1. Binding Corporate Rules Controller

Safran adopted Binding Corporate Rules (BCR) in 2010.

In application of WP256 and during the review and validation of Controller BCRs Safran's: "While in accordance with article 46-5 of the GDPR, authorisations by a Member State or supervisory authority made on the basis of Article 26(2) of Directive 95/46/EC will remain valid until amended, replaced or repealed, if necessary, by that supervisory authority, groups with approved BCRs should, in preparing to the GDPR, bring their BCRs in line with GDPR requirements" and on the other hand : " Such updated BCRs can be used without having to apply for a new authorization or approval".

Safran's BCRs for data processing are appended to the Group's internal procedure in order to make them applicable and binding for all Safran companies, regardless of their location.

1. Purpose and legal framework of the Binding Corporate Rules (or BCR)

This document lists all the rules and obligations relating to the protection of Personal Data to be applied by Safran and its Subsidiaries for Data Transfer. These rules are commonly referred to as *Binding Corporate Rules* (hereinafter "*BCR*").
The Safran BCR are mentioned in the Group procedure for the Management of the Protection of Personal Data in the Group Procedures database.
They were approved in 2010 by the competent European personal data supervisory authorities and reviewed in 2018.
The BCR apply to all Safran Subsidiaries through the incorporation of BCRs into procedure for the Management of the Protection of Personal Data. The GRPs implemented are binding on all Safran Subsidiaries.
As such, Safran undertakes to comply with them, to ensure that they are respected by its Subsidiaries and enforced by its Employees.
The Safran BCR comply with the regulations listed below:

- the European Union (hereinafter referred to as "EU") regulation including the European Parliament and Council Regulation 2016/679 of April 27, 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as "GDPR");
- the documents of the article 29 working group and the European Data Protection Board: WP74, WP 153, 154, 155 and 256 relating to the drafting of the BCR.

2. Scope

Safran and its Subsidiaries process Data in an automated or non-automated (i.e. paper) way in the course of their activities, including:

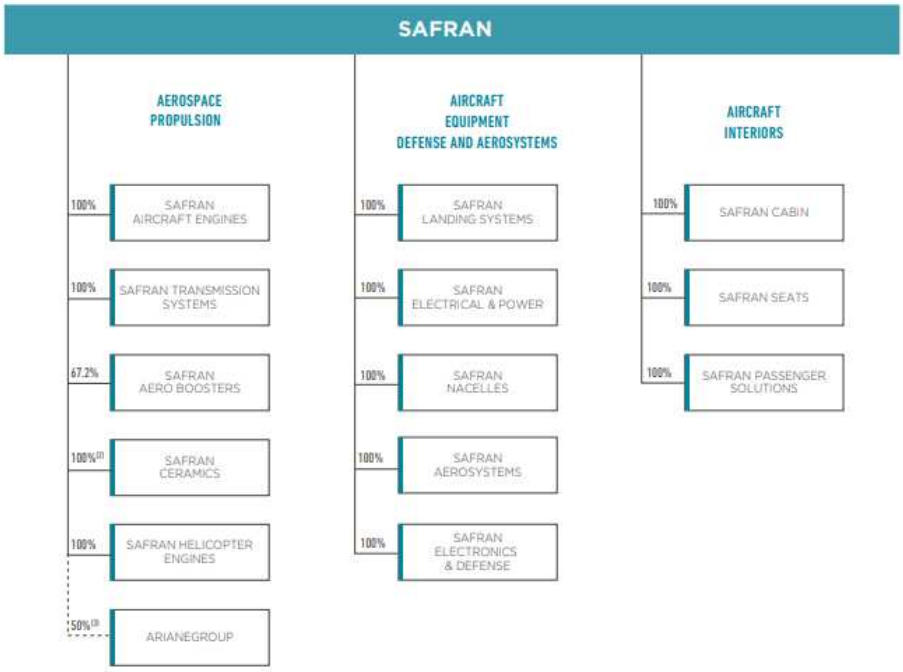
- Administrative management of the companies and Human Resources Management: recruitment, payroll, mobility, career management, training, job and skills forecasting, annual appraisal, benefits management, compliance with legal requirements (reporting to organizations), health, safety and environment;
- Business process management: work planning (e.g. directories, internal industrial projects or in relation with Partners, Customers or Suppliers, audits, quality), provision and security of IT resources and applications (e.g. messaging, IT tools, work and collaboration platforms, directories, IT media, applications and networks)
- Management of internal/external communication and marketing activities: external contact files, sending letters or emails of promotional information and/or news of products and services, providing photographs and videos for the purpose of organization of reports and events, publication and dissemination of communication media, leading the network of communicators, collaborative spaces and websites, online surveys and polls;
- Customers, Suppliers, Partners management.

In this context, Data Transfers are carried out by Safran and its Subsidiaries.
The Safran BCR apply solely to Data collected and processed by Safran and its Subsidiaries located in the EU and then transferred to one or many Subsidiaries whatever its localization.

All Data Subject in Transfers implemented by Safran or one of its Subsidiaries (Employees, Customers, Suppliers and Partners and Persons in Relationship with Safran) may avail themselves of the Safran BCR.
All new Safran companies in the EU and outside the EU will apply these BCRs in accordance with Group procedure Personal Data Protection Management.

3. Responsibility and structure

Tier 1 companies are defined in Safran's Reports en corporate Governance as companies that are wholly-owned directly by Safran SA, with the exception of Safran Aero Booster, in which the Belgian State holds a minority stake.
These Tier 1 companies are identified in Safran's Reports en corporate Governance available on the website: www.safrangroup.com.
Each Tier 1 Company that has signed a unilateral undertaking including the attached BCRs will be liable in the event of a breach of these BCRs by itself or by its own subsidiaries that have also subscribed to the BCRs.



