AIR LIQUIDE GROUP PRIVACY POLICY

Table of contents

INTRODUCTION

Air Liquide is committed to respecting the appropriate standards on privacy and data protection in all countries where it operates.

Data protection and privacy laws apply in several countries where Air Liquide is present and provide for obligations on the way Personal Data (i.e. any information relating to an identified or identifiable natural person) can be collected, used, disclosed. In addition, these laws grant individuals certain rights in relation to their Personal Data.

Thus, this Group Privacy Policy (Policy) aims to define a common framework on privacy and data protection within Air Liquide by setting out global rules to be applied by all Air Liquide entities and employees worldwide when collecting, using or transferring Personal Data from one country to another.

The Policy also aims to address the manner in which Personal Data from the European Economic Area (EEA) and Switzerland is handled to ensure that it is adequately protected when transferred within the Air Liquide Group outside the European Economic Area (EEA) and Switzerland in accordance with European Data Protection rules.

This Policy complies with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("GDPR")[1].

Air Liquide will ensure that all existing and newly hired employees are made aware of this Policy and are provided with appropriate training on this Policy on a regular basis. Furthermore, Air Liquide will be auditing compliance with all aspects of this Policy.

This Policy does not substitute any applicable national data protection and privacy laws and regulations in countries where Air Liquide operates. Local laws must be followed at all times and will take precedence over the Policy where they provide for stricter standards on privacy and data protection.

The Policy will be published on Air Liquide's website (www.airliquide.com) and intranets.

The Appendix 1 of this Policy provides all the definitions of the terms used in this Policy.

[1] As such, this Policy together with the Air Liquide Intra-Group Agreement, constitute Air Liquide's Binding Corporate Rules (BCRs) which have been approved by European Data Protection Authorities as providing an adequate level of protection to the processing and transfer of Personal Data within Air Liquide in accordance with the European Union Data Protection Directive (95/46/CE) which regulates privacy and personal data protection practices within the European Union.

1. SCOPE

This Policy sets out a framework for Personal Data processing activities including the collection, use and disclosure of Personal Data carried out by or on behalf of entities of the Air Liquide Group. A description of the structure and a list of the contact details of Air Liquide Group are available on Air Liquide's website (Air Liquide organisation & localisation).

It also addresses transfers of Personal Data within Air Liquide globally, including from group entities located in the EEA and Switzerland to group entities located outside the EEA and Switzerland to ensure that such data is adequately protected when being transferred. The world map of Air Liquide operations is available on Air Liquide's website (Air Liquide organisation & localisation).

Thus, the purpose of the Policy is to provide for global rules to be followed by all Air Liquide employees worldwide when handling and/or transferring the following Personal Data within all Air Liquide entities for the following purposes:

- Human resources Personal Data, including Personal Data of Air Liquide' current and former employees, temporary workers, trainees and job applicants (identity information, professional contact and organization information, contract information, salary and benefits related information, job qualifications and performance information, information for management and eligibility to share holdings, emergency contact information);

- Personal Data of Air Liquide' business contacts within customers, prospects and vendors (identity information, contract information, billing information, information provided as part of satisfaction surveys);

- Health Personal Data concerning individuals to whom Air Liquide may provide specific services to address health issues (in particular respiratory issues) and medical devices (identity information, contact information and pathology, prescription and treatment).

In case of a conflict between national laws and the rules set out in this Policy, the relevant Local or Regional Data Protection Officer or Information Protection Coordinator (as the case may be) will decide on the actions that need to be taken and in case of doubt will consult with the relevant Data Protection Authority.

2. GLOBAL RULES TO BE FOLLOWED BY AIR LIQUIDE GROUP FOR THE COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

Rule N°1 – Personal data must be collected for specific, explicit and legitimate purposes

European Data Protection rules require Personal Data to be collected for specific, explicit and legitimate purposes, i.e. the reasons for which Personal Data will be used.

This implies for Air Liquide to ensure that the purpose for which Personal Data is collected is:

- set within limits,
- relevant to Air Liquide's activity,
- clearly communicated to concerned individuals,
- legally allowed.

Also, it must be ensured that Personal Data collected for a specific purpose, as stated to the individual by Air Liquide, is not further used in a way which is incompatible with the initial purpose of collection.

The purposes for which Air Liquide processes Personal Data are:

- Management of human resources and payroll, including administrative management, career, performance and development plans management, compensation and benefits, management of recruitment, management of mobility and of expatriates, management of data on current and former employees holding or eligible to Air Liquide shares.
- Management of business relationships with customer, prospects and vendors including for billing, marketing and public relations, market analysis and reporting.
- Developing and maintaining global customer relationships. This includes providing healthcare support to individuals through appropriate healthcare services and products/medical devices, as well as researches and products and services development.

Rule N°2 – Ensure that there is a legal ground for the processing of personal data

Prior to any Personal Data collection and processing Air Liquide must make sure that one of the following conditions is met:

- Air Liquide has obtained consent from the concerned individual to the collection and processing of his/her Personal Data, **OR**
- The data processing is required in order to enter into a contract with the concerned individual or for the performance of the contract with the individual; **OR**
- There is a legitimate interest for Air Liquide to process the Personal Data, provided that this does not cause an unreasonable prejudice to the interests or rights of the concerned individuals ; **OR**
- The processing of Personal Data is necessary (i) to protect the individual's vital interest (i.e. in case of a life or death situation), or (ii) to enable Air Liquide to comply with a legal obligation, or (iii) to perform tasks of public interest (such as administering justice, exercising statutory, governmental or other public functions).

Furthermore, specific conditions apply to the collection of information on an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data for the purpose of unique identifying a natural person, health condition, and sex life or sexual orientation. Please refer to Rule n°5 to learn more.

Rule N°3 – Ensure that only adequate, relevant and limited personal data is collected and retained for a limited period of time

In consideration of the purpose and context of the processing as well as individuals concerned, Air Liquide must make sure that it will only collect Personal Data which is necessary and appropriate for the intended purpose of use and that such data is proportionate to the purpose of use.

Furthermore, Air Liquide will ensure that only accurate, complete Personal Data is processed and that the Personal Data is only kept as long as needed, and not "just in case", with respect to the purpose for which it was collected and is intended to be used. Moreover, Air Liquide will keep the Personal Data as far as possible up to date.

Rule N°4 – Be transparent to individuals whose personal data is collected on how their personal data will be used

Air Liquide must ensure that individuals, whose Personal Data it processes, receive clear and complete information notice, in an easily accessible way, on how and by whom their Personal Data will be used.

More specifically, Air Liquide will provide information to individuals on:

- The identity of the Data Controller of Personal Data, **AND**
- The purposes for which Air Liquide collects Personal Data, and where Personal Data is used in a new way, what such new purposes are.

