Brunel International N.V.
Global Data Protection Policy

About Brunel
Founded in 1975, Brunel is a global specialist delivering customised project and workforce solutions to drive sustainable industry transformations through technology and talent. With a broad international presence and a strong network of experts worldwide, we deliver Project and Consulting Solutions, Workforce Solutions and Global Mobility Solutions that transform global projects in Renewables, Conventional Energy, Mining, Life Sciences, Future Mobility, Industrials & Technology and many other sectors. Guided by our passion for people and a commitment to integrity, we recognize our ability to create positive social and environmental impact. Our strategy embeds Environmental, Social, and Governance (ESG) principles at the heart of everything we do, driving sustainable and responsible growth across all markets.

Scope
This policy applies to all Brunel regions and entities, covering every aspect of our operations and partnerships.

1. Introduction
In the performance of its business, Brunel processes Personal data of business partners, candidates, and employees. It is essential that all Brunel employees who work with Personal data are aware of the applicable data protection rules for Brunel. This Data Protection policy provides a framework for this purpose and binds all Brunel group companies and Brunel employees. This policy is based on the principles of the General Data Protection Regulation (GDPR) (EU) 2016/679. When local privacy legislation requires stricter measures than described in this Data Protection policy or related policies or procedures, the local regulations prevail over this Data Protection policy, upholding the principles of this policy. Where local privacy obligations conflict with the content of this Data Protection policy or related policies or procedures, local privacy experts should obtain advice from the Brunel Data Protection team.

2. Definitions

Brunel	Brunel International N.V. and its subsidiaries, and their branches.
Controller	The person or organisation which, alone or jointly with others, determines the purposes and means of the processing of Personal data.
Data Protection Impact Assessment (DPIA)	A measure to demonstrate compliance, with Data protection regulations and identify and limit risks for individuals.

Brunel Data Protection team	The team responsible for data projection compliance within Brunel.
Data subject	The person whose Personal data is being processed.
Lead supervisory Authority	The Dutch data protection authority (Autoriteit Persoonsgegevens).
Personal data	Any information relating to an identified or identifiable natural person ('Data subject').
Privacy by default	The implementation of appropriate technical and organisational measures to ensure that by default Personal data is not made accessible to an indefinite number of persons.
Privacy by design	The implementation of technical and organisational measures at the earliest stages of the design of the processing operations, in such a way that data protection principles are safeguarded right from the start.
Processing	Any operation or set of operations that is performed on Personal data, whether or not by automated means, such as collection, storage, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, combination, restriction, erasure or destruction.
Processor	A natural or legal person, public authority, agency or other body which processes Personal data on behalf of the Controller.
Supervisory Authority	An independent public authority responsible for monitoring the compliance with data protection regulations.
Third party recipient	A natural or legal person, public authority, agency or another body, to which the Personal data are disclosed, other than the Data Subject, Controller or Processor.

3. Starting points of the Brunel Data Protection Policy

3.1 Principles for processing of personal data

Lawful, fair and transparent
In processing Personal data, Brunel protects the individual rights and interests of the Data subjects. Brunel processes Personal data fairly and in accordance with applicable legislation. Brunel actively informs the Data subject of the manner in which its Personal data is being processed. As a matter of principle, Brunel collects Personal data directly from the Data subject.

Restriction to a specific purpose
Brunel processes Personal data only for the purposes for which they were originally collected and in a manner that is compatible with those purposes.

Data minimisation
Brunel only processes Personal data that is adequate, relevant and limited to what is necessary for the purpose(s).

Data quality
Brunel keeps Personal data accurate and up to date. If Personal data is not accurate, Brunel takes reasonable steps to rectify or delete this data.

Data retention
Brunel does not retain Personal data longer than necessary for the realisation of the purposes for which Personal data is processed or as permitted by law.

Need-to-know principle
Brunel ensures that employees have access to Personal data on a need-to-know basis only. This means that employees have access to Personal data only as such access is required for the proper fulfilment of their task or duty.

Integrity and confidentiality
Brunel uses appropriate technical and organisational measures to protect Personal data against unauthorised access, unlawful processing, loss, destruction and damage.

Accountability
Brunel demonstrates compliance with the data protection regulations by:

- Performing a DPIA before the start of a new project that involves Personal data;
- Carrying out a legitimate interest assessment when processing is based on legitimate interest;
- Enforcing Privacy by design and Privacy by default in the event of new developments with Personal data involved;
- Keeping a register of Personal data breaches that documents all Personal data breaches and security incidents;
- Demonstrating vendor due diligence, monitoring compliance and third parties' contracts;
- Keeping records of consent given by Data subjects;
- Having a cookie management procedure in place.

