Charter for the Protection of Personal Data of Crédit Agricole Group Employees

Table des matières

PURPOSE

The Crédit Agricole Group (the "Group") complies with personal data protection regulations, including those relating to the personal data of its employees[1].

In preparation for the changes to the regulations governing personal data protection that will occur when the General Data Protection Regulation (GDPR) comes into effect on 25 May 2018[2], the Group has decided to formalise this "Charter for the Protection of Personal Data of Crédit Agricole Group Employees" (the "Charter").

The Charter states all processing of employees' personal data performed within the Group, the basic data protection principles applicable to these operations and the way in which the Group upholds regulatory compliance. It is applicable to all Group employees in their relations with the Group.

The Charter consists of two parts. Part 1 describes the basic principles governing the processing of employees' personal data. Appendix 1 provides detailed information on the processing of employees' personal data; this part is completed by each Group entity.

[1] The term "employee" refers to any individual with an employment contract or similar, including seconded and loaned personnel, as well as workers in apprenticeships or under vocational training contracts. This definition also covers trainees and temporary workers.

[2] EU Regulation 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.

1. HOW DOES THE GROUP PROCESS EMPLOYEES' PERSONAL DATA?

1.1 Definitions

The following definitions apply in the Charter:

1. **Personal Data** : Any information relating to an identified or identifiable employee, i.e. an employee who can be identified either directly or indirectly, in particular via references to an identifier or to one or more elements specific to their identity. Personal data includes employee contact details, information on their education or professional experience, employment-related administrative information or information relating to the hardware and software used by employees;

2. **Processing**: Any operation (or set of operations) performed on personal data, including, for example, its collection, organisation, storage, modification, use, transmission, distribution or erasure;

3. **Purpose**: The reason for processing personal data. The purposes of personal data processing in the context of this Charter are stated in §1.3 below;

4. **Recipient**: Any natural or legal person, public authority, service or other organisation to which personal data is disclosed;

5. **Controller:** The entity that defines the purpose of the personal data processing and the resources used to perform said processing. The controller of processing that uses employees' personal data is generally the Group entity that employs the employee; in special cases, however, the controller may be another Group entity;

6. **Processor:** Any entity other than the process manage that processes personal data on behalf and at the request of the controller. A Group entity may therefore be a processor for another Group entity. For example, companies that provide IT or consulting services to the controller, or which are entrusted with HR management services, are considered to be processors.

1.2 Data Protection Officer (DPO)

Appendix 1 contains the contact details of the data protection officers (DPOs) appointed by Group entities.

DPOs are responsible for the regulatory compliance of personal data protection. Each entity's DPO ensures that its personal data processing complies with the GDPR. Entities involve their DPOs immediately in all personal data protection matters. DPOs are also responsible for liaising between their entity and the personal data protection authorities.

DPOs perform their duties entirely independently and are bound by non-disclosure obligations governing their duties.

1.3 In what circumstances are employees' personal data used?

The Group processes employees' personal data in order to manage the following:

- Employees (career management, performance appraisals, training monitoring, administrative management, medical examination follow-up, secondments, seminars, surveys, retirement, social protection etc.);
- Internal recruitment and employee mobility;
- Compensation and reimbursement of expenses;
- Employee share ownership and savings plan
- Labour relations (careers of employee representatives and management of employee representation bodies) and industry elections;
- Requests from employees regarding certain Group programmes and facilities (for example, the Group banking offering, support for the disabled, accommodation requests and social support);
- Prevention and combating of fraud and identification of Internet connections;
- Fighting of corruption and statutory and regulatory compliance relating to finance;
- Provision of IT tools and management of the related access and permissions;
- Video surveillance systems;
- Access to premises.

Appendix 1 of the Charter contains more detailed information about these processes.

1.4 What personal data protection principles does the Group apply?

Employees' personal data is processed in accordance with the following personal data protection principles:

1. **Legal, fair and transparent processing**: Employees' personal data must always be collected and processed (the for a specific purpose "legal basis"). No processing that breaches the principles defined in this Charter and the GDPR may be performed. Furthermore, clear, comprehensive and transparent information must be provided to all employees regarding the processing of their personal data;

2. **Restricted purposes**: Employees' personal data must always be collected and processed for specific purposes determined from the outset;

3. **Lean data**: Only personal data that is strictly necessary in order to achieve the stated purposes may be collected from employees. No personal data superfluous to the processing performed may be collected or used;

4. **Accuracy**: Employees' personal data must always be accurate and regularly updated. All reasonable measures must be taken to ensure that any inaccurate data is either corrected or erased;

5. **Limited retention**: Employees' personal data must not be stored for longer than needed to achieve the purposes for which it was collected. It may also be stored or archived for the legally required retention periods.

6. **Security**: Employees' personal data must be stored and processed securely and confidentially.

1.5 What is the legal basis for the processing of employees' personal data?

All processing involving employees' personal data must have a legal basis.

Accordingly, their personal data may only be processed if this is justified on any of the following grounds:

1. To enable **performance of a contract** between the employee and the processor. For example, the employment contract between an employee and their employer requires a variety of personal data on the employee's administrative situation to be processed.

2. To comply with a **legal obligation** binding the controller. Such obligations may stem from legislative provisions or rules based on collective bargaining agreements applied by the Group.

3. To address a **legitimate interest** of the controller. The nature of legitimate interests may be legal (for example, to exercise or uphold certain rights), administrative (for example, to transfer information within the Group) or technical (for example, to secure networks and data). If personal data is processed on the basis of a legitimate interest, all necessary precautions must be taken to ensure that employees' interests, rights and basic freedoms are not infringed.

