GROUP DATA
PROTECTION & PRIVACY POLICY

SARIA SE & Co. KG | **Status:** December 2022

Content

I. POLICY GOALS

Terms such as "he", "his" or "him" may refer equally to persons of both male and female genders; for ease of reading, only the masculine form is used below. "Processor" and other masculine terms are generic masculine personal designations taken from the law in this way.

The term Data Protection Officer (hereinafter DPO) within this Group Policy, including his rights and obligations, extends beyond the meaning of Article 37 GDPR and specifically includes any natural person who has been determined as the competent contact person for any data privacy and protection matters of his respective organizational unit.

The protection of personal data is a vital concern to the entirety of the SARIA Group and shall therefore be considered in all of our corporate procedures. We process the personal data of our employees and business partners exclusively in accordance with our data processing principles and in compliance with the applicable law. Considered to be a key quality ingredient in strengthening the trust of our employees, business partners, and the public at large, we are determined to uphold well-functioning data privacy and protection management.

This Policy defines the conditions of cooperation between all SARIA Group Companies. It particularly contains provisions to safeguard an appropriate level of data protection in an international context. It is the primary objective of this Policy to create a common framework, reduce the potential for liability and enhance legal certainty on an international group level.

II. SCOPE

This Policy applies to SARIA SE & Co. KG, all of the Group Companies controlled by it (hereinafter referred to as Group Companies) as well as all of their employees and executive members. The term controlled refers to a majority interest that exists if the majority of shares of a legally independent enterprise is held by another enterprise or if another enterprise is entitled to the majority of voting rights. The term furthermore infers that SARIA SE & Co. KG may enforce the adoption of this policy directly or indirectly, based on its voting majority, majority management representation, or by agreement.

The Policy applies to the processing of personal data wholly or partly by automated means and to the processing of personal data other than by automated means which form part of a filing system or are intended to form part of a filing system unless domestic laws broaden the scope of application.

The Policy applies to the processing of personal data:

a) by Group Companies and their subsidiaries located within the EU/EEA or another country to which this Policy may extend ("EU/EEA-based companies");

b) by Group Companies and their subsidiaries established outside the EU/EAA, to the extent that they offer goods or services to natural persons within the EU/EEA and / or monitor the behavior of natural persons within the EU/EEA ("third country companies with offers for the EU/EEA");

c) by Group Companies and their subsidiaries established outside the EU/EEA, to the extent they have received personal data directly or indirectly from companies that are subject to the Policy under a) or b), or if such data has been disclosed to them ("third country companies receiving data from the EU/EEA").

III. ENFORCEABILITY:

The provisions of this Policy are binding on all Group Companies operating within its scope. The Group companies, their management, and employees are therefore responsible for complying with this Policy in addition to the applicable EU regulations and national data protection laws. Group Companies are not authorized - subject to any potential legal requirements - to make any arrangements that deviate from this Policy.

IV. LEGAL INTERACTIONS:

The provisions of this Policy are not intended to replace supranational or domestic laws but to serve as a supplement to applicable data privacy laws. The content of this Policy shall be observed in the absence of corresponding national laws. In the event of conflict between the applicable data privacy law and this Policy, or if compliance with this Policy would result in a violation of data privacy laws, any laws and regulations shall prevail. Any instance of a potential conflict shall be reported to the Chief Compliance Officer to find a practical solution that complies with the rationale of this Policy and the applicable law. Each organizational unit may decide to adopt additional and / or supplemental policies applicable to their jurisdiction insofar as they do not conflict with the Group Policy.

V. GENERAL PROCESSING PRINCIPLES

Any duties listed in the General Processing Principles constitute third party beneficiary rights for the data subject.

(1) LAWFULLNESS

Personal data shall be processed in a lawful manner and good faith. Data Processing may only take place if and insofar as the processing activity is based on a sufficient legal basis. This also applies to data processing between Group Companies. The mere fact that both the transferring and receiving Group Company are affiliated with the SARIA Group does not readily constitute such legal basis.