3.2 Legal grounds of processing personal data

Data processing based upon a (pre) contractual relationship
Brunel processes the Data subject's Personal data for the execution of its contract with Brunel.

Data processing based on legal obligation
Brunel processes Personal data if processing is necessary for compliance with a legal obligation to which Brunel is subject to.

Data processing based on legitimate interest
Brunel processes Personal data if processing is necessary for the purposes of the legitimate interests, except where such interests are outweighed by the interests the Data subject.

Data processing based on consent
Brunel informs the Data subject of the intended data processing. Brunel asks consent for each processing purpose and documents a given consent. The Data subject can withdraw its consent as easy as it was given at all times.

Data processing based on a vital interest
Brunel processes Personal if processing is necessary in order to protect the vital interests of the Data subject.

4. Rights of data subjects

Data subjects can exercise the following rights, some rights can be exercised at all times; other rights can be exercised under certain conditions only. Brunel may request Data subjects to provide additional identification in this regard.

- **Withdrawal** of consent for processing Personal data;
- **Access** to Personal data;
- **Correction** of inaccurate Personal data;
- **Deletion** of Personal data if no longer necessary for Brunel;
- **Objection** to the processing of Personal data on the basis of a legitimate interest of Brunel or another controller, if Data subjects have major interests for making such an objection;
- **Restriction** on the processing of Personal data in cases determined by law;
- **Data transfer** of the Data subject's own Personal data provided to Brunel in cases determined by law;
- **Lodging complaint** with the national supervisory authority about the processing of Personal data by Brunel.

5. Sharing personal data

For some business processes of Brunel, it is necessary to share personal data.

Sharing within Brunel
Within the Brunel group, Personal data are only shared with employees authorised to access this data. All employees are subject to confidentiality.

Sharing with third parties
Brunel shares Personal data with external parties whereby both parties have their own responsibilities concerning the protection of Personal data.

Sharing with official authorities
Brunel only discloses Personal data to official authorities if there is a legal obligation to do so.

Safeguards
Brunel has an Inter Group Agreement in place for the transfer of Personal data to its subsidiaries. Each Brunel subsidiary is bound by the Inter Group Agreement. Brunel concludes data processing agreements with third parties that process Personal data on behalf of Brunel. When transferring to recipients in countries without an adequate level of protection, Brunel uses generally accepted standard provisions to ensure that Personal data is adequately protected. These recipients are also assessed for their ability to ensure the secure processing of Personal data and the rights of data subjects.

6. Security of personal data

Brunel gives priority to the adequate security of Personal data. Brunel adopts physical, technical, and organisational measures to ensure the security of Personal Data, including the prevention of alteration, loss, damage, unauthorised processing or access. These measures are documented within the Data Security Management policy, which is reviewed periodically.

Under the Data Breach policy, Personal data breaches are reported as soon as possible to the supervisory authority, unless the Personal data breach is unlikely to result in a risk to the rights and freedoms of the Data subject. Depending on the nature and extent of the breach, Brunel informs the Data subject involved.

7. Roles and responsibilities

7.1 Management responsible

The Global Head of IT & Digital owns the global data protection policy and programs, overseeing their implementation across all regions. The Chief Information Security Officer is responsible for the data process, internal audits and certification (ISO27001) processes across all regions.

7.2 Brunel data protection team and local privacy experts

Brunel International N.V. appointed a central data protection team (“Brunel Data Protection team”).
The local Brunel subsidiaries can have their own local privacy experts. Local privacy experts are responsible for local privacy issues and act as first point of contact. They cooperate intensively with the Brunel Data Protection team, for example in case of a data breach. The Data Protection Officer form parts of the Brunel data protection team and reports to the Chief Financial Officer.

7.3 Brunel employees

All Brunel employees are responsible for ensuring observance of this Data Protection policy and compliance with national data protection regulations.

7.4 Lead supervisory authority

Where the processing of Personal data takes place in the context of the activities in more than one state, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) will act as Lead supervisory authority for Brunel.

8. Changes to the data protection policy

Brunel can change this Data Protection policy. Brunel encourages all employees to consult this Data Protection policy on a regular basis. Brunel communicates changes to this policy via its company intranet to all internal employees and when relevant for contractors. The Brunel Data Protection team reviews the Data Protection policy periodically.

9. Contact

For questions or comments regarding this data protection policy, please contact privacy@brunel.net