



**blooming**

# **Privacy Statement**

**Date:**

**12-09-2024**

## Identity and contact details of the data controller

blooming hotel and conference estate

- Het Hof
- Zandhoeve

Collectively referred to as blooming

Duinweg 5

1861 GL Bergen (NH)

E-Mail address: [welkom@weareblooming.com](mailto:welkom@weareblooming.com)

## 1. Introduction

We are aware that you place your trust in us regarding the handling of your personal data. We therefore see it as our responsibility to protect your privacy. On this page, we inform you about which data we collect when you use our website, why we collect this data, and how we use it to improve your user experience. This way, you understand exactly how we operate. This privacy statement applies to the services of blooming hotel and conference estate b.v. blooming hotel and conference estate b.v.

This privacy statement applies to all forms of information we collect through this website or other related means (for example, if you contact us via email, call our reception, or send us a message via social media

## 2. Which personal data do we process from you?

We process personal data from you as the data subject. These are personal data that you have directly or indirectly provided to us. We process the following personal data from you:

- General contact details;
- First name;
- Last name;
- Email address;
- Phone number
- Gender
- Credit card information (anonymized);
- Business contact details;
- Bank details;
- License plate.

## 3. For what purposes is your data processed?

- To draft and execute the service agreement;
- To contact you in response to inquiries made via the website;
- To establish and maintain contact (by mail, phone, or email);
- To keep an accurate night register;
- To send newsletters;
- To provide relevant information regarding your booking;
- To send direct marketing emails;

## 4. Who has access to your personal data?

As the data subject, it is important for you to know which individuals within blooming have access to your personal data. The staff in the sales department process your personal data that you have provided to us through a booking on our website or via email/phone/contact form.

Therefore, the staff in the sales department will have access to your personal data. Additionally, the front office staff will have access to your data to check you in and out. Finally, you as the data subject have control over your personal data. This is further explained in section 7, 'What rights do I have as a data subject?'

## 5. Why does blooming process your data?

blooming's processing of your personal data is only justified if one of the (six) legal bases is met:

- We are entitled to process your personal data because it is necessary for the performance of the service agreement in which you are a party.
- Additionally, we are entitled to process your personal data because certain data processing is required by law (night register);
- The processing is necessary for the protection of the legitimate interests of the data controller or a third party, except where the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, override those interests (balancing of interests);
- You have explicitly given us consent to process your personal data for one or more specific purposes (consent declaration);

## 6. To whom is your personal data disclosed?

In certain cases, it is necessary for blooming to disclose your personal data to third parties. In the situations described below, blooming is required to provide your data.

### **Performance of Agreement**

Disclosing your personal data to third-party organizations is permissible when it is necessary to fulfill our contractual obligations to you. This includes processing your reservation, handling payments, and using a third party for processing your booking and iDEAL payments.

We disclose personal data to our partners so they can process data on our behalf according to our instructions and in compliance with our privacy policy and privacy laws and regulations. Our partners include, among others, our IT providers and the administrators of our PMS system.

### **Legal Obligation**

If required by law, we will disclose your personal data. For example, the police may request data from us in the context of a fraud investigation. Additionally, as a hotel, we are required to maintain a night register and remit tourist taxes. In this regard, the municipality may request information from the night register.

## 7. Which rights do you have as a data subject?

As a data subject, you have several rights. You have the right to ask blooming about the personal data we process about you, the purpose and nature of the processing, and information about third parties with whom your personal data is shared.

You have the right to request blooming to update, correct, or delete your personal data (if the personal data is no longer necessary for the purpose for which it was collected). In principle, we retain your personal data until the reasonable or legal retention period has expired.

You can exercise your aforementioned rights at any time. You should contact the Privacy Officer if you:

- Wish to access the processed personal data;
- Want to request an update, correction, deletion, or blocking of your personal data;
- Additionally, you can withdraw your consent for the processing of your personal data at any time;
- Wish to object to a processing activity;
- Want to file a complaint;
- You can also file a complaint with the designated authority (AP). Through the link below, you can submit a privacy complaint to the AP.
- <https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/gebruik-uw-privacyrechten/klacht-melden-bij-de-ap>

blooming may deny your request if it endangers the privacy of others, is unreasonable or repetitive, or requires disproportionately large efforts. blooming will inform you within a reasonable time whether your request has been approved or denied, along with the reason for the denial.