The processing of personal data is lawful if one of the following circumstances of permission are applicable. Any adjustment to the original purpose of a processing activity shall constitute the obligation to reevaluate the overall legality of that processing activity.

(2) PROCESSING CUSTOMER AND BUSINESS PARTNER DATA

(2.1) PROCESSING IN CONTEXT OF CONSENT:

Personal data may be processed based on the consent of the data subject. Before giving consent, the data subject shall be informed in accordance with this Data Privacy Policy and the applicable law. The declaration of consent shall be obtained in writing or electronically. In some circumstances, such as telephone conversations, consent may also be accepted verbally. In any event, specifically including verbal declarations of consent, the declaration of each data subject shall be documented in a central data privacy registry (Record Of Processing Activities).

(2.2) PROCESSING IN CONTEXT OF CONTRACTUAL RELATIONSHIPS:

Personal data of customers, business partners, prospective customers and prospective business partners may be processed for the purpose of establishing, performing, or terminating a contract. Processing personal data in the context of contractual relationship furthermore covers the support of customers and partners if that support relates to the purpose of the contract.

Prior to the establishment of a contractual relationship, personal data may be processed to realize any relevant pre-contractual measures vis-á-vis the customer and other business partners. Interested parties may be contacted during the contract preparation stage using the data they have provided. Any restrictions expressed by the interested party shall be observed.

(2.3) PROCESSING IN CONTEXT OF LEGAL RIGHTS AND OBLIGATIONS:

Personal data may be processed if national laws require or permit the processing of personal data. The scope of the processing activity shall be strictly limited to the requirements of the law and never exceed what is legally necessary.

(2.4) PROCESSING IN CONTEXT OF LEGITIMATE INTEREST:

Personal data may be processed based on legitimate interest if the controller can establish a legal or commercial interest and the data subject's interests do not outweigh the interests of the Data Controller. When relying on a legitimate interest to justify a processing activity, for each corresponding processing activity, the Data Controller shall assess whether the data subjects' interests worthy of legal protection outweigh the legitimate interests in processing. The assessment shall be documented in a central data privacy registry.

(3) PROCESSING EMPLOYEE DATA

In the context of employment relationships, personal data may be processed to establish, perform and terminate an employment relationship. Upon rejection, the applicant's data shall be deleted taking into account any legal rights or obligations allowing for a prolonged period of retention. Sharing the applicant's data with other Group Companies or using the applicant's information for any further application procedures shall require the data subject's consent. In the context of an established employment relationship, processing personal data shall be strictly limited to the purpose of that relationship unless one of the following conditions are met.

If necessary, during the application procedure and subject to applicable national laws, additional personal data from third parties may be collected and processed. In cases of doubt, a declaration of consent from the data subject shall be obtained.

Furthermore, any processing of employee data related to the employment relationship, which did not originally aid in creating, performing, or terminating that relationship may be processed if either one of the following justifications can be established:

(3.1) LEGAL RIGHTS OR OBLIGATIONS:

Employee data may be processed if national laws require or permit the processing of employee data. The scope of the processing shall be strictly limited to the requirements of the law and never exceed what is legally necessary. If national laws leave room for interpretation or are ambiguous in any other way, the data subjects' interests worthy of protection shall be considered.

(3.2) COLLECTIVE BARGAINING AGREEMENTS:

Employee data may be processed if the processing activity has been authorized through a collective bargaining agreement provided that such agreement was concluded within the constraints of the law and specifies the precise terms of a processing activity.

(3.3) CONSENT:

Employee data may be processed if the data subject consents to such processing. Declarations of consent must be given voluntarily without any threat or inference of negative consequences should the data subject decide to withhold consent, as involuntary declarations of consent are legally invalid. Although consent may be given free of any form requirements, it should be obtained in writing or electronically and only in exceptional cases verbally. Before giving consent, the data subject shall be informed pursuant to the applicable Law and this Data Privacy Policy. Any grant of consent shall be documented in a central data privacy registry.

