

# Personal Data Protection & Privacy Policy

Protecting your personal data

# Introduction

As a responsible company we know it is essential to protect your personal information. Whether you are an employee, customer, supplier or visitor to our office – we will collect and process your personal data in line with legal requirements, best practice and individual expectations.

This policy will help us in that commitment. Data privacy laws and regulations differ depending on the country; this policy provides a consistent, minimum standard of working and helps us to ensure we are globally compliant. Our policy also demonstrates to the regulators that we consider good handling of personal data as a key business principle, and an integral part of our Code of Conduct.

Any breaches of this policy could have serious consequences for us: damage to our brand reputation; financial penalties and limitations on our ability to use personal data. Breaches could also result in criminal sanctions.

It is critical we all read and follow this policy - including our contractors, subcontractors and colleagues.

Our policy explains our approach to handling personal data, and covers the following areas:

- the minimum standards to be adopted
- our responsibilities
- your responsibilities
- your rights under data privacy legislation
- our approach to using third parties to process personal data.

The 'data controller' for the Berge Bulk group (including all vessel-owning companies, management companies and holding company) is Berge Bulk Singapore Pte Ltd (BBSGN). This includes Berge Bulk Maritime Pte Ltd, Berge Bulk Shipping Pte Ltd and Berge Bulk UK.

As 'data controller', BBSGN provides oversight through the Global Personal Data Protection & Privacy Policy, processes and procedures. Each legal entity shall adhere to the Global Personal Data Protection & Privacy Policy, processes and procedures.

# Our Global Personal Data Protection & Privacy Policy

## 1.1. Legal Requirements

Data privacy legislation strikes a balance between our need to collect, hold, use and disclose personal data - and your rights and privacy expectations as an individual. Personal data privacy legislation means we will be held to account if we mis-handle your personal information.

Personal data privacy legislation is not the same in every country. Our company references the PDPA and GDPR standards as a baseline.

In some countries, there are serious consequences, including criminal sanctions, both for individuals and companies who breach data privacy laws. So, we have decided that:

- each legal entity within our organisation will be responsible for the personal data which it collects, uses, processes, or has processed on its behalf (e.g. by a third-party supplier)
- it is your responsibility to uphold the principles of personal data privacy in the business and follow all laws and proper procedures
- contractors (individual or corporate) should behave like employees when processing personal data, except where we specify otherwise in their contract terms.

Each legal entity must assess risk in fulfilling its responsibilities for personal data, considering:

- listing the processing of personal data, the data processed and the media they rely on
- assessing the risks generated by each processing operation
- implementing and assessing planned measures
- carrying out periodic audits with necessary action plans.

BBSGN has a designated Data Protection Officer (DPO) to manage risk and compliance matters. The role of DPO includes, but not limited to:

- Ensuring compliance with data protection rules
- Fostering a Data Protection Culture
- Advising on personal data protection obligations
- Assisting with Data Protection Impact Assessments (DPIAs)
- Acting as a contact point for data subjects and regulatory authorities
- Facilitating data subjects in exercising their rights
- Educating employees about compliance
- Conducting regular audits
- Managing personal data breaches

Berge Bulk Data Protection Officer may be contacted at [dpo@bergebulk.com](mailto:dpo@bergebulk.com).

## **1.2. Processing of personal data**

### **1.2.1 Personal data**

Personal data is any information about living, identifiable individuals. This can be information which relates to someone's professional or private life. It includes basic data such as name or private contact details, as well as more sensitive types of data such as name, birth date, NRIC, racial origin, or medical data. We collect and use personal data in both paper and electronic form.

### **1.2.2 Berge Bulk and personal data**

We need to collect, use and often transfer personal data for business reasons and to benefit various groups of people, including, but not limited to:

- prospective, current and ex-employees
- sub-contractors
- suppliers of goods / services
- clients and customers
- visitors to our sites

### **1.2.3 Processing of employees' personal data**

We will use your personal data, and information obtained from other sources, for (but not limited to):

- personnel administration such as recruitment; employee performance management and professional development
- management activities such as planning
- payroll and pensions administration
- travel management
- building and managing external relationships, for example suppliers and customers
- purposes required by law or regulation

We aim to make sure that personal data held about you is accurate and up to date, both whilst you are working for us and after. It is your responsibility to notify us straight away if there are any changes in your personal circumstances, so that we can keep your information updated.

### **1.2.4 Requests for access, correction, deletion and/or withdraw consent to collect, use and/or disclose (share) personal data**

You may submit your request to Berge Bulk Data Protection Officer (DPO) through email at [dpo@bergebulk.com](mailto:dpo@bergebulk.com)

Requests shall be reviewed and actioned within a reasonable timeframe, unless required by law or for legitimate business purposes.

The Company may from time to time, receive requests to provide employment verification (or reference checks) of former employees. The Company shall require such requests to be in writing, with written authorization by the former employee whose data is being requested.

The Company shall limit the data shared with requestor to business information such as job title, start and end date of employment, whether employment was terminated on voluntary or involuntary basis.

