GLOBAL RECRUITMENT AND EMPLOYMENT PRIVACY POLICY

The Schreiber Foods Group ("**Schreiber**" or "**Schreiber Group**") is a global group made up of various entities that operate all around the world. It is a customer-brand leader in cream cheese, natural cheese, processed cheese, beverages, and yogurt – including plant-based options.

I. SCOPE

This *Global Recruitment and Employment Privacy Policy* (this "Policy") explains how Schreiber collects and uses personal data during Schreiber's recruitment and selection processes, and employment contractual relationships. Particularly, Schreiber collects information on individuals who have applied for employment, and on those who are currently or were formerly a part of our workforce, such as employees, officers and directors, interns, contractors, and other individuals who perform or have worked for Schreiber or have performed work under commission for Schreiber, whether employed by Schreiber or not, as well as their dependents, beneficiaries, and emergency contacts.

II. LEGAL FRAMEWORK

While this Policy is global in nature, its objective is to comply with local requirements in each country where applicants and employees are located, thus, where this policy conflicts with local requirements, those laws will take precedence.

The Supplements of this Policy include additional applicable requirements for each country where Schreiber operates, including compliance with the GDPR for European Schreiber entities.

III. GENERAL TERMS

1. The Data Controller

The data controller will be, in each case, the Schreiber entity that is processing the personal data in the employment or recruitment context, as indicated in each of the Supplements of this Policy ("**We**", "**Schreiber**", or "**Data Controller**").

2. Collected Data

For the purposes of this Policy, the ***Data Subjects*** of this Policy will be understood as the applicants for job positions posted by Schreiber and the employees currently or formerly employed by Schreiber, which will compromise of the following:

Applicants' data

Schreiber may collect and or treat the following information when necessary and legally allowed to by local law ("**Personal Data**"):

- **Contact Information**: address, phone number and e-mail address.
- **Personal information**: name and surname, citizenship, ID, signature, date and place of birth.
- **Professional information**: skills, job history (including position history, title history, current and past outside business interests and directorships, effective dates and past pay groups), education history and qualifications, worker history and any other information included in their CV.

- **Interview data**: Personal data collected from interviews and outcomes of any recruiting exercises completed with the candidate, including personality/reasoning ability tests and, for certain roles, recordings of presentational based interviews.

- **Travel data**: Personal data we process if Schreiber is arranging travel for on-site interviews, such as passport information.

- **Immigration and Visa information**: Information related to their immigration status and visa requirements.

- **Background check data**: Information received from internal and external reference and background checks, including criminal records at offer stage only.

- Any other information they provide to us that would contribute to the identification of themselves as a natural person.

In addition to the collection, processing and use of Applicant Data, Schreiber may collect, process and use, in some cases and always when necessary and legally allowed to, the following special categories of data (hereinafter, "**Sensitive Applicant Data**"):

- **Information concerning disabilities**: including the degree of disability;

- **Voluntary Sensitive information**: gender identity, ethnicity, and demographic data. This information will only be used to evaluate and improve Schreiber´s diversity and belonging efforts on an aggregate level. In the context of recruitment, it will be processed separately from the application and, whether the applicant chooses to answer, it will not affect their job application.; and

- **Psychometric data**: such as the obtained from psychometric tests that may be involved in the recruitment process.

2.1. Employees' Data

Schreiber may collect and treat the following information when necessary and legally allowed to by local law ("**Personal Data**"):

- **Identifying data**: name and surname, signature, employee ID or staff, professional email, business address, business phone, nationality, identification number or passport information on driver's license number, social security, insurance information health and pension and tax identification number;

- **Personal information**: date and place of birth, gender, descent data, contact details in case of emergency of relatives and partners;

- **Professional information**: office, position, range, type of employee, management level, type of day (full or split time and percentage), weekly working hours default, information on hours worked, center work, division, department, job level, responsible (name and identification), roles supporting start and termination reference to contract status, employment history (including posts, positions and interests and management positions present historical and past, effective dates and previous wage groups), educational background and qualifications, work history (including file-record changes in databases HR) and reasons for termination;

- **Background check data**: information obtained from checking credit information systems;

- **Information about salary and benefits of the employee**: information about their base salary, their bonus and commission, amounts and percentages of increases,

benefits, insurance benefits (including information about them and their descendants that we provide the insurance, pension plans, identification number tax, bank account details and payment dates, purchase personal data, information on accrued wages, wage group and information on pensions;

- **Information on remuneration in the form of equity instruments**: shares or units of management positions, data on all restricted stock units or other rights to shares awarded, canceled, exercised, acquired not acquired or outstanding in their favor;

- **Time monitoring information, phone calls and access to systems or buildings**: access by card, data on Internet use, e-mail and telephone, mobile content, email and chat and similar data, data recording calls and conference calls;

- **Performance and disciplinary information**: performance reviews, evaluations and qualifications, information on disciplinary charges, disciplinary proceedings and any warning, complaint data and any results;

- **Organizational data**: identifiers for computer systems and access credentials, details of companies, localization cost centers, organizations.

In addition to the collection, processing and use of employee data, Schreiber collects, processes and uses the following special categories of personal data with the utmost care and only in some cases when necessary and legally allowed to by local regulations, ("**Sensitive Employee Data**"):

- **Medical and health data**, such as the number of days off, information on accidents for purposes of insurance, risk prevention and compliance with legal obligations (such as reporting obligations), information on disabilities in order to accommodate the workplace and compliance legal obligations, information on maternity leave for personal planning and compliance with legal obligations.

- **Biometrics** provided that they allow the unambiguous identification of confirming a person such as fingerprints, facial images (video surveillance), or dactyloscopy data.

- **Background Check Data:** such as information on criminal records and information obtained from checking credit information systems.
- **Other sensitive information**: such as disability information for compliance with applicable legal obligations or trade union membership for tax purposes.

Should an applicant or employee provide Schreiber any personal data of third parties, such as data from relatives or from their partner, it is understood they agree to comply with the obligation to inform or, where appropriate, obtain their express consent to do so before providing such data to Schreiber, under the terms of this notice.