(3.4) LEGITIMATE INTEREST:

Employee data may be processed if the employer can establish legal or commercial interests that are not outweighed by the data subjects' interests worthy of protection. For relying on legitimate interests in the context of employment relationships, the employer shall properly document its process of balancing the interests of the employer with the ones of the data subject(s).

Control measures such as performance checks are not permitted unless there is a legal obligation or justified reason to establish such measures. Even in instances where legitimate interests seem well founded from the perspective of the employer, the Data protection officer (hereinafter referred to as DPO) of the organizational unit shall be contacted to determine the proportionality and overall appropriateness of any given measure in this regard. The DPO's conclusions shall be documented in a central data privacy registry.

(4) HIGHLY SENSITIVE DATA

Highly sensitive personal data (i.e. any data pursuant to Article 9 GDPR) may be processed only if it is expressly permitted or prescribed by supranational or national law, if the data subject expresses consent, or if it is necessary for the assertion, exercise or defense of legal claims relating to the data subject. Any processing of highly sensitive data requires the utmost care, not limited to but especially relating to the maintenance of adequate technical and organizational measures to ensure the overall security of corresponding processing activities. Any measures or procedures with regard to the processing of highly sensitive personal data shall be coordinated with and approved by the DPO of the irrespective organizational unit.

(5) AUTOMATED DECISION MAKING & PROFILING:

Data subjects may be subjected to a fully automated decision that could imply negative legal or similar consequences on them if such a decision is necessary for the conclusion or performance of a contract, or if the data subject has given consent. Such decision-making may also include profiling in some instances, for example where individual personality characteristics are evaluated to determine creditworthiness. Upon the occurrence of automated decision-making and profiling, the data subject shall be notified about its occurrence as well as the outcome of the procedure. The data subject shall be given the opportunity to have the decision reviewed by the controller.

(6) TRANSPARENCY DUTIES:

The controller shall inform the data subjects about the context and purpose of the processing of their personal data pursuant to Articles 13 and 14 of the GDPR, or if the data is out of the scope of the GDPR, or any applicable national law. The data subject shall be informed by a meaningful overview of the intended processing procedure generally before the processing activity takes place and whenever a processing activity occurs the first time. The information shall be concise, transparent, and intelligible. If a Group Company receives personal information from a third party, the Group Company shall inform the data subject within a reasonable time, however at the latest within one month after it has obtained the data. Exceptions to the requirement of informing the data subject about processing activities involving personal data not directly obtained from the data subject may be made only if the data subject is already aware of the processing activity, any applicable law expressly prescribes the recording or disclosure of personal data, or if is impossible for the responsible party to inform the data subject or would involve a disproportionate effort.

(7) PURPOSE LIMITATION:

Personal data shall only be processed based upon the determination of a specific and legitimate purpose prior to the collection of personal data. The processing purpose shall not be altered in a way that would be incompatible with the original purpose serving as a justification for the original processing activity.

(8) DATA MINIMIZATION:

The processing of personal data shall be limited to what is adequate and relevant, both in a quantitative and qualitative sense, strictly relating to the purpose for which the personal data is collected. Depending on the nature of the purpose as well as the proportionality of the effort in pursuing a processing activity, anonymized or statistical data shall be used.

(9) DATA ACCURACY:

Personal data shall accurately reflect the data subject's personal and factual circumstances. Specifically, it shall be ensured that the personal data stored is objectively correct and, if required, up to date. Appropriate measures shall be adopted to ensure that incorrect or incomplete data is deleted, corrected, or supplemented by additional information.