Each of the Subsidiaries undertakes to collaborate with the tier-1[1] companies in the event of direct or indirect legal action.
When a Subsidiary that is submitted to these BCR located outside the EU breaches their content, the courts and other competent authorities as well as the data subjects may bring an action against the Safran company subject to the Group's procedure for managing personal data protection. This breach will then be treated as if it had taken place in the Member State where the responsible Safran company is located.
Each Safran Subsidiary qualified as a Data Controller within its scope must be able to provide proof of its compliance with the GDPR. This obligation includes keeping a record of processing activities, the conduct of impact assessments when necessary and the implementation of technical and organizational measures to ensure the implementation of principles related to the protection of personal data and to facilitate their respect as well as the respect of the contents of these BCR.
The registered office of Safran SA is located at 2, boulevard du Général Martial Valin, 75015 PARIS, France.
The list of the Safran companies to which the terms of the BCR apply is available in the Safran Reports en corporate Governance on the group website: www.safran-group.com[2].

4. Conflict between a national law and the requirements of the BCR

The Safran BCR provide a minimum standard applicable to Data transferred by Safran and its Subsidiaries who are submitted to the BCR.
In addition, Subsidiaries must comply with their local laws and regulations applicable to the Processing and the security and confidentiality of the Data.

[2] Table of subsidiaries and holdings Article R. 123-197.2° of the French Commercial Code

If the local legislation ensures a higher level of data protection than that recognized by the Safran BCR, the local legislation requirements take precedence over the BCR.
If the local legislation ensures a lower level of data protection than that recognized by the Safran BCR, the requirements stipulated in the Safran BCR take precedence over the local legislation concerning the transferred Data.
Any question or difficulty of compliance between a national law and the requirements of the Safran BCR is addressed to the Group Safran Data Protection Officer (hereinafter referred to as the "*Group DPO*")[3], who may consult the relevant European data protection supervisory authorities.
In addition, the Group DPO communicates to the competent supervisory authority the legal obligations incumbent on a Safran entity in a country outside the EU, where they may have a significant adverse effect on the guarantees provided by the Safran BCR.

5. General Rules for Personal Data Processing

Safran and its Subsidiaries undertake to observe the principles set out below.

5.1. Lawfulness of the Processing

Data must be processed in a fair and lawful manner.
It must be collected for specific, explicit and legitimate purposes. It must not be subsequently processed in a manner incompatible with those purposes.
The Data Processing concerned are based at least on one of the following legal grounds:

- The Consent of the Data Subject, or;
- the performance of a contract (work, purchase, sale, provision of services, etc.) to which the Data Subject is party, or the performance of pre-contractual measures taken at the request of the latter, or;
- the compliance with a legal obligation to which Safran or one of its Subsidiaries is subject, or;
- the safeguarding of the vital interests of the Data Subject or of another natural person, or;
- the performance of a public interest mission or the exercise of public authority in which Safran or one of its Subsidiaries is invested, or;
- the necessity for the legitimate interests pursued by Safran or one of its Subsidiaries or by a Third Party, unless the interests or fundamental rights and freedoms of the Data Subject prevail.

5.2. Quality of Personal Data

It must be adequate, relevant and not excessive (principle of minimization of the data collected) with regard to the purposes for which it is collected and, if necessary, updated.
The Data retention period must be defined and proportionate to the purposes of the Processing.

5.3. Category of Personal Data concerned

The list of Data Processing and Personal Data appears in Appendix 2 Nature, purposes of the Data, categories of Processing and Data Subject.

6. Processing of specific categories of Personal Data

6.1. Automated individual decisions

No evaluation or decision producing legal effects or affecting a person in a significant manner will be made solely on the basis of automated Data Processing, including Profiling.
If an automated decision is made on the basis of the conclusion or performance of a contract between Safran and the Data Subject or on the explicit Consent of the Data Subject, Safran and its Subsidiaries shall put in place appropriate measures to protect the rights, freedoms and legitimate interests of the Data Subject. The latter has the right to ask for explanations to understand the logic, express his or her point of view and challenge the decision.

6.2. Sensitive personal Data

[3] Safran.dpo@safrangroup.com

Processing of so-called sensitive Data, that is to say Data that reveals the racial or ethnic origins, political opinions, religious or philosophical beliefs or labor union membership, as well as the processing of genetic or biometric Data for the purpose of uniquely identifying a natural person, Data concerning the health, sexual life or sexual orientation of a natural person is prohibited except if:

- the Data Subject has given explicit Consent to the Processing of such sensitive Data, except where applicable law prohibits it, or
- the Processing is necessary in order to exercise the specific obligations and rights of the Data Controller in the field of the Employment Act to the extent permitted by national law, providing adequate safeguards, or
- the Processing is necessary in order to protect the vital interests of the Data Subject or another person when the Data Subject is physically or legally incapable of giving Consent, or
- the Processing concerns sensitive Data that is clearly made public by the Data Subject, or
- the Processing of sensitive Data is necessary for the establishment, exercise or defense of a legal claim, or
- Processing of sensitive Data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of medical services, and where such sensitive Data is processed by a health care professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of non-disclosure;
- Processing is necessary for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes, respecting the essence of the right to Data protection.

In the context of their activities, Safran and/or its Subsidiaries may be required to process sensitive Data. Each Processing of sensitive Data by Safran and/or its Subsidiaries is subject, where relevant in light of the GDPR, to a privacy impact assessment in order to protect the rights and freedoms of the Data Subjects.

6.3. Data relating to convictions and criminal offenses

Data Processing relating to criminal convictions and offenses or security measures is implemented only under the control of the public authority or carried out on the basis of a legal obligation providing guarantees of security and confidentiality.
Due to the nature of Safran's and its Affiliates' Data Processing and activities, these companies may be required to process Data relating to convictions and criminal offenses or security measures. The Safran entity responsible for processing will, in setting up said processing, respect the special provisions relating to this type of Data Processing.

7. Transfer of Personal Data outside the European Union

7.1. Intra-Group Personal Data Transfers

Data Transfers in the context of Processing not included in the scope of this BCR and carried out from a Safran member company located in the EU to a non-EU Safran member company are subject to:

- the “standard contractual clauses” issued by the European Commission or;
- any future instrument put in place by the European Commission or established by European regulations and subject to national administrative formalities.