In addition, depending on the country concerned and on the specific circumstances of the processing to ensure that such processing is carried out fairly, Air Liquide will also provide information on:

- The contact details of the Group Data Protection Officer,
- The legal basis for the processing,
- Where the processing is based on the legitimate interests pursued by Air Liquide, the legitimate interests pursued by Air Liquide or by a third party,
- The recipients or categories of recipients of the Personal Data,
- The period of time for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period,
- Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the Personal Data and of the possible consequences of failure to provide such Personal Data,
- The existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual,
- The rights of the individual under this Policy,
- The right to lodge a complaint either before the Data Protection Authority in the EU Member State of his/her habitual residence, place of work or place of the alleged infringement or before the competent court of the EU Member State where the Exporting Entity has an establishment or where the individual has his/her habitual residence,
- The means to exercise those rights,
- Any transfers of Personal Data outside the EEA or Switzerland and the existence or absence of an adequacy decision by the Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

The above listed information will be given upon collection of Personal Data or as soon as practicable thereafter.

Where the collection of Personal Data is performed indirectly (i.e. such as from a business partner, a recruitment agency), Air Liquide will make sure that the concerned individual is informed of the information listed above and of the following element:

- The categories of Personal Data concerned,
- From which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources.

As an exception to these rules, Air Liquide may not provide information notice to individuals where this would involve a "disproportionate effort" or in specific cases permitted by law. In determining what does not constitute a "disproportionate effort", Air Liquide will assess such effort against whether the absence of information would have a detrimental effect on individuals.

Rule N°5 – Ensure that the processing of sensitive personal data is allowed

Depending on the country where you are located, **specific restrictions may apply to the processing of Sensitive Personal Data** i.e. information relating directly or indirectly to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data for the purpose of unique identifying a natural person, health condition, and sex life or sexual orientation.

This is because Sensitive Personal Data, as defined above, are generally considered to be of a private nature and may present a risk to be used in a discriminatory way with adverse consequences for concerned individuals.

In accordance with European Data Protection rules, the collection of Sensitive Personal Data by Air Liquide is not allowed as a principle. However, there are exceptions, and Air Liquide can be authorized to process Sensitive Personal Data if:

- The processing of such data is necessary and relevant to achieve Air Liquide's business purposes, **AND**
- When one of the following conditions is met:
  - ✓ Air Liquide obtains consent from the concerned individual to the processing of his/her Sensitive Personal Data, **OR**
  - ✓ The processing of Sensitive Personal Data is necessary (i) to allow Air Liquide to comply with its obligations under employment law, or (ii) to protect the vital interests of the concerned individual or another person where this person is physically or legally incapable to give his/her consent (i.e. cases of life and death), or (iii) to establish, exercise or defend a legal claim; **OR**
  - ✓ The individual has made public his/her Sensitive Personal Data.

Air Liquide will not process personal data relating to criminal convictions and offences, unless it is carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

Contact the Local or Regional Data Protection Officer or Information Protection Coordinator (as the case may be) to obtain advice on whether you are allowed or not to collect Sensitive Personal Data in accordance with applicable data protection and privacy laws.

Rule N°6 – Uphold rights of individuals

In accordance with applicable data protection and privacy laws, individuals whose Personal Data is processed by Air Liquide shall be able to request Air Liquide:

- Whether Air Liquide holds Personal Data on him/her;
- To access to Personal Data processed by Air Liquide on him/her together with information on the purposes for which it is being processed and to whom the Personal Data is disclosed;
- To rectify or erase (in accordance with applicable laws and regulations) Personal Data that Air Liquide processes on him/her;
- To obtain restriction of processing (in accordance with applicable laws and regulations);
- To receive the Personal Data concerning him/her, which he/she has provided to Air Liquide, in a structured, commonly used and machine-readable format and to transmit those Personal Data to another controller without hindrance from Air Liquide to which the Personal Data have been provided;
- To object upon legitimate grounds to the processing of Personal Data by Air Liquide.

Air Liquide must ensure that individuals are informed on these rights in accordance with Rule N°4 above.

As there are often strict timescales for answering to such requests, they must be forwarded as soon as possible to the relevant Local or Regional Data Protection Officer or Information Protection Coordinator (as the case may be).

The procedure for handling individual's requests in relation to their Personal Data is further described under section 4 Complaints and requests in relation to this Policy below.

Rule N°7 – Ensure that individuals are able to object to direct marketing communications

Prior to sending any direct marketing communications, Air Liquide will ensure that concerned individuals have been informed on their right to object to the use of their Personal Data for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing, and have been provided with effective means to opt-out from receiving direct marketing communications and from profiling when it is related to such direct marketing.

Also, where an individual objects to receiving direct marketing, Air Liquide will accurately record this choice so as to ensure that no further direct marketing communications are sent to concerned individuals.

Rule N°8 – Prevent solely automated individual decision-making, including profiling

European data protection laws aim to prevent that decisions with respect to an individual be taken solely on the basis of automated Personal Data processing, including profiling, without any human intervention, as such decisions may produce legal effects or similarly significantly affect the concerned individual.

Where decisions are made by automated means, Air Liquide will ensure that individuals have the right to know the logic involved in the decision and will take the necessary measures to protect the legitimate interests of individuals.

Rule N°9 – Ensure security and confidentiality of personal data

Air Liquide will implement appropriate technical and organizational measures to ensure the security and confidentiality of Personal Data it collects and uses.

More specifically, Air Liquide will have in place appropriate measures taking into account the nature of the Personal Data involved and the risks presented by the processing, to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where processing involves transmission of personal information over a network, and against all other unlawful forms of processing.

In this respect, Air Liquide will take appropriate steps to inform and train Air Liquide employees regarding the security and confidentiality requirements that apply to the collection, use and disclosure of Personal Data they may process during the performance of their duties.

In addition, when Air Liquide wishes to entrust the processing of Personal Data to a Data Processor - either an entity of the group or an external service provider – , acting on its behalf, Air Liquide must ensure that a written agreement is put in place with the Data Processor in compliance with article 28 of the GDPR.

The relevant Local or Regional Data Protection Officer or Information Protection Coordinator (as the case may be) will notify without any undue delay any Personal Data breaches to the Group Data Protection Officer, as well as to the BCRs member acting as a controller when BCRs member acting as a processor becomes aware of a data breach, and individuals where the Personal Data breach is likely to result in a high risk to their rights and freedoms. Furthermore, any Personal Data breaches should be documented (comprising the facts relating to the Personal Data breach, its effects and the remedial action taken) and the documentation should be made available to the Data Protection Authority on request.

Rule N°10 – Implement appropriate measures for transfers

Where Air Liquide transfers Personal Data to entities of the Air Liquide Group located in countries outside the European Economic Area (EEA), or outside Switzerland, those transfers are covered by Air Liquide's BCRs and no additional measures are to be implemented to address these transfers of Personal Data.