3. Purpose of the data collection

The above-mentioned Personal Data is necessary for the selection process and/or managing the employment contract and fulfilling Schreiber's obligations as an employer. In this sense, we will treat the ***Data Subject***´s data to the extent permitted or required by applicable law for the following purposes:

a) Applicants' data

- To assess qualifications, suitability, and eligibility for a position as an employee or contractor, and the terms of any offer;

- To enter into a contract or employment relation with the applicant (if they have made an offer) and to make working arrangements such as place of work and working hours;
- To contact references or other individuals who may provide information to Schreiber about their employment history or fitness for employment or contract work with us, as permitted by law;
- For financial planning and budgeting;
- To contact the applicant in case more information is needed to make a decision;
- To provide the applicant information about their offer, contract, or terms of employment to third parties in connection with transactions, such as a prospective purchaser, seller, or outsourcer;
- To conduct diversity and equal opportunity initiatives as permitted and/or requested by law (except in the Czech Republic, where we data regarding gender and ethnicity will not be asked);
- To make staffing decisions; and
- To evaluate and improve the recruitment process.

b) Employees' Data

- Manage and provide the employees' remuneration, including managing and providing their salary bonus and other incentives that may apply;
- Manage and provide benefits that are applicable and other work-related pensions, including notification of rights to obtain and use certain benefits;
- Manage staff, including managing work activities, providing performance evaluations and promotions, developing and maintaining organizational charts, matrix management, team management and templates of the entity and entities belonging to the group management professional travel, to carry out activities talent management and career development, management and approval of permits, provide references and manage ethics and compliance trainings;
- Comply with applicable laws and requirements relating to employment and manage such requirements as may be Income Tax for Individuals, deductions for social security and labor law or immigration;
- Ensure compliance with Company procedures that may apply, including internal reporting systems, physics, computer and network security, and internal investigations;
- Contact an employee, other employees within the group and/or third parties (such as potential or existing business partners, suppliers, customers, end users or agents of the authorities for lawful and compulsory communication);
- Communicate with employee-designated contacts in case of emergency;
- Respond to requests and requirements of regulators or other authorities within or outside their country;
- Fraud prevention activities and safety, as may be preventing fraud, misuse of computer systems, or bleaching, physical security, computer security and network or internal investigations according to the IT Schreiber policies;

- Compliance and corporate financial responsibilities, including internal or external audits and analysis, cost control and budgeting;

- Control obligations of employees, including evaluation of work performance, to the extent permitted by applicable law; and

- To develop Diversity, Equity & Inclusion ("DEI") Programs, and to plan *ad hoc* activities in benefit of the employees and share anonymized information internally.

4. Legal basis

Schreiber treats personal data to the extent permitted by applicable law for a variety of legitimate business purposes, all exclusively in connection to the recruitment process and with employment relations.

Schreiber collects and processes Personal Data under the lawful ground of the consent of the Data Subject, where consent is *freely given, specific, informed and unambiguous*. Additionally, Schreiber may process Personal Data when one of the following applies:

i. processing is necessary for the performance of a contract where the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
ii. processing is necessary for compliance with a legal obligation to which the controller is subject (such as the regulation on social security or tax);
iii. processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
iv. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and
v. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child.

For the processing of Sensitive Data, which may include information on gender and ethnicity, Schreiber will require the Data Subjects´ explicit consent to process it and it will be used:

i. Compliance with legal obligations;
ii. For equality and diversity purposes;
iii. For the fulfillment of obligations and for the exercise of specific rights in the field of labor law, taxes, social security and social protection; and
iv. For preventive or occupational medicine purposes.

The legal basis will depend on the local laws of the country where the applicable Schreiber entity is located, where the candidate is applying to or the employee is working for,. Please, go to the Supplements at the end of this Policy for further information.

5. Data sources

Schreiber gathers candidate data via application forms in Workday, but also from the interview and any form of communication during the recruitment process. Even if a job posting is advertised through third-party platforms, their Personal Data will only be collected by Schreiber through the Workday platform and their data will be protected by Schreiber.

If the applicant becomes an employee, the applicant data will be stored as employee data, as well as any other information required by Schreiber to execute their employment contract via email or Workday forms.

Moreover, Schreiber may also obtain their personal information from third parties such as former employers, employment agencies, credit reference agencies, or other background check providers, service providers and references.

6. Storage of data

Schreiber stores Personal Data in Workday, One Drive, and hard copies. Only hiring managers or hiring team members will have access to Applicant Data, so they can contact those candidates. Moreover, only HR managers will have access to Employee Data.

7. Security measures

Schreiber uses organizational, technical, and administrative measures designed to protect and manage personal information securely.

In the event of a security breach, the Data Controller will notify the relevant national authority and the persons whose data has been compromised within the timeframe applicable by local law.

A security breach of personal data includes any unauthorized:

- loss or destruction of personal data;
- theft, loss or copying of personal data;
- use, access or processing of personal data; or
- damage or alteration of personal data.

The affected Data Subject may notify Schreiber through the DPO email *dpo@schreiberfoods.com*.

8. Data transfers

8.1. Recipients

Schreiber is a global group made up of various entities; to ensure that the purposes of the data processing can be performed, personal information of applicants or employees may be shared with the entities within the Group network included in the Supplements. If Schreiber shares data in this way, the categories of individuals who have access to personal information will be limited.

Schreiber may transfer applicant or employee data to other entities of the Schreiber Group for the pursuit of legitimate interests of the Company for internal management purposes, as well as for relocation of employees, as can be to facilitate internal communication and management tasks to other group entities, administration and human resource planning at group level (including template, estate planning, forecasting and budgeting, investment decisions, training management and performance, etc.) and to be able to meet the employment relationship within our global structure (i.e. to facilitate global cooperation and movement of employees within the group).