7.2. Transfers between Safran subsidiaries

As an example, Safran can transfer data to the following countries: Australia; Belgium; Brazil; Canada; China; Czech Republic; Finland; France; Germany; Hong Kong; India; Japan; Malaysia; Mexico; Morocco; Netherlands; Poland; Russia; Singapore; South Africa; South Korea; Spain; Switzerland; Taiwan; Thailand; Tunisia; United Arab Emirates; United Kingdom; United States; Vietnam.

7.3. Transfer of personal Data to Co-contractors

In accordance with European Data Protection provisions related to data subprocessing, the implementation of Processing by a co-contracting party on behalf of a Data Controller must be governed by a contract or other legal act binding on both parties. The Co-contractor may be named as the Data Controller or Data Processor.

The Co-contractor named as Data Processor must act solely on instructions from the Data Controller, is responsible for the implementation of the security and confidentiality measures and must provide sufficient guarantees regarding the technical, organizational and confidentiality security measures governing the Data Processing to be performed.
Non-Safran Co-contractors located in the EU or in a country recognized by the European Commission as providing an adequate level of protection are bound by a written agreement stipulating the European rules for the subcontracting of Data Processing, including security and confidentiality.
Transfers to Co-contractors named as non-Safran Data Processors and located outside the EU are subject to the European regulations on subcontracting and those relating to the Transfer of Personal Data to Co-contractors located in countries outside the EU. For this purpose, these Data Transfers are governed by adequate "standard contractual clauses" or by any future instrument put in place by the European Commission or established by European regulations.
Transfers to Co-contractors named as non-Safran Data Controllers and located outside the EU are governed by adequate standard contractual clauses or by any future instrument put in place by the European Commission or established by European regulations.

8. Transparency of information and rights of the Data Subjects

8.1. Transparency of information

The Data Subjects are informed when the Data is Collected:

- of the identity and contact details of the Data Controller or his/her representative;
- of the contact details for the Data Protection Officer of the relevant company;
- of the purposes and the legal basis of the Processing;
- of the Data categories;
- of the categories of Data recipients;
- of the Data retention period or the criteria for determining it;
- of the legitimate interests of the Data Controller when Consent is not required;
- of the existence of rights of access, rectification, erasure, restriction, and portability;
- of the existence of a right to object;
- of the right to lodge a complaint with a supervisory authority and any competent jurisdiction;
- of the source from which the Data originates and, where appropriate, a statement indicating whether it is or is not from publicly available sources.

And if appropriate:

- of the possibility of withdrawing their Consent at any time without prejudicing operations undertaken prior to withdrawal;
- of the existence of Data Transfer outside the EU, the guarantee which protects the Data in the country of destination and the means of obtaining a copy or the place where it has been made available;
- of the existence of automated decision making, useful information about the underlying logic, and the significance and intended consequences for the Data Subject.
- To this end, information is brought to the notice of the Data Subjects by any means (document, intranet space, posting, user guide, etc.).
- When the Data has not been obtained from the Data Subject, the obligation to inform the Data Subject does not apply:
    - if the Data Subject is already informed or;
    - if the provision of this information proves impossible, if it involves a disproportionate effort or;
    - if the obtainment, communication or confidentiality are expressly established by the law.

Furthermore, each Data Subject has the right to inquire, at reasonable intervals and without delay or excessive costs, about the nature of the Data concerning them processed by Safran.

8.2. Rights of the Data Subjects

The Data Subject has the right:

- to access their Data: Data Subjects can obtain confirmation that their Data is processed or not. If Data is processed, Data Subjects may know: the purpose of Processing, the categories of Data concerned, the Recipients, the envisaged retention period or the criteria used to determine this duration, the existence of other rights, information regarding the source of the Data, the existence of automated decisions, information on the underlying logic, the significance and expected consequences, the existence of Transfers and the guarantees provided.
- to receive a legible copy of all their processed Data on request.
- to obtain the rectification of their Data, in particular if Data is incomplete or inaccurate, by providing proof of the veracity of these Data;
- to obtain the erasure of their Data, except legal obligations and the rights of third-parties lodging an objection: when it is no longer necessary, when they withdraw their Consent, when they exercise their right to object in particular concerning commercial prospection, when the Data is subject to unlawful processing or where required by law;
- to obtain restricted processing when the accuracy of the Data is disputed, when illegal Processing is subject to objection with retention of the Data, when it is no longer necessary for the Processing but used in a judicial framework, when the Data Subjects are waiting for a decision on their right to object;
- to obtain notice of the requested rectification, erasure or restriction of processing unless such communication proves impossible or requires disproportionate effort.
- to obtain the portability of their Data in an easily reusable form and transmit it freely to a third party when:
    - the Data has been supplied by the Data Subject, and the automated Processing is based either on the Consent of the Data Subject, or is the consequence of the performance of a contract with the Data Subject or the performance of pre-contractual measures taken at their request;
- to object, at any time, for reasons related to their particular situation, to Processing of their Data based on the legitimate interest of the Data Controller, unless the Processing in question is required by law or unless there are legitimate and compelling reasons prevailing over the rights of the Data Subject. When the objection is justified, Processing must cease.
- to not be subject to decisions based exclusively on automated Processing, including profiling;
- to be informed of bodies or any national law that may oppose compliance with the measures contained in these BCR (see §4 above);
- to ask Safran to provide evidence of compliance with the Data protection principle by design and by default;
- to lodge any complaint and/or claim to the Group DPO or to the Company DPO;
- to assert Safran's duty of cooperation with any competent supervisory authority (see §17 below)
- to lodge any claim with the supervisory authority or the competent jurisdiction in the event of a breach by Safran or one of its subsidiaries of the provisions of the BCR listed above. The Data Subject will have the opportunity to choose between the relevant supervisory authority based on their place of residence, place of work or the place where the alleged breach of the regulation took place. Similarly, the Data Subject has the freedom to choose the competent jurisdiction according to the place where the Data Controller and/or the Data Processor are established or the place of residence of the Data Subject.
- to obtain compensation for any material or non-material damage resulting from a potential infringement.

