ARBONIA

Directive on the handling of Data (Data Protection Directive)

16 June 2020

ARBONIA

TABLE OF CONTENTS

ARBONIA

1 PURPOSE AND OBJECTIVE

For the fulfilment of statutory and contractual obligations, the collection and processing of personal data is essential. In this context, the data protection regulations applicable in the respective countries must be complied with. This directive demonstrates how Arbonia AG and its group companies (hereinafter collectively referred to as "Arbonia", or if an individual group company, hereinafter referred to as "Group Company") handle personal data. The provisions laid down shall be construed as minimum standards. If local data protection laws provide for stricter regulations, these shall be complied with. Any local regulations for the implementation of this directive shall also be observed.

The purpose of this Directive on the handling of Data („**Data Protection Directive**" or "**Directive**")is to establish, implement, maintain, and continually improve compliance with data protection in accordance with the requirements of the European Union General Data Protection Regulation 2016/679 (the **GDPR**) and any other applicable local data protection laws (together the **Applicable Data Protection Law**).

Failing to comply with the Applicable Data Protection Law exposes the Arbonia Group to risks of reputation damage and heavy fines (e.g. up to 4% of the global turnover under GDPR). It may also expose our customers and employees to specific data protection risks, such as identity theft or financial loss. Compliance with the Applicable Data Protection Law will help us maintaining confidence in the Arbonia organization and ensuring successful business operations.

The objective of this Directive is to provide the framework for such data protection compliance within the Arbonia Group. In particular, it aims to implement general principles of processing Personal Data (the **Data Protection Principles**) provided for in Section 6 for which Arbonia Group companies are accountable in case they act as Data Controller under GDPR, the requirement for adequate technical and organizational measures and the Data Security Incident reporting as a minimum standard for all Arbonia companies and it applies to all employees of Arbonia as well as to the members of the Board of Directors of Arbonia AG.

Furthermore, it provides a framework for additional requirements relevant for Data Controllers and Data Processors under the GDPR (or similar Applicable Data Protection Law) described in Section 7.

2 TERMS AND DEFINITIONS

For the purpose of this Data Protection Directive the following terms and definitions apply:

Anonymized Data means personal identity that can never be traced by anyone, or if the personal identity could be recreated only with an unreasonable amount of time, expense and labor.

Applicable Data Protection Law means the European Union General Data Protection Directive Regulation 2016/679 (the **GDPR**) or any other applicable national data protection laws that have similar regulation.

Business Process Owner means a natural person being a Responsible under this Data Protection Directive and having responsibility over a Personal Data processing activity and respective IT-Application.

Consent means the consent of the Data Subject which means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

Data Security Incident means an event where there is justified suspicion that Personal Data is being illegally captured, collected, modified, copied, transmitted or used. This can pertain to actions by Third Parties or employees.

Data Subject means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.

Data Repository means a record of processing activities under the Data Controller's responsibility. That record shall contain all of the following information: (i) the name and contact details of the Data Controller and, where applicable, the joint controller, the controller's representative and the Local Data Protection Coordinator; (ii) the purposes of the Processing; (iii) a description of the categories of data subjects and of the categories of

Personal Data; (iv) the categories of recipients to whom the personal data have been or will be disclosed including recipients in Third Countries; (v) where applicable, transfers of Personal Data to a Third Country, including the identification of that Third Country and the documentation of suitable safeguards; (vi) the envisaged time limits for erasure of the different categories of Personal Data; (vii) a general description of the technical and organizational security measures.

Data Protection Officer or Data Protection Coordinator or **DPC** means the person as described in Section 5.

Personal Data means any information (including Special Categories Personal Data) relating to a Data Subject, i.e. concerning an identified or identifiable natural person, such as name, date of birth, e-mail address, religion, location information, online data (IP address, location information, etc.), identification numbers (social insurance number, ID card number, etc.), physical characteristics (gender, skin colour, hair colour, eye colour, etc.), and customer data), governed by Applicable Data Protection Regulation.

