Gostyń, 29 January 2026
NOTICE OF A POTENTIAL PERSONAL DATA BREACH

Dear Madam,
Dear Sir,

ApartHotel Gostyń, ul. Ks. Olejniczaka 2, operated by Minicentrum Gostyń Sp. z o.o., with its registered office in 64-100 Leszno, ul. Narutowicza (hereinafter referred to as the "Controller"), in fulfilling its obligations as a data controller within the meaning of Article 4(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR), hereby informs you that a potential personal data breach has been detected, which may have concerned your personal data. Therefore, we kindly ask you to read the following information carefully.

Description of the nature of the potential breach

On 11 December 2025, employees of our IT service provider informed us that one of the servers containing a database of our customers' data had most likely been hacked. This database also contained your data from reservations made. The verification conducted so far has not shown that the attackers gained direct access to the database. There is also no certainty that your data was downloaded; however, at this stage such a possibility cannot be excluded.

The categories of personal data that may potentially have been affected by the security incident include:

- data relating to our facility,
- reservation dates and reservation amounts,
- data of our hotel guests (provided directly in the reservation, e.g. name, surname, email address, phone number, data included in accounting documents such as invoices and receipts, potentially including PESEL number if provided, or other data entered in the reservation),
- issued accounting documents (invoices, receipts).

At present, we do not confirm that criminals accessed your personal data; however, in order to exercise due diligence and counteract potential effects of the identified incident, we inform you of the measures taken and the possible adverse consequences for you.

Description of possible consequences of the potential personal data breach

As a precaution, we inform you about possible consequences should it be confirmed that criminals downloaded your personal data. If such circumstances are confirmed, we will inform you in a separate communication (at present, to our knowledge, this has not occurred).

If confirmed, potential consequences may include the use of your data by third parties for financial gain at your expense. The personal data may also be used to induce you to make payments for non-existent liabilities or to obtain additional personal data from you that were not originally affected by the breach, which could result in incurring other obligations, such as online purchases or fraudulent loans or credits from non-banking institutions.

Potentially disclosed data may also be used to create online accounts in your name (e.g. on social media or email services), rent items in your name and then steal them.

Recommended actions you may take to mitigate potential effects

If you suspect unauthorized use of your personal data, please contact relevant authorities, e.g. the Police.

Please pay attention to any correspondence addressed to you (using your personal data) by persons claiming to represent our hotel. Please verify such situations with us directly using the contact details provided at the end of this letter. In particular, be alert to fraud attempts involving impersonation of our identity and reference to reservation data, sent via email or messaging apps (e.g. WhatsApp), where you are asked to settle payments for your stay or provide personal data by

clicking links in messages. Do not respond to such messages or click any links.
Also pay attention to paper correspondence and carefully review its content, as it may include confirmations of agreements you never concluded or false payment demands relating to reservations at our facility. Such cases should be verified directly with the entities involved and, in doubtful situations, reported to the Police. We also remind you that in the case of distance consumer contracts, you usually have the right to withdraw within 14 days without consequences.
In case of suspicious emails, pay particular attention to:

- suspicious attachments (especially ZIP or RAR archives),
- suspicious links in messages,
- requests to provide additional personal data.

Such emails may contain malware or be used to obtain further sensitive data such as bank account numbers, credit card numbers, or login credentials. We therefore recommend particular caution and the use of up-to-date antivirus software.
Please also review the passwords you use for online services (social media, email, portals, online banking). Passwords should not contain easily guessable words or elements based on your personal data (e.g. names, dates of birth, PESEL number, ID document number, phone number).
If you suspect misuse of your data, you may also:
a) Check your credit history with the Credit Information Bureau (BIK) – collects data on loans from banks and credit unions: https://www.bik.pl/
b) Check your data in the National Debt Register (KRD): https://krd.pl/
c) Consider reserving (blocking) your PESEL number via the mObywatel app or a municipal office: https://www.gov.pl/web/gov/zastrzez-pesel
Due to the detailed nature of this letter, please do not disclose its content to untrusted persons, as this could facilitate misuse of your data.

Security measures implemented
Immediately after discovering the incident, together with our IT provider, we took steps to counteract the incident and its potential effects. We activated internal incident response procedures, disconnected affected IT resources, replaced them with new secured ones, and verified user accounts to ensure attackers no longer have access. Internal data protection services and authorities — Police, CERT, and the President of the Personal Data Protection Office — were notified.

Contact with the Data Controller
If you have further questions, please contact us at:
apartamenty.gostyn@gmail.com
+48 665 25 00 25
We are continuously monitoring the situation and will provide updates if new findings arise.

Yours sincerely,
Michał Biegajski
President of the Management Board
Minicentrum Gostyń Sp. z o.o.