To exercise their rights, the Data Subject shall contact the Group DPO at: safran.dpo@safrangroup.com.

9. Rights of Third Party beneficiaries

As Third Party beneficiaries, the Data Subjects enjoy the rights recognized in § 8.2 of these BCR and in particular:

- the right to not be subject to decisions based exclusively on automated Processing, including profiling
- the right to compensation for any material or non-material damage as a result of an infringement of the rights guaranteed by these BCR;
- the right to lodge a complaint in the event of infringement of these BCR before the competent national courts and/or the competent European data supervisory authorities:

- Before the competent jurisdiction of the company (or its Subsidiary) located in the EU responsible for the non-compliant Processing;
- Before the jurisdiction of the company (or its Subsidiary) located in the EU subject to the Group's procedure for managing personal data protection ;
- To the competent European data supervisory authorities
  The competent national supervisory authority for personal data in France is the Commission Nationale Informatique et Libertés (CNIL), 3 place Fontenoy, TSA80715, 75334 PARIS Cedex 07, France.

The burden of proof regarding the alleged infringement rests with the company Safran headquartered in the EU and having agreed to take the responsibility and the necessary measures to repair the acts of its Subsidiaries related to the Safran BCR and located outside the EU.

10. Security and confidentiality of Personal Data

10.1. Protective measures

Safran and its Subsidiaries undertake to protect the Data against the destruction, loss, deterioration, unauthorized disclosure of Data transmitted, retained or otherwise processed, or unauthorized access to such Data, accidentally or unlawfully.
Technical and organizational security measures must be implemented with regard to the nature of the categories of Data to be protected and the risks associated with the intended purposes: pseudonymization; encryption; means to guarantee the confidentiality, integrity, availability and constant resilience of the systems and services; means allowing the restoration of availability and the timely access to data in the event of a physical or technical incident; procedures to test, analyze and regularly evaluate the effectiveness of technical and organizational measures to ensure the safety of Data Processing.

10.2. Data Breach

Safran and its Subsidiaries undertake to notify the competent European Data Protection Authority of any breach of security resulting in an accidental or unlawful impact (destruction, loss, alteration, unauthorized disclosure) on the Data and giving rise to a proven risk to the rights and freedoms of the Persons Concerned within a maximum of seventy-two (72) hours after becoming aware of the breach, by indicating :

- type of breach ;
- nature, sensitivity and volume of the Data concerned;
- ease of identification of the Data Subject by the use of the Data;
- seriousness of the consequences for individuals as well as their duration over time;
- potential characteristics of the Data Subject (e.g., a child or other vulnerable individual);
- special characteristics of the Data Controller;
- number of Data Subject.

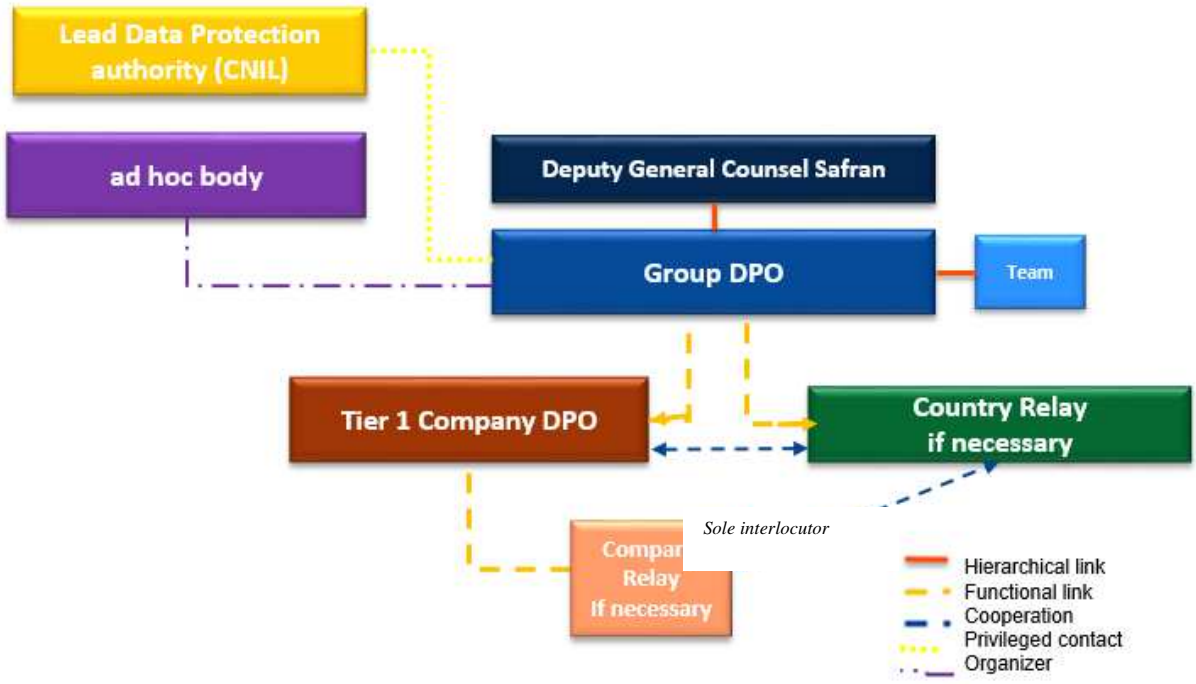
Safran and its Subsidiaries communicate in clear and simple terms to the Data Subjects as soon as possible any security breach involving a proven and high risk to their rights and freedoms.
Any person finding a Data breach must immediately notify one of the following persons: the Group Personal Data Protection Officer, the Personal Data Protection Officer of the company concerned, the Group or Company Information Systems Security Manager or the Group or Company Security Manager.
The person thus informed will contact the parties involved in order to quickly put an end to the breach and carry out the necessary formalities.

