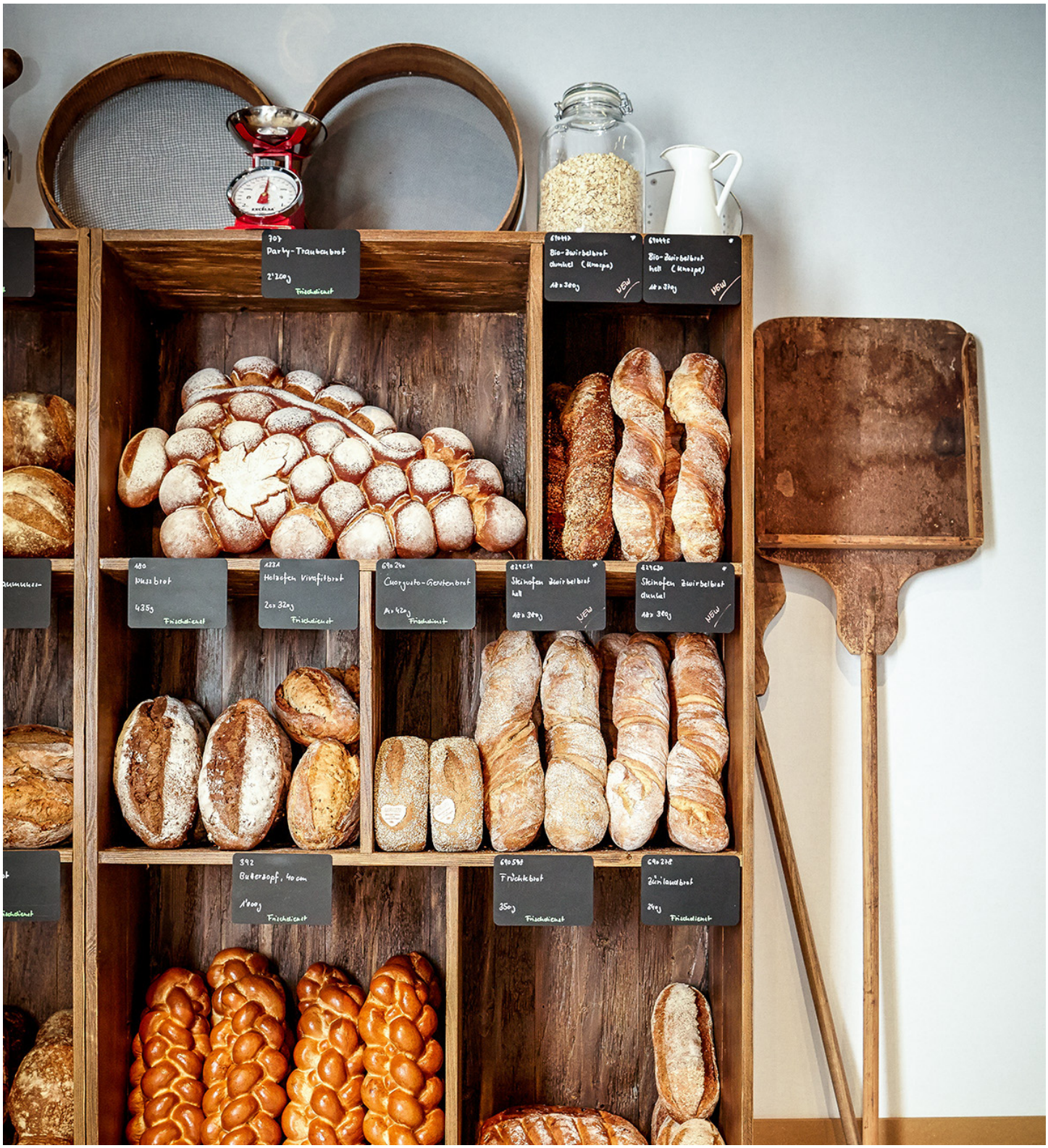
DECEMBER 2023

ARYZTA
SERVING INSPIRATION

DATA PROTECTION POLICY FOR GROUP COMPANIES



Policy Owner:	The Data Privacy Steering Committee
Contact:	dataprivacy@aryzta.com
Policy became operational on:	19/09/2019
Date last reviewed:	[•]
Related Documents:	• Retention & Deletion Policy • Personal Data Breach Procedure

