

# Privacy Policy

At BAM we respect privacy

[www.bam.eu](http://www.bam.eu)



# In this policy

---

<b>1.0</b>	<b>Introduction</b>	<b>2</b>
<b>2.0</b>	<b>BAM Golden Privacy Rules</b>	<b>3</b>
<b>3.0</b>	<b>Our privacy approach</b>	<b>4</b>
3.1	Data Privacy Impact Assessment	
3.2	Processing of personal data by BAM	
	3.2.1 <i>Purposes for processing personal data of employees</i>	
	3.2.2 <i>Purposes for processing personal data of third parties</i>	
3.3	Use for other purposes	
3.4	Quantity and quality of data	
3.5	Information, access and rectification	
3.6	Security and confidentiality	
3.7	Automated decisions and profiling	
3.8	Transfer personal data to third parties	
3.9	Personal data breach	
3.10	Complaints procedure	
<b>4.0</b>	<b>Governance</b>	<b>5</b>

# Policy statement: At BAM we respect privacy

At BAM, we respect the privacy rights of our staff, customers, suppliers and business partners. We are committed to managing personal data in a professional, lawful and ethical way.

The Executive Board of Royal BAM Group nv (BAM) is committed to respecting the privacy rights of our staff, customers, suppliers and other third parties we work with. Being transparent about how we deal with personal data helps to build trust.

We are committed to ensuring that BAM, all our employees and all third parties performing services for or on behalf of us, only collect and process personal data necessary for legal and regulatory or for legitimate organisational purposes.

The Executive Board aims to ensure that everyone who works with (sensitive) personal data within BAM understands the importance of protecting privacy and complies with this Privacy Policy.

Compliance with these requirements requires an overarching and standardized approach for the protection of privacy. If we do not comply with the data privacy legislation, we risk causing harm to individuals, being ordered to cease the processing, and could face fines or litigation. We are also putting BAM's reputation at risk. The data privacy legislation places greater emphasis on the documentation that BAM must keep to demonstrate our accountability for privacy.

The Executive Board regards the responsibility of everyone in implementing this policy to be fundamental to BAM meeting its stated commitments. The Executive Board has appointed a Group Privacy Officer to oversee the implementation of this policy and ensure governance and compliance with its intent.

This policy is reviewed for continuing suitability at least annually and revised as often as may be appropriate.

## **Executive Board**

Royal BAM Group nv

# 1.0 Introduction

---

The Privacy Policy applies to the processing by BAM of personal data of employees and third parties including customers, suppliers and business partners.

Personal data is all information relating to (an) identified or identifiable individual(s) (such as name, date of birth and contact details).

More sensitive information (such as race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, gender and sexual orientation and criminal convictions and offences) is sensitive personal data and subject to more stringent requirements.

The Privacy Policy applies to all BAM companies. All Operating Companies (including Group staff departments) will therefore implement this Policy throughout their systems and business processes.

This Privacy Policy does not replace any safeguards that local data privacy law may already provide to employees, those; will remain in place.

## 2.0 BAM Golden Privacy Rules

---

The Golden Privacy Rules apply to the processing of all personal data by BAM:

- 1 The processing is in compliance with BAM policy and data protection legislation
- 2 The processing is for specific, determined, legitimate business purposes
- 3 The access to and processing of data is limited to only that necessary
- 4 The data is kept accurate, complete and up to date, is only kept as long as is necessary for the intended purpose and is then securely destroyed
- 5 All personal data is treated as confidential and stored to prevent unlawful or unauthorised sharing, access or processing, accidental loss, destruction or damage
- 6 Everyone has a duty to report any suspected data breaches
- 7 The reasons for collecting and processing personal data are determined and are clearly communicated to the relevant individuals
- 8 A data protection agreement must be in place before any personal data is given to a third party
- 9 The rights of individuals to access, correct, restrict and remove their personal data will be respected
- 10 Identify privacy risks before implementing new business processes or services such as new IT systems

When in doubt about how to apply the BAM Golden Privacy rules, or if you have any further questions relating to privacy, please contact the Privacy Officer of your Operating Company or the Group Privacy Officer.

## 3.0 Our privacy approach

---

### 3.1. Data Privacy Impact Assessment

Prior to the implementation of each new process or system that includes the processing of personal data a quick scan of the impact of the envisaged processing operations on the protection of personal data shall be carried out. Where the outcome of the quick scan shows that the processing of personal data is likely to result in a high risk for individuals a data privacy impact assessment shall be carried out and the measures identified in the Data Privacy Impact Assessment shall be implemented.

