odpowiadać na tego typu wiadomości ani klikać w linki.**

Prosimy również zwracać uwagę na ewentualną korespondencję przekazywaną drogą papierową i dokładnie zapoznawać się z ich treścią, ponieważ mogą to być na przykład potwierdzenia zawarcia określonej umowy (której sam(a) Pani/Pan nigdy nie zawierał(a) lub fałszywe wezwania do zapłaty z tytułu dokonanych rezerwacji w naszym obiekcie. Wszelkie tego typu zdarzenia należy niezwłocznie weryfikować bezpośrednio z podmiotami, które są stroną zawartych umów, a w wątpliwych przypadkach zgłaszać na Policję. Przypominamy również, że w przypadku umów konsumenckich zawieranych na odległość zazwyczaj w takim przypadku przysługuje prawo odstąpienia od umowy w terminie 14 dni bez ponoszenia żadnych konsekwencji.

Z kolei w przypadku otrzymania zawiadomienia drogą elektroniczną (mailową) o podobnym charakterze, jak wskazany powyżej, 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 Pani/Pana 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.

Prosimy również zwrócić uwagę na hasła dostępu jakich używa Pani/Pan korzystając z zasobów sieci Internet (np. kont społecznościowych, kont e-mail, portali, bankowości elektronicznej). Hasła te nie powinny zawierać w swojej składni łatwych do odgadnięcia wyrazów lub ich części, w szczególności bazujących na Pani/Pana danych osobowych (np. imion, nazwisk, daty urodzenia, numeru PESEL, serii i numeru dokumentu tożsamości, numeru telefonu).

W przypadku podejrzenia wykorzystania Pani/Pana danych w sposób nieuprawniony istnieje także możliwość:

- a) sprawdzenia swojej historii kredytowej w Biurze Informacji Kredytowej – jest to instytucja gromadząca i przetwarzająca dane o wszystkich pożyczkach zaciąganych w bankach i SKOK-ach. W BIKu wskazane są informacje o kredytach spłacanych terminowo i zaległościach płatniczych. Szczegółowe informacje opisane są pod następującym linkiem: <https://www.bik.pl/>

- b) sprawdzenie swoich danych w Krajowym Rejestrze Długów – KRD umożliwia monitorowanie rejestru zapytań dotyczących wniosku o kredyt. Szczegółowe informacje opisane są pod następującym linkiem: <https://krd.pl/>

Ze względu na zamieszczony 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 Pani/Pana danych osobowych.

Opis zastosowanych środków bezpieczeństwa w celu zaradzenia naruszeniu ochrony danych osobowych lub zminimalizowania jego ewentualnych negatywnych skutków

Niezwłocznie po ujawnieniu opisanego wyżej incydentu, wspólnie z naszym dostawcą usług IT, podjęliśmy działania mające na celu jak najszybsze przeciwdziałanie incydentowi oraz jego potencjalnym skutkom, w szczególności uruchomiliśmy wewnętrzną procedurę reagowania na potencjalne naruszenia ochrony danych osobowych, wyłączyliśmy zasoby IT objęte atakiem, zastąpiliśmy je nowymi, dodatkowo zabezpieczonymi, przeprowadziliśmy weryfikację kont użytkowników, aby mieć pewność, że atakujący nie mają już dostępu do naszych baz danych.

O zaistniałym zdarzeniu zostały poinformowane wewnętrzne służby odpowiedzialne za ochronę danych osobowych, a także organy – Policja, CERT, Prezes Urzędu Ochrony Danych Osobowych.

Kontakt z Administratorem danych

W przypadku dodatkowych pytań jesteśmy do Pani/Pana dyspozycji.

Na bieżąco monitorujemy sytuację związaną ze stwierdzonym incydem i w przypadku dodatkowych ustaleń, będziemy je na bieżąco Państwu przekazywać. Jednocześnie w przypadku dodatkowych pytań z Państwa strony informujemy, że istnieje możliwość kontaktu z nami

pod adresem e-mail: repcja@hotelgostyn.pl

lub telefonicznie: [665250025](tel:665250025)

Z wyrazami szacunku,

Michał Biegajski