(10) PRIVACY BY DESIGN & PRIVACY BY DEFAULT:

The principle of Privacy by Design aims to ensure that the Group Companies define state-of-the-art strategies and measures to incorporate data protection principles into their corporate operating procedures at the stage of conceptualizing a processing activity. The principle of Privacy by Default aims to ensure that the configuration of any system or service concerned with the processing of personal data shall, by default, revert to the most privacy-friendly option necessary to achieve the purpose of processing. This includes specifically, but is not limited to:

- Processing scope, storage, and retention periods as well as accessibility;
- Pseudonymization of personal data whenever possible and proportionate in terms of the processing activity's foreseeable effort;
- Utmost transparency about procedural functionalities and the processing of personal data;
- Giving data subjects the choice to decide on the processing of their personal data whenever possible;
- Enabling the operators of procedures and systems to devise and enhance security features.

By adhering to the aforementioned principles, every Group Company shall implement and maintain appropriate technical and organizational measures (hereinafter referred to as TOMs) throughout the entire life cycle of its processing activities in order to ensure that the adherence to these principles at all times.

(11) ERASURE & ANONYMIZATION:

Personal data may only be stored for as long as it is necessary to achieve the purpose for which the personal data is being processed. Accordingly, personal data shall be deleted or anonymized as soon as the purpose of the corresponding processing activity ceases to exist unless any legal obligations (e.g. retention periods) continue to be applicable. The responsibility for the implementation of deletion and anonymization routines shall be borne by the respective departments of each Group Company in cooperation with the organizational unit's DPO. Any corporate procedure or system which processes personal data shall be technically capable of, whether manually or automated, erasing or anonymyízing personal data. Erasure requests from a data subject shall be followed up and addressed by the organizational unit's DPO within due time considering any statutory temporal requirements.

(12) INFORMATION SECURITY:

Personal data shall be protected from unauthorized access, any unlawful processing or transfer, as well as accidental loss, alteration, or destruction. Before introducing new methods of data processing, particularly relevant in the context of new IT-Systems, state-of-the-art TOMs proportionate to the risks of the processing activity and the nature of the personal data shall be defined and put in place. Each TOM shall be documented in the Record of Processing Activities. Any department responsible for processing personal data shall consult with the organizational unit's Information Security Officer and DPO to determine the overall appropriateness of the TOMs.

(13) EXTERNAL TRANSMISSION:

Any transmission of personal data to recipients outside the SARIA Group Companies shall correspond to the General Processing Principles as set forth by this Group Policy. The transmission shall be subject to the organizational unit's prior approval, which shall be contingent on an assessment of the validity of the legal basis for transmission. The recipient or processor outside the SARIA Group shall be required to use and handle the personal data only in accordance with the predefined purpose.

In the event of cross-border transmission of personal data, including the grant of access from another country, the relevant foreign legal requirements for the transfer of personal data shall be complied with. Particularly, personal data from the EU/EEA may only be processed outside the Group Companies in third countries, if the recipient can demonstrate a data protection level that is at least equal to the standards of this Data Privacy Policy. Suitable measures in this context could be:

- Transfers based on an adequacy decision;
- Standard Contractual Clauses of the European Commission;
- The recipient's participation in an EU-accredited certification system ensuring adequate data protection safeguards;
- Recognized binding corporate rules of the recipient to create an adequate level of data protection.

Transferring personal data to public authorities is only permitted if and insofar the transmission is not disproportionate or excessive to what could be considered necessary in a democratic society. In the event of a conflict between the transmission requirements in this Data Privacy Policy and the demand of the public authority, the governing legal department of the respective jurisdiction shall find a practical solution that fulfills the purpose of this Data Privacy Policy.