CONTENTS

1. WHAT IS THE PURPOSE OF THIS POLICY?

This Data Protection Policy (the "**Policy**") sets out how ARYZTA AG and its affiliates and subsidiaries (going forward "**ARYZTA**", "**we**" or the "**Company**") protect Personal Data.

It is a set of principles, rules and guidelines all Employees must follow to ensure group-wide minimum standard to protect Personal Data. Data protection compliance is an important basis for trusting relationships with business partners and customers, for protecting ARYZTA's reputation and for the protection of ARYZTA and its Employees from legal risks (including fines, civil claims and investigations).

This Policy builds on the requirements defined in Swiss and EU data protection laws, i.e., the Swiss Federal Act on Data Protection ("**FADP**") and the EU General Data Protection Regulation ("**GDPR**"), that ARYZTA adheres to as a group-wide minimum standard.

In addition to this Policy, all ARYZTA group entities are required to comply with all applicable local data protection laws when Processing Personal Data. ARYZTA group entities must define and communicate to their Employees any requirements that are applicable to their Processing of Personal Data in addition to or deviating from those set forth in this Policy, it being understood that deviations from this Policy shall require a specific basis in applicable local law.

Defined terms in this Policy shall have the meaning defined in the respective section in which they are written in **bold**. Please also refer to the glossary at the end of this Policy (Appendix 1).

2. WHO DOES THIS POLICY APPLY TO?

This Policy applies to all ARYZTA employees, consultants, interns, temporary workers, independent contractors and agency workers who have access to Company Data (together referred to as "**Employees**" or "**you**").

In case of conflict between this Policy and a separate agreement concluded between ARYZTA and an Employee, the stricter regulation shall apply unless the respective agreement expressly states otherwise.

3. WHAT IS THE SCOPE OF THIS POLICY?

This Policy applies to all Personal Data Processing activities undertaken in the course or for the purpose of ARYZTA's business activities by ARYZTA and its Employees, irrespective where such Personal Data is stored (e.g. on an Employee's own device).

In addition to this Policy, all other ARYZTA policies, instructions and regulations shall apply, including those that also address data protection and privacy.

Any additional local legal or regulatory requirements of individual group companies shall apply in addition to this Policy.

4. RESPONSIBILITIES

4.1. Data Privacy Steering Committee

The Company's point of contact on data protection matters is the Data Privacy Steering Committee ("**DPC**"), who can be contacted at dataprivacy@aryzta.com.

The DPC shall:

a) advise the Company and its Employees of their obligations under the applicable data protection law;
b) monitor compliance with the applicable data protection law, the Company's policies with respect to data protection, and monitoring training and audit activities relating to data protection compliance;
c) provide advice where requested on data protection impact assessments;
d) cooperate with and act as the contact point for the local data protection authorities (if no data protection officer was appointed).

The DPC shall in the performance of their tasks have due regard to the risk associated with Processing operations, taking into account the nature, scope, context and purposes of Processing.

4.2. Managing Directors and Heads of Business Services

All Managing Directors and Heads of Business Services are responsible for ensuring that all Employees within their area of responsibility comply with this Policy, and for implementing appropriate local guidelines, practices, processes, controls and training to ensure that compliance.

4.3. Business Owners

In day-to-day business operations, the respective Business Owners oversee the specific Processing activities in their responsibility and ensure for such Processing activities that Personal Data is Processed in line with applicable data protection laws and in accordance to the internal guidelines, including this Policy. If the Business Owner is in doubt as to the compliance of any Personal Data Processing activity with this Policy and applicable data protection law, the Business Owner shall seek the advice of the DPC.