Processing or **processing** means any operation or set of operations which is performed on Personal Data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transfer, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Special Categories Personal Data means data about racial and ethnic origin, political opinions, religious or philosophical beliefs, criminal convictions, union membership, the health, sexual life of the Data Subject or genetic data, biometric data for the purposes of uniquely identifying a natural person.

Third Country means all nations not being a European Union or European Economic Area country or a country with a data protection adequacy level that is considered sufficient by the EU Commission (cf. list of adequacy level countries: https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en#dataprotectionincountriesoutsidetheeu).

Third Party means anyone other than the Data Subject, the Data Controller or the Data Processor (including, for example, business partners, sub-contractors, credit reference agencies and others), and persons who, under the direct authority of the controller or

processor, are authorized to process Personal Data. In a case of Personal Data Processing under authority the Data Processors are legally not third parties under the Data Protection Legislation, because they are assigned by law to the responsible entity.

3 SCOPE

3.1 Organizational Scope

This Data Protection Directive applies to all Arbonia Group Companies, to all employees of Arbonia as well as to the members of the Board of Directors of Arbonia AG. It is to be implemented in a legally binding manner in each Group Company.

3.2 Laws, Regulations, Standards and Guidelines

This Data Protection Directive comprises the GDPR requirements and internationally accepted data privacy principles without replacing the existing national laws. It supplements the applicable national data privacy laws. The relevant national law will take precedence in the event that it conflicts with this Data Protection Directive, or it has stricter requirements than this Data Protection Directive. The content of this Data Protection Directive must also be observed in the absence of corresponding national legislation.

If this Data Protection Directive contradicts the regulations in a specific country, the specific regulations of this Directive may be adopted in a local directive in consultation with the Head of Legal & Compliance. However, the basic content and purpose of the provision concerned must not be amended.

4 REGULATORY BASIS

This Data Protection Directive is based on the GDPR and globally accepted, basic principles on data protection.

5 ROLES AND RESPONSIBILITIES

- The Managing Director of a Group Company[1] is responsible to:
  1. ultimately ensure that the respective legal entity meets its legal obligations in relation to processing of Personal Data.

[1] In the case of Group Companies which do not conduct operational business, this responsibility shall be defined separately in consultation with the Head of Legal & Compliance.

2. ensure that the requirements in this Directive are met (including Data Security Incident notification).
3. ensure that the Data Repository is filled and maintained by the business process owner at Group Company level.
4. appointing a formal local data protection officer (internal or external) (hereinafter referred to as "Data Protection Officer") if this is required by the locally applicable data protection regulation. This appointed person must be announced to the Head of Legal & Compliance and to Internal Audit by the middle of each year.
5. appointing a local data protection manager (hereinafter referred to as "Data Protection Coordinator") if the locally applicable data protection regulation does not prescribe the appointment of a formal, Local Data Protection Officer. This appointed person must be announced to the Head of Legal & Compliance and to Internal Audit by the middle of each year.

- Local Data Protection Coordinator or Data Protection Officer ("DPC") appointed by the Managing Director of a Group Company[2] shall:
  1. monitor compliance with this Data Protection Directive and with the policies of the Data Controller or Data Processor in relation to the protection of Personal Data, including the assignment of responsibilities and the related audits
  2. inform, advise and supervise the Data Controllers, Data Processors and the employees who carry out processing duties in line with this Data Protection Directive
  3. provide advice where requested as regards to the Personal Data protection impact assessment and monitor its performance, as well as any other Personal Data issues assigned under this Directive
  4. monitor the Data Repository which is maintained by the respective Group Company and filled in by the business process owner, keep the record up to date and, on an annual basis, shall confirm to the Managing Director and Head of Legal & Compliance that the list is complete and up to date by the middle of each year.
  5. serve as the point of contact for the Head of Legal & Compliance and keep this person informed of the responsibility, risks and problems regarding the protection of Personal Data
  6. provide assistance – from a data protection perspective – to the IT department responsible for IT applications with respect to the inspection and approval of new IT applications used at Group Company level to process Personal Data as well as any IT application used to process specific categories of Personal Data
  7. approve – from a data protection perspective – the transfer of Personal Data to a third country
  8. act as the local contact point for the supervisory authority on issues relating to data processing, and cooperate with the Supervisory Authority
  9. handle requests from personnel involved in the processing of Personal Data

[2] In the case of Group Companies which do not conduct operational business, this responsibility shall be defined separately in consultation with the Head of Legal & Compliance.