Where Air Liquide intends to transfer Personal Data to a third party, i.e. which is not a member of the Air Liquide Group, located in countries outside the European Economic Area (EEA), or outside Switzerland, as these transfers are not covered by the BCRs:

- Air Liquide must ensure that those countries have been recognized by the European Commission as providing an adequate level of protection to Personal Data.
- If the country where the third party is located has not been recognized by the European Commission as providing an adequate level of protection, Air Liquide will implement appropriate measures in accordance with European Data Protection laws to ensure that Personal Data is adequately protected when being transferred to these countries by signing contracts for the transfer of Personal Data based on the standard contractual clauses adopted by the European Commission.
- Alternatively, and on an exceptional basis and only for non-massive and non-structural transfers, when the country where the third party is located does not provide adequate protection in accordance with the European Commission's decisions, Air Liquide may rely on one of the following conditions to transfer Personal Data to such country:
    - ✓ The concerned individual gives consent to Air Liquide for the transfer of his/her Personal Data, after having been informed of the possible risks of such transfers for him/her due to the absence of an adequacy decision and appropriate safeguards;
    - ✓ Air Liquide needs to carry out the transfer of Personal Data to perform or conclude a contract with concerned individual;

- ✓ The transfer of Personal Data is necessary (i) to protect the individual's vital interests (i.e. in case of a life or death situation), or (ii) to allow Air Liquide to establish, exercise or defend a legal claim, or (iii) for reasons of public interest;
- ✓ The transfer covers Personal Data publicly available (for instance from a public register).

Contact the Local or Regional Data Protection Officer or Information Protection Coordinator (as the case may be) to obtain advice on what needs to be done before transferring Personal Data in accordance with applicable data protection and privacy laws.

3. OBLIGATION TO BE RESPONSIBLE FOR AND ABLE TO DEMONSTRATE COMPLIANCE WITH THE BINDING CORPORATE RULES

Air Liquide hereby commits to comply with the accountability principle and be responsible for, and able to demonstrate, compliance with the BCRs.

In order to demonstrate compliance, Air Liquide needs to maintain a record of all categories of processing activities carried out in line with the requirements as set out in article 30.1 of the GDPR. This record should be maintained in writing, including in electronic form, and should be made available to the Data Protection Authority on request.

When required, data protection impact assessments will be carried out for processing operations that are likely to result in a high risk to the rights and freedoms of individuals. Moreover, where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk, the competent Data Protection Authority, prior to processing, will be consulted.

Air Liquide ensures that appropriate technical and organisational measures, which are designed to implement data protection principles and to facilitate compliance with the requirements set up by the BCRs in practice, is implemented (data protection by design and by default).

In order to avoid non-compliance with the BCRs:

i. Air Liquide warrants that no transfer is made to a BCR member unless the BCR member is effectively bound by the BCRs and can deliver compliance.

ii. The Data Importer commits to promptly inform the Data Exporter if it is unable to comply with the BCRs, for whatever reason, including when local laws and practices affect compliance with the BCR (see Section 6 of the BCR below).

iii. Where the Data Importer is in breach of the BCRs or unable to comply with them, the Data Exporter will suspend the transfer.

iv. The Data Importer will, at the choice of the Data Exporter, immediately return or delete the personal data that has been transferred under the BCRs in its entirety, where:

- the Data Exporter has suspended the transfer, and compliance with this BCRs is not restored within a reasonable time, and in any event within one month of suspension; or
- the Data Importer is in substantial or persistent breach of the BCRs; or
- the data importer fails to comply with a binding decision of a competent court or Competent Data Protection Authority regarding its obligations under the BCRs.

The same commitments apply to any copies of the data. The Data Importer commits to certify the deletion of the data to the Data Exporter.

Until the data is deleted or returned, the Data Importer continues to ensure compliance with the BCRs.

In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred personal data, the Data Importer warrants that it will continue to ensure compliance with the BCRs, and will only process the data to the extent and for as long as required under that local law.

For cases were applicable local laws and/or practices affect compliance with the BCR-C, the Section 6 of the BCR below applies.

Furthermore, Air Liquide will be auditing compliance with all aspects of this Policy, including methods and action plans ensuring that corrective actions have been implemented where necessary. Audits will be carried out every year.

In addition to the regular audits, the Data Protection Officers ("DPO"), the other privacy professionals, or any other competent function in the organisation may request specific audits (ad hoc audit) to be carried out.

In the event audits will be carried out by external auditors, such auditors will be entrusted under the following conditions: the external auditor must be independent and bound by an obligation of confidentiality by means of a contract in writing.

Regarding internal audits, the Air Liquide Group Audit Department will decide on the audit plan/programme and will conduct the audit. Air Liquide commits that DPOs should not be the ones in charge of auditing compliance with the BCRs, if such situation can result in a conflict of interests. Air Liquide also commits that the persons in charge of deciding on the audit plan/programme and of conducting the audit are guaranteed independence as to the performance of their duties related to these audits.

The results of the audits will be communicated to the Data Protection Officer or other privacy professionals, and to the Board of L'Air Liquide SA.

Air Liquide acknowledges that the Competent Data Protection Authorities can have access to the results of the audits upon request.

4. COMPLAINTS AND REQUESTS IN RELATION TO THIS POLICY

If an individual is concerned that his/her Personal Data have not been processed in accordance with this Policy, and/or wishes to exercise one of his/her rights as set out under Rule N°6 above, he/she can bring his/her complaint or address his/her request preferably in writing for the quality of treatment of the complaint or request:

- **for Air Liquide employee,** to the Local or Regional Data Protection Officer or Information Protection Coordinator (as the case may be) whose contact information are available on Air Liquide Intranet;
- **for other individual** via a specific form accessible via a link on the Air Liquide's institutional Internet website. Through this form the individual will be able to provide information regarding her/his complaint (personal contact information, nature of his/her relation with Air Liquide, type and object of her/his claim, the Air Liquide entity concerned by this complaint). Based on this information, the relevant Local or Regional Data Protection Officer or Information Protection Coordinator will initiate the treatment of the complaint. Data subject should provide valid contact information to ensure the efficiency of the procedure.

For all persons, the Group Data Protection Officer can also be contacted by regular post at: Data Protection Officer, 75, quai d'Orsay 75007 Paris, France.

Once such request and/or complaint is received, it will be handled by the Local or Regional Data Protection Officer or Information Protection Coordinator (as the case may be) who will lead the necessary investigations together with the relevant staff internally. The Local or Regional Data Protection Officer or Information Protection Coordinator (as the case may be) will also act as a point of contact and as such will inform the concerned individual of the outcome of his/her complaint and/or request as applicable.

Regarding individuals who are in the EU, if the individual is not satisfied by the replies, the individual has the right to lodge a complaint either before the Data Protection Authority in the EU Member State of his/her habitual residence, place of work or place of the alleged infringement or before the competent court of the EU Member State where the Exporting Entity has an establishment or where the individual has his/her

habitual residence. The individual has the right to lodge a complaint before the competent court and before a Data Protection Authority without having to first lodge a complaint with Air Liquide.