4. In certain circumstances, personal data may be processed at the request of the employees themselves, that is to say, with their **consent**.

   An employee's consent must always be given freely informed and explicit (generally in writing). Employees may decide to withdraw their consent at any time.

   However, doing so does not affect the validity of any processing already performed with the employee's consent.

5. To **safeguard human life**.

1.6 In what circumstances are employees required to provide personal data?

The Group entity acting as the controller may be required to collect personal data in order to comply with a legal obligation or fulfil a contract. This applies, for example, to the collection of employees' social security numbers, which are required when the employer pays social security contributions to the relevant organisations. It may also be necessary to collect information when hiring a new employee, so that the associated administrative formalities can be completed.

Whenever personal data is collected, the employees must be informed of whether or not they are obliged to reply, and told the consequences of failing to provide the requested information.

1.7 Who receives employees' personal data?

For the purposes of the processing described above, employees' personal data may in certain cases be disclosed to a variety of recipients, including Group entities, independent companies such as processors (for example, independent consultants or IT solution or hosting service providers), and authorities or organisations (e.g. social security organisations, pension funds, etc.).

Group entities acting as controllers must choose processors that provide adequate guarantees that the processing will comply with the principles of the GDPR and that the personal data will remain confidential and secure.

If a recipient of personal data is located in a country outside the European Union, the recipient must comply with local legal requirements that provide a suitable level of protection, or, in the case of companies in the United States, comply with the Privacy Shield (a self-certification mechanism recognised by the European Commission), or else provide guarantees ensuring an equivalent level of protection.

These guarantees may be in the form of the standard contractual clauses on personal data protection adopted by the European Commission (namely, a transfer agreement between the controller and a processor, stating the respective obligations upon each if personal data is transferred outside the European Union).

1.8 How is employees' personal data secured?

Solutions used to store and process employees' personal data must satisfy the security prerequisites specified by the Group's Information Systems department and are subject to stringent approval and audit procedures.

The Group has implemented technical and organisational measures to ensure that employees' personal data remains secure and confidential. These include:

- Access control and user permissions for IT equipment used to process employees' personal data;
- Ensuring the security of technical infrastructures (including workstations, networks and servers) and data (for example, backups and business continuity plan);
- Restricting who is authorised to process personal data, depending on the purpose of the processing and the resources allocated;
- Strict non-disclosure obligations binding the Group's processors;
- Rapid response procedures in the event of a security incident involving employees' personal data.

1.9 How is employees' personal data stored?

Employees' personal data is stored for as long as is necessary in order to achieve the purpose(s) for which it was collected, comply with statutory data storage obligations or enable entities to establish employees' rights (for example, pension rights). It may also be stored or archived for statutory minimum retention periods.

Throughout the storage period, only "need-to-know" individuals with the appropriate permissions may have access to employees' personal data, based on the purposes of the intended processing.

At the end of the storage period, employees' personal data must be either permanently erased or irreversibly anonymised.

1.10 What rights do employees have regarding the processing of their personal data?

All employees may exercise the following rights at any time:

1. **Right to access**: Employees may obtain information regarding the nature, source and use of their personal data. Whenever personal data is disclosed to third parties, employees may also obtain information concerning the identities or categories of the recipients;

2. **Right to rectification**: Employees may request that inaccurate or incomplete personal data be corrected or supplemented;

3. **Right to erasure**: Employees may request that their personal data be erased, particularly if it is no longer necessary for the performed processing. The controller must erase personal data promptly, except in the cases provided for in the Regulation, and specifically, in cases where personal data is processed in order to comply with a legal obligation;

4. **Right to restrict processing**: Employees may request that their personal data be made temporarily unavailable to prevent its subsequent processing, for example by moving their data to a different processing system, in the following circumstances:

    - if the employee disputes the accuracy of the processed personal data (for example in case of error related to the employee's civil status), for a period allowing the controller to verify the accuracy of these data;

    - if the processing is illegal and the employee objects to the erasure of their data and demands that its use be restricted;

    - if there are no longer any grounds for storing the employee's personal data but the employee wishes it to be retained by the controller, for the purpose of exercising or defending their legal rights;

    - if the employee has opposed processing for the time required in order to check whether the legitimate reasons of the controller should prevail over those of the employee;

5. **Right of opposition**: Employees may oppose certain processing involving their personal data for reasons relating to their specific circumstances, except where legitimate and essential reasons for the processing prevail over the data subject's interests, rights and basic liberties or for the purpose of exercising or defending their legal rights;

6. **Right to portability**: Whenever personal data is processed after obtaining the employee's consent or required for the performance of a contract, the employees concerned may ask to receive their personal data provided to the controller, in a widely-used and structured electronic format;

7. **Right to issue instructions in case of death**: Employees may issue instructions regarding the processing of their personal data in the event of their death[3].

[3] Applicable in France only

To exercise these rights, employees may contact the individuals or departments responsible for managing the exercising of such rights, at the addresses provided in Appendix 1. The controller undertakes to examine requests submitted by employees within the time limits specified in the GDPR.

Employees may also submit a complaint to the relevant data protection authority (see Appendix 1 for contact details) if they consider that any personal data processing does not comply with the GDPR.

1.11 Charter applicability and amendments

The Charter shall be applicable with effect from 25 May 2018.

The Charter is available to download from each intranet Group entity, at the following address: [link to Charter]. It is liable to change, in response to regulatory or processing changes.

2. APPENDIX 1 – DETAILED INFORMATION ON THE PROCESSING OF EMPLOYEES' PERSONAL DATA

This part is completed by each individual entity.