4.4. Employees

Employees who Process Personal Data in the scope of ARYZTA's business activities must comply with this Policy and any additional local requirements. Employees must immediately report a possible breach of this Policy to the respective Business Owner or, if appropriate, to the DPC.

As Data Subjects, Employees are responsible for:

a) taking note of the current version of the ARYZTA Workplace Privacy Notice;
b) ensuring that Personal Data about them provided to the Company is accurate and up to date.

5. ACCOUNTABILITY

The Company must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Company is responsible for and must be able to demonstrate compliance with applicable data protection law.

Managing Directors, Heads of Business Services and Business Owners must therefore apply adequate resources and controls to ensure and to document compliance with applicable data protection law and this Policy.

If Data Subjects' Consent is obtained, Business Owners must ensure that they have evidence of Consent and keep record of all Consents obtained.

6. DATA PROTECTION PRINCIPLES

When Processing Personal Data, Employees need to comply with the principles set forth below. Deviations from these principles may be possible in individual cases provided that the Business Owner determines that such deviation is in line with applicable local data protection laws.

6.1. Lawfulness

ARYZTA may collect and Process Personal Data only in accordance with applicable law. Whenever possible, we avoid Processing Special Category Personal Data and Disclosing such data to Third Parties. If this is necessary in individual cases, the Business Owner has to check whether and under what conditions this is permissible under applicable law. The Business Owner should consult the DPC for guidance before making the decision.

If the FADP or GDPR is applicable, the Business Owner must additionally ensure that we have a reasonable legal basis to Process Personal Data:

1. The Data Subject has given his or her Consent after adequate information. However, as Data Subjects may withdraw their Consent at any time and it may be difficult to prove that Consent was validly obtained in the specific case, Business Owners should use other legal bases for the Processing of Personal Data if possible;
2. The Processing is necessary for the performance of a contract with the Data Subject;
3. To meet our legal compliance obligations;
4. To protect the Data Subject's vital interests (i.e. matters of life or death);
5. To pursue our legitimate interests or legitimate interests of a third party, which are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The specific legitimate interest or interests that the Company is pursuing when Processing Personal Data will need to be set out in the relevant Privacy Notices.

6.2. Proportionality

Personal Data must be adequate and limited to only what is necessary for achieving the stated purpose. You should therefore not collect Personal Data that is not relevant for the stated purpose. Conversely, Personal Data must be adequate to ensure that we can fulfill the purposes for which it was intended to be Processed. Further, Business Owners may only grant access to Personal Data to those Employees that need it to fulfill their duties in the course of their employment with ARYZTA.

You have to avoid Processing Personal Data that is not needed. We do not collect or Process Personal Data for non-specific or non-current purposes. Where a legitimate purpose can be achieved without or with less extensive Processing of Personal Data, you have to refrain from Processing Personal Data to the extent not required.

When Personal Data is no longer needed for the specified purposes and we do not need to legitimately retain it (e.g., to comply with legal retention obligations or for reasons of litigation), you should ensure that it is safely deleted in accordance with the Company's Retention & Deletion Policy. Alternatively, the reference to a Data Subject may be removed through anonymisation if we wish to continue using the data but the personal reference is no longer needed, e.g. for statistical purposes.

6.3. Transparency and Good Faith

We have to ensure that Processing of Personal Data is transparent for the Data Subject. We act in good faith in connection with the Processing of Personal Data and avoid surprising Processing activities that the Data Subjects could not reasonably expect or that could cause them harm.

We must provide specific information to Data Subjects about the Processing of their Personal Data. Such information will usually be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand what happens to their Personal Data. The information has to include, in particular:

- Name and contact details of the Data Controller;
- Categories of Personal Data collected;
- Purposes of Processing;
- Sources from which we obtain Personal Data if it is not collected directly from the Data Subject;
- Legal basis of Processing (to the extent required);
- Categories of recipients we may disclose Personal Data to;
- Countries to which we may disclose Personal Data to and how an appropriate level of data protection is ensured;
- How long we retain the Personal Data or the criteria used to determine this period;
- Whether we use Personal Data for the purpose of automated individual decisions;
- Data Subject rights.