More details on the complaints and requests procedure is available in APPENDIX 3 – COMPLAINTS AND REQUESTS HANDLING PROCEDURE

5. THIRD PARTY BENEFICIARY RIGHTS

Individuals whose Personal Data will be collected and used in the EEA and Switzerland and transferred outside the EEA and Switzerland shall be able to enforce the principles set out in Appendix 6 as third party beneficiaries and pursue his or her complaint, in case of any breach of one of the enforceable elements of the BCRs as enumerated in APPENDIX 6 – PRINCIPLES WHICH ARE ENFORCEABLE AS THIRD PARTY BENEFICIARY RIGHTS, against:

- L'Air Liquide SA, if the entity responsible for a breach of the BCRs is established outside of the EEA or Switzerland, by bringing a complaint before the relevant local Data Protection Authority in the country in which L'Air Liquide SA is established (i.e. in France) or in the country in which the individual is employed or has his/her habitual residence and/or by bringing an action before the relevant local court in which L'Air Liquide SA is established (i.e. in France) or in the country in which the individual is employed or has his/her habitual residence; OR
- the Exporting Entity, if such entity is responsible for a breach of the BCRs, by bringing a complaint before the relevant local Data Protection Authority in the country in which the Exporting Entity is established or in the country in which the individual is employed or has his/her habitual residence and/or by bringing an action before the relevant local court in which the Exporting Entity is established or in the country in which the individual is employed or has his/her habitual residence

In addition, if the concerned individual can establish that he/she has suffered damage as a result of a breach of this Policy, he/she is entitled to receive compensation directly from:

- L'Air Liquide SA, if the entity responsible for a breach of the BCRs is based outside of the EEA or Switzerland, for the damage suffered; OR
- the Exporting Entity, if such entity is responsible for a breach of BCRs, for the damage suffered.

The concerned individual may be represented by a not-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf.

6. LOCAL LAWS AND PRACTICES AFFECTING COMPLIANCE WITH BCRS

Air Liquide will use the BCRs as a tool for transfers outside the EEA or outside Switzerland, only where an assessment of the law and practices in the third country of destination applicable to the processing of the Personal Data by an entity member of the Air Liquide Group acting as Data Importer, including any requirements to disclose personal data or measures authorising access by public authorities, do not prevent such entities acting as a Data Importer from fulfilling its obligations under these BCRs. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these BCRs.

When assessing the laws and practices of the third country of destination, the members of the Air Liquide Group have taken due account in particular of the following elements:

i. the specific circumstances of the transfers or set of transfers, including the length of the processing chain, the number of actors involved; envisaged onward transfers within the same third country or to another third country, including the type of entities involved in the processing (the Data Importer and any further recipient of any onward transfer); the purpose for which the data are transferred and processed; the categories and format of the transferred personal data; the economic sector in which the transfer or set of transfers occurs; the location of the processing, including storage, and transmission channels used.

ii. the laws and practices of the third country of destination, relevant in light of the circumstances of the transfer, including those requiring the disclosure of data to public authorities or authorising access by such authorities and those providing for access to these data during the transit between the country of the Data Exporter and the country of the data importer, as well as the applicable limitations and safeguards.

iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the BCRs, including measures applied during the transmission and to the processing of the personal data in the country of destination.

Air Liquide entities acting as Data Importers warrant that in carrying out the assessment they have made their best efforts to provide Air Liquide entities acting as Data Exporters with relevant information and agree that they will continue to cooperate with the Air Liquide entities in ensuring compliance with these BCRs.

Also, where any safeguards in addition to those envisaged under these BCRs should be put in place, L'Air Liquide SA, and the Data Protection Officer or Information Protection Coordinator (as the case may be) will be informed and involved in such assessment.

Air Liquide Group warrants that it will document appropriately the assessment, as well as the supplementary measures selected and implemented, and make it available to the Competent Data Protection Authority upon request.

Any Air Liquide entity acting as a Data Importer agrees to promptly notify any Air Liquide entity acting as a Data Exporter if, when using these BCRs as a tool for transfers, and for the duration of the BCRs membership, it has reasons to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the BCRs, including following a change in the laws of the third country or a measure (such as a disclosure request). This information is also provided to L'Air Liquide SA.

Upon verification of such notification, the Air Liquide entity acting as Data Exporter, along L'Air Liquide SA and the Data Protection Officer or Information Protection Coordinator should commit to promptly identify supplementary measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the Air Liquide entity, acting as Data Exporter and/or Data Importer to address the situation, in order to enable them to fulfil their obligations under the BCRs. The same applies if an Air Liquide entity acting as Data Exporter has reasons to believe that an Air Liquide entity acting as its Data Importer can no longer fulfil its obligations under this BCRs.

Where the Air Liquide entity acting as Data Exporter, along with the Liable BCR member and the Data Protection Officer or Information Protection Coordinator, assesses that the BCRs – even if accompanied by supplementary measures – cannot be complied with for a transfer or set of transfers, or if instructed by the Competent Data Protection Authorities, it commits to suspend the transfer or set of transfers at stake as well as transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the transfer is ended.

Following such a suspension, the Air Liquide entity acting as Data Exporter has to end the transfer or set of transfers if the BCRs cannot be complied with and compliance with the BCR is not restored. In this case, personal data that have been transferred prior to the suspension, and any copies thereof, should at the choice of the Air Liquide entity acting as a Data Exporter, be returned to it or destroyed in their entirety.

L'Air Liquide SA and the Data Protection officer or Information Protection Coordinator will inform all other BCR members of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of transfers is carried out by any other BCR member or, where effective supplementary measures could not be put in place, the transfers at stake are ended or suspended.

Data Exporters have the duty to monitor, on an ongoing basis, and where appropriate, in collaboration with Air Liquide entities acting as data exporter, developments in the third countries to which the Data Exporters have transferred personal data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

7. OBLIGATIONS OF THE DATA IMPORTER IN CASE OF GOVERNMENT ACCESS REQUESTS

Without prejudice to the obligation of the BCR members acting as Data Importers to inform the Data Exporter of its inability to comply with the commitments contained in the BCR (see Section 6 Local laws and practices affecting compliance with BCRs above):

i. The BCR member acting as Data Importer will promptly notify the Data Exporter and, where possible, the data subject (if necessary with the help of the Data Exporter) if it:
    a. receives a legally binding request by a public authority under the laws of the country of destination, or of an another third country, for disclosure of personal data transferred pursuant to the BCRs; such notification will include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided;
    b. becomes aware of any direct access by public authorities to personal data transferred pursuant to the BCRs in accordance with the laws of the country of destination; such notification will include all information available to the Data Importer.

ii. If prohibited from notifying the Data Exporter and / or the data subject, the Data Importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the Data Exporter.

iii. The Data Importer will provide the BCR member acting as Data Exporter, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the Data Importer is or becomes partially or completely prohibited from providing the Data Exporter with the aforementioned information, it will, without undue delay, inform the Data Exporter accordingly.

iv. The Data Importer will preserve the abovementioned information for as long as the personal data are subject to the safeguards provided by the BCRs, and shall make it available to the Competent Data Protection Authorities upon request.

v. The Data Importer will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and principles of international comity.