10.3. Privacy by design and by default

Safran implements technical and organizational measures from the design stage of Processing so that the principles of Data protection are taken into account right from the design stage.
Similarly, Safran is committed to minimizing data during Processing in terms of scope, retention period and accessibility.

11. Internal organization

The Safran Personal Data protection organization is based on the appointment of a Group Personal Data Protection Officer (“Group DPO”) and Personal Data Protection Officers for each tier-1 company (“Company DPO”), assisted if necessary by personal data protection relays within the company sites, Subsidiaries within or outside the EU as well as country relays.



12. Tasks of the DPOs

All Safran companies that meet the criteria of article 37 of the GDPR have appointed a personal data protection officer and, when the DPO has deemed it relevant, personal data protection relays within establishments, subsidiaries or countries.

12.1. Group DPO

The Group DPO ensures compliance of the Group with regard to personal data protection.
The Group DPO is tasked with putting in place internal Personal Data protection governance, adapting it to the context, coordinating it and ensuring its effectiveness.

The Group DPO is officially registered with the competent national personal data supervisory authority. As Safran has its head office in France, the lead authority is the French data protection authority, the CNIL (Commission Nationale de l’Informatique et des Libertés).

12.2. Company DPO

The Company DPO, whose appointment is mandatory within each tier-1 company, is responsible for ensuring compliance of the company and its subsidiaries and sub-subsidiaries, in France and abroad, with the personal data protection regulations.
If necessary the Company DPO may designate relays in the sites, subsidiaries and sub-subsidiaries in France and abroad.

The Company DPO is functionally attached to the Group DPO.

The Company DPO appointed for a tier-1 company is officially registered with the competent national personal data supervisory authority.

12.3. Personal data protection relays

On instruction from the Company DPO, a personal data protection relay can be appointed within the company sites, subsidiaries or countries. In such cases they are functionally attached to the Company DPO of the company with capital or operational responsibility.
If required by the local regulations, the relay is registered with the competent national personal data supervisory authority.

13. Audit program

The Group DPO carries out audits within the Group scope in France and abroad to verify in particular compliance with Safran BCR and applicable local regulations.

The Company DPOs can carry out audits within their scope (the companies for which they are responsible as well as the subsidiaries in UE and abroad).

Any relay can alert the Company DPO to major changes in the regulations and request that an audit be held. The Company DPO can initiate the audit, assisted by the relay.

The Group DPO has access to all audits and audit results conducted within the Group.

If necessary and relevant, the results of all the audits are made available to the network for the continuous improvement of good practices of the Group companies. The audits are made available to data supervisory authority by simple request.
If the audit results reveal serious and/or recurring non-compliance, the Group DPO or the Company DPO will inform the Director of the entity concerned.
If audit results reveal recurrent practices or non-compliance and/or affecting several companies, the Group DPO shall inform the Group Director of Audits and Internal Oversight ((hereinafter referred to as “DACI”).
The DACI regularly conducts, in accordance with its methodological reference, Internal Audits of management, performance and compliance of Group subsidiaries; the correct application of the BCR is then part of the compliance checks. In addition, and especially in light of the alerts reported by the DPO, the DACI can trigger specific Internal Audits addressing the points of fragility or identified non-compliance.

14. Communication

Safran facilitates the provision of its BCR to any Data Subject by posting them on the Safran intranet site, the Group procedures area and its corporate website.
Safran undertakes to communicate to Group companies via internal communication networks and to Persons Concerned via the corporate website this version and any substantial changes to its BCRs.

15. Training program

Safran implements training programs aimed at Employees having permanent or regular access to the Data or being involved in the collection of this Data or in the development of tools.
Training material on the Safran BCR is available on the intranet. For those who do not have access to the intranet, training materials are sent by email by the Group DPO, Company DPO, relays or the Human Resources Department.

16. Management of complaints and contacts

Any Data Subject may contact his or her company relay, the Group DPO or the Company DPO (or relay if any) for any request for information and/or complaint as a result of the infringement of these BCR by a Subsidiary.

- Groupe Safran Data Protection Officer
- Email: safran.dpo@safrangroup.com
- Internet: www.safran-group.com

After issuing an acknowledgment of receipt, the Group DPO or Company DPO (or relay if any) shall process the request within a reasonable time and in all cases within the legal deadline of a maximum of one month (may be extended to two additional months in the case of a complex request or numerous requests).
The answer is in the same format as the request, unless requested otherwise by the Data Subject and in accordance with the legal deadline and without costs.

In the event of a negative response from Safran to a complaint, the company will inform the Data Subject by justifying the content of the response and inform the person of their right to lodge a complaint with the supervisory authority or the competent jurisdiction (pursuant to the provisions of paragraph 8.2).
In the event of a positive response from Safran to any complaint, the company will inform the Data Subject of the decision and any corrective action taken. Similarly, the Data Subjects will be informed of their right to lodge a complaint with the supervisory authority or the competent jurisdiction (in accordance with the provisions of paragraph 8.2).
A Safran procedure specifies the procedures for managing the rights of individuals. This procedure is included in Appendix 2 of this document.

17. Cooperation with the European Data Supervisory Authorities

Safran undertakes to record any substantial changes to its BCR and to communicate them to the competent European data supervisory authorities.
No Transfer to a new entity of the Group of these BCRs shall be made within the framework of the BCRs before the new entity complies with Group Procedure on Personal Data Protection Management.
All Safran companies undertake to cooperate with the competent supervisory authorities and to accept in good faith any audit procedure carried out by one of the latter within the company. The suggestions and recommendations formulated by any competent supervisory authority shall be taken into account and passed on within the Safran company subject to such suggestion and/or recommendations.
The Group DPO maintains the updated list of Safran companies in the EU, which have signed the BCR Application Agreement, which it transmits once a year to the Lead Authority. He or she keeps track of and records updates and provides necessary information to the Data Subjects or to the personal Data supervisory authorities upon request.
In the event of a substantial change in the content of the BCR, which may affect the level of protection conferred by these BCR, the Group DPO will inform the European data supervisory authorities via the supervisory authority.
The communications addressed to a competent European Data supervisory authority by the Group DPO are made by any means capable of providing evidence of such communications.