VI. DATA PROTECTION IMPACT ASSESSMENT

Before introducing entirely new processing activities and in particular when using new technologies, or in the event of making significant changes to existing processing activities, Group Companies shall, as part of their risk analysis, conduct an assessment of the impact of processing activity (hereinafter referred to as DPIA) to determine whether the processing activity poses a high risk to the data privacy rights of the data subjects. The nature, scope, context, and purpose of the data processing activity shall be taken into account. Should the risk to the rights and freedoms of the data subjects remain high even after performing the DPIA, and considering all measures to mitigate the risks, the DPO of the Group Company shall contact the competent data protection supervisory authorities for further guidance on the issue. The DPIA shall be documented in a central data privacy registry.

VII. DOCUMENTATION OF DATA PROCESSING PROCEDURES

Each Group Company shall maintain documentation of any processing activities in a Record of Processing Activities. The record may be administered from one central position which oversees the entire jurisdiction or organizational unit. The record shall be maintained in written or electronic form and shall be made available to the competent supervisory data protection authorities upon their request.

VIII. PROCESSING ON BEHALF

Processing on behalf refers to processing activities where a contractor processes personal data as a service provider (hereinafter referred to as Processor) on behalf of, and in line with, the instructions of the data controller (hereinafter referred to as Controller). In such instances, a data processing agreement (hereinafter referred to as DPA) shall be concluded with external Processors outside of the SARIA Group and Processors inside the SARIA Group. The conclusion of a DPA shall not relieve the Controller of his responsibility in connection to the performance of the data processing activity.

Controller Provisions:
When concluding a DPA, the organizational unit's DPO in cooperation with the corporate department issuing the DPA shall be responsible to comply with the following requirements:

- The processor shall be chosen based on its ability to provide the required technical and organizational measures to ensure an appropriate level of data security;
- The DPA contains the minimum requirements in line with Article 28 GDPR;
- The DPA shall be concluded in writing or electronic form and it shall be stored in a central data privacy registry.

Before the commencement of data processing in this context, the Controller shall conduct a suitable assessment to review the processor's ability to comply with the obligation set out above. Any specifications provided by the organizational unit's DPO shall be observed. In particular, the Processor may demonstrate its compliance with the processing requirements by presenting a suitable certification. Depending on the determined risk of the processing activity, regular reviews to re-evaluate the processing activity shall take place. Any measures in relation to the conclusion of a DPA shall be documented in a central data privacy registry.

Processor Provisions:
The following provisions shall apply to both internal and external Processors. The Processor shall process personal data only in accordance with the Controller's documented instructions, notwithstanding any obligations under Union- or Member State Law.

Processors may include other Group Companies or third parties (hereinafter referred to as Subcontractors) to process personal data only based on the Controller's prior consent. Consent in this context shall only be given if the processor subjects the Subcontractor to legally binding measures that demonstrate data protection obligations equal to the level of safeguards provided by this Group Policy and the applicable law, specifically including any technical and organizational measures. The form of consent as well as any information requirements in the event of changes proposed to the contractual relationship between processor and subcontractor shall be set forth in the Service Agreement and/or Data Processing Agreement.

Processors are obligated to support the controller in complying with its data protection obligations, particularly through providing sufficient information on and safeguarding the following:

- The handling of inquiries and other invitations by the competent supervisory authorities;
- The General Processing Principles pursuant to Section V of this Group Policy;
- The Processing on Behalf provisions pursuant to Section VIII of this Group Policy;
- The Rights of Data Subjects pursuant to Section X of this Policy;
- The Notification of Data Protection Incidents pursuant to Section XII of this Policy.

If the applicable law requires the Processor - or its Subcontractor - to process personal data in violation of the Controller's instructions or prevent the Processor - or its Subcontractor - from fulfilling its obligations under this Group Policy or the DPA, the Processor or its Subcontractor shall notify the Controller without undue delay, unless the relevant legal provision explicitly precludes such notification. In any such event, the controller shall have the right to suspend data transmission and terminate the DPA.

Unless strictly prohibited for valid reasons, the Processor shall notify the Controller about any legally binding inquiries from the competent supervisory authority for disclosure of personal data.