#### **1.2.5 Processing of non-employee personal data**

We often process personal data about individuals other than employees - such as customers, business contacts, visitors to sites, suppliers, website users and shareholders. We do this for several reasons, including:

- health and safety purposes
- visitor management
- business and market development
- building and managing external relationships
- planning and delivery of goods and services
- research and development
- knowledge management
- training
- other purposes required by law or regulation

#### **1.2.6 Processing of sensitive personal data**

Sensitive personal data is defined under the PDPA and EU legislation as information about an identifiable individual, racial or ethnic origin; political opinions; religious or other similar beliefs; trade union membership; physical or mental health conditions; sexual life, sexual orientation; biometric or genetic data and/ or personal data relating to criminal offences and convictions. We work to this definition, and will not collect this type of information unless:

- you agree that we may do so, based on a full understanding of why the data is being collected, e.g. in order to process pre-employment checks. In exceptional circumstances, we may rely on consent given on your behalf, for example, by a family member, or
- we need to do so to meet our obligations or exercise our rights under employment law e.g. for reporting on ethnicity, or
- in exceptional circumstances such as where the processing is necessary to protect your vital interests e.g. you need access to specific drugs to ensure your health, or
- in circumstances permitted by data privacy laws. This does not mean however that we can collect sensitive data without appropriate judgment. We always need to decide, and be able to justify, how necessary it is to collect this information, and if there is any alternative to doing so.

#### **1.2.7 Monitoring of personal data**

There may be situations where, for quality control, training, security and/or investigation purposes, we monitor recordings of your telephone, internet access/ usage and email communications. This is explained in more detail in our Employee Handbook.

### **1.3. Our responsibilities**

We are committed to complying with personal data privacy legislation in all the countries we engage in when processing your data. To demonstrate this commitment, we will ensure that:

- we monitor changes in personal data privacy legislation and implement these as appropriate
- everyone managing and handling personal data understands that they are responsible for following good personal data privacy practice
- everyone managing and handling personal data is appropriately trained and adequately supervised
- anyone with a question about handling personal data knows where to go for advice and is supported in knowing what to do
- queries about handling personal data are promptly, professionally and courteously dealt with
- processes for handling personal data are clearly described in policies and procedures to ensure excessive data is not collected; data is not stored for longer than necessary; confidentiality and security is always respected
- methods, such as collection and destruction, of handling personal data are regularly reviewed
- any personal data handling breaches are logged, fully investigated, and reported to the appropriate regulatory authority where necessary.

Our Heads of Function have the responsibility for ensuring our personal data privacy standards are followed in their business area.

#### **1.3.1 Fair and lawful processing**

We process your personal data where we need it to:

- enter into a contract with you, or
- comply with a legal obligation, or
- protect your vital interests in a 'life or death' situation, or
- process the personal data to pursue our legitimate interests, or
- for any other purpose permissible under relevant privacy laws

A legitimate interest is when we have a business or commercial reason to use your information, provided this is not over-ridden by your own rights and interests.

You have the right to withdraw consent for us to process and disclose your data, but this may impact our ability to fulfil our contract with you, for example paying you your salary. Refer to paragraph 1.2.4 for more information on how to submit your request.

#### **1.3.2 Accuracy of data**

It is our responsibility to have procedures and systems in place to ensure that:

- we do not collect excessive personal data

- personal data is adequate, relevant, accurate and up to date for the intended purposes
- we process personal data only for the purposes specified in this policy, associated local policies or in information provided to you.

### **1.3.3 Retention of personal data**

We will ensure that your personal data is only retained for an appropriate amount of time - given the purposes for which the data is used - except where another law requires us to keep the data for a certain length of time. In the absence of legislated duration of personal data retention, we shall adhere to the following personal data retention periods:

- Employment Termination – 6 years after the last day of employment
- Recruitment Profiles – 3 years upon receipt of a profile

Deletion of personal data shall be done in a secure and confidential manner.

Any consent given in relation to personal data, shall, subject to all applicable laws and regulations, survive death, incapacity, bankruptcy or insolvency of any such individual.

### **1.3.4 Security of data**

We will maintain organisational, physical and technical security arrangements in relation to the personal data we hold. We will ensure that those arrangements are appropriate to the risks represented by the processing of and the nature of the personal data. Where appropriate these arrangements will include provisions for 'need to know' access to personal data.

We will ensure that appropriate diligence activities are carried out in relation to the security of personal data, both before and after we use it and/or take responsibility for it.

### **1.3.5 Sharing personal data with service providers**

We often use third party suppliers to process personal data for employment purposes e.g. for payroll processing; psychometric testing for development purposes; recruitment purposes; benefits administration; storage of personal data on a secure network. We also share with, but not limited to, custom brokers, shipping lines, airlines & other transportation, sub-contractors, liability brokers and bodies as required by your location needs or requested by any regulatory authority.