10. handle requests for information from data subjects regarding the Personal Data that Arbonia has collected, respond to such requests, or if the request concerns several Arbonia Group Companies, handle this in cooperation with Corporate IT (also see 7.4 below)
11. check and approve any contracts or agreements which have been drawn up or pre-checked by the business process owner, with Data Processors that may process personal data on behalf of the Arbonia as set out in Section 7.2.
12. monitor the external Local Data Protection Officer if such an appointment has been made
13. report incidents relating to data security in accordance with the Data Breach Notification Directive (see 9 below and the "Arbonia Data Breach Policy") .

- The IT board in conjunction with Corporate IT is responsible for:
  1. defining the standards to apply across the Group and general IT controls (GITC) which are to be observed when storing data

- The respective IT department which serves a Group Company is responsible for:
  1. using relevant standards and policies and performing the general IT controls (GITC) to ensure that systems, services and equipment used for storing data meet acceptable security standards (access control / data erasure) taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons
  2. endeavoring that the Data Controller and the Data Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk as set out in Section 8.
  3. approving – from a data protection perspective – new IT-application processing Personal Data, following consultation with the Data Protection Coordinator or Data Protection Officer.
  4. performing regular checks and scans to ensure that security hardware and software is functioning properly. The results of the data protection controls must be to the Data Protection Coordinator or Data Protection Officer
  5. evaluating data security of any third-party services (e.g. Data Processors) the company is considering using to process Personal Data (For example, cloud computing services)
  6. running a list of Data Security Incidents and and reporting incidents relating to data security to Corporate IT
  7. coordinating and responding to requests for information from data subjects regarding Personal Data that the Arbonia Group Company served by the respective IT department has collected about the data subjects (also see 7.4 below).
  8. reporting identified incidents or risks relating to data security in accordance with the Data Breach Notification Directive (see 9 below and the "Arbonia Data Breach Policy")

- Corporate IT in cooperation with the IT department responsible for serving a Group Company is responsible for:
  1. carrying out regular inspections and scans to ensure that the security hardware and software is functioning correctly. The results of the data protection inspections must be reported to the relevant Data Protection Officer.
  2. maintaining a central list of incidents relating to data security.
  3. reporting identified incidents or risks relating to data security in accordance with the Data Breach Notification Directive (see 9 below and the "Arbonia Data Breach Policy").

- Internal Audit is responsible for:
  1. when conducting audits in accordance with the regular audit planning, to verify on a risk-based approach that the organisational procedures comply with the essential requirements set out in this data protection directive

- The business process owner is responsible for:
  1. ensuring that the Local Data Protection Officer is consulted in an appropriate and timely manner on all matters necessary to assess the processing of Personal Data.
  2. drawing up or pre-checking all contracts or agreements intended for processors who may be tasked with processing Personal Data on behalf of Arbonia, as defined in section 7.2.
  3. filling in the Data Repository which is maintained by the respective Group Company, keeping the record up to date and, by the end of April each year, sending confirmation to the Data Protection Coordinator or Data Protection Officer that the entries are complete and up to date.
  4. assessing the risks of new processing activities for Personal Data as regards the personality and the fundamental rights of the data subject before the new activities are implemented, and – if the risk of processing is likely to be high – performing a data protection impact assessment in advance

6 DATA PROTECTION PRINCIPLES FOR PROCESSING PERSONAL DATA

Every Group Company acting as a Data Controller processing Personal Data has to ensure that it can demonstrate compliance with the following **6 (six) essential Data Protection Principles**:

1. Only process Personal Data if you can demonstrate a valid Legal Ground according to Applicable Data Protection Laws and inform the Data Subject of the identity and the contact details of the Data Controller, the kind and Legal Grounds of personal data you collect, the respective storage period and the purpose for which you are collecting Personal Data.