### 3.2. Processing of personal data by BAM

BAM processes the personal data of:

- Employees, including job applicants, former employees of BAM and temporary workers working under the direct supervision of BAM such as independent contractors and trainees;
- Third parties, including customers, suppliers and business partners

#### 3.2.1. Purposes for processing personal data of employees

BAM processes personal data of employees necessary for the following purposes:

- Human resources and personnel management
- Business process execution and internal management
- Health, safety, security and integrity
- Organisational analysis and development, management reporting and acquisition and divestitures
- Compliance with laws and regulations

The legal basis for the processing of any personal data shall be one or more of the following:

- necessary for the performance of a contract to which the individual is a party, or to take steps to enter into a contract;
- necessary for compliance with a legal obligation to which the organisation is subject;
- necessary for protecting the vital interests of the individual;
- necessary to perform a task carried out in the public interest or exercise of official authority of the organisation;
- necessary for the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual.

Employee consent is generally not a legitimate basis for processing personal data of BAM employees, because employee consent is not considered by the data protection authorities to be given freely. One of the purposes listed above must exist for any processing of personal data of BAM employees.

#### 3.2.2. Purposes for processing personal data of third parties

BAM processes personal data of third parties necessary for the following purposes:

- Assessment and acceptance of a customer
- Conclusion and execution of agreements
- Health, safety, security and integrity
- Business process execution, internal management and management reporting
- Relationship management and marketing
- Development and improvement

The legal basis for the processing of any personal data of third parties is the same as set out in 3.2.1 above.

### 3.3. Use for other purposes

Personal data will only be processed if one of the purposes as listed in this Policy exists and for purposes that are closely related to the purposes listed in this Policy. Depending on the sensitivity of the relevant personal data and whether use of the personal data for a closely related purpose has potential negative consequences for the individual, this secondary use may require additional measures. Whether a closely related purpose exists must be assessed before the start of the processing for such secondary purpose and the appropriate Privacy Officer must be consulted.

### 3.4. Quantity and quality of data

BAM shall restrict the processing of personal data to those data that are adequate for and relevant to the applicable purpose. BAM shall take reasonable steps to delete personal data that are not required for the applicable purpose.

BAM generally shall retain personal data only for the period required to serve the applicable purpose or to the extent necessary to comply with an applicable legal requirement. Promptly after the applicable storage period has ended, the data shall in accordance with the applicable privacy regulations be securely deleted or destroyed, anonymised, or transferred to an archive (unless this is prohibited by law or an applicable records retention schedule).

Personal data must be accurate, complete and kept up-to-date to the extent necessary for the purpose for which the personal data are processed.

Where BAM requires a person to update their own personal data, BAM shall remind the individual at least once a year to do so.

### 3.5. Information, access and rectification

Prior to the processing of data, BAM provides to individuals information with respect to the processing of their personal data in accordance the BAM Privacy Statement for employee data and the BAM Privacy Statement for customer, subcontractor, supplier and business partner data. This information includes information with respect to the purpose(s) of the processing and information necessary to ensure fair and transparent processing.

Each individual may request an overview of their personal data processed by or on behalf of BAM. Where reasonably possible, BAM will provide an overview of the source, type, purpose, categories of recipients and envisaged retention period.

If the personal data is incorrect, incomplete or not processed in compliance with the applicable laws and regulations, the individual may have their personal data rectified, erased, blocked, or its processing restricted. In addition, each individual shall have the right to receive their personal data and have the right to transmit those data to another controller.

### 3.6. Security and confidentiality

BAM has taken appropriate reasonable technical and organisational measures to protect personal data from misuse or accidental, unlawful, or unauthorised destruction, loss, alteration, disclosure, acquisition, access or other processing. To achieve this, BAM has developed and implemented the BAM Information Security Policy and underlying standards.

Employees are authorised only to access personal data to the extent necessary to serve the applicable legitimate purpose and to perform their job.

Employees who have access to personal data shall meet their confidentiality obligations.

### 3.7. Automated decisions and profiling

Automated tools may be used to make decisions about individuals, but decisions with a negative outcome for the individual may not be based solely on the results provided by the automated tool. This restriction will not apply if:

- i. the use of automated tools is necessary for the performance of a task carried out to comply with or authorised by law; or
- ii. the decision is made by BAM for the purposes of entering into, managing or performing a contract with the individual; or
- iii. the individual has given their explicit consent

When processing sensitive personal data, these exceptions will not apply.

In the cases referred to in (ii) and (iii), BAM will take suitable measures to safeguard the legitimate interests of the individual, e.g. by providing the individual with an opportunity to express their point of view.