Where this is the case, we are using a 'data processor' under the terms of privacy legislation and must always put in place contractual terms to safeguard the personal data we share with them.

Personal data also needs to be treated with particular care in countries which do not have data privacy laws, or whose laws do not provide a level of protection

equivalent to the standard within the EU. Therefore, we will not transfer personal data to other companies for processing unless they agree to abide by a data privacy standard at least as high as this policy; or enter into a contractual arrangement which includes the approved EU standard clauses for transfers of personal data outside of the EU. Our responsibilities extend to the sub-contractor level, so it is important to ensure that appropriate contractual controls are always in place to minimise our risks. The only exceptions are where:

- the transfer is necessary to protect your vital interests in a 'life or death' situation
- to enter into or perform a contract with you (or for your benefit)
- you have consented to the transfer.

#### **1.3.6 Storage and management of confidential, sensitive, personal data**

Employees are strongly advised to avoid storing confidential, sensitive and personal data onto their laptops or other local devices. Sensitive / confidential / personal data includes, but is not limited to, personal identifiable information, salary information, employee performance reviews, financial records, and any other confidential information.

Employees must use Company approved secured storage platforms such as SharePoint and/or Microsoft Teams for storing, accessing and working on such sensitive data. These service platforms have been vetted for security and compliance.

Access to sensitive data must be restricted based on the principle of least privilege, i.e. employees should only have access to the data necessary for their role.

Employees must report any suspected personal data breaches or security incidents immediately to the IT department and DPO.

### **1.4. Your responsibilities**

It is the responsibility of all of us to make sure that our company complies with all personal data privacy laws. Whenever personal data is collected or used in any way, the principles set out in this policy, and any associated documents, must be followed by those of us handling the personal data. We have created six key privacy messages, based on legislative requirements, in section 1.5 which everyone in our business must follow when processing personal data.

In some countries, certain breaches of personal data privacy legislation can lead to personal criminal liability for you as well as us. Failure of employees to comply with their responsibilities under this policy and any associated procedures or guidelines may be deemed as misconduct and result in disciplinary action.

### 1.5. Six key privacy messages for our employees

Good personal data privacy compliance can be summarised into six key messages. Please make sure you understand and apply them whenever you are handling personal data:

1. **Transparency and choice** – when we collect personal data, we will only use it for the specific purpose we have promised.
2. **Quality** – personal data must be accurate and kept up to date. The data must be relevant to the reason we are collecting and processing it – and we need to make sure we do not collect information we do not need.
3. **Security** – we must take appropriate steps to protect the personal data we hold. We do not want it getting into the wrong hands, or even lost. Things to consider when thinking about security measures are the nature of the data and the potential effects of losing it. We will need to make sure our third parties do the same.
4. **Transfer** – some countries restrict the transfer of personal data depending on where you are moving the data is going to and what safeguards are in place in that new location. You will need to check if restrictions apply, and if so, whether any control mechanisms are in place (such as inter-group agreements between the transferring and receiving companies).
5. **Retention** – we must only keep personal data for as long as we need it (and in relation to the purpose we collected it). Retention policies must be followed, and data destroyed properly.
6. **Access and rectification** – if an individual request access to their data we need to provide this in a timely manner. We will also need to change any factually incorrect data where requested.

### 1.6. Individuals' rights

It is important that you understand your individual rights when it comes to personal data privacy. This section highlights certain rights we all have, whether we are employees or not, in relation to our personal data.

#### 1.6.1 Right of access

You have the right to ask for a copy of the personal data held about you, and for any inaccuracies in the information to be corrected.

We have a process to deal with these requests, whether they are received from yourself, other individuals or third parties acting on your behalf. The actual steps within the process may differ depending on the region you are in, so to exercise this right you should contact your HR representative for information.

#### 1.6.2 Right of correction

Anyone may ask that we correct the personal data we hold about them. If we agree that the data is incorrect, we will delete or correct the data. If we do not

agree that the data is incorrect, we will note within the relevant record the fact that you consider the data to be incorrect.

#### **1.6.3 Right to object to direct marketing**

We will abide by any request from you not to use your personal data for direct marketing purposes.

#### **1.6.4 Right to object to processing for compelling reasons**

You may want us to stop processing your personal data for various reasons. If you do, and we think the reason is compelling and legitimate we will discuss the possibility of stopping the processing of your data straight away with you.

### **1.7. Governance**

We will make sure that we:

- facilitate compliance with our policy
- allow you to exercise your personal data privacy rights
- listen, consider and respond to any complaints that this policy has not been followed

If you want to exercise your personal data privacy rights or need assistance with any of the actions outlined in this policy, please contact your local data privacy contact or the Global Personal Data Protection & Privacy Policy function.

**It is important you remember that any breach of this policy (or the policies referred to within it) may, following an investigation, result in disciplinary action potentially up to and including dismissal.**

### **1.8. Where to find out more**

If you have any questions regarding this policy or require further clarification, please contact [dpo@bergebulk.com](mailto:dpo@bergebulk.com).