2. Always adhere to the purpose the Personal Data was collected for.

3. Only collect/process Personal Data that you really need.
4. Keep Personal Data correct and delete inaccurate Personal Data.
5. Keep Personal Data only for the legal retention periods you really need.
6. Keep Personal Data confidential and only share what you really need to share.

6.1 Fairness, Lawfulness and Transparency

Personal Data may only be processed for purposes specifically permitted as described below, and this must be done in a transparent way. Hence, Personal Data must be processed in a legal and fair manner and observe the individual rights of the Data Subjects. This may include Personal Data Arbonia receives directly from a Data Subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise), and Personal Data Arbonia receives from Third Parties.

Under Applicable Data Protection Laws, Personal Data can be processed lawfully with of one of the **5 (five) legal grounds** (the **Legal Grounds**) set out in the GDPR. These grounds include:

1. **Contract**: Processing Personal Data is necessary for the performance of a contract with the Data Subject or in order to take steps at the request of the Data Subject prior to entering into a contract, or
2. **Consent**: Processing Personal Data is based on Consent (opt-in model) by Data Subject for one or more specific purposes. The granting of Consent must be documented, or
3. **Legal Obligation**: Processing Personal Data is based on a legal obligation applying to Arbonia. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions, or
4. **Public Interest**: Processing is necessary for the performance of a task carried out in the public interest, or
5. **Legitimate Business Interest**: Processing is proportionate for a legitimate business interests pursued by Arbonia or the Third Party to whom the Personal Data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject. Legitimate interests are generally of a legal (e.g. collection of outstanding receivables / by collective agreement of works council / asserting, exercising or defending legal claims regarding the Data Subject) or commercial nature (e.g. avoiding breaches of contract).

Transparency requests that the Data Subject must be informed of how his/her Personal Data is being handled. In general, it is therefore recommended to collect Personal Data directly from the Data Subject (and not through a Third Party). When the Personal Data is processed the Data Subject must be informed of:

- the identity and the contact details of the Data Controller and, where applicable, of the controller's representative in the EU
- the contact details of the Data Protection Officer or Data Protection Coordinator, where applicable;
- the purpose of Personal Data Processing as well as the legal basis for the processing , and
- Third Parties recipients or categories of Third Parties to whom the data might be transmitted.
- If applicable, a Third Country processing information and reference to the appropriate safeguards.

6.2 Purpose Limitation

Personal Data can be processed only for the purpose that was communicated to the Data Subject before the Personal Data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation. The Data Controller must notify the Data Subject about the purpose for which Arbonia processes his/her Personal Data when Arbonia first collects the Personal Data, or as soon as possible thereafter. In any processing for advertising purposes or marketing programs, the Data Subject must be given and explicitly be informed about his/her right to object from processing its Personal Data. Insofar, each Data Controller shall implement a complaints handling that ensure that opt-outs are respected.

6.3 Data Minimization

Only process the Personal Data that you really need. Before processing Personal Data, you must determine whether and to what extent the processing of Personal Data is necessary in order to achieve the purpose for which it is undertaken. Personal Data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.

6.4 Accurate and Kept Up to Date

Personal Data must be correct, complete, and – if changes occur – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete Personal Data are deleted, corrected, supplemented or updated. It is the responsibility of all who work with Personal Data to take respective reasonable steps (for example, by confirming a Data Subject's details if they call, or by removing a stored telephone number from the database where it is no longer used by a Data Subject).

6.5 Limited Storage Time

Only keep Personal Data for the retention periods you really need. Personal Data must be deleted after as soon as it is no longer necessary for the intended purposes or the consent is revoked or objected to a use based on legitimate interest and Arbonia company has no overriding legitimate grounds. In some cases, longer retention periods may permit to hold Personal Data because we are required by law (e.g. under tax and commercial law), or Personal Data are required for the establishment, exercise or defense of legal claims.

6.6 Confidentiality and Data Security

Keep Personal Data confidential at all times and only share what you really need to share. The "need to know" principle applies, meaning employees and Third Parties may only have access to Personal Data if and to the extent required for the performance of the purpose. This requires a careful concept that details specific access rights for each business process, including the implementation and approval of roles and responsibilities (access rights concept). Recipients of Personal Data must be informed of the confidentiality of the Personal Data **and be subject to a non-disclosure agreement / confidentiality agreement** (which can be part of an employment agreement or the like). Exception: Recipient is under professional respectively legal confidentiality obligation.