The Data Importer will, under the same conditions, pursue possibilities of appeal.

When challenging a request, the Data Importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the personal data requested until required to do so under the applicable procedural rules.

vi. The Data Importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It will also make it available to the Competent Data Protection Authorities upon request.

vii. The Data Importer will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

In any case, transfers of personal data by a BCR member to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society according the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (as to the consequences of such cases, see Section 6 Local laws and practices affecting compliance with BCRs above).

8. CREATION OF A NETWORK OF DPOS

Air Liquide commits to designate a DPO, where required in line with Article 37 of the GDPR, or any other person or entity (such as a chief privacy officer) with responsibility to monitor compliance with the BCRs.

The network of DPOs or other privacy professionals is described in IntroductionAPPENDIX 2 – ORGANISATION FOR DATA PROTECTION.

The DPO or other privacy professionals may be directly contacted by using the contact form accessible here: https://contactprivacy.airliquide.com/.

9. TERMINATION

A BCR member acting as Data Importer, which ceases to be bound by the BCRs may keep, return, or delete the personal data received under the BCRs.

If the Data Exporter and Data Importer agree that the data may be kept by the Data Importer, protection must be maintained in accordance with Chapter V of the GDPR which regulates the transfers of personal data to third countries or international organisations.

10. UPDATE OF THE POLICY

This Policy may be amended notably to take into account applicable data protection and privacy laws. To ensure that any changes to the Policy are recorded and made available, Air Liquide will:

- Keep an updated list of all changes to the Policy together with a list of Air Liquide Group members that are required to comply with it. This list will be held by the Digital Security Department of L'Air Liquide S.A.
- Notify all Air Liquide Group members of changes to the Policy.
- Inform concerned individuals whose Personal Data is processed in accordance with this Policy about any update of this Policy and of the list of BCR members, e.g. by way of publishing any new version without undue delay, and more specifically via Air Liquide's intranet with respect to employees, and via Air Liquide's website with respect to customer, prospects, vendors and other concerned individuals.

- Report at least once a year to the relevant Data Protection Authorities, any substantial changes to the Policy or to the list of Air Liquide Group members bound by it together with a brief explanation for such changes OR the absence of changes to the Privacy Policy.

Furthermore, Air Liquide will ensure that no transfer of Personal Data is made to any new member of the Air Liquide Group until such new member effectively adheres and is bound by this Policy and can deliver compliance.

Where a modification would possibly affect the level of the protection offered by the BCRs or significantly affect the BCRs (i.e. changes to the binding character), it must be promptly communicated to the relevant Data Protection Authorities, via the competent Data Protection Authority.

APPENDIXES

APPENDIX 1 – DEFINITIONS

Air Liquide: means any Air Liquide entity worldwide

Air Liquide Group: means L'Air Liquide S.A and all its subsidiaries worldwide.

Binding Corporate Rules (BCRs): means this Policy and the Third Party Beneficiary Agreement which are adhered by Air Liquide, for the purpose of ensuring an adequate level of protection for European Personal Data transfers.

Data Controller: means the Air Liquide entity which alone or jointly with others determines the purposes and means of the processing of Personal Data.

Data Exporter or Exporting Entity: means an Air Liquide Entity in the EEA or Switzerland that Transfers European Personal Data to a Relevant Country.

Data Importer: means an Air Liquide Entity in a Relevant Country receiving the Personal Data from a Data Exporter or Exporting Entity.

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

European Data Protection Authorities: means a Data Protection Authority in the European Economic Area or Switzerland.

Intra-Group Agreement: means the agreement between L'Air Liquide S.A and all L'Air Liquide S.A affiliated companies worldwide which grants third party beneficiary rights to individuals whose Personal Data are processed by Air Liquide.

Personal Data: means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

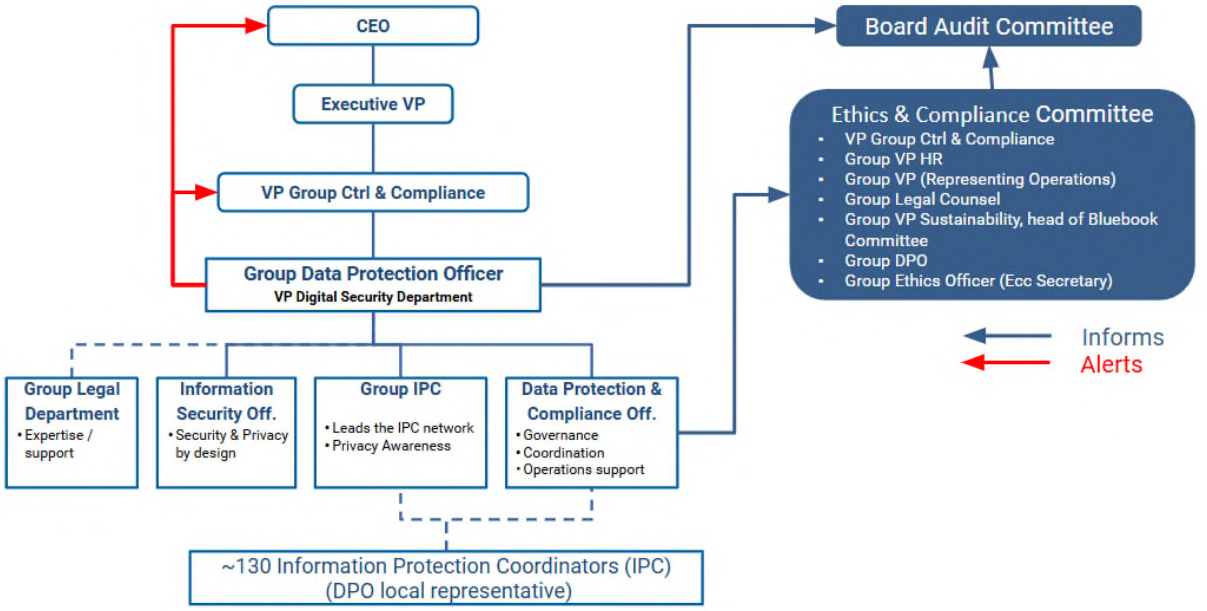
Relevant Country(ies): means the country(ies) other than those in the EEA and countries in respect of which the European Commission has issued an adequacy decision under Article 45of the GDPR

Responsible Entity: means

- L'Air Liquide SA if the entity responsible for a breach of the BCRs is based outside of the EEA or Switzerland; OR
- The Exporting Entity if such entity is responsible for a breach of the BCRs.

Sensitive Personal Data: means any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data for the purpose of unique identifying a natural person, data concerning health or sex life or sexual orientation.

