Global Policy

Data Privacy

Purpose

This Corporate Global Policy is intended to provide a baseline for compliance with data privacy laws as they apply to the company and its subsidiaries when processing personal data.

Orbia processes personal data related to employees, job applicants, customers, suppliers, vendors, and others. Orbia is committed to processing personal data in full compliance with data privacy laws.

Certain categories of personal data may be further categorized as a "special category of personal data" or "sensitive" personal data. Particular care is needed when processing special categories of personal data or sensitive personal data, as extra rules may apply depending on the applicable local laws.

Data privacy laws are not intended to prevent the processing of personal data, including sharing personal data within our company, but to ensure that it is done fairly, in a secure and transparent manner, and without adversely affecting any individual rights.

You are responsible for actively supporting a data privacy compliance culture:

a. Ensure that your team members are aware of the importance of data privacy laws;
b. Ensure that your team members understand their own role in complying with data privacy laws; and
c. Ensure that your team members understand how other policies are related to this Policy. In the case of doubt please contact the Legal Department.

Definitions

1. "**Personal data**" means any information relating to an identified or identifiable living individual. An individual is 'identifiable' where they can be identified, directly or indirectly, including (but not limited to) by reference to an identifier such as a name, an ID number, location data, or an online identifier. An individual is identifiable directly when no other information is necessary to identify them. An individual might be indirectly identifiable when it is necessary to combine other information held by or likely to come into possession of the company to identify them. It applies to digital or physical information. In some jurisdictions, the definition of what constitutes "personal data" (and, therefore, what the relevant laws apply to) may be broader or narrower than this.

Examples of personal data: name; contact details; salary information; health information; staff ID number; staff performance reviews; financial information; marketing preferences; purchasing history; IP address etc.

2. **"Processing"** means any activity in relation to the personal data such as reading, editing, sending, receiving, storing, etc.

3. **"Sensitive Personal Data"** (or “sensitive personal data”) may include information that requires additional protection such as race, ethnic origin, political opinions, religious or philosophical beliefs, health, genetic data, biometric data (in some circumstances), sexual orientation, sex life, criminal offences (including alleged offences and proceedings), marital status, financial information, trade union membership, and may include other similar private information. In some jurisdictions, the definition of what constitutes a “special category of personal data”/” sensitive personal data” may be broader or narrower than this.

Scope

This Policy applies to all individuals working for or on behalf of Orbia worldwide, regardless of the place where Orbia operates or maintain business. Ignorance or misunderstanding of the rules is no excuse for violations. Further details of the requirements of local data privacy laws are set out in our local data privacy policies.

Principles Governing Data Processing Activities

Orbia and its subsidiaries are deeply committed to process personal data in a manner that provides a consistent and adequate level of protection for the personal data by the following principles:

1. **Notice/Transparency**
   Personal data will only be processed in a manner which has been notified to the individuals to whom the personal data relates as required by applicable local data privacy laws. The notice given to the individuals will explain the purpose of the processing and make the individuals aware of their rights by their personal data.
2. **Purpose limitation**
   Personal data will only be processed for specified and lawful purposes. Where required by local data privacy laws, we will not permit personal data to be processed for any further purposes or in any further manner which is incompatible with the purpose for which it was collected unless there is a lawful reason to do so.
3. **Lawful reason for processing**
   Personal data can only be processed where there is a lawful reason for the processing. Where required by local data privacy laws, it might be required to obtain the individual’s consent before processing their personal data for a particular purpose. In other instances, consent may not be required – for example, if the processing is necessary for the performance of a contract with the individual. Furthermore, we may not need consent where the processing is in the legitimate interests of Orbia or its subsidiaries and does not cause unfair prejudice to the individual. The requirements may be more rigorous where the personal data processed is a “special category of personal data”. Please refer to the relevant local data privacy policy for more information.
4. **Quality**
   Orbia is committed in complying with local data privacy laws to ensure that personal data is kept accurate and up to date. Employees processing data are responsible for data confidentiality and accuracy. All employees have a key role to play in ensuring their personal data is accurately maintained and up to date.

5. **Proportionality**
   Orbia will only collect minimum amount of personal data required in relation to the purpose of the processing as required by applicable local data privacy laws.

Examples of proportionality: Orbia may want to collect customer email addresses for a specific direct marketing email campaign. In this instance it would not be proportionate for Orbia to also collect the mobile phone numbers of the customers because the mobile phone numbers are not relevant to the purpose of the processing.