We communicate this information through Privacy Notices. The current Privacy Notices and templates are available from the DPC.

Before Processing Personal Data, Business Owners have to ensure that the Processing activity is included in the relevant Privacy Notice provided to the Data Subject. If not, Business Owners have to ensure by other means that the above information is provided to the Data Subject in a reasonable manner, unless waiving this information is permitted in an individual case by applicable law, e.g. if the Data Subject already has the relevant information or the Processing of the Personal Data is provided for by applicable law.

If Personal Data is collected from Third Parties, Business Owners take appropriate measures to ensure that these Third Parties have fulfilled these or comparable information obligations. Business Owners will ensure that the above information is provided to the Data Subject within one month after ARYZTA has obtained the Personal Data, unless such information proves impossible or would involve a disproportionate effort.

6.4. Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be subsequently Processed in a way that is different or incompatible with those purposes. You may only Process Personal Data to the extent performing your job duties requires it, but not for other purposes.

Subsequent changes to the purpose of Processing may be permitted in limited cases under the applicable law, for example, if the Data Subjects have given their consent or the change of purpose is required for reasons of applicable law. Therefore, if you wish to Process Personal Data for a purpose that is not compatible with the original purpose, the Business Owner needs to consult the DPC.

To assess whether the intended purpose is compatible with the original purpose, the Business Owner must take into account factors such as:

1. The link between the original purpose/s for which the Personal Data was collected and the intended further Processing;
2. The context in which the Personal Data has been collected – in particular the Company-Data Subject relationship. You should ask yourself if the Data Subjects would reasonably anticipate the further Processing of their Personal Data;
3. The nature of the Personal Data, in particular whether it involves Special Category Personal Data;
4. The consequences of the intended further Processing for the Data Subjects.

In case of doubt, the Business Owner has to consult the DPC.

6.5. Accuracy

Personal Data must be accurate for the purpose of the Processing and, where necessary, kept up to date. You should ensure that Personal Data is recorded in the correct files and implement adequate measures to ensure accuracy of the Personal Data Processed.

Incomplete records can lead to inaccurate conclusions being drawn and in particular, where there is such a risk, you should ensure that relevant records are completed.

You must take all reasonable steps to destroy or amend inaccurate records promptly and update out-of-date Personal Data where necessary.

6.6. Security, Integrity and Confidentiality

ARYZTA is required to implement and maintain appropriate safeguards to protect Personal Data from unauthorised or unlawful Processing or accidental loss, destruction or damage, taking into account in particular the risks presented to Data Subjects.

Appropriate safeguards include the use of encryption and pseudonymisation where appropriate. It also includes protecting the confidentiality (i.e. that only those who need to know and are authorised to use Personal Data have access to it), integrity and availability of the Personal Data. Managing Directors and Heads of Business Services shall ensure that the effectiveness of those safeguards to ensure security of our Processing of Personal Data are regularly evaluated, tested and where necessary improved.

You are also responsible for protecting the Personal Data that you Process in the course of your duties. You must therefore handle Personal Data in a way that guards against accidental loss or disclosure or other unintended or unlawful Processing and in a way that maintains its confidentiality. You must exercise particular care in protecting Special Category Personal Data. To that end, you must comply with all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction, in particular with all applicable aspects of relevant policies of ARYZTA. You must not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance to protect Personal Data.

7. REGISTER OF PROCESSING ACTIVITIES

To the extent required by law, the individual ARYZTA group companies keep full and accurate registers of their Processing activities.

These registers shall include, in particular, the name and contact details of the Company, the name and contact details of the Data Protection Officer (if required), clear description of the categories of Personal Data, categories of Data Subjects, Processing activities, Processing purposes, third-party recipients of the Personal Data, the countries to which Personal Data is disclosed and the guarantees to safeguard such disclosure, the retention period or the criteria to determine the retention period, and a description of the security measures in place.