Additionally, Schreiber may transfer Personal Data to the following third parties:

- Schreiber may transfer Personal Data to **government agencies and public and regulatory entities** (e.g. tax authorities), institutions of social security, courts, and public authorities, all in accordance with the applicable law.
- Schreiber may also share Personal Data with **service providers and contractors**, (such as Workday) or external advisors (e.g., legal advisors, lawyers, auditors), who perform services on the company´s behalf or that are necessary for business purposes and act as data processors on the company´s behalf. As part of normal operations, Schreiber

contracts with third party service providers or other group entities to carry out certain global HR management activities (i.e., global directory, global benefits, global recruitment), IT related tasks (i.e., for maintenance of secure global systems and networks) or who provide advisory services.

The information of Schreiber recruitment database is not used for marketing purposes.

In order for Schreiber to share any of the applicants' and employees' personal information for reasons not described in this notice, Schreiber shall inform them beforehand, with reasonable notice, so they can exercise their Data Subject rights set out in Section 10.

8.2. International transfers

In connection with Schreiber's business and for applicant, employment, administrative, management, and legal purposes, Schreiber where necessary may transfer Personal Data across country borders in accordance with the applicable law. Such transfers include members of our group of entities and third-party service providers, including other jurisdictions in which Schreiber is established. For example, some of the systems that Schreiber uses in connection with its business (such as Workday) are hosted in the US. Schreiber will ensure that any transfer is lawful, including putting in place legal safeguards and ensuring that there are appropriate security arrangements.

In the case of transfers of personal data from the European Union ("EU") to destinations outside the European Economic Area ("EEA"), they will only be made on the basis of appropriate safeguards and in accordance with the applicable data protection laws, thus ensuring that Personal Data will be protected to the level which applies in the EU/EEA. In general, we achieve this by using EU Standard Contractual Clauses, which may be found at the European Commission's website at Standard contractual clauses for international transfers.

In case of transfers of personal data from other non- European entities Schreiber will only transfer to countries with an adequate level of protection of personal data, where there are adequate guarantees of compliance with the principles and rights of Data Subject.

Schreiber takes steps to establish that all recipients will provide an adequate level of data protection and that appropriate technical and organizational security measures are in place to protect Personal Data against accidental or unlawful destruction, loss or alteration, unauthorized disclosure or access, and against all other unlawful forms of processing.

When it is required by local law to process Sensitive Applicant Data, this information will only be transferred outside of the country of origin if permitted by applicable law.

9. Data retention periods

Schreiber will keep personal data as necessary or permitted by applicable local laws. After that, Schreiber will remove personal information from their systems and records and/or take the necessary steps to properly anonymize so that they cannot log in again.

If an application leads to an employment contract, relevant information Schreiber collects about the applicant during the hiring process will become a part of their employment record and retained in accordance with both: Schreiber´s privacy policies for employee data and the applicable laws.

The conservation periods of Personal Data in each country will mostly depend on the necessity for the establishment, exercise and defense of any claims as permitted by applicable law. Schreiber may also keep non-successful applicant data after the recruitment process is finished if they provide consent to store them for future recruitment processes.

The retention periods are the ones permitted by the national laws of each country, they are included in *Schreiber's Data Retention Policy* and in this Policy's Supplements.

Once the retention period is over, records that contain personal information and sensitive information as outlined above shall be destroyed in such a manner that information cannot be reconstructed or retrieved. Paper documents shall be shredded.

Electronic files shall be permanently and thoroughly deleted from all online and offline storage media using existing digital shredding techniques to prevent data reconstruction. If detailed historical transactions are to be retained, all personally identifiable data (name, home address, home telephone number) will be destroyed.

10. Rights of the Data Subject

Schreiber recognizes a number of rights in relation to the applicants' and employees' personal data. The exercise of these rights may be limited[1] by the legislation of national data protection as applicable:

- **Right of access**: right to obtain information about the personal data processed concerning themselves, including the categories of personal data processed, the purpose of the processing and the recipients or categories of recipients. The requester will receive a response in a maximum time of 1 month and will be provided with an electronic copy of their Personal Data.

- **Right of rectification**: right to request corrections to any inaccuracies. Schreiber shall provide a response in a maximum time of 1 month and provide a free, electronic copy of their personal data.

- **Right of withdrawal** ("right to be forgotten"): right to request the deletion of their personal data and stoppage its processing. Every piece of information regarding their person will be deleted after 1 month of receiving the request. Nonetheless, Schreiber may need to keep some personal data; and if we do, we will need to explain why.

- **Right to restriction of processing:** right to restrict the processing of their personal data so that it can only be processed with their consent, except:

    - for the establishment, exercise or defense of legal claims;

    - for the protection of the rights of another natural or legal person; and

    - for reasons of important public interest of the Union or of a Member State.

- **Right of portability:** right to receive personal data concerning themselves, which they have provided to Schreiber, in a structured, commonly used and machine-readable format, so that they may transmit their data to another entity. They also have the right to request transmission of their personal data from one controller to another through the company.

- **Right of opposition:** to object, on grounds relating to their particular situation, at any time to processing of personal data. The controller shall no longer process the Data Subject personal data unless they demonstrate compelling legitimate grounds for the

[1] In certain jurisdictions where Schreiber operates, the exercise of the listed rights may be subject to limitations. For instance, some of these limitations could arise from i) applicable law preventing their exercise, ii) potential harm or infringement on the rights of others, iii) when it would obstruct legal proceedings or the functions of authorities, iv) when the processing of personal data is necessary to fulfill legally acquired obligations by the Data Subject, among other considerations.

processing which override their interests, rights and freedoms as Data Subject or for the establishment, exercise or defense of legal claims.

- **Rights relating to automated decision making:** to not be subject to a decision based solely on automated processing. Schreiber does not make automated decisions in relation to recruitment.

In case the Data Subject exercises any of the abovementioned rights, Schreiber will comply to their request according to its Data Subjects´ Rights Policy. In the case the Data Subject is deceased, their rights may be exercised by a person appointed by them or, in the absence of an appointed person, by the Data Subject's successors.