Personal Data must be secured with suitable organizational and technical measures to prevent unauthorized access, unlawful processing or disclosure, as well as accidental loss, modification or destruction (cf. Section 8).

7 ADDITIONAL OBLIGATIONS UNDER GDPR OR OTHER SIMILAR APPLICABLE DATA PROTECTION REGULATION

7.1 Accountability Principle

An Arbonia Group Company subject to the GDPR (or similar Applicable Data Protection Regulation) has to ensure that it can demonstrate compliance with Applicable Data Protection Law (so-called "Accountability" principle). Accordingly, these Group Companies must – in addition to the general requirements established in this Data Protection Directive – implement and maintain the following points, with the Managing Director of the respective Group Company ultimately responsible for ensuring their implementation and maintenance:

1. Local Data Protection Coordinator or Local Data Protection Officer: Appointment of a dedicated Local Data Protection Coordinator or Local Data Protection Officer

2. Maintain the Data Repository: an inventory on the processing activities regarding Personal Data is to be maintained and kept up to date

3. Legitimation check: Lawful processing of Personal Data in compliance with valid Legal Grounds must be checked, especially when processing Special Categories Personal Data

4. Control Data Processor: Conclude data processing agreement with Data Processors or as Data Processor when delivering or receiving Personal Data under authority according to Art. 28 GDPR.

5. In case of Joint Controllers provide for a Joint Controller Agreement in accordance to Art. 26 GDPR.

6. Employees of Arbonia shall be informed about the Personal Data Processing activity.

7.2 Rules for Data Processors (especially Service Partners)

The Data Controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that Personal Data processing will meet the requirements of Article 28 GDPR and ensures the protection of the rights of the Data Subject.

For shared services within Arbonia , an agreement is in place which allows Personal Data to be transferred provided that there are legitimate legal grounds for transferring this Personal Data in accordance with the applicable data protection legislation.

7.2.1 Providing Personal Data to Data Processor (Outbound)

Personal Data processing under authority means that a provider is hired to process Personal Data without being assigned responsibility for the related business process (i.e. service providers, outsourced services). In such an event a data processing contract for processing Personal Data under authority must be concluded with external providers. The respective Arbonia Group Company is the Data Controller and retains full responsibility for correct performance of Personal Data processing by the Data Processor.

The respective Business Process Owner must ensure that the current model data processing agreement is used to contract such service providers or an equivalent similar contract provided by the service provider to meet Article 28 GDPR requirements. Alternatively, a service provider may document its compliance with data security requirements by presenting suitable and approved EU certification. Any deviation from such security standard must be approved by the Data Protection Officer or Data Protection Coordinator in cooperation with Corporate IT. Existing contracts must be reworked and include a data processing contract in writing within one year since enacting this Data Protection Directive.

7.2.2 Receiving Personal Data as Data Processor (Inbound)

If Personal Data is transferred by a Third Party to a Arbonia Group Company, it must be ensured that the Personal Data (i) can be used for the intended purpose, (ii) was collected with lawful grounds (it recommended to ask for a written confirmation), and (iii) a data processing contract sufficient to Article 28 GDPR is in place.

7.3 Cross-Border Transfer of Personal Data

In the event of cross-border transfer of Personal Data, the relevant national requirements for disclosing Personal Data abroad must be met. Under GDPR, a transfer of Personal Data may take place within the EU, the EEA or to a country where the European Commission has decided that such a country meets appropriate safeguards that ensures an adequate level of protection. Such a transfer shall not require any specific authorization. The European Commission has so far recognized i.a. Switzerland as providing adequate protection (cf. current list of countries: < https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >).