The Managing Directors and Heads of Business Services shall ensure that the registers are maintained, up to date and accurate, and that copies are provided to the DPC. They may delegate this task to responsible Employees. In case of changes to existing Processing activities or in case of new Processing activities, the Business Owners shall inform the relevant Managing Directors and Heads of Business Services resp. the Employees responsible for keeping the register and provide all necessary information.

8. DATA PRIVACY BY DESIGN AND BY DEFAULT

We are required to implement privacy-by-design measures when Processing Personal Data, to ensure compliance with data-protection principles. The Business Owners must therefore ensure that by default data protection compliance is built into any project, process or system that results in the Processing of Personal Data and that only Personal Data which is necessary for each specific purpose is Processed. The obligation applies, in particular, to the volume of Personal Data collected, the extent of the Processing, the period of storage and the accessibility of the Personal Data.

9. DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

The Company must carry out DPIAs in respect of high-risk Processing before that Processing is undertaken.

Business Owners have to conduct a DPIA and report such DPIA to the DPC in the following cases:

a) The use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes) that are likely to result in a high risk to the rights and freedoms of Data Subjects;
b) Automated Processing including Profiling;
c) Large scale Processing of Special Category Personal Data;
d) Large scale, systematic monitoring of a publicly accessible area (e.g. CCTV monitoring of a public footpath).

A DPIA must include:

a) A description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
b) An assessment of the necessity and proportionality of the Processing in relation to its purpose;
c) An assessment of the risk to Data Subjects;
d) The risk-mitigation measures in place and demonstration of compliance.

Business Owners must review the DPIA at least every 3 years or immediately if:

a) The Processing activity changes materially; or
b) New risks associated with the Processing activity become know.

The Business Owners must report the review of a DPIA to the DPC.

10. AUTOMATED DECISION MAKING

As a matter of principle, ARYZTA does not subject Data Subjects to decisions based exclusively on automated processes if these decisions may have legal or negative effects on the Data Subject. Exceptions must be discussed with the DPC and approved by the relevant Business Owner.

If we rely on automated decisions, we provide safeguards to protect the Data Subject's legitimate interests, including by informing the Data Subject about the automated decision in a Privacy Notice, by giving the Data Subject the opportunity in each case to express his or her point of view and to challenge the decision before a human being.

11. TRAINING AND AUDIT

We are required to ensure that all Employees undergo sufficient training to enable them to comply with data protection law. You must undergo all mandatory data privacy related training. This training and other learning resources are available online – contact the DPC on dataprivacy@aryzta.com for detailed information about the training available.

Business Owners must regularly review all the systems and processes under their control to ensure compliance with this Policy.

12. DATA PROTECTION OFFICER

To the extent required by applicable local law, the individual ARYZTA group companies will each appoint a Data Protection Officer who shall in particular be responsible for the following tasks and functions:

- Contact for the Data Subjects and for authorities;
- Training and advising Employees on data protection issues;
- Participation in the application of data protection regulations.

Otherwise, the DPC acts as contact for internal and external inquiries in the area of data protection.

13. REPORTING A PERSONAL DATA BREACH

Under the applicable law, we may be required to report to the relevant Data Protection Authority any Personal Data Breach where there is a risk or, as the case may be, a high risk to the rights and freedoms of the Data Subject. In certain cases, in particular if it is necessary for their protection, we may have to notify the Data Subjects of a Personal Data Breach.

We have put in place procedures to deal with any suspected or occurred Personal Data Breach and will notify Data Subjects or the appropriate Data Protection Authority where we are legally required to do so.

If you know or suspect that a Personal Data breach has occurred, you should immediately inform your manager / Head of function and the DPC, and follow the instructions in the ARYZTA Personal Data Breach Procedure.