11. Data Protection Officer

As in some jurisdictions where Schreiber operates, a Data Protection Officer is registered before local governmental authorities, if a Data Subject wants to exercise any of the abovementioned rights, has any complaints, inquiries or further questions, they may contact the Data Protection Officer (DPO) of the company through the email address: *dpo@schreiberfoods.com*, unless otherwise stated in the specific Supplement of the applicable country.

11.1. Functions of the Data Protection Officer

The primary role of a Data Privacy Officer ("DPO") and its equivalent in other jurisdictions, is to ensure personal information of staff, customers, providers or any other individual in relation with the company are processed in accordance with data protection regulations in each country where Schreiber is based. In order to ensure this compliance it shall:

- Ensure that controllers and Data Subjects are informed about their data protection rights, obligations and responsibilities and to advise and raise awareness about them;
- Give advice and recommendations to every Schreiber entity about the interpretation or application of the data protection rules, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- To provide advice where requested as regards the data protection impact assessment and monitor its performance;
- Ensure data protection compliance within Schreiber and help it to be accountable in this respect;
- Handle queries or complaints on request by partners, the controller, other person(s), or on its own initiative;
- Cooperate with national and local data protection authorities; and
- To act as the contact point for the data protection authorities on issues relating to processing, including prior consultation, and to consult, where appropriate, with regard to any other matter.

12. Changes to this data protection policy

Schreiber reserves the right to adapt or modify this Policy to at any time to reflect current data processing activities, complying at all times with the applicable laws. In case of any changes made, Schreiber will communicate such changes to the Data Subject either through the email provided for the treatment of its Personal Data or through a notification to the specified domicile.

SUPPLEMENTS FOR EACH COUNTRY WHERE SCHREIBER OPERATES

(IN ALPHABETICAL ORDER)

BELGIUM

If Data Subjects provide personal data as part of a recruitment process in Belgium, the following additional information applies.

The legal basis of Belgium for data storage and protection is the General Data Protection Regulation ("GDPR") 2016/679 and the Act of 30 July 2018 on the Protection of Natural Persons with Regards to the Processing of Personal Data ("the Act").

The national data protection authority is the **Data Protection Authority** (in Dutch: 'Gegevensbeschermingsautoriteit' / in French: 'l'Autorité de protection des données'). [https://www.autoriteprotectiondonnees.be / https://www.gegevensbeschermingsautoriteit.be]

The Data Controller in Belgium is:	**Address:**
Schreiber Foods Belgium, SPRL	Rue de Maredsous, Denée 13, 5537, Anhée Belgium

In addition:

1. If we process (reproduce/disclose) Data Subjects picture, we will ask for their active and explicit consent (by means of a paper consent form or by ticking a box electronically). This does not apply to pictures they have voluntarily provided (such as in CV, or via chat or video conferencing tools) or if Schreiber has another legal basis to process it (e.g. pictures on access badges, the relevant legal basis for which is our legitimate interest in ensuring the security of our premises).

2. We will ask for Data Subjects´ explicit consent if we carry out reference checks with third parties, and keep them informed when we request information from external organizations and persons.

3. Monitoring of diversity and equal opportunities: as there is currently no exception for Belgian companies from the prohibition on processing special personal data as part of a diversity policy, we will not process any special personal data for this purpose unless otherwise permitted under applicable law or will do so on an anonymous basis only.

4. When we use video surveillance, we will observe the provisions of national collective bargaining agreement no. 68.

5. The "Autorité de Protection de Données" underline that there is no requirements in respect of period of retention of employment´s personal data. However, good practices note five years after employment relationship was finished.

Neither regarding period of retention for applicant´s Personal Data there is a legal provision Subsequently, at the end of recruitment process personal data of applicant should be erased[2].

6. Without prejudice to any other remedies, the Data Subject also has the right to lodge a complaint to the APD-GBA at any time.

[2] Recrutement des candidats | Autorité de protection des données (autoriteprotectiondonnees.be)

7. In the event of a security breach, the Data Controller will notify the relevant national authority and the persons whose data has been compromised within 72 hours.

BRAZIL

If Data Subjects provide personal data as part of a recruitment process in Brazil, the following additional information applies.

The legal basis of Brazil for data storage and protection is the Brazilian General Data Protection Law ("LGPD") (in Portuguese**:** *Lei Geral de Proteção de Dados Pessoais*), Federal Law no. 13,709/2018 of August 14, 2018, which entered into force on September 18, 2021.

The LGPD is Brazil´s data protection regulation and applies to any processing operation of Personal Data.

For the purposes hereof:

- The processing operation of Personal Data is carried out in Brazil; and
- The purpose of the processing activity is aimed at the offering or provision of goods or services, or at the processing of data of individuals located in Brazil, or the personal data collected in Brazil.

The LGPD does not contain specific employment provisions, but its provisions cover employment data.

The monitoring of corporate email and internet use is allowed, but employees should be notified that they cannot expect privacy in the use of these work tools.

The national data protection authority is the National Data Protection Authority (in Portuguese: *Autoridade Nacional de Proteção de Dados* – ANPD), as created by the Law No. 13,709/2018 (LGPD) ANPD – Autoridade Nacional de Proteção de Dados (www.gov.br).

The Data Controller in Brazil is:	**Address:**
Schreiber Foods do Brasil Industria Alimenticia Ltda.	Avenida Manoel Ribas, Parque Industrial, Rio Azul, Parana, CEP 84560-000 Brasil

In addition:

1. The Data Controller and operator must keep records of the data processing operations they carry out, mainly when the processing is based on a legitimate interest.

2. The Data Controller responsibilities include: i) accepting complaints and communications from data subjects, providing clarifications and taking action; ii) receiving communications from the national authority and taking action; iii) guiding the entity's employees and contractors on the practices to be adopted in relation to the protection of personal data; and and iv) performing such other functions as may be determined in complementary rules.