### 3.8. Transfer personal data to third parties

BAM only transfers personal data to a third party if there is a Data Protection Agreement (“DPA”) with such party and to the extent necessary to serve the purpose for which the personal data are processed and to the extent that this purpose is permitted under this Policy.

There are two categories of third parties:

- **Processors:** These are third parties that process personal data solely on behalf of BAM and at its direction and includes parties to which BAM only discloses personal data to third parties or where BAM provides remote access to personal data to a third party.
- **Controllers:** These are third parties that process personal data and determine the purposes and means of the processing

BAM concludes a data processing agreement (DPA) with processors and controllers.

If the third party is a controller or you are not clear about whether the third party is a controller or processor please contact the Privacy Officer of your Operating Company to assist you.

Personal data must not be transferred outside the EU without the prior written approval of the Group Privacy Officer or the Privacy Officer of an Operating Company.

### 3.9. Personal data breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by BAM. Examples are the loss of a USB-key, visibility of personal data of employees on internet or the intrusion by a hacker.

In case of a personal data security breach the BAM Data Breach Procedure will be applicable. A security breach must be reported to the Group Privacy Officer or the Privacy Officer of the relevant Operating Company. The (Group) Privacy Officer will assess whether the security breach qualifies as data security breach.

In the case of a personal data breach, the (Group) Privacy Officer shall without undue delay and, where feasible, no later than 72 hours after BAM having become aware of it, notify the personal data breach to the competent supervisory authority of the Operating Company’s country, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individual(s).

In case of a personal data breach BAM shall report such personal data breach to the individual(s) concerned if the personal data breach is likely to result in a high risk to the rights and freedoms of the individual within a reasonable period of time following discovery of such breach.



### 3.10. Complaints procedure

Individuals may file a complaint regarding compliance with this Policy or violations of their rights under applicable law with the appropriate Privacy Officer.

The appropriate Privacy Officer shall notify the Group Privacy Officer, initiate an investigation and when necessary, advise the business on the appropriate measures for compliance and monitor, through to completion, the steps designed to achieve compliance.

Within four weeks of BAM receiving a complaint, the appropriate Privacy Officer shall ensure the individual is informed in writing of BAM's position with regard to the complaint and any action BAM has taken or will take in response or when the individual will be informed of BAM's position.

An individual may file a complaint with the Group Privacy Officer if the resolution of the complaint by the appropriate Privacy Officer is unsatisfactory to the individual.

## 4.0 Governance

The table below depicts the roles and responsibilities of the main participants for privacy.

Role(s)	Responsibilities
Executive Board	The Executive Board of BAM is ultimately accountable for privacy. The Executive Board is responsible for providing direction on and commitment to privacy. This includes approving and endorsing the Privacy Policy. Additionally, the Executive Board shall actively promote information privacy. The CFO is the first point of contact.
OpCo management, Directors Corporate functions and Line Management	OpCo management and Directors Corporate functions are accountable for privacy within their OpCo and Corporate function. At each level, Line Management is responsible for the implementation, promoting privacy awareness, execution and monitoring compliance with the Privacy Policy.
Group Privacy Officer (part of GRC function)	The Group Privacy Officer is appointed by the Executive Board. The Group Privacy Officer defines strategy, policies and group wide initiatives, makes sure governance is effective, actively promotes privacy awareness and provides oversight of the execution. Furthermore, data protection issues are discussed with the Privacy Officer of the Operating Company (including Group support functions). Reports on cross-OpCo status are provided to the Executive Board
Group Privacy Council	The Group Privacy Council comprises dedicated members from Group HR, ICT, Legal, and Procurement and is being chaired by the Group Privacy Officer. This team coordinates the cross-OpCo privacy initiatives and the development and updating of the privacy policy and related templates. Furthermore, data privacy issues are discussed including follow up actions.
Privacy Officers at Operating Companies	Each OpCo has appointed a Privacy Officer. The primary objective of the OpCo Privacy Officer is to oversee, steer and support the OpCo and the Group Privacy Officer with implementing and managing privacy policy requirements and promote privacy awareness. The OpCo Privacy Officer reports to OpCo management and functionally to the Group Privacy Officer on incidents and compliance to the privacy standards.

**Royal BAM Group nv**

Runnenburg 9  
3981 AZ Bunnik  
P.O. Box 20  
3980 CA Bunnik  
The Netherlands  
Telephone +31 (0)30 659 89 88  
info@bam.nl  
www.bam.eu

Established at Bunnik  
Trade Register number 30058019