The Head of Department / Business Unit / Region in which the Personal Data Breach occurred must ensure that all evidence relating to Personal Data breaches is retained in particular to enable the Company to maintain a record of such breaches, as required under applicable data protection law, including

1. The facts surrounding the breach;
2. Its effects;
3. The remedial action taken.

14. DISCLOSING PERSONAL DATA TO THIRD PARTIES

14.1. General Remarks

Personal Data must not be disclosed to any Third Party unless appropriate contractual arrangements have been put in place or the Disclosure is otherwise permitted under applicable data protection laws.

Therefore, before the Disclosure of any Personal Data to a Third Party, the Business Owner needs

- to determine whether such Third Party will have the role of a Data Controller or a Data Processor, and
- to ensure that the appropriate contractual arrangements are in place or the Disclosure is otherwise permitted under applicable data protection laws.

14.2. Third-Party Data Processors

Where the Processing of Personal Data is delegated to a Third Party as a Data Processor on behalf of ARYZTA, the responsibility for the security and appropriate use of that data remains with ARYZTA.

A third-party Data Processor may be engaged only if the following requirements are met:

a) The delegation of the Processing to the Data Processor does not breach a contractual or statutory obligation of confidentiality of ARYZTA.
b) The Data Processor Processes the disclosed Personal Data only as permitted to ARYZTA and according to ARYZTA's instructions;
c) The Data Processor must provide sufficient guarantees about its security measures to protect the Processing of Personal Data. Business Owners overseeing arrangements with third-party Data Processors should request that the Data Processor complete the ARYZTA Data Processor Due Diligence Questionnaire. If the Data Processor does not have satisfactory security measures in place, ARYZTA should not share Personal Data with that Data Processor until such measures are put in place;
d) A written contract establishing must be entered into;
e) A data processing agreement, available from the DPC, must be signed by the relevant ARYZTA group company and the Data Processor. In particular, such agreement needs to set out at least
    i. That the Data Processor will Process the Personal Data only according to ARYZTA's instructions;
    ii. Which categories of Personal Data will be Processed and for which purposes;
    iii. That any Personal Data collected or Processed in the course of work undertaken for the Company is kept securely and confidentially;
    iv. A minimum standard of technical and organisational measures implemented and maintain to protect Personal Data;
    v. That all Personal Data is returned to the Company upon completion of the work, including any copies that may have been made, or, alternatively, the Personal Data is securely destroyed and the Company receives notification in this regard from the Data Processor;
    vi. That the Company receives prior notification of any Disclosure of Personal Data to any other organisation or any person who is not a direct employee of the contractor;
    vii. Any Personal Data made available by the Company, or collected in the course of the work, is not Disclosed outside the EU, EEA or Switzerland without prior written consent from the Company.

If at some point the Data Processor cannot ensure the required security of Personal Data or does not comply with ARYZTA's instructions with respect to the delegated Processing activities, the cooperation with the Data Processor may have to be terminated. In this case, the DPC must be contacted immediately.

For further guidance about the use of Data Processors, please contact the Data Privacy Steering Committee.

14.3. Third-Party Data Controllers

If the Third Party is considered a Data Controller, a case-by-case assessment is required to determine the appropriate measures that need to be implemented to ensure compliance with the applicable data protection laws.

Personal Data that is not publicly known must be kept confidential. Instructions from ARYZTA resp. the responsible Managing Directors and Heads of Business Services in this respect have to be complied with.

15. LIMITATIONS ON THE DISCLOSURE OF PERSONAL DATA ABROAD

The GDPR and the FADP restrict the Disclosure of Personal Data to countries outside the EU, the EEA or Switzerland in order to ensure that the level of data protection afforded to Data Subjects is not undermined.

You may only Disclose Personal Data to recipients outside the EU, the EEA or Switzerland if one of the following conditions applies:

1. The European Commission or the Swiss Federal Council has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms. Please contact the DPC for guidance;
2. Appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism. Please contact the DPC for guidance;
3. The Disclosure is from the EEA to an organisation located in the U.S. that is certified under the "EU-U.S. Data Privacy Framework", a framework approved by the European Commission for Transfers of Personal Data from the EEA to certified organisations in the U.S.;
4. The Disclosure is from Switzerland to an organisation located in the U.S. that is certified under the "Swiss-US Data Privacy Framework" (once such framework has been approved by the Swiss Federal Council and entered into force).