3. In accordance with Article 18 of the LGPD, the Data Subject has the right to request the Data Controller the: i) confirmation of the existence of the processing; ii) access to the data; iii) correction of incomplete, inaccurate or outdated data; iv) anonymization, blocking or deletion

of data that are unnecessary, excessive or processed in violation of the provisions of this Law; v) portability of data to another service or product provider, upon express request and subject to commercial and industrial secrets, in accordance with the rules of the supervisory body; vi) deletion of Personal Data processed with the consent of the data subject, except in the cases provided for in article 16 of the LGPD; vii) information on public and private entities with which the data controller has shared data; viii) information on the possibility of not giving consent and on the consequences of refusal; and ix) revocation of consent, pursuant to article 8, paragraph 5 of the LGPD.

4. In this sense, the ANPD may determine that the controller must prepare an Impact Report on Protection of Personal Data, including sensitive data, referring to its data processing operations, pursuant to regulations, subject to commercial and industrial secrecy. The report must contain at least a description of the types of data collected, the methodology used for collection and for ensuring the security of the information, and the analysis of the controller regarding the adopted measures, safeguards and mechanisms of risk mitigation.

5. Brazilian data protection legislation does not include any specific provisions on processing personal data for equality and diversity purposes. Therefore, we do not process special personal data for these purposes without the Data Subject´s consent.

Any kind of background checks will be carried out only if strictly necessary in connection with the duties assigned.

6. The personal data of an employee shall be deleted after processing. However, Schreiber may reserve the right to retain data after its processing, as long as access by a third party is forbidden and exclusively for the following reasons:

a. Compliance with a legal or regulatory obligation by the controller;
b. Studies conducted by a research entity, ensured whenever possible, the anonymization of personal data, in this case the data shall be anonymized; and
c. Transfer to a third party, provided that it is in accordance with the legislation in force.

7. The LGPD does not address the post-termination of retention. Otherwise, it allows to retain personal data even after processing have been finished in order to comply with legal obligations (article 15 and 16).

8. In the event of a security breach, the Data Controller will notify the relevant national authority and the persons whose data has been compromised within reasonable period of time (article 48.1).

CZECH REPUBLIC

If Data Subjects provide personal data as part of a recruitment process in the Czech Republic, the following additional information applies.

The legal basis of Czech Republic for data storage and protection is the General Data Protection Regulation ("GDPR") 2016/679 and Act No. 110/2019 Coll. ("ZZOÚ").

The national data protection authority is Úřad pro ochranu osobních údajů. [http://www.uoou.cz/]

The Data Controller in Czech Republic is:	**Address:**
Schreiber Czech Republic s.r.o	Konopišťská 905, 256 01 Benešov, Czech Republic

In addition:

1. **Applicant´s Personal Data**. Pursuant to article 30 of Law number 262/2006, Schreiber may only ask for personal data strictly related to employment contract. Relevant information about academy grades, expertise, skills, and knowledge as regard role or position could be requested. By contrast, during recruitment process the requirements related to personal data to nationality, racial or ethnic origin, political opinions, trade union membership, religious or philosophical belief, sexual orientation are not allowed, unless special legal provision permit it and were necessary for compliance with that legal obligation to which Schreiber is subject (article 12 Law number 435/2004)[3]. Additionally, the applicant/candidate may ask Schreiber for legal requirements regarding special categories of personal data.

2. The maximum amount of time the personal data of an applicant can be kept is 2 years.

The maximum amount of time the personal data of an employee can be kept is 5 years after the termination of the contract.

3. Without prejudice to any other remedies, Data Subjects also have the right to lodge a complaint to the Úřad pro ochranu osobních údajů at any time.

4. In the event of a security breach, the Data Controller will notify the relevant national authority and the persons whose data has been compromised within 72 hours.

[3] https://www.uoou.cz/zamestnavatele/ds-5057/archiv=0&p1=2619

FRANCE

If Data Subjects provide personal data as part of a recruitment process in France, the following additional information applies.

The legal basis of France for data storage and protection is the General Data Protection Regulation ("GDPR") 2016/679 and the French Data Protection Act.

The national data protection authority is the Commission Nationale de l'Informatique et des Libertés (CNIL) http://www.cnil.fr/ https://www.cnil.fr/en/contact-cnil.

The Data Controller in France is:	**Address:**
Schreiber France S.A.S.	2, Grand rue, Cléry Le Petit, 55110France
	37 Avenue Gambetta, 5000 Bar-le-Duc, France

In addition:

1. Under French data protection legislation, Data Subjects have the right to give instructions on what happens with their personal data after their death.

2. Rights as a Data Subject can be restricted notably to avoid obstructing administrative investigations, inquiries or procedures, to safeguard the prevention, investigation, detection and prosecution of criminal offences, as well as of administrative enquiries, or to protect the rights and freedoms of others.

3. In cases of transfer of data to territories outside the European Union the data processor must inform the CNIL about such transfers, as well as shall provide the CNIL with a binding and enforceable commitment to apply appropriate safeguards to Data Subjects' rights and freedoms in the concerned third country.

4. In France, sensitive data can be processed, insofar as the purpose of the processing requires it, in operation *implemented by employers or administrations concerning biometric data strictly necessary to control access to workplaces and to equipment and applications used in the context of tasks entrusted to employees, agents, trainees or service providers*.

5. The maximum amount of time the personal data of an employee can be kept is 5 years after the termination of the contract (for instance, to keep evidences files related to payroll).

6. In case of personal data related to **applicants**, these could be retained for a certain period of time which must be defined by the Data Controller. This period of time includes the recruitment process and then the Personal Data must be erased or anonymized. For further information, you may check Fiche 9 from Guide Recruitment (*Les fondamentaux en matière de protection des données personlles et questions-responses)*[4]"

[4] https://www.cnil.fr/sites/cnil/files/atoms/files/guide_referentiel_-_recrutement.pdf#page=49

7. Without prejudice to any other remedies, the Data Subject also has the right to lodge a complaint to the Commission Nationale de l'Informatique et des Libertés at any time.

8. In the event of a security breach, the Data Controller will notify the relevant national authority and the persons whose data has been compromised within 72 hours.