6. **Retention**
   Many local data protection laws require that we retain the personal data for only so long as is necessary in relation to the purposes for the processing. You are also required to comply with the relevant document retention policies where applicable.

7. **Onward transfers**
   Orbia does not authorise any third party to process personal data collected or received without previously taking steps to ensure that the third party maintains the same level of protection for the personal data as required by the relevant data privacy laws. Orbia requires entering into a contract with the third party to ensure that they are contractually obliged to protect the personal data. Any contract with third parties for this purpose requires the Chief Compliance Officer authorization.

8. **Individuals' rights**
   Orbia is committed to processing personal data in compliance with individuals' data privacy rights. In some countries, individuals may have a number of rights including the following:

   - right to information: Individuals have a right to be informed about the processing of their personal data (see principle 1 above);
   - right to access and receive a copy of their personal data: Individuals are entitled to receive confirmation as to whether or not their personal data is being processed and, if so, to access it and be provided with certain information in relation to it, such as the purpose(s) for which it is processed, the persons to whom it is disclosed and the period for which it will be stored;
   - right to rectification: Individuals can require the correction of any inaccuracies in relation to their personal data without undue delay;
   - right to request erasure of personal data ('right to be forgotten'): Individuals can require the erasure of their personal data, without undue delay, if it is no longer needed for the purpose for which it is being processed or if it is unlawfully processed or if erasure is required to comply with a legal obligation. There are some exceptions to this right;
   - right to restrict processing of their personal data: Individuals can require the restriction of processing of their personal data in certain circumstances including if the personal data is inaccurate or if the processing is unlawful;
   - right to receive a copy of their personal data in a portable format ('data portability'): Individuals can, in certain circumstances, receive their personal data in a structured, commonly used and machine-readable format so that it can be transferred to another company;
   - right to object: Individuals can object to:
     - any decision which is based solely on "automated processing" (i.e. without any human involvement); and
     - the processing of their personal data where the lawful reason for processing it is that it is necessary for a legitimate business interest;

- right to withdraw their consent to the processing of their personal data: Where the lawful reason for processing personal data is that the individual has consented to the processing, individuals have the right to withdraw their consent to processing of their personal data at any time. If this happens, the processing of their personal data must stop unless there is another lawful reason which will apply to the processing – in which case, the individual must be informed about this.

These rights may differ between local data privacy laws (i.e. not all of them will be available in all jurisdictions) and certain exceptions/limitations/qualifications may apply to the exercise of these rights. Any employee who wishes to exercise any of their data privacy rights shall contact the Legal Department. Any employee who receives a request from an individual who wishes to exercise any of their data privacy rights shall contact the Legal Department as soon as possible (as Orbia may be legally required to respond within a short timescale).

9. **Data security**
Orbia is committed to apply the standards required by data privacy laws to protect the personal data process both from a technical security and organizational security perspective. Every employee plays a key role in ensuring Orbia protects personal data. Details of these security measures is contained in the IT Security Handbook.

In some jurisdictions/regions (including the European Economic Area), Orbia may be under a legal obligation to notify the relevant local Data Protection Authority (i.e. the body responsible for regulating data privacy laws in the relevant country) of any breaches of security (within very short timescales) and, in some cases, the individuals affected by the breach. Orbia shall, where required to do so by local privacy laws, put in place local policies to cover this (such as [Orbia Europe IT Security Management Policy and Process within the European Economic Area) which are to include details of whom you should contact (and how quickly) if you become aware of a breach.

In case of doubt please consult the Legal Department.

Sharing of Personal Data

a. **Sharing Personal Data within Orbia**
Personal data can be shared within Orbia in full compliance with this policy and any other requirements of applicable local data privacy laws. For example, sharing customer data would require the sharing to have a lawful reason, have a specified purpose, comply with the notice/transparency principle and that the security of the personal data is ensured.

However, the data privacy laws of some countries including those within the European Economic Area also require that specified contractual obligations are agreed between the parties to protect the personal data before the sharing can take place. Orbia has put in place a global personal data sharing agreement (the **"Intra-group Agreement"**) which contains these contractual obligations (including those required where personal data is transferred outside of the European Economic Area) and which protects transfers of personal data made pursuant to that Intra-group Agreement. Those Orbia entities sharing and receiving personal data pursuant to the Intra-group Agreement shall comply with the terms of the Intra-group Agreement.