Business Owners have to seek guidance from the DPC before any Disclosure of Personal Data to Third Parties outside Switzerland or the member states of the EU or the EEA without at least one of the above mechanisms in place.

The Disclosure of Personal Data to countries outside of the EU, EEA or Switzerland may be permitted in individual cases if the Disclosure is necessary for one of the reasons set out in the applicable data protection law, including:

a) The performance of a contract between ARYZTA and the Data Subject (e.g. Employees' relocation to a third country);
b) Reasons of overriding public interest;
c) To establish, exercise or defend legal claims;
d) To protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent;
e) The Data Subject has provided explicit Consent to the proposed Disclosure after being adequately informed of the Disclosure and any potential risks.

16. DATA SUBJECTS' RIGHTS

Depending on the applicable data protection law, Data Subjects may have certain rights in relation to the way their Personal Data is managed. These may include the right to:

1. Withdraw Consent at any time;
2. Request access to their Personal Data that we Process;
3. Object to our Processing of Personal Data;
4. Request the erasure of their Personal Data;
5. Ask us to correct inaccurate or incomplete Personal Data;
6. Restrict in particular circumstances e.g. if the accuracy of the data is contested;
7. Ask us for a copy of the safeguards under which Personal Data is transferred abroad;
8. Object to being subject to decisions based solely on automated Processing;
9. Make a complaint to the appropriate data protection authority;
10. In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

Therefore, ARYZTA may receive request of Data Subjects who want to exercise their rights (in particular, access requests). The Company may have the right to restrict or deny Data Subjects' rights in the individual case based on reasons set forth in the applicable data protection law.

Managing Directors and Heads of Business Services must ensure that there is a clear process in place on how to process and how to respond to any Data Subjects' requests and that this process complies with the applicable local laws. They should consult the DPC.

In any case, you must do the following before responding to a request:

- Verify the identity of the requester, e.g. by requesting a proof of identification (copy of passport, copy of driving license, copy of recent utility bill etc.). If someone makes a request on behalf of another person (e.g., lawyer on behalf of a client), the person making the request must provide evidence of their authority to make the request on behalf of the Data Subject, e.g. by providing a power of attorney or the Data Subject's written consent;
- Assess the background of the request (e.g., are there any reasons ARYZTA may want to refuse or restrict the Data Subject's rights?);
- Assess whether the Data Subject is entitled to exercise the right under the applicable law;
- Assess whether there are legal reasons for refusal or restriction of the Data Subject's right under the applicable law;
- Keep an audit trail of requests and actions taken in response to a request.

17. DIRECT MARKETING

We are subject to certain laws when marketing to our customers and any other potential user of our services. Managing Directors and Heads of Business Services need to ensure that local legal requirements are complied with.

In general, Personal business contact details, e.g. John.Smith@aryzta.com, are Personal Data and are therefore subject to the applicable data protection laws. In contrast, impersonal business emails, e.g. sales@aryzta.com, are not Personal Data and are therefore not subject to the applicable data protection laws.

Further, prior Consent is usually required for electronic direct marketing sent to individuals (for example, by email, text or automated calls). However, exceptions may be applicable in certain cases, for example when sending marketing texts or emails if contact details were obtained in the course of a sale to that person, they are marketing similar products or services.

To the extent that we engage in electronic direct marketing, we will in all cases offer recipients a free method (except for the cost of a telephone call or mailing) to opt out of receiving further advertising of this type.

A recipient's objection to direct marketing must be promptly honoured. Please note that it is illegal to make receiving direct marketing a contractual obligation. If a Data Subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

18. BREACH OF DATA PROTECTION LAWS AND THIS POLICY

All Employees are expected to comply with this Policy. Any breach of this Policy by Employees will be taken seriously and, in case of a significant breach, may result in disciplinary actions.