Upon termination of the DPA or the provision of processing services, at the discretion of the Controller, the Processor shall delete or return all personal data it was provided with by the Controller.

The Processor – or its Subcontractor – shall notify the Controller about any asserted claims, requests, or complaints from a data subject.

IX. JOINT CONTROLLERSHIP

In the event of multiple Group Companies jointly defining the means and purposes of processing personal data (hereinafter referred to as Joint Controllers), the Joint Controllers shall conclude an agreement specifying their tasks and responsibilities vis-à-vis the data subjects whose data they process. For the conclusion of such agreements, the requirements of Article 26 GDPR shall be observed.

X. RIGHTS OF THE DATA SUBJECT

Any inquiries or complaints submitted by the data subject falling under this section of the Group Policy shall be answered within one month. Considering the complexity and quantity of submissions, the response deadline may be extended by a maximum of two additional months. In such instances, the data subject concerned shall be informed accordingly.

A data subject in the EU/EEA may, as further specified by applicable EU and/or national law, exercise the following rights vis-à-vis the accountable Group Company or, if such Group Company is the Processor, vis-à-vis the Controller:

Information and Access Rights: Data subjects shall have the right to be informed about how their personal data is processed by the Group Company and to which corresponding rights they are entitled. Upon request, data subjects shall receive a copy of their personal data unless the interests of third parties worthy of protection prohibit this (pursuant to Articles 12-15 GDPR).

Rectification Rights: Data subjects shall have the right to obtain from the Controller without undue delay the rectification of inaccurate or incomplete personal data concerning him (pursuant to Articles 16, 19 GDPR).

Deletion Rights: Data subjects shall have the right to obtain from the Controller the erasure of personal data concerning him without undue delay. The Controller shall have the obligation to erase personal data without undue delay where the legal basis for processing ceases to be applicable, the legitimate purpose has lapsed, or the data subject withdraws consent to the processing activity. Existing retention periods and the Controller's interests worthy of protection prohibiting the deletion of personal data shall be observed (pursuant to Articles 17, 19 GDPR).

Restriction Rights: Data subjects shall have the right to restrict the processing of personal data if the accuracy of the data concerned is in dispute, or if the Group Company no longer needs the data while the data subject needs the data in the pursuance of legal claims. The data subject may also request the Group Company to restrict the processing of his data if it would otherwise have to delete the data or if it is reviewing an objection by the data subject (pursuant to Articles 18, 19 GDPR).

Data Portability Rights: Data subjects shall have the right to receive the personal data relating to them in a common machine-readable format, which includes the entitlement to transmit this data to a third party, provided that the processing activity follows an automated procedure and it is technically feasible to transmit such data (pursuant to Article 20 GDPR).

Objection Rights: Data subjects shall have the right to object to a processing activity based on the legitimate interest of a Group Company or a third party if the data subject can manifest valid reasons relating to their particular circumstance. The right to object shall not apply if the Group Company or a third party can present compelling reasons which support the continuance of the processing activity, or if the processing activity occurs to exercise or defend legal claims of the Group Company. As the result of a legitimate objection, notwithstanding the aforementioned exclusionary factors, the objection shall culminate in the deletion of the respective personal data (pursuant to Article 21 GDPR).

Complaints Procedure: Data subjects shall have the right to lodge a complaint with the respective Group Company's DPO if they assume that their privacy rights or this Group Policy have been violated. Complaints may be submitted in written form, electronically via e-mail or the integrity whistleblower hotline as well as verbally via telephone or in a personal setup. The Group Company established in the EU/EEA that exports the data will assist data subjects whose personal data was collected in the EU/ EEA in establishing the facts and the assertion of their rights under this Policy against the Group Company that imports the data. Any complaint of a data subject as well as the entire procedure to resolve the issue shall be documented in a central data privacy registry. Should a data subject be dissatisfied or disagree with the outcome of a Group Company's decision, he shall have the right to challenge such decision or conduct by way of appeal. Accordingly, he may apply to the competent national supervisory authority of the country of his habitual residence, place of work, or place of the alleged infringement. Notwithstanding the right and procedure to appeal a Group Company's decision, the data subject is free to bring a complaint to the attention of the competent supervisory authority at any time. A data subject may also initiate legal proceedings as detailed in the following section of this Group Policy. Complaints and other data protection requests submitted by the data subject shall be handled with due consideration of statutory timelines.