A transfer of Personal Data to a Third Country it is only allowed subject to additional appropriate safeguards, meaning if the recipient can prove that it has a data protection standard equivalent to this Data Protection Directive (e.g. i) binding corporate rules, ii) EU standard contract clauses for contract data processing in third countries with the provider and any subcontractors[3], iii) approved code of conduct by supervisory authority, iv) participation of the provider in a certification system accredited by the EU for the provision of a sufficient data protection level or v) individual agreements between data controller and data processor subject to the authorization from the competent supervisory authority) and information of the data subject. This obligation does not apply if transfer is based on a legal obligation. Any such transfer needs approval by the Data Protection Officer or Data Protection Coordinator.

If Personal Data are transferred within Arbonia , the Group Company importing the Personal Data is obligated to cooperate with any inquiries made by the relevant supervisory authority in the country in which the exporting Group Company has its registered office, and to comply with any observations made by the respective supervisory authority with regard to the processing of the transmitted Personal Data.

7.4 Dealing with Information Request by Data Subject

Data Subjects are entitled to make a formal information request for details of the Personal Data held by Arbonia and may request the following:

[3] See Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0087 >

Right of access:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling
- where personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards.

Right of rectification:

- The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure ('right to be forgotten')

- The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
2. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) GDPR, or point (a) of Article 9(2) GDPR, and where there is no other legal ground for the processing;
3. the data subject objects to the processing pursuant to Article 21(1) GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) GDPR;
4. the personal data have been unlawfully processed;
5. the personal data have to be erased for compliance with a legal obligation Applicable Data Protection Law to which the controller is subject;

6. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) GDPR.

Right to restriction of processing:

- The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;
- the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

The Data Subject should be asked to make its request in writing, either via email or by post and addressed to the respective Local Data Protection Officer. Information shall be provided by the Local Data Protection Officer to the Data Subject without undue delay but in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Data Protection Officer or Data Protection Coordinator of the Data Controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. The Data Subject cannot be charged for its request to access the information a Group Company holds about him/her, unless where requests from a Data Subject are manifestly unfounded or excessive, in particular because of their repetitive character. Request of a Data Subject concerning several Arbonia Group Companies have to be passed on to Corporate IT for coordination and a reply.

7.5 Carrying out a data protection impact assessment

Where a planned new type of processing for Personal Data – in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing – is likely to result in a high risk to the rights and freedoms of the natural person, an assessment of the impact of the envisaged processing activities on the protection of Personal Data is to be carried out prior to the processing.

Before implementing new processing activities, the resulting risks to the personality and the fundamental rights of the data subject are therefore to be assessed. In the case of new IT applications, this is to be taken into account as part of the approval procedure. If an initial assessment concludes that a planned new type of processing for Personal Data is likely to result in a high risk to the data subject, a data protection impact assessment is to be carried out.

Queries regarding the need for a data protection impact assessment or queries which arise while an impact assessment is being carried out are to be directed to the Local Data Protection Coordinator or Local Data Protection Officer. Once the data protection impact assessment has been carried out, this is to be communicated to the Local Data Protection Coordinator or Local Data Protection Officer, and an opinion is to be sought from the Local Data Protection Coordinator or Local Data Protection Officer.

If a data protection impact assessment indicates that the processing would result in a high risk to the data subject and no actions are taken to mitigate the risk, the Supervisory Authority is to be consulted before the new processing activities are implemented.

8 SECURITY OF PERSONAL DATA

Personal Data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether Personal Data is processed electronically or in paper form.
Data Controllers and Data Processors need to implement appropriate technical and organizational measures to protect data against unlawful processing. These measures must be based on (i) best practice, (ii) the risks of processing, and (iii) the need to protect the Personal Data (determined by the process for information classification), including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The technical and organizational measures for protecting Personal Data are part of the Corporate Information Security Management and must be adjusted continuously to the technical developments and organizational changes.

Security procedures may in minimum include:

- Entry controls: Any stranger seen in entry-controlled areas should be reported.

- Secure lockable drawers or filing cabinets: Desks and cupboards should be kept locked if they hold confidential information of any kind. Personal Data is always

confidential information. Employees should make sure paper and printouts containing Personal Data are not left in in general sight, like on a printer. If Personal Data is stored with authorisation on removable media (like a CD, memory stick or DVD), these must be kept locked away securely when not being used.