APPENDIX 2 – ORGANISATION FOR DATA PROTECTION



APPENDIX 3 – COMPLAINTS AND REQUESTS HANDLING PROCEDURE

See separate document

APPENDIX 4 – LIABILITY

- Where the entity responsible for a breach of BCRs is established outside of the EEA or Switzerland, L'Air Liquide SA accepts responsibility for and agrees to take the necessary action to remedy the entity' acts and to pay compensation for any damages suffered by a European data subject resulting from the entity's violation of the BCRs.

  The burden of proof stays with L'Air Liquide SA to demonstrate that such entity was not liable for the violation of the BCRs resulting in the damages claimed by the individual. If L'Air Liquide SA can prove that such entity based outside of the EEA or Switzerland is not liable for the violation, L'Air Liquide SA may discharge itself from any responsibility.

- Where the Exporting entity is responsible for a breach of BCRs, the Exporting Entity accepts responsibility for and agrees to take the necessary action to remedy its acts and to pay compensation for any damages suffered by a European data subject resulting from its violation of the BCRs.

  The burden of proof stays with the Exporting Entity to demonstrate that it was not liable for the violation of the BCRs resulting in the damages claimed by the individual. If the Exporting Entity can prove that it is not liable for the violation, it may discharge itself from any responsibility.

APPENDIX 5 – COOPERATION WITH DATA PROTECTION AUTHORITIES

Air Liquide will cooperate with Data Protection Authorities and other relevant regulators where required by local law. To that end, all Air Liquide Group members:

- Undertake to co-operate and assist each other in order to respond in a reasonable time period to any relevant request from the competent Data Protection Authority, and
- Agree to be audited by competent Data Protection Authorities, including where necessary, on-site,
- Will cooperate with the Data Protection Authorities with regard to any decisions made by such authorities.

Any dispute related to the Competent Data Protection Authorities' exercise of supervision of compliance with the BCRs will be resolved by the courts of the Member State of that Data Protection Authority, in accordance with that Member State's procedural law. The BCR members agree to submit themselves to the jurisdiction of these courts.

APPENDIX 6 – PRINCIPLES WHICH ARE ENFORCEABLE AS THIRD PARTY BENEFICIARY RIGHTS

- Data protection principles (Art. 47.2.d of the GDPR and Section 1.3.1 of EDPB's Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules

- Transparency and easy access to BCRs (Art. 47.2.g of the GDPR and Section 1.3.1, Section 1.7 of EDPB's Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules)

- Rights of information, access, rectification, erasure, restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling (Art. 47.2.e and Art. 15, 16, 17,18, 21, 22 of the GDPR)

- Notification regarding rectification, erasure or restriction (Art. 47.2.e and Art. 15, 16, 17,18, 21, 22 of the GDPR).

- National legislation preventing respect of BCRs (Art. 47.2.m of the GDPR and Section 5.4.1 of EDPB's Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules)

- Right to complain through the internal complaint mechanism of the companies (Art. 47.1.i of the GDPR and Section 3.2 of EDPB's Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules)

- Cooperation duties with Data Protection Authorities relating to compliance obligations covered by this third party beneficiary clause (Art. 47.2.k of the GDPR and l, Section 4.1EDPB's Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules)

- Liability and jurisdiction provisions (Art. 47.2.e of the GDPR and f, Section 1.3.1, 1.4 of EDPB's Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules): in particular, the right to lodge a complaint with the competent Data Protection Authority in the Member State of his/her habitual residence, place of work or place of the alleged infringement, pursuant to art. 77 GDPR) and before the competent court of the EU Member States where the Data Controller has an establishment or where the individual has his/her habitual residence pursuant to Article 79 GDPR).

APPENDIX 7 – GDPR'S ARTICLES REFERRED TO IN THE BCRS

See separate document

AIR LIQUIDE GROUP PRIVACY POLICY
COMPLAINTS AND REQUESTS HANDLING PROCEDURE

Table of Contents

This document sets out the procedure which applies to all Air Liquide entities when a Data Subject (i.e. any individual whose personal data is processed by Air Liquide) raises a complaint in relation to a data protection and privacy matter or exercises any of his/her applicable rights under local data protection and privacy laws and regulations, and/or under the Air Liquide Group Privacy Policy.

1 Definition & terms

"Claim": means a complaint in relation to a data protection and privacy matter (including issue and breach) under local data protection and privacy laws or in relation to Air Liquide's Group Privacy Policy or a request concerning specific privacy rights provided for by local applicable data protection and privacy laws (right of access, rectification, erasure, restriction, portability, objection, not to be subject to decision based solely on automated processing, including profiling)

"DPO representative": means a Local or Regional[1] Data Protection Officer or Information Protection Coordinator (as the case may be) representing the Group Data Privacy Officer in the entities of the Air Liquide Group.

2 General procedure for handling Claims

A Data Subject may raise a Claim by contacting preferably in writing for the quality of treatment of the Claim:

- for Air Liquide employee, the DPO representative whom contact information are available on Air Liquide Intranet ;

- for other Data Subject, via a dedicated form accessible via a link on the Air Liquide's institutional Internet website. Through this form the individual will be able to provide information regarding her/his Claim (personal contact information, nature of his/her relation with Air Liquide, type and object of her/his Claim, the Air Liquide entity concerned by this Claim). Based on this information, the relevant DPO representative will initiate the treatment of the Claim. Data Subject should provide valid contact information to ensure the efficiency of the procedure.

[1] Please note that "Regional" can be activity or geographical level.

2.1 Type of the Claims

In several jurisdictions, local data protection and privacy laws provide that Data Subjects have a right to raise a Claim, i.e:

- ✓ a request regarding:
  - Access to personal data processed about them and obtain a copy of their personal data,
  - Rectification of personal data if it is found to be incomplete and/or inaccurate,
  - Erasure of personal data concerning them,
  - To obtain restriction of processing,
  - To receive the personal data concerning them, which they have provided to Air Liquide, in a structured, commonly used and machine-readable format and to transmit this personal data to another data controller without hindrance from Air Liquide to which the personal data has been provided,
  - To object to the processing of their personal data, on grounds relating to their particular situation, and to object free of charge to the processing of their personal data for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing,
  - Not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them,
- ✓ a complaint regarding:
  - A suspected data breach or issue related to data protection and privacy.

2.2 Who can make a Claim?

Claims may be made by all Data Subjects including employees, customers, suppliers, vendors and contact persons of Air Liquide, provided that their personal data are processed by Air Liquide in jurisdictions where local applicable data protection and privacy laws provide for a right to raise a Claim. Claims may also be raised by authorized representatives of the Data Subject where provided and in accordance with applicable laws.

The Data Subject can only make a request in respect of personal data relating to him/her.

2.3 Processing of the Claim

Each DPO representative is responsible for reviewing, processing and responding to all Claims from Data Subjects in her/his country or region. Where appropriate, the DPO representative will be assisted in this regard by other departments which may be involved during investigation, depending on the nature of the matter.
Furthermore, any Air Liquide employee who receives any Claim from a Data Subject in relation to data protection matters must immediately forward it to the DPO representative.