XI. LIABILITY & JURISDICTION

Liability:
The Group Company established in the EU/EEA (hereinafter referred to as Data Exporter) which initially transferred personal data to a Group Company established in a third country, or any other third party established in a third country, shall assume liability for any violation of this Group Policy by such third country Group Company or external party established in a third country. The assumption of liability explicitly includes the obligation to remedy unlawful situations and to compensate for material and non-material damages caused as a direct result of a breach of this Group Policy by a Group Company. The Data Exporter may be partially or fully exempt from the liability if it can be proven that the third country Group Company that received data from the EU/EEA Group Company is not responsible for the action which resulted in any damage. The burden of proof rests with the Data Exporter who initially transferred the data.

Place of Jurisdiction:
Data subjects may initiate legal action before the courts of the jurisdiction of the Controller, the Processor, or at the place of his habitual residence. The data subject who claims an infringement of this Policy in the context of a processing activity involving any third country can assert his legal claims against both the data importing and the data exporting company in the EU/EEA. Therefore, the data subject may bring the alleged infringement and the resulting legal claims before the competent courts and regulatory authorities either at the establishment of the controller or at his habitual residence.

XII.DATA PROTECTION INCIDENTS & NOTIFICATION REQUIREMENTS

A data protection incident is a personal data breach if there is a breach of security leading to the unlawful destruction, alteration, unauthorized disclosure, or use of personal data. In the event of a potential breach of the data protection and information security requirements (hereinafter referred to as data protection incident), the Group Companies involved shall facilitate an investigation, mitigation measures and potentially inform the competent supervisory authority and/or the data subjects of the nature of the breach.

Should the personal data breach be likely to result in a risk to the rights and freedoms of the data subjects concerned, the competent supervisory authority shall be informed by the Data Controller within 72 hours after the Data Controller has become aware of the incident. Where the notification of the supervisory authority does not occur within 72 hours, the notification of the supervisory authority shall be accompanied by reasons for the delay. Additionally, the affected data subjects shall be notified by the Data Controller if the data breach is likely to result in a high risk to their personal rights and freedoms. Data Processors are obliged to report data protection incidents to the controller immediately after becoming aware of such instances.

If a data protection incident has been identified or is suspected within a Group Company, or their area of responsibility, all employees are obliged to report the incident immediately to the organizational unit's DPO or via the SARIA Integrity Line. Any data protection incident including its follow-up measures shall be documented and stored in a central data privacy registry. The documentation shall be made available to the competent supervisory authority upon request.

XIII. DATA PROTECTION ORGANIZATION

Responsibility: The members of the managing organs of the Group Companies are responsible for the data processing activities within their area of accountability. They are obliged to ensure that the legal data protection requirements arising out of any applicable domestic laws and this Group Policy are met. Management, within their respective sphere of responsibility, shall safeguard an appropriate level of data protection through organizational, staff-related, and technical measures. Any employee shall be responsible for compliance with the requirements set forth by this Group Policy as well as any applicable law.

Awareness & Training: The Group Company's Management shall ensure that its employees receive regular data protection training, including the content and handling of this Policy, if they have constant or frequent access to personal data, are involved in the collection of data or in the development of tools used to process personal data.