- Methods of disposal: Paper documents should be shredded and disposed of securely when no longer required. This also applies to Personal Data that is usually stored electronically but has been printed out.

- Data stored electronically: Personal Data should be password-protected in accordance with the current password policy and should never be shared among employees. Where applicable with respect to electronic data, Personal Data must be stored and retrieved on IT server systems and in structured IT applications rather than unencrypted on local computers.

- Electronically collected Personal Data given by the Data Subject: The identity of the Data Subject shall be verified preferably by a double-opt-in process (meaning second mail with validation of provided email address). In the event website or app access is restricted to registered users (i.e. user account), the identification and authentication of the data subject must offer a security protection proportionate to the respective content during access.

- Exercising caution when sharing Personal Data: Personal Data should not be shared informally. The "need to know" principle applies. A concept of breakdown and separation for each business process, as well as implementation, of roles and responsibilities is mandatory. Personal Data must be encrypted before being transferred electronically. The information technology manager can explain how to send Personal Data to authorized external contacts.

- Seeking guidance: In the case of questions or doubt regarding an aspect of data protection or regarding obligations arising from this Data Protection Directive, advice is to be sought from a line manager, from the respective Local Data Protection Officer or from Legal & Compliance.

The GDPR requires to consider privacy at the earliest stage. Privacy by design holds that organizations need to consider privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing personal data. Privacy by default means that when a system or service includes choices for the individual on how much personal data he/she shares with others, the default settings should be the most privacy friendly ones. Accordingly, any new IT application is subject to an internal approval procedure in which the new IT application is to be assessed, including in relation to data protection legislation

9 DATA SECURITY INCIDENT REPORTING

Many Applicable Data Protection Regulations ask for an immediate notification of Data Security Incidents to the regulator. Hence, all incidents relating to data security must be immediately reported to the relevant Data Protection Coordinator or Data Protection Officer, irrespective of whether a local system or a Group system is concerned, in accordance with the procedure described in the Arbonia policy relating to Data Security Incidents ("Data Breach Policy"). If the IT department identifies incidents or risks relating to data security, these must be reported in accordance with the Data Breach Policy.

The goal is to preserve applicable data security breach notification obligations according to Applicable Data Protection Law (e.g. under GDPR at the latest within 72 hours after becoming aware of it).

In such an event the emphasis must be to meet any applicable data security breach notification deadlines and prompt action to investigate an incident to determine whether personal data have indeed been breached. Corporate IT must hold a Arbonia Group internal security breach register so that any reporting duties under national law can be complied with and ensure respective deputy rules are enacted to comply with breach notice at all times. Corporate IT or the Group's Legal and Compliance department are to be informed about any breaches before they are reported to a national authority.

Any additional instructions issued by Corporate IT and the local IT departments must be strictly observed.

10 CONSEQUENCES IN CASE OF NON-COMPLIANCE

Compliance with this Directive is of utmost importance to Arbonia Group and the public perception of Arbonia Group. Improper processing of Personal Data, or other violations of the data protection laws, may also be criminally prosecuted in many countries and result in claims for compensation of damage. Within Arbonia, a violation of the rules set forth in this Directive may result in sanctions pursuant to the law and/or the relevant (employment) contract.

11 EXCEPTIONS

Deviations from the provisions of this directive and the supplements are permissible only after approval of the Head of Legal & Compliance.

ARBONIA

12 INFORMATION

Information in connection with the data protection directive shall be obtained from the Head of Legal & Compliance.

13 EFFECTIVE DATE

This directive comes into force as from 17 June 2020 and replaces the directive on the handling of data (data protection directive) of 5 December 2013.

Arbon, 16 June 2020

Arbonia AG

Alexander von Witzleben
Chairman of the Board of Directors / CEO

Andrea Wickart
Head of Legal & Compliance / General Secretary

Supplements to this Arbonia Data Protection Directive

The following supplements in their most current version further substantiate this Data Protection Directive:

- - Data Subject Request and Deletion Policy
- - Data Breach Policy
- - Data Privacy Statement for Employees

This document is valid without a signature.