Once a Claim is received, the DPO representative will do his/her best to acknowledge receipt to the Data Subject in writing within 5 business days and in any case no later than 15 business days and will open a case-file (electronic or manual) for each Claim received. The file will contain the relevant documentation, including correspondence, both internal and with the Data Subject. The DPO representative will also maintain a register of all Claims received to log information on the date of receipt of the Claim, the way they were processed and resolved.

Where appropriate and depending on the nature of the breach, subject matter of the Claim, the DPO representative may delegate the handling of the Claim to the Legal or any other relevant department within Air Liquide. In such a case, the DPO representative will act as a point of contact for the Data Subject and the Air Liquide department designated to handle the complaint and will inform the Data Subject of the outcome of his/her Claim.

A Data Subject making a Claim will need to provide sufficient information to enable the DPO representative to identify him/her.

The DPO representative will consider and respond to a Claim from a Data Subject as follows:

a) He or she will ask the Data Subject making a Claim to prove his/her identity, for example, by providing a copy of his/her ID or any other satisfactory document to verify the Data Subject's identity.

b) He or she may request the Data Subject to provide any additional information as may be necessary or desirable to better define his/her Claim, or to help Air Liquide locate the relevant data or assess the validity of the Claim. The Data Subject making such Claim must provide appropriate documentation to the satisfaction of the DPO representative to substantiate the Claim.

c) He or she will assess if the Claim falls within the scope of any exemptions provided for by the applicable data protection and privacy laws and regulations, or other applicable country laws. He or she will also assess whether the Claim is abusive based on the frequency, the number, the repetitive or systematic nature of the Claims and can decide not respond to such Claims unless required by local law. If this is the case, he or she will fully document any decision to withhold the data on the basis of an exemption provided in the applicable data protection and privacy laws, or other applicable country laws. This will form part of the case-file, as described above.

d) He or she will where relevant contact the relevant departments and functions likely to process personal data concerning the Data Subject. Such departments and functions will co-operate with the DPO representative and supply any necessary information and data as the DPO representative deems appropriate.

e) Once he or she is satisfied that he/she has obtained all useful and complete information, he/she will ensure that the answer to the Claim does not infringe the data privacy rights of another Data Subject.

f) He or she will inform the Data Subject of the outcome of his/her Claim.

2.4 Response time

Data Subjects shall be provided with a response to their Claim, including through the implementation of any remedial actions, within a maximum delay of:

- One (1) month since the Claim was addressed to an Air Liquide Entity established in the European Union. That period may be extended by two further months where necessary, taking into account the complexity and number of the Claims. In such case, the DPO representative will inform the Data Subject of any such extension within one month of receipt of the Claim, together with the reasons for the delay **Or**

- Two (2) months since the Claim was addressed to an Air Liquide Entity established outside of the European Union

unless a shorter maximum period applies under applicable data protection and privacy laws.

3 Specific treatments in regard of the type of request, subject matter of the Claim

3.1 Right of access

The Data Subject has a right to request the following:

- to know whether Air Liquide processes personal data concerning him/her,
- the purposes for which such data are processed,
- the categories of data undergoing processing,
- the recipients or categories of recipients of such data,
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period,
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the Data Subject or to object to such processing,
- the right to lodge a complaint with a data protection authority,
- where the personal data are not collected from the data subject, any available information as to their source,
- a copy of the actual data processed about him/her.

Where provided by the local applicable law of the country where the Data Subject is located, if such processing of personal data may result in automated decisions, the Claim relating to the right of access may also cover the existence of automated decision-making, including profiling, and meaningful information about the logic involved in such automatic processing of data concerning the Data Subject, as well as the significance and the envisaged consequences of such processing for the Data Subject.

In addition to the general procedure, to handle specifically a Claim relating to the right of access:

a) Where the information to be provided as a result of such Claim contains data about another Data Subject, the DPO representative will provide the requested information only if:
   - it is possible to delete or conceal the data identifying the other Data Subject, or
   - the other Data Subject has consented to such a disclosure, or
   - in cases where a consent has not been sought or has proven impossible to obtain, and where it is impracticable to delete or conceal the data identifying the other Data Subject, the DPO representative determines that under the circumstances of that particular case it is appropriate and reasonable to provide the data.

The DPO representative will fully document any considerations and decisions in this respect and include it in the case-file described in Section 2.3 above.

b) The data to be provided to the Data Subject must be presented in an intelligible form. Any codes used must be clearly explained and the data translated in a language comprehensible to the Data Subject concerned.

c) The requested data will be provided to the Data Subject concerned in a written form or, where agreed, the Data Subject will be given the opportunity of viewing the requested data.

d) Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the requested data will be provided in a commonly used electronic form.

e) For any further copies requested by the Data Subject, the Air Liquide entity acting as data controller and concerned by this request may charge a reasonable fee based on administrative costs.

3.2 Right of rectification

The Data Subject may request that the personal data processed about him/her by Air Liquide be corrected where he/she considers such data inaccurate or incomplete.

On receipt of such a request, the DPO representative should verify that, taking into consideration the information communicated by the Data Subject concerned, the data processed are actually inaccurate or incomplete.

If the verification process shows that the data are actually inaccurate or incomplete, the DPO representative will instruct the relevant department or function to correct or complete the data. If the verification process shows the data in question to be accurate, the DPO representative shall make a note of the findings and communicate this to the Data Subject.

When the information has been rectified, the department or function will send a copy of the rectified data to the DPO representative who, in turn, will forward this to the Data Subject concerned to confirm that his/her request has been considered, and where appropriate, processed.

Where it is determined that incorrect and/or incomplete information was communicated to other Air Liquide and/or third party entities, the DPO representative will instruct the relevant department or function to communicate the rectified data to those entities for rectification, unless such operation is impracticable or involves a disproportionate effort.

3.3 Right to erasure

The Data Subject may request that the personal data processed about him/her by Air Liquide be erased where one of the following grounds applies:

a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

b) the Data Subject withdraws his/her consent to the processing of his/her personal data and there is no other legal ground for the processing;

c) the Data Subject objects to the processing of his/her personal data where the processing is based either on a public interest ground or on the legitimate interests of Air Liquide and there are no overriding legitimate grounds for the processing;

d) the Data Subject objects to the processing of his/her personal data where they are processed for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing;

e) the personal data have been unlawfully processed;

f) the personal data have to be erased for compliance with a legal obligation in the legislation of a country to which Air Liquide is subject; or

g) the personal data have been collected regarding children in the context of information society services.

By way of exception, the Data Subject may not obtain the erasure of his/her personal data where the processing of his/her personal data is necessary:

a) for exercising the right of freedom of expression and information;

b) for compliance with a legal obligation which requires processing by Union or Member State law to which Air Liquide is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in Air Liquide;

c) for reasons of public interest in the area of public health;

d) for archiving purposes in the public interest, scientific or historical research purpose in so far as the right of erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e) for the establishment, exercise or defence of legal claims.