The sharing may also result in the need for one or more of Orbia's subsidiaries (outside of the European Economic Area) to register the sharing with and sometimes obtain the approval of the relevant Data Protection Authority (i.e. the body responsible for regulating data privacy laws in the relevant country). Local data privacy laws may also require that an additional data processing agreement is entered into between the parties between whom

the personal data is shared. If applicable, further information can be found in our local data privacy policies. If in any doubt, consult the Legal Department.

b. **Sharing Personal Data Outside of Orbia**

Orbia may sometimes be required by law to share personal data outside of the company for example, in response to law enforcement request. If you receive such a request, consult with the Legal Department to establish whether Orbia is required or allowed to share the personal data.

Orbia also may want to share personal data with third parties for specific services purposes involving processing of personal data. Such sharing must be compliant with all relevant local data privacy laws and this policy. This may involve a requirement to enter into data processing agreements and data transfer agreements. (Please note that the Intra-group Agreement does not apply to sharing personal data outside of Orbia.) Outside of the European Economic Area, the transfer may also require registration with and sometimes approval from a relevant Data Protection Authority.

Examples of sharing personal data – within and outside of our group: Orbia may seek to obtain personal data about customers of its European subsidiaries, so that it can conduct a review into the purchasing levels of customers across the whole group. This will involve the European subsidiaries sharing customer personal data. In order to share the personal data, Orbia will need to ensure that the sharing complies with local data privacy requirements. In this instance, the subsidiaries will need to ensure that the sharing is documented in the Intra-group Agreement, to ensure compliance with local privacy laws and that the personal data relating to customers is protected.

Furthermore, Orbia may want to engage a third party to assist it with the review of customer spending levels. This means the third party will have access to the customer personal data. In this instance, Orbia subsidiaries will be required to enter into data transfer agreements directly with the third party and any other corporate entity that might be involved (as the Intra-group Agreement will not apply).

The European subsidiaries would also need to ensure that the relevant individuals had been notified about the sharing.

Privacy by Design, Impact Assessments and Data Minimisation

Orbia will ensure that data privacy requirements are taken into account during the inception of any project or process that requires processing personal data.

Orbia shall carry out data privacy impact assessments before processing data that may have a significant impact on individuals. If required to carry out such assessments, further details will be contained in local data privacy policies.

Consult with the Legal Department before launching any project processing personal data.

Further to the ‘Proportionality’ Principle Orbia may be required by local data privacy laws to anonymise or pseudonymise personal data so we are not unnecessarily using it in personally identifiable form. For example, if the objective of analysis could be achieved by using aggregated information with names and other individual identifiers removed.

Accountability

Where applicable under local data privacy laws, Orbia may be required to demonstrate its compliance with such laws (‘Accountability Principle’). Information about where Orbia is required

to do this, and how it will comply with the Accountability Principle, will be set out in local data privacy policies.

Amendments

Deviations or changes to these Policies require the approval of Orbia Vice President & General Counsel.

Reporting a concern

Because we all have a stake in Orbia's success, it is in all of our interest to help ensure that our business is conducted to the highest ethical standards, and that our reputation remains untarnished. For this reason, we strongly encourage you to report any situation you know or suspect about that may involve illegal, unethical or otherwise improper business activity, as well as all instances of employee violations of this or any other of the Orbia policies. Doing so will allow the company to address the issue and take appropriate corrective action.

If you have a good-faith belief or concern related to improper or illegal conduct, you should immediately bring it to the attention of Orbia:

- Log in here from any computer with an Internet connection and clicking on the Orbia Whistleblower Line link to file a web report.

Orbia will not tolerate retaliation against you due to your report or participation in any internal investigations, as long as you have acted in good faith and believe what you reported to be true.

Retaliation may be grounds for discipline up to and including dismissal, consistent with applicable local laws. The company will treat any good-faith reports or discussions in confidence consistent with legal requirements and subject to the need to conduct a thorough investigation where appropriate. In certain cases, and consistent with applicable laws, information may be shared with local law enforcement or other authorities.

Acknowledgement and adherence

I hereby acknowledge that I have read and understood this Policy and the provisions contained herein within and commit to the obligations established in the same.

I understand that violations of this Policy may result in disciplinary action including suspension without pay and/or discharge. I certify that this is a true and correct statement by my signature below:

SIGNATURE: _____

DATE: _____