Organization: The organizational unit's DPO is independent in the performance of his tasks. The DPO shall ensure adherence to any applicable national and international data protection laws. He monitors compliance with this Group Policy, within his geographical and/or organizational scope of responsibility. Data subjects may contact the DPO responsible for their jurisdiction at any time to express their concerns, ask questions, request information, or lodge complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled with confidentiality. The geographical scope of each Data Protection Officer corresponds to the compliance organization of the group. Specifically, the following organizational division shall apply with respect to data protection:

- Germany
- France
- United Kingdom
- Spain
- Northern Europe
- Italy
- Poland
- Czech Republic
- Austria
- Romania
- Belarus / Russia
- Van Hessen
- Bioiberica

The SARIA Group has established a compliance organization, which is geared towards the specific requirements of data protection and privacy and described in greater detail in a separate internal regulation. The compliance organization supports and supervises the Group Companies regarding compliance with data protection laws. It defines the content of the data protection training and stipulates the criteria for the group of participants.

International Data Privacy Committee: To enhance the overall level of data protection within the SARIA Group and to effectively pursue the objectives of this Group Policy, the organizational units shall form an International Data Privacy Committee (IDPC). The IDPC shall meet bi-annually to discuss general developments in the area of data protection within their organizational units, points of concern in relation to the Group Policy as well as any other issues the organizational units may face in light of complying with any applicable data protection requirements. The scheduling of the IDPC meetings will be handled by the organizational unit Germany, acknowledging the sittings of the Compliance Board.

Reporting: The Chief Compliance Officer in cooperation with the DPO of the organizational unit Germany shall inform the SARIA Compliance Board annually on the data protection status of each of the organizational units. The content of the reports shall be based on a predefined set of key performance indicators. To facilitate such reporting measures throughout the whole SARIA Group, each organizational unit shall prepare annual progress reports (Document: SARIA Data Privacy International: OE Progress Report) and make them available to the Chief Compliance Officer until the 15th of January of each calendar year.

Audits and other control measures: Compliance with this Policy may be reviewed at Group level regularly on a risk-based approach, or specific request from the Chief Compliance Officer, by way of an internal or external compliance risk assessment in form of audits concerning specific data protection topics and other checks. The results shall be reported to the Chief Compliance Officer and to the from the organizational unit appointed DPO.

Sanctions: The unlawful processing of personal data and further similar offenses against data protection law may be prosecuted under administrative as well as criminal law in many countries and may further form the basis for potential compensatory claims. Breaches for which individual employees are responsible can lead to disciplinary action under employment law.

XIV. AMENDMENTS, ACCSESSION & COOPERATION WITH PUBLIC AUTHORITIES

Amendments:
After prior deliberation of the International Data Privacy Committee (IDPC), SARIA's Board of Directors may amend this Group Policy or adopt additional Policies at any time, and the Members agree to abide by the terms thereof provided that (a) any amendments do not bind the Member in less than thirty (30) calendar days from the date that notice of such action is given to the organizational unit's DPO in electronic form; and (b) no such amendment or new Policy has any retroactive effect.

Ratification & Accession:
As part of the ratification procedure, each organizational unit, its entities, its staff, and executive members shall adhere to the principles of this Group Policy by way of decision through SARIA's Board of Directors. The organizational unit shall appoint at least one natural person who shall be responsible for data protection and privacy within his organizational unit.

Cooperation with public authorities:
Group Companies that carry out or participate in processing in third countries are obligated to cooperate with the responsible supervisory authorities in matters concerning problems, inquiries, or other procedures in connection with the processing of personal data in the context mentioned above. This encompasses the duty to accept lawful audits by supervisory authorities. In addition, all lawful instructions from the responsible supervisory authorities based on processing procedures in third countries or provisions of this Policy shall be complied with.


Bioiberica
VAN HESSEN
ecoMotion
SARVAL
SECANIM
BIOCEVAL
ReFood
pure bioenergy
SINOVA

SECANIM ecoMotion ReFood pure Biokraft SINOVA

SARVAL BIOCEVAL Bioiberica VAN HESSEN

www.saria.com