18. Final provisions

The Safran BCRs are made binding by the incorporation of the present in Group Procedure on Personal Data Protection Management.
No Data Transfer can take place before the importing entity is legally bound by the Safran BCRs.
Any tier-1 Company or Subsidiary leaving the Safran scope loses the benefit of the Safran BCR. Nevertheless, Data collected while the tier-1 company or Subsidiary was a member of Safran must continue to be processed in accordance with the Safran BCR.
The Group DPO is responsible for updating the Safran BCR, which are validated by the competent European Data supervisory authorities through the intermediary of the Lead Authority.

Appendix 1: Definitions of terms used

The terms used will have the following meanings:

- "Lead supervisory authority ": Competent Data supervisory authority in the country where Safran has its headquarters and principal place of business.
- "Customers," "Suppliers" and "Partner": any individual with whom Safran has or intends to maintain business relationships, including prospects, consultants, shareholders or any other business partners.
- "Co-contractor": the natural or legal person who is a party to a legal transaction with Safran or one of its Subsidiaries.
- "Consent": any manifestation of free will, specific, enlightened and unambiguous by which the Data Subject accepts, by a declaration or by a clear positive act, that Personal Data concerning them may be subject to Processing.
- "Recipient": the natural or legal person, public authority, the service or any other body that receives the communication of Personal Data, whether or not it is a Third Party. The authorities that may receive communications of Personal Data as part of a particular inquiry, however, are not considered Recipients.
- "Personal Data" or "Data": any information directly or indirectly identifying a natural person, in particular by reference to one or more specific elements specific to their physical, physiological, psychological, economic, cultural or social identity (e.g. name, registration number, photograph, date of birth, fingerprint, etc.).
- "Employees": temporary or permanent Employees, expatriate or Employees on assignment, apprentices and trainees.
- "Subsidiaries": the European and non-European Subsidiaries of Safran companies.
- "Group" or "Safran": the Safran parent company, the companies of the Group in the EU and their Subsidiaries.
- "Data Subject": the person to whom the Processed Data relates.
- "Connected Person": job applicants, retirees and former Employees.
- "Profiling": any form of automated Data Processing consisting of using Data to evaluate certain personal aspects relating to a natural person, in particular in order to analyze or to predict elements relating to the job performance, economic status, health, personal preferences, interests, reliability, behavior, location or movements of this natural person.
- "Data Controller": the natural or legal person, public authority, department or any other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of processing are determined by national or community legislation or regulations, the Data Controller or the specific criteria to designate it may be determined by national or European law.
- "Data Processor": the natural or legal person, public authority, department or any other body that processes Personal Data on behalf of the Data Controller.
- "Third Party": the natural or legal person, public authority, or any other body other than the Data Subject, the Data Controller, the Data Processor and persons who, reporting directly to the Data Controller or the Data Processor, are entitled to process the Personal Data.
- "Processing": any action performed, in whole or in part, on Personal Data, by automated or non-automated means including: collection, consultation, recording, organization, storage, modification, usage, disclosure or erasure of Personal Data.
    - "Transfer": any access, communication, copy or transfer of Personal Data through the intermediary of a network or any communication, copy or transmission of such Personal Data from one medium to another, regardless of the type of support, insofar as this Data is intended to be processed in the destination country located outside the European Union.

Appendix 2: List of Data Processings

Nature, Purposes of the Data, Categories of Treatments and Data Subject

Typology of Treatment and purposes	**Nature and category of Processings**
• Administrative management of the companies and Human Resources Management: recruitment, payroll, mobility, career management, training, job and skills forecasting, annual appraisal, benefits management, compliance with legal requirements (reporting to organizations), health, safety and environment;	Employees, Connected Person • Identification Data • Personal life Data • Data relating to professional life • Computer Data • Economic and financial Data • Location Data • Health-related Data • - Social Security Numbers or Personal Registry Numbers
• Business process management: work planning (e.g. directories, internal industrial projects or in relation with Partners, Customers or Suppliers, audits, quality), provision and security of IT resources and applications (e.g. messaging, IT tools, work and collaboration platforms, directories, IT media, applications and networks)	Employees, Customers, Partners, Suppliers, • Identification Data • Data relating to professional life • Computer Data • - Login Data
• Management of internal/external communication and marketing activities: external contact files, sending letters or emails of promotional information and/or news of products and services, providing photographs and videos for the purpose of organization of reports and events, publication and dissemination of communication media, leading the network of communicators, collaborative spaces and websites, online surveys and polls.	Employees, Customers, Suppliers, Partners, Connected Person • Identification Data • Data relating to professional life
• Customers, Suppliers, Partners management,	Customer, Supplier, Partner : • Contact Data • Invoicing Data • - Trade Preferences

Appendix 3 Management of the rights of Data Subjects

The purpose of this procedure is to explain what these rights are and the process to follow in order to respond to a data subject's request to exercise these rights.

1. General outline

1. Objective of this guide

Regulations confer to data subjects rights on their personal data.

The term “data subjects” refers to all individuals concerned by a data processing, i.e. the persons whose data are collected and processed by Safran.

European regulation 2016/679 on the protection of personal data confers rights to data subjects who data are processed within the European Union (EU) and, provided that conditions are met, to companies established outside the EU.

2. Definitions

Personal data: any information regarding a natural person who can identified directly or indirectly by reference to an identification number or to one or more elements that are specific to him or her.

Data subject: an individual whose personal data are processed by the data controller.

Safran: designates Safran and its subsidiaries.

Data controller: natural or legal person or judicial entity, public authority, department or any other organization which determines the purposes (aims) and means (methods) of the data processing.

Data processing: any action performed in full or in part on personal data, automatically or otherwise (ex: collection, use, transmission, organization, erasing).