GERMANY

If Data Subjects provide personal data as part of a recruitment process in Germany, the following additional information applies.

The legal basis of Germany for data storage and protection is the General Data Protection Regulation ("GDPR") 2016/679 and the Bundesdatenschutzgesetz (BDSG).

The national data protection authority is the German Federal Data Protection Authority (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit). In Baden-Wuerttemberg, the authority is Der Landesbeauftragte für den Datenschutz in Baden-Württemberg (https://www.baden-wuerttemberg.datenschutz.de)

The Data Controller in Germany is:	**Address:**
Schreiber Foods Europe GmbH	Im Unteren Feld 18, 88239 Wangen im Allgäu, Germany

In addition:

1. Once applicants have been rejected by the employer, their data shall be erased. However, unsuccessful applicants have the option of asserting claims under the General Equal Treatment Act (AGG). The time limit for asserting such claims under Section 15(4) AGGis 2 months. They then have a further 3 months following the assertion of the claim to take legal action under the Labor Court Act.

Due to the abovementioned time periods for asserting claims, as well as the time for processing and posting, we will keep applicant data for a maximum of 6 months so as to be able to defend any AGG claims[5].

2. The maximum amount of time the personal data of an employee can be kept is 4 years after the termination of the contract.

3. Under Section 26 of the Federal Data Protection Act (BDSG), personal data may be processed to detect crimes only if there is a documented reason to believe the Data Subject has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the Data Subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason.

4. Under Section 26 of the Federal Data Protection Act (BDSG), if Data Subjects´ personal data is processed on the basis of consent, Schreiber shall take into account whether they are able to freely give it. This may include where there is an economic advantage for them, or where we are pursuing the same interests. Consent will normally be requested in written or electronic

[5] https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/04/Ratgeber-Besch%C3%A4ftigtendatenschutz.pdf

form unless a different form is appropriate because of special circumstances. Where Schreiber relies on consent, we ensure Data Subjects are fully informed, and they have the right to withdraw consent.

5. We may also process special personal data on the basis of collective agreements if it were necessary to comply with legal obligations derived from labor law, social security and social protection law, and there was no reason to believe that the Data Subjects have an overriding legitimate interest in us not processing the personal data.

6. Without prejudice to any other remedies, Data Subjects also have the right to lodge a complaint to Der Landesbeauftragte für den Datenschutz at any time.

7. In the event of a security breach, the Data Controller will notify the relevant national authority and the persons whose data has been compromised within 72 hours.

INDIA

If Data Subjects provide personal data as part of a recruitment process in India, the following additional information applies.

The legal basis of India for data storage and protection is the Digital Personal Data Protection Act, 2023 ("DPDP Act"), the Information Technology Act, 2000 (the Act) and the Information Technology Rules, 2011 (IT Rules). The Indian Data Protection Supervisory Authority is the Data Protection Board of India ("DPBI") which has the power to carry out investigations for non-compliance and to impose fines.

The Data Fiduciary in India is:	**Address:**
Schreiber Dynamix Dairies Private Limited	215 Atrium Building, Unit 1018, 10th Floor, Andheri Kurla Road, Andheri East, Mumbai 400 0 93, India
	E-94, MIDC, Bhigwan Road, Baramati, Maharashtra 413133, India
	Plot No. 2B & 3A, A Block, Food Processing Park, Krishnagiri Road, Kuppam, Andhra Pradesh 517425, India
	International Mega Food Park, Village Dabwala Kala, Tehsil Arniwala, Fazilka Punjab 152124, India

The Data Fiduciary in India is:	Address:
	Pentagon Tower 2, Survey No.146, Pune-28, Maharashtra, India

In addition:

1. For the purpose of this Supplement, the Data Controller, in this case, Schreiber Dynamix Dairies Private Limited, will be referred to as the **Data Fiduciary**, which according to the DPDP Act refers to the entity that determines the purpose and means of processing Personal Data.

2. For the purpose of this Supplement, the Data Subject will be referred to as the **Data Principal** in accordance with the DPDP Act.

3. The Data Principal shall have the right to access, correction, rectification, completion, updating, erasure of its personal data for the processing of which they have previously given consent; including nominating individuals, consent as referred to in clause (a) of section 7 of the DPDP Act, and the right to grievance redressal[6], following any requirement or procedure under any law for the time being in force.

4. The Data Fiduciary will adopt all necessary technical and organizational measures to ensure the security of the Personal Data. In case of a Personal Data breach, the DPBI and the affected Data Principal will be immediately informed.

5. The Data Fiduciary will appoint a Data Protection Officer, so they can answer on behalf of the Data Fiduciary the questions, if any, raised by the Data Principal about the processing of its personal data as well as to exercise its right to grievance redressal. The inquiries shall be sent to the email: *dpo@schreiberfoods.com*.

6. By Section 13A of the Wages Act, employee records should be kept for 3 years after the last payroll entry in India.

7. The record retention of Personal Data is a minimum of 5 years for other HR documents as per the Retention Policy of the Data Fiduciary.

8. The maximum amount of time the personal data of an applicant can be kept is 1 year.

9. When disciplinary actions are taken that result in a legal process, the Data Fiduciary will retain the documents of its employees until the case is disposed from the appropriate Court.

[6] Refers to the availability of an easily accessible point of contact to address complaints from the Data Principal.

MEXICO

If Data Subjects provide personal data as part of a recruitment process in Mexico, the following additional information applies.

The legal basis of Mexico for data storage and protection is The Federal Law on the Protection of Personal Data held by Private Parties (the "Law") (in Spanish: *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*).

The national data protection authority is the National Institute for Transparency, Access to Information and Personal Data Protection ("INAI") (in Spanish: *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*) [INAI – Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales].