A breach of data protection laws can have a significant impact on ARYZTA's reputation. Besides reputational damage, ARYZTA can be fined up to the higher of 4% of global annual turnover or €20 million under the GDPR.

In addition to potential regulatory fines, Data Subjects can also file a civil claim against ARYZTA for breach of their data protection rights and ARYZTA can be subject to investigations and orders by the competent data protection authorities such as the Swiss Federal Data Protection and Information Commissioner.

Under the FADP, Employees may (upon request made by the Data Subject to the local police) further be subject to individual criminal sanctions (fines up to CHF 250'000) in case of wilful non-compliance with specific rules, in particular:

- Non-compliance with the obligation to provide the minimum information about the Processing to Data Subjects by providing no, false or incomplete information;
- Wrongful or incomplete response to a Data Subject access request;
- Transfer of Personal Data to recipients outside of Switzerland or the EEA without complying with the statutory requirements;
- Delegation of the Processing of Personal Data to a Data Processor without complying with the statutory requirements;
- Non-compliance with the minimum data security requirements;
- Disclosure of confidential Personal Data to Third Parties.

19. CHANGES TO THIS POLICY

We reserve the right to change this Policy at any time without notice, so please check regularly to obtain the latest copy.

20. CONTACT INFORMATION

The Company's point of contact on data protection matters is the Data Privacy Steering Committee, who can be contacted at dataprivacy@aryzta.com.

APPENDIX 1: GLOSSARY OF TERMS

Automated Decision-Making: when a decision is made which is based solely on automated Processing (including profiling) which produces legal effects or significantly affects an individual. Automated Decision-Making is only permissible if certain conditions are met.

Business Owner: means the Employee who is responsible for the relevant Processing activity (risk owner), i.e., the Employee who decides on the relevant aspects of the Processing activity in day-to-day business operations.

Company Data: means any information, whether kept electronically or physically in writing, owned or licensed by the Company.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.
Data Controller: the person or organisation that determines when, why and how to Process Personal Data. It is responsible for establishing practices and policies in accordance with the applicable data protection law. The Company is the Data Controller of all Personal Data relating to it and used delivering education and training, conducting research and all other purposes connected with it including business purposes.

Data Processor: a person or organisation Processing Personal Data on behalf of ARYZTA and according to ARYZTA's instructions.

Data Protection impact assessment (DPIA): tools and assessments used to identify and reduce risks of a data Processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data.

Disclosure: transmitting or making Personal Data accessible to other ARYZTA companies or Third Parties (including remote access to data).

DPC: Data Privacy Steering Committee.

Employees: ARYZTA Employees, consultants, interns, temporary workers, independent contractors and agency workers who have access to Company Data.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Category Personal Data and pseudonymised Personal Data if we have the means for reidentification but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about a Data Subject's actions or behaviour.

Personal Data Breach: any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, Personal Data. It can be an act or omission.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee, job candidates or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes disclosing, transmitting or transferring Personal Data to Third Parties. In brief, it is anything that can be done to Personal Data from its creation to its destruction, including both creation and destruction.

Profiling: any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated Processing.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Category Personal Data: Personal Data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person (e.g. passport photocopy);
- Data concerning health;
- Data concerning a natural person's sex life or sexual orientation;
- Data relating to social assistance measures;
- Criminal convictions and offences including the alleged commission of offences or proceedings for offences or alleged offences.

Third Parties: any individual or organization outside ARYZTA, e.g. external service providers, suppliers etc.

Version control – for internal use

Version Number	Modified by	Modifications made	Date approved	Approved by
Version 1	CHRO/General Counsel	–	13-Dec-23	NomCo

ARYZTA AG
Ifangstrasse 9
8952 Schlieren
Switzerland
Tel: +41 (0) 44 583 42 00
Fax: +41 (0) 44 583 42 49
info@aryzta.com
www.aryzta.com