In these cases, Air Liquide is not obliged to erase the personal data relating to the Data Subject.

On receipt of a request for erasure, the DPO representative should verify that, taking into consideration the information communicated by the Data Subject concerned, one of the above-mentioned grounds applies.

If the verification process shows that one of the above-mentioned grounds applies, the DPO representative will instruct the relevant department or function to erase the data. If the verification process shows that none of the above-mentioned grounds applies or that Air Liquide has a legitimate reason not to erase the data (i.e. one of the five above–mentioned exceptions applies), the DPO representative will make a note of the findings and communicate this to the Data Subject.

When the information has been erased, the department or function will notify the DPO representative who, in turn, will confirm to the Data Subject concerned that his/her request has been considered and that the data has been erased.

Where it is determined that the Data Subject's personal data was communicated to other Air Liquide and/or third party entities, the DPO representative will instruct the relevant department or function to inform those entities that the Data Subject has requested the erasure of that data, unless such operation is impracticable or involves a disproportionate effort.

3.4 Right to restriction of processing

The Data Subject may request from Air Liquide to obtain the restriction of the processing of his/her personal data where one of the following conditions applies:

a) the Data Subject contests the accuracy of the personal data for a period. The restriction of the processing will enable Air Liquide to verify the accuracy of the personal data;

b) the processing is unlawful and the Data Subject opposes the erasure of the personal data and requests the restriction of its use instead;

c) Air Liquide no longer needs the personal data for the purposes of the processing, but such personal data are required by the Data Subject for the establishment, exercise or defence of legal claims; or

d) the Data Subject has objected to processing on grounds relating to his/her particular situation pending the verification whether the legitimate grounds of Air Liquide override those of the Data Subject.

On receipt of such a request, the DPO representative should verify that, taking into consideration the information communicated by the Data Subject concerned, one of the above-mentioned conditions applies.

If the verification process shows that one of the above-mentioned conditions applies, the DPO representative will instruct the relevant department or function to restrict the processing of the personal data. If the verification process shows that none of the above-mentioned conditions applies, the DPO representative will make a note of the findings and communicate this to the Data Subject.

When the processing of the personal data has been restricted, the department or function will notify the DPO representative who, in turn, will confirm to the Data Subject concerned that his/her request has been considered and that the processing has been restricted. Before the restriction of processing is lifted, the DPO representative will inform the Data Subject.

Where it is determined that the Data Subject's personal data was communicated to third party entities, the DPO representative will instruct the relevant department or function to inform these third party entities that the processing of that data has been restricted, unless such operation is impracticable or involves a disproportionate effort.

3.5 Right to object

3.5.1 Right to object to direct marketing, including profiling to the extent that it is related to such direct marketing

The Data Subject has the right to object to receiving any promotional and marketing materials by post, telephone, email or any other form of communication provided by Air Liquide. The Data Subject also has a right to object to Air Liquide processing of his/her data for any direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing.

Upon receipt of an objection to direct marketing purposes, the DPO representative will ask the departments or functions concerned to cease processing the Data Subject's data for direct marketing purposes.

Upon receipt of an objection to profiling to the extent that it is related to such direct marketing, the DPO representative will ask the departments or functions concerned to cease profiling the Data Subject.

When the profiling of the Data Subject has ceased, the department or function will notify the DPO representative who, in turn, will confirm to the Data Subject concerned that his/her Claim relating to the right to object to direct marketing including profiling, has been considered and that the profiling has been ceased.

Upon receipt of an objection to profiling which is not related to direct marketing, the DPO representative will make a note of the findings and communicate this to the Data Subject.

3.5.2 Right to object on grounds relating to his/her particular situation

Air Liquide will abide by any request from a Data Subject to stop the processing of his/her data, including profiling, on grounds relating to the Data Subject's particular situation.

The Data Subject can object to the processing of his/her personal data which is based either on the necessity to perform a task carried out in the public interest or on the legitimate interests pursued by Air Liquide and where Air Liquide has no compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject and finds the request to be legitimate and appropriate.

On receipt of such a request, the DPO representative should verify that, taking into consideration the information communicated by the Data Subject concerned concerning his/her particular situation and Air Liquide's compelling legitimate grounds for the processing, this right applies. If the verification process shows that this right applies, the DPO representative will instruct the relevant department or function to cease the processing of the Data Subject's data concerned by the request. If the verification process shows that this right does not apply, the DPO representative will make a note of the findings and communicate this to the Data Subject.

When the processing of the personal data has ceased, the department or function will notify the DPO representative who, in turn, will confirm to the Data Subject concerned that his/her request has been considered and that the processing has ceased.

3.6 Right to portability

Air Liquide will abide by any request from a Data Subject to exercise his/her right to portability. The right of portability is composed of:

- a right for the Data subject to receive from Air Liquide his/her personal data which he/she has provided to Air Liquide and which Air Liquide must provide in a structured, commonly used and machine-readable format;

- a right for the Data Subject to transmit the data to another controller.

The right to portability applies when the following conditions are met:

a) the processing is based on consent or on the performance of a contract or pre-contractual measures, and

b) the processing is carried out by automated means.

If the verification process shows that the above-mentioned conditions apply, the DPO representative will instruct the relevant department or function to gather, in a structured, commonly used and machine-readable format:

i. data actively and knowingly provided by the Data Subject (for example, mailing, address, age, etc.),
ii. observed data provided by the Data Subject by virtue of the use of a service or a device restrict the processing of the data.

In contrast, inferred data and derived data which is created by Air Liquide on the basis of the data provided by the Data Subject is not within the scope of the right to data portability. The DPO representative will then, at the choice of the Data Subject provide the requested data to the Data Subject or transmit such data to another controller.

If the verification process shows that the above-mentioned conditions do not apply or the request of the Data Subject does not concern the data provided by the Data Subject or observed data, the DPO representative will make a note of the findings and communicate this to the Data Subject.

3.7 Right not to be subject to decision based solely on automated processing, including profiling

The Data Subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or similarly significantly affects him/her.

This right does not apply if the decision:

a) is necessary for entering into, or performance of, a contract between Air Liquide and the Data Subject;
b) is authorised by Union or Member State law to which Air Liquide is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests; or
c) is based on the Data Subject's explicit consent.

AIR LIQUIDE GROUP PRIVACY POLICY
GDPR'S ARTICLES REFERRED TO IN THE BCRS

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Article 16

Right to rectification

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

Article 17

Right to erasure ('right to be forgotten')

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

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

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

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 18

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 21

Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Article 23

Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Article 28

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:
    a. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
    b. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
    c. the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.
2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.
3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. [1]In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Chapter V – Transfers of personal data to third countries or international organisations – Articles 44 to 50

Article 44

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international

organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;
(b) binding corporate rules in accordance with Article 47;
(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47

Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
(d) the transfer is necessary for important reasons of public interest;
(e) the transfer is necessary for the establishment, exercise or defence of legal claims;
(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

Article 77

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 79

Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.