3. Scope of application

This guide is enforceable against Safran and its subsidiaries by any data subject whose:

- personal data are processed by Safran or its subsidiaries within the European Union irrespective of the location of the data subject ;
- personal data have been collected by Safran or its subsidiairies withtin the European Union then transferred outside whatever the location of the data subject;
- personal data have been collected by Safran or its subsidiairies outside the European Union when the processing targets a data subject located on the European Union territory to offer a good or a service whether free of charge or against payment or to monitor his/her behavior.

  Example: A Safran company established in the US collecting the data of the users of a mobile application addressed to an European public.

2. Rights of data subjects

4. Right of information

2.1.1 Definition

The right of information is a fundamental right for data subjects. It aims at explaining which processings are made on personal data and what are the modalities to exercise their other rights.

2.1.2 Content

The information is given **at the time of data collection from the data subject**. The information must be available at any time during the existence of the processing. It must as well be recalled and adapted following events such as data breaches[4] or the substantial modification of the processing.

It contains:

- the identity and the contact details of the controller, either of Safran or one of its subsidiaries, or its representative;
- the contact details of the data protection officer;
- the purposes of the processing for which the personal data are intended and the legal basis for the processing;
- the categories of personal data collected;
- the recipients or categories of recipients of the personal data;
- the retention period of the personal data or the criteria used to determine that period ;
- the legitimate interests pursued by the controller when consent is not required;
- the existence of the rights of access, rectification, erasure, restriction and portability;
- the existence of the right to object;
- the right to lodge a complaint with the data protection authority;
- A telephone number, postal or electronic address through which the person concerned can exercise its rights.

And where pertinent:

- the possibility to withdraw the consent at any time without affecting any operations performed before such withdrawal;
- the existence of transfer of personal data outside the European Union, the suitable safeguards and the means to obtain a copy of them or where they have been made available;
- the existence of automated decision-making, meaningful information about the logic involved and the significance and the consequences for the data subject;
- whenever personal data are reused, the data subject is informed of the new purpose and of any useful necessary informations;
- **In France only**, the right to define specific or general directives on the retention, the erasure and the communication of the data subject's personal data after his/her death.

When the information is not collected directly from the data subject, Safran has one month to inform the person and must indicate the source from which personal data have been collected and specify if they are issued from public or non public sources.

2.1.3 Modalities

The information must be written, easily accessible and understandable. It must allow the data subjects to understand the consequences of the processing on their private life and their personal data.

2.1.4 Modification of the information

In case of substantial changes to the processing, data subjects must be informed sufficiently in advance in order for them to have enough time to:

- Understand the modification and its consequences;
- Exercise their rights;
- Remove their consent if it is necessary for the data processing.

5. Right of access by the data subject

A data subject can obtain the confirmation as to whether or not his/her personal data are being processed.

Where that is the case, the data subject has the right to know:

[4] Cf. GRM-0156 Personal data breach.

- the purpose of the processing;
- the categories of personal data concerned;
- the recipients;
- the duration for which their data will be stored or the criteria used to determine such duration;
- the existence of his/her other rights contained in this paragraph 3;
- the information on the source of the personal data where the data is not collected from the data subject;
- the right to lodge a complaint with a data protection authority;
- the existence of automated decision-making meaningful information about the logic involved and the significance and the consequences for the data subject;
- the existence of transfer of personal data outside the European Union, the suitable safeguards.

Depending on the choice of the data subject, his/her health data can be communicated directly to him/her or through a chosen practitioner.

The right to access is personal. Therefore, a data subject can only access his/her personal data.

6. Right to rectification

A data subject has the right to obtain:

- without undue delay[5] the rectification of inaccurate personal data concerning him/her;
- the completion of his/her personal data by providing evidence of their veracity.

7. Right to erasure

A data subject has the right to obtain the erasure of his/her personal data without undue delay where:

- such personal data are no longer necessary for the initial purpose of their collection/processing;
- the data subject withdraw his/her consent given specifically for a processing where no other legal ground justifies the processing;
- the data subject exercise his/her right to object and there are no overriding legitimate grounds;
- the personal data have been unlawfully processed;
- a legal obligation requires it.

The personal data must be erased without undue delay.

The personal data cannot be erased if the processing is based on a legal obligation or for the establishment, exercice or defense of legal claims.

When Safran has made public data subject to a procedure of erasure, Safran must take all reasonable measures (technical, organizational etc.) to inform third companies to obtain the delition of any link to these data and any other existing copy/reproduction.

8. Right to restriction of processing

The right to restriction allow for the suspension of a processing (i.e. the use of the data) during the processing of a request from a data subjects concerning his/her other rights.

Example: the restriction of a processing of one data subject's data who contested the accuracy of his/her data and filed a request for rectification.

The data subject has the right to restrict the processing of his/her personal data where:

[5] cf. 5.1 Turnaround time

- the accuracy of such personal data is contested by the data subject for a period enabling the controller to verify their accuracy;
- the processing is unlawful and the data subject opposes the erasure and requests the restriction of their use instead;
- the controller no longer needs the personal data for the pruposes of the processing but they are required by the data subject for the establishement, exercice or defense of legal claims;
- the data subject has objected to the processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Once the data has been restricted, with the exception of storage, the personal data can only be processed with the data subject's consent or for the establishment, exercise or defense 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 European Union or a member State.

The data subject is informed by the controller before the restriction of processing is lifted.

9. Right to data protability

Any data subject has the right to receive his/her data in the format easily reusable and the right to freely transmit those data to another controller.

The right to data portability applies to data processing based on:

- the consent of the data subject whether the data processed is categorized as sensitive or not;
- the processing is necessary for the performance of a contract to which the data subject is party;
- the processing is carried out by automated means either based on: the data subject's consent or the performance of a contract entered into with the data subject.

