Gostyń, 12 December 2025

NOTICE OF A POTENTIAL PERSONAL DATA PROTECTION BREACH

Dear Madam,
Dear Sir,

ApartHotel Gostyń, with its registered office at Minicentrum Gostyń Sp. z o.o.,
hereinafter referred to as the “Controller”, acting in compliance with 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, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR), hereby informs you that a potential personal data protection breach has been detected which may have concerned your personal data.
Therefore, we kindly ask you to carefully read the information provided below.

Description of the nature of the potential breach

On 11 December 2025, employees of our IT service provider informed us that a hacking incident had most likely occurred on one of the servers hosting a database containing our Clients’ data. This database also included your data provided in connection with accepted reservations.

The verification carried out so far has not indicated that the attackers gained direct access to the database, nor is there confirmation that your data was downloaded. However, at this stage, such a possibility cannot be entirely ruled out.

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

- data related to our property,
- reservation dates and reservation amounts,
- data of our hotel guests (provided directly in reservations, e.g. first name, last name, e-mail address, telephone number, or other data entered during the reservation process),
- issued accounting documents (invoices, receipts).

At present, we do not confirm that unauthorized persons have gained access to your personal data. Nevertheless, in order to exercise due diligence and to mitigate any potential consequences of the identified security incident, we hereby inform you of the actions taken and of the possible adverse effects the incident may have for you.

Description of possible consequences of a potential personal data breach

Acting with utmost caution, we inform you of potential consequences should it be confirmed that your personal data has been obtained by unauthorized persons.
If such circumstances are confirmed, you will be informed in a separate notice (as of today, according to our knowledge, such confirmation has not occurred).

If confirmed, potential consequences of a breach of your personal data may include the use of your data by third parties, among others, for the purpose of obtaining financial benefits at your expense. The disclosed data could also potentially be used to induce you to make payments for non-existent liabilities or to obtain additional personal data that was not originally affected by the breach, which could in turn lead to incurring further obligations, such as making online purchases or fraudulently obtaining loans or credits from non-banking institutions.

The disclosed data may also be used to create online accounts in your name (e.g. on social media platforms or e-mail services) or to rent goods using your personal data and subsequently misappropriate them.

Recommended actions to mitigate potential effects of the breach

If you suspect that your personal data has been used without authorization, please contact the appropriate public authorities, such as the Police.

Please pay close attention to any correspondence addressed to you (using your personal data) by individuals claiming to represent our hotel. We kindly ask you to verify such situations with us on an ongoing basis by contacting us at the address provided at the end of this notice.

In particular, please be especially vigilant with regard to any attempts at fraud involving impersonation of our identity and references to reservation details, sent via e-mail or instant messaging services (e.g. WhatsApp), in which you are asked to settle payments for your stay at our hotel or to provide personal data by clicking on links included in the message. Please do not reply to such messages and do not click on any links.

Please also pay attention to any correspondence received in paper form and read its contents carefully, as it may include, for example, confirmations of contracts that you never entered into or fraudulent payment demands related to reservations at our property. Any such incidents should be immediately verified directly with the entities indicated as parties to the contracts, and in doubtful cases reported to the Police.

We also remind you that in the case of consumer contracts concluded remotely, you are usually entitled to withdraw from the contract within 14 days without any consequences.

If you receive electronic (e-mail) notifications of a similar nature, please pay particular attention to:

- suspicious e-mail attachments — attachments should not be sent in archive formats such as ZIP or RAR,

- suspicious links included in the message content,

- requests to provide additional personal data (e.g. to confirm your identity).

Such e-mails may contain malicious software (e.g. viruses, trojans) or be used to attempt to obtain additional personal data, such as bank account numbers, credit card details, or login credentials (e.g. usernames and passwords). Therefore, we recommend exercising particular caution when opening such messages.

We also recommend using antivirus software with an up-to-date virus signature database. Please pay attention to the passwords you use when accessing Internet resources (e.g. social media accounts, e-mail accounts, online portals, electronic banking). Passwords should not contain easily guessable words or elements, particularly those based on your personal data (e.g. first name, last name, date of birth, PESEL number, ID document number, or phone number).

If you suspect unauthorized use of your data, you may also consider:
a) checking your credit history with the Credit Information Bureau (Biuro Informacji Kredytowej – BIK), which collects and processes data on all loans taken out at banks and credit unions. Detailed information is available at:
https://www.bik.pl/

b) checking your data in the National Debt Register (Krajowy Rejestr Długów – KRD), which allows monitoring of inquiries related to credit applications. Detailed information is available at:
https://krd.pl/

Due to the detailed nature of this notice, we kindly ask you not to disclose its contents to unauthorized persons, as this could facilitate actions aimed at the misuse of your personal data.

Description of security measures taken to address the breach or minimize its potential negative effects

Immediately after the incident described above was identified, together with our IT service provider, we undertook actions aimed at counteracting the incident and its potential effects as quickly as possible. In particular, we initiated an internal procedure for responding to potential personal data breaches, disabled the affected IT resources, replaced them with new and additionally secured systems, and verified user accounts to ensure that the attackers no longer have access to our databases.

The incident was reported to the internal units responsible for personal data protection, as well as to the relevant authorities — the Police, CERT, and the President of the Personal Data Protection Office.

Contact with the Data Controller

If you have any additional questions, we remain at your disposal.
We are continuously monitoring the situation related to the identified incident and will keep you informed of any further findings.

You may contact us by e-mail at: **recepcja@hotelgostyn.pl**
or by phone: **+48 665 250 025**

Yours sincerely,
Michał Biegajski