The Responsible of Personal Data in Mexico is:	**Address:**
Schreiber México, S.A. de C.V.	Circuito Mexiamora Norte 401 Parque Industrial Santa Fe I Silao, Guanajuato, Mexico CP 36275

In addition:

1. For the purpose of this Supplement, the Data Controller, in the case, Schreiber México, S.A. de C.V., will be called the **Responsible** for the treatment of Personal Data (treatment is understood as indicated in article 3 section XVIII of the "Law"), including sensitive, financial and patrimonial data of the Data Subjects.

2. The Data Subject by their own right or through their legal representative may request the Access, Rectification, Cancellation, or Opposition ("ARCO Rights") of their Personal Data, by any of the following means:

a) By written request addressed to the "Data Protection Department" at Schreiber Mexico's address; or
b) By email request to *confidencialidad@schreibermexico.com*.

3. The requests submitted must meet the requirements of Article 29 of the Law, including:

a) The name of the Data Subject and its address or other means to communicate the response to the request;
b) The documents that prove the Data Subject's identity or, if applicable, the legal representation of the Data Subject;
c) The clear and precise description of the Personal Data for which it seeks to exercise any of the ARCO Rights; and
d) Any other element or document relevant for the request.

4. Transferring Personal Data to other Schreiber entities will occur when a legal basis exists for the purposes stated in this Policy, it is instructed by the Data Controller or when required by a competent authority.

5. In compliance with Article 37 of the Regulation of the Law (in Spanish: *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*), Schreiber Mexico will keep the Personal Data for the time necessary for the fulfillment of the purposes that justified the processing, following all applicable provisions.

6. In compliance with Article 804 of the Federal Labor Law, Schreiber Mexico will keep the Personal Data of its Employees for the duration of the labor relationship and up to 1 year after its termination.

7. Once the purposes of the processing of Personal Data have been fulfilled, and when there is no legal or regulatory provision to the contrary, Schreiber Mexico will proceed to the cancellation and deletion of such data.

8. In the event of a security breach, the Data Controller will notify the INAI and the persons whose data has been compromised within 72 hours.

9. Any changes made to this Policy, will be duly notified by the Responsible to the Data Subject by the email provided for the treatment of its Personal Data, and in defect, its domicile.

PORTUGAL

If Data Subjects provide personal data as part of a recruitment process in Portugal, the following additional information applies.

The legal basis of Portugal for data storage and protection is the General Data Protection Regulation ("GDPR") 2016/679 and the Law no. 58/2019 of August 8, Personal Data Protection Law (in Portuguese: *Lei n.º 58/2019 de 8 de Agosto, Lei Da Proteção De Dados Pessoais)*.

The national data protection authority is Comissão Nacional de Protecção de Dados (CNPD). [http://www.cnpd.pt/]

The Data Controller in Portugal is:	**Address:**
Schreiber Foods Portugal, S.A.	Zona Industrial Rua A 6000-459 Castelo Branco, Portugal Avenida Santa Teresa do menino Jesus, 6, 8º D (Miraflores Office Center) 1495-161 Algés, Lisboa, Portugal

In addition:

1. The implementation video surveillance systems with sound recording are not allowed except in cases where the monitored premises are closed or where there is prior authorization from the national regulator.

Any personal data recorded by remote surveillance will generally only be used in the context of criminal proceedings. In that situation, such personal data may also be used to establish disciplinary responsibility.

2. Background checks will be carried out only if strictly necessary in connection with the duties assigned and to the extent that this would be allowed under the applicable law.

3. For the purposes of the mandatory notification of the data protection officer to the supervisory authority, in the context of Article 37 (7) of the GDPR, the Comissão Nacional de Proteção de Dados (CNPD) established the applicable procedure for notification. The specific form can be found on the CNPD website should be completed and submitted online.

4. The maximum amount of time the personal data of an applicant can be kept until the consent be withdrawn.

4.1. The processing cannot include Personal data related to private life but relevant information to valid the aptitude to work and be properly justified and written, or health unless the requirements linked to nature of the position and its task be justified and written.

4.2. The maximum amount of time the personal data of an employee can be kept is 3 years after they have left the company.

5. Without prejudice to any other remedies, Data Subjects also have the right to lodge a complaint to the Comissão Nacional de Protecção de Dados at any time.

6. In the event of a security breach, the Data Controller will notify the relevant national authority and the persons whose data has been compromised within 72 hours.

7. In general terms, the processing of Personal Data related to employment is not based on consent but on the Employement Agreement (article 28).

SINGAPORE

If Data Subjects provide personal data as part of a recruitment process in Singapore, the following additional information applies.

The legal basis of Singapore for data storage and protection is the Personal Data Protection Act of 2012 (No. 26 of 2012), amended by the Personal Data Protection (Amendment) Act 2020.

The national data protection authority is Personal Data Protection Commission [Personal Data Protection Commission Singapore | PDPC]

The Data Controller in Singapore is:	**Address:**
Schreiber Foods Asia Pte. Ltd	8 Marina Boulevard, Marina Bay Financial Centre, Singapore (0189981)

In addition:

1. In case of a data breach, Schreiber must notify the Commission as soon as practicable and in any case no later than three calendar days after the day the organization makes the above

assessment of a notifiable data breach. If the data breach results in, or is likely to result in, significant harm to the affected individual(s), an organization must also notify each affected individual in any manner that is reasonable in the circumstances.

2. When the Commission receives a complaint, it will first determine if the complaint involves the collection, use or disclosure of personal data. Afterwards, the Commission may be of the opinion that the complaint by an individual against an organization is more appropriately resolved by mediation, and may, under section 48G(1) of the PDPA, without the consent of the complainant and the organization, refer the matter to mediation under a dispute resolution scheme.

3. The maximum amount of time the Personal Data of an applicant can be kept is 2 years for consideration of future job opportunities (where applicable) from the date of submission of application.

The maximum amount of time the personal data of an employee can be kept is 2 years after the termination of the contract.

4. In the event of a security breach, the Data Controller will notify the relevant national authority and the persons whose data has been compromised within 72 hours.

SPAIN

If Data Subjects provide personal data as part of a recruitment process in Spain, the following additional information applies.