The right to data portability applies only if the data:

- is personal data concerning the data subject;
- if those data where actively and **knowingly provided** by the data subject or if those data where generated by and collected from his/her activities or observed on his/her behavior (excluding any result of any subsequent analysis of his/her behavior made by safran);

When it is technically possible, the data subject can ask the controller to directly transfer his/her data to a third party.

10. Right to digital death

In **France**, the data subject has the right to define specific or general directives on the retention, the erasure and the communication of his/her personal data after his/her death.

The directives are recorded with a digital trustworthy third party certified by the French data protection authority. Those directives can be amended or revoked at any time by the data subject.

In the absence of any directive, the heir of the data subject can exercice those rights to the extend necessary for :

- the organization and the settlement of the succession of the deceased;
- the consideration of his/her death to close user accounts;
- the objection to the pursuit of the processing concerning him/her;
- the update of his/her personal data.

This right can not override any legal obligation on retention or archiving.

11. Right to object

At any time, the data subject has the right to object, on grounds relating to his/her particular situation, to a processing on his/her data based on the legitimate interest pursued by the controller or a third party.

Except when compelling legitimate interest overrides the interests of fundamental rights and freedoms of the data subject or for the establishment, exercice or defense of legal claims, the controller cannot process those data.

The objection on direct marketing purposes can not be exempted.

12. Right of claim and action

Any data subject can lodge a claim with Safran or its subsidiaries as a result of the infringement of this guide or of any applicable regulation on data protection.

Any data subject can lodge a complaint with the competent data protection authority if he/she considers that Safran infringed the regulation on data protection.

He/she can as well refer to a court when he/she wants to contest the decision of the said authority or the lack of decision within three months following the introduction fo a request.

Any data subject can refer to a court if he/she considers that his/her rights were breached by a processing carried out by Safran.

Any decision from Safran, from its subsiadries or from a data protection authority may be subject to an effective judicial remedy in the courts of the State of the European Union in which the data subject is or of the State in which Safran is located.

13. Right to compensation for damages

Any person who suffered a direct material or non-material damage as a result of the infringement of the European regulation on data protection has the right to receive compensation from Safran for the damage suffered.

When Safran is defined as data processor, Safran is responsible only when it has not respected the legal obligations or if it has acted outside or against the guidelines given by the data controller.

Safran is not liable when it is not responsible for the damage.

3. Limit for exercice rights

14. Limitation to the right of information

The information of the data subject is not mandatory:

- When the data was collected directly from the data subject:
  - the data has been collected directly from the data subject and he/she has been duly informed of all points listed at “3.2.1 Content”. The controller must be able to demonstrate the aforementioned conditions.
- When the data was not collected directly from the data subject:
  - the data has been collected directly from the data subject and he/she has been duly informed of all points listed at “3.2.1 Content”. The controller must be able to demonstrate the aforementioned conditions;
  - the provision of such information is impossible or would require a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or in so far as providing the information is likely to render impossible or seriously impair the

achievement of the objectives of that processing. The controller must be able to justify its choice;

- The controller is subject to a national or European legal obligation requiring to obtain or disclose personal data and which provides appropriate measures to protect the data subject's legitimate interests;
- the personal data must remain confidential subject to an obligation of professional secrecy regulated by European or Member State law

15. Abusive or unfounded requests

When claims of data subjects are manifestly unfounded or excessive, in particular because of their repetitiveness, Safran may :

- charge a reasonable fee;
- refuse to act on the request.

Safran shall bring the proof of the manifestly unfounded or excessive character of the claim.

Safran may refuse to act on the request if the identification of the data subject can not be brought.

The exercice of the right in particular the right to access and the right to portability may not prejudice the rights and freedoms of others.

16. Legal limits

The rights of data subjects can be restricted in particular when the processing concerns:

- the protection of the data subject or the rights and freedoms of a third party;
- national security or defense and public security;
- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
- the general public interest (monetary, budgetary, taxation, public health and social security);
- the protection of judicial independence and judicial proceedings;
- the enforcement of civil law claims.

4. Modalities of answers to data sujects

17. Chronology of a request filled by a data subject

Every request filled out by a data subject will follow the chronology described below:

- The data subject fills out a request to the DPO;
- The request is processed by the DPO and the concerned departments;
- Once the request is processed and the informations provided or not, the data subject acknowledges the decision and where petinent the information he/she received;
- The case is closed and the evidence is stored.

18. Request of a data subject

Every data subject can fill out a request to exercise his/her rights on his/her data processed by Safran.

The request can be filled by writing (electronic or paper) or orally by providing a proof of his/her identity. In case of doubt as to the identity of the data subject, Safran can require additional information to bring evidence as to his/her identity.

19. Reply of Safran to the data subject

The reply of Safran to the data subject must be concise, transparent, understandable and easily accessible in clear and simple terms.
The actors in charge of processing these requests are[6]:

- the DPO Company or the local data protection contact
- In the absence of the above: the DPO Group safran.dpo@safrangroup.com

If necessary to process the request, the DPO transfers the request to the pertinent deparments (Human resources etc.).

The information must be provided in the format chosen by the data subject (paper, electronic, orally).

20. Turnaround time

Safran answers any claim by data subjects without undue delay and to a maximum period of one month from the reception of the claim.
When the claim is complex or numerous, the delay may be extended by two further months. Safran informs the data subject of the extension and its reasons within the month of the reception of the claim.

If Safran does not follow up on a claim, it informs the data subject within the month of the reception of the claim and explains the reasons of its inaction and the possibility to lodge a complaint with the data protection authority and an appeal.

21. Evidence of the reply given by Safran

Safran must be able to bring evidence of the reply given to the data subject whether the information was provided or not. The data subject must acknowledge to confirm that his/her request was processed.

22. Retention period

The claims and complaints of data subjects will be stored for two (2) years from the closure of the case.

23. Notification of the data recipients

Following a rectification, limitation or erasure of data, Safran notifies this action to every data recipient to whom the data have been communicated unless this would prove to be impossible or require disproportionate efforts.

Safran gives to the data subject the information on these recipients if he/she asks to be informed on that point.