## 8. "Which obligations does blooming have to protect your privacy in the workplace?"

When processing your personal data, we are required to safeguard your privacy as much as possible. We implement appropriate technical and organizational measures to protect your personal data to the best of our ability.

This includes, among other things, that:

- Data must be adequate, relevant, and not excessive for the legitimate purpose;
- The use, purpose, and method of processing must be clearly communicated to the data subjects (transparency);
- Data subjects must be given the opportunity to exercise their rights (access, correction, deletion, and blocking);
- Personal data must be deleted where possible and not retained longer than necessary; for this, we have a document specifying how long we keep data;
- Personal data must be secured with appropriate technical and organizational measures.

We work hard to protect your personal data from unauthorized access, alteration, disclosure, or destruction of the information we keep, particularly by:

- blooming adheres at all times to this privacy statement regarding all personal data we collect from you;
- blooming restricts the use and disclosure of your personal data and ensures that third parties with whom we share such information handle it with the privacy and security it deserves;
- blooming has established physical, technical, and administrative procedures to ensure and secure the information we collect.

## 9. What must blooming do to secure your personal data?

The General Data Protection Regulation (GDPR) does not prescribe specific measures or security standards. According to the law, the security must be appropriate for the sensitivity of the personal data and the risks associated with the processing. The costs of the measures are also taken into account. However, this does not diminish the fact that implementing information security is very important to us.

Examples of implemented security measures include:

- Security and Authorization Policy (access on a need-to-know basis only): blooming has established a procedure to assess what rights an employee should have, ensuring that not every employee has access to all rights.
- Logical Access Control (strong passwords and/or multi-factor authentication): blooming has guidelines for passwords, specifying their requirements, and outlines which information services require multi-factor authentication.
- Patch Management (timely deployment of security updates).
- Internet Connection Security (e.g., via SSL/TLS technology).
- Internal Network Security (firewalls with appropriate configuration).
- Antivirus Software.
- Encryption of devices or databases containing personal data: blooming provides encrypted laptops and mobile phones.
- Physical Access Security (e.g., fences, locks, alarm systems, cameras): blooming has policies in place for physical security.
- Ongoing Employee Training in recognizing data breaches, handling personal data, and information security.

With all external parties who may process your personal data, clear agreements regarding the processing and security of your personal data have been established. These agreements are documented in a data processing agreement.

## 10. About what should we actively inform you?

The obligation to inform is very important. Through this Privacy Statement, we aim to provide you with information, and additional details will be provided where necessary.

When the Privacy Statement changes, you will be notified. This Privacy Statement always includes the following:

- The purposes of data processing;
- The methods used for data processing;
- An overview of the data that is collected, along with the retention periods;
- Who has access to which data and when;
- How the data is secured;
- The rights of the employee.

## 11. Privacy contact person at blooming

blooming has appointed an external Privacy Officer to help the organization comply with GDPR requirements. The external Privacy Officer performs at least the following tasks:

- Ensuring compliance with laws and regulations, as well as adherence to the privacy policy;
- Advising the organization on privacy matters;
- Advising the management on conducting Data Protection Impact Assessments (DPIAs);
- Serving as a central point of contact for questions and complaints about the privacy policy.

At blooming, Stephan van Hulst has been appointed as the external Privacy Officer.  
Contact details : [privacy@weareblooming.com](mailto:privacy@weareblooming.com)

Phone number: 053-8527788

## 12. Transfer of personal data to a country outside the EU

In certain cases, we provide your personal data to external parties (when necessary). They may use this personal data solely for the execution of the relevant service. When we exchange personal data with other parties, we make written agreements that are aligned with applicable laws and regulations.

When personal data is transferred to parties outside the European Economic Area (EEA), it will be done in accordance with legal requirements, such as establishing appropriate agreements regarding the level of data protection in that country.

## 13. Retention Periods

We do not retain your personal data longer than strictly necessary to achieve the purposes for which your data was collected. When there are legal obligations for data retention, we will comply with them. All personal data will be destroyed when it is no longer needed. The processing register contains information on how long blooming retains personal data.