The legal basis of Spain for data storage and protection is the General Data Protection Regulation ("GDPR") 2016/679 and the Organic Law 3/2018 of December 5, 2018, on the Protection of Personal Data and Guarantee of Digital Rights ("LOPDGDD") (in Spanish: *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales*).

The national data protection authority is the Spanish Data Protection Authority ("AEPD") (in Spanish: *Agencia Española de Protección de Datos*) [www.aepd.es].

The Data Controllers in Spain are:	**Address:**
Schreiber Europe, S.L.	Calle de Anabel Segura nº11, Edificio C, 1ª Planta, Alcobendas, 28.108 Madrid, España
Schreiber Foods España, S.L.	Ctra. N-400 KM, 57.300, 45350 Noblejas, Toledo, España Ctra. Navalmorales, 45600 Talavera de la Reina, Toledo, España

The Data Controllers in Spain are:	**Address:**
Schreiber de Canarias, S.L.	C. de José Miguel Galván Bello, 0, 38009 Santa Cruz de Tenerife, Canarias, España

In addition:

1. In Spain, the protection of individuals in relation to the processing of personal data is a Fundamental Right protected by Article 18.4 of the Spanish Constitution, which is protected and guaranteed by the LOPDGDD. In addition, the set of labor legislation should be taken into account.

2. The Data Controllers stated above will be responsible of the processing of Personal Data for position fulfillment within each respective entity and the handling of employee data for individuals hired by each entity. Any transfer of Personal Data between entities will be clearly communicated to the Data Subject.

3. The maximum amount of time the personal data of an applicant can be kept is 1 year after the recruitment process is closed.

4. The maximum amount of time the personal data of an Employee can be kept, is: (i) for labor and social security data 4-5 years (depending on the specific scenario); (ii) for tax documentation 4 years; (iii) for prevention of money laundering documentation 10 years; (iv) and for video surveillance systems data 1 month, unless there is a need to keep them for a longer period to show that an infringement has taken place, in accordance with the applicable personal data protection requirements.

5. Pursuant to Art. 32 of LOPDGDD, Schreiber shall be obliged to block data in cases where the Data Subject exercises the right to rectification or erasure of the data.

6. The processing of Personal Data related to employment is not based on consent. Instead of consent, the processing is based on employment agreement, legal obligation and legitimate interest pursued by the controller.

7. Without prejudice to any other remedies, the Data Subjects also have the right to lodge a complaint with the AEPD at any time.

8. In the event of a security breach, the Data Controller will notify the AEPD and the persons whose data has been compromised within 72 hours.

9. The AEPD has issued a Guideline concerning personal data within the context of employment relationship.[7]

[7] https://www.aepd.es/documento/la-proteccion-de-datos-en-las-relaciones-laborales.pdf

UNITED KINGDOM

If Data Subjects provide personal data as part of a recruitment process in the United Kingdom, the following additional information applies.

The legal basis of the UK for data storage and protection is the Data Protection Act 2018.

The national data protection authority is the Information Commissioner's Office (ICO) [For the public | ICO].

The Data Controller in the UK is:	**Address:**
SCHREIBER FOODS UK LIMITED	Brunel Way, Stroudwater Business Park, Stonehouse, Gloucestershire GL10 3SX

In addition:

1. Under Schedule 1(8) of the Data Protection Act 2018, Schreiber Foods is allowed to require special data relating to gender and ethnicity when *necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained*. Schreiber, however, still require Data Subjects´ consent to manage this data.

2. The maximum amount of time the Personal Data of an employee can be kept is 6 years after the termination of the contract.

3. The maximum amount of time the personal data of an applicant can be kept is 1 year.

4. Without prejudice to any other remedies, Data Subjects also have the right to lodge a complaint to the Information Commissioner's Office at any time.

5. In the event of a security breach, the Data Controller will notify the relevant national authority and the persons whose data has been compromised within 72 hours.

UNITED STATES OF AMERICA

If Data Subjects provide personal data as part of a recruitment process in the United States of America, the following additional information applies.

The legal basis of United States for data storage and protection is a complex medley of national, state and local privacy laws and regulations.

The Data Controllers in the US are:	**Address:**
Schreiber International, Inc.	400 N. Washington, Green Bay, WI 54301
	2122 S Hardy Dr, Tempe, AZ 85282
	2522 S Pinnacle Hills Pkwy # 107, Rogers, AR 72758
	1112 West Fairview, Carthage, MO 64836
	127 W. Claxton Avenue, Carthage, MO 64836
	935 Nusbaum Place, Clinton, MO 64735
	10 Dairy St, Monett, MO 65708
	108 W North St, Mount Vernon, MO 65712
	208 East Dykeman Rd, Shippensburg, PA 17257

The Data Controllers in the US are:	**Address:**
	923 County Rd 176, Stephenville, TX 76401
	885 N 600 W, Logan, UT 84321
	2180 West 6550 North, Smithfield, UT 84335
	1695 Mills Street, Green Bay, WI 54302-2642
	920 Sextonville Rd, Richland Center, WI 53581
	2101 Bohmann Drive, Richland Center, WI 53581-0637
	807 Pleasant Valley Rd, West Bend, WI 53095
	5252 Clay Ave SW, Grand Rapids, MI 49548
Green Bay Machinery Co., Inc.	400 N. Washington, Green Bay, WI 54301
Schreiber Foods, Inc.	400 N. Washington, Green Bay, WI 54301

In addition:

1. There is no national authority for data protection in the US. However, the Federal Trade Commission has jurisdiction over most commercial entities, as well as has authority to issue and enforce federal privacy regulations to protect consumers against unfair or deceptive trade practices, including unjust privacy and data security practices. General State Attorneys have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states.

2. The maximum amount of time the Personal Data of an employee can be kept is generally 3 years after the termination of the contract, although it may change depending on the State where the Data Subject is based.

3. The maximum amount of time the Personal Data of an applicant can be kept is generally 1 year since the hiring decision, although it may change depending on the State where the Data Subject is based.