Credit Agricole CIB's Data Protection Charter in terms of recruitment

(updated on 12/16/2020)

CRÉDIT AGRICOLE
CORPORATE & INVESTMENT BANK

Content

Purpose

Crédit Agricole CIB (CACIB, the “Bank”) complies with personal data protection regulations, including those relating to the personal data of the candidates [1] for a position in the Bank.

In preparation for the changes to the European regulations governing personal data protection that will occur when the General Data Protection Regulation (GDPR) comes into effect on 25 May 2018 [2] , the Bank has decided to formalise this “Charter for the Protection of Personal Data for Crédit Agricole CIB in terms of recruitment “ (the “Charter”).

The Charter states all processing of candidates’ personal data performed a t Crédit Agricole CIB, the basic data protection principles applicable and the way in which the Bank upholds regulatory compliance. It applies to candidates applying to a position in a Crédit Agricole CIB entity in Europe but also to candidates residing in the EU and applying in an entity outside the EU.

[1] The term “candidate” refers to any individual, external to Crédit Agricole CIB, contacting or being contacted by a Crédit Agricole CIB entity for the purpose of presenting his/her candidature to any position within Crédit Agricole CIB, for an employment contract or any other related type of contract, including an apprenticeship, a vocational training contract, or an internship.

[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. DEFINITIONS

The following definitions apply in the Charter:

1. **Personal Data:** Any information relating to an identified or identifiable candidate. For example, personal data can be candidates' contact details in a resume or cover letter;
2. **Processing**: Any operation (or set of operations) performed on personal data, including, for example, its collection, organisation, storage, modification, use, consultation, 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 §3 below;
4. **Recipient**: Any natural or legal person, public authority, service or other organisation to which personal data is disclosed;
5. **Data 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 candidates' personal data is the Crédit Agricole CIB entity that is looking to recruit.
6. **Processor:** Any entity other than the process manager that processes personal data on behalf and at the request of the data controller. A Crédit Agricole CIB entity may therefore be a processor for another Group entity. For example, companies that provide IT or consulting services to the data controller, or which are entrusted with HR management services, are considered to be processors.

2. WHAT ARE THE DATA PROTECTION PRINCIPLES APPLIED BY CRÉDIT AGRICOLE CIB?

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

1. **Legal, fair and transparent processing**: Candidates' personal data must always be collected and processed 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 candidates regarding the processing of their personal data;
2. **Restricted purposes**: Candidates' 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 candidates. No personal data superfluous to the processing performed may be collected or used;
4. **Accuracy**: Candidates' 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**: Candidates' personal data must not be stored for longer than needed to achieve the purposes for which it was collected.
6. **Security**: Candidates' personal data must be stored and processed securely and confidentially.

3. IN WHAT CASES ARE CANDIDATES' PERSONAL DATA USED? WHAT IS THE LEGAL BASIS FOR THE PROCESSING OF CANDIDATES' PERSONAL DATA?

1. Managing applications, conducting and following interviews and the selection process, in particular complying with obligations linked to the fight against financial crime (screening pre-selected candidates against International Sanctions lists), managing recommendations and references, pre-recruitment and establishing hiring promises and contracts, and managing a pool of candidates.

   These processes are necessary to execute precontractual dispositions or for the legitimate interests pursued by the processing manager.

   When candidates' consent to the use of their personal data is required, this consent by the candidate concerned is always free, specific, informed and explicit. It must be expressed by a clear and positive action or declaration.

2. Manage access to premises and potential video surveillance of the premises.

   These processing are justified by a legitimate interest, which consists of ensuring security of goods and individuals (in the real time and afterwards). In this case, candidates may oppose certain processing involving their personal data for reasons relating to their specific circumstances (unless the data controller proves that there are legitimate and essential reasons for the processing to prevail over the data subject's interests, rights and basic liberties or for the purpose of exercising or defending their legal rights).

   The processing of personal data communicated by candidates is not based on profiling.

4. IN WHAT CIRCUMSTANCES ARE CANDIDATES REQUIRED TO PROVIDE PERSONAL DATA?

Some personal data may be necessary to review candidatures by Crédit Agricole CIB. Candidates will be informed about it during the data collection process, by an asterisk or in an equivalent way.

In the case this data is not communicated, or if consent is eventually withdrawn for data already provided, the data controller will not be able to process the candidature.

5. WHO RECEIVES CANDIDATES' PERSONAL DATA?

For the purposes of the processing described above, candidates' personal data may in certain cases be disclosed to a variety of recipients, including:

- Crédit Agricole Group entities, including Crédit Agricole CIB entities,
- IT – Data processing firms, test editors, or data processors in charge of access to premises and eventual
  video surveillance providers.
- Recruitment agencies.
- Services in charge of the fight against financial delinquency

These guarantees can be Standard Contractual Clauses adopted by the European Commission to protect personal data, the application of which is effective in the importing country, (i.e. a transfer contract between the

processing manager and a recipient specifying the obligations of the processing manager and the recipient in the event of the transfer of personal data outside the European Union)

6. HOW IS CANDIDATES' PERSONAL DATA SECURED?

Solutions used to store and process candidates' personal data must satisfy the security prerequisites specified by Crédit Agricole CIB's Information Technology department and are subject to stringent approval and audit procedures.

Crédit Agricole CIB has implemented technical and organisational measures to ensure that candidates' personal data remains secure and confidential. These include:

- Access control and user permissions for IT equipment used to process candidates' 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 its processors;
- Rapid response procedures in the event of a security incident involving candidates' personal data;

7. HOW LONG IS CANDIDATES' PERSONAL DATA STORED?

Candidates' personal data linked to the processing of applications mentioned in 1. of paragraph 3 are kept as detailed below:

(i) When the candidate is not selected:

- Data kept in the active database for eighteen (18) months from the last use of the internal recruiting tool by the candidate;
- After 18 months the data is deleted;

At all times a candidate can remove his/her account in the application. The button "delete my account" automatically and permanently deletes the candidate's account and all his/her applications.

(ii) When the candidate is selected

- During the working relationship: data kept in the active database;
- When the work contract is terminated, according to the process considered and subject to special texts:

o Data is kept in the active database for ten (10) years;

o Then intermediary archiving for a maximum of fifty (50) years (for all data: work contracts, interviews, pay slips, retirement documents …);

o Thereafter the data is deleted.

Personal data collected for managing access to the premises is stored for three (3) months. Personal data collected for the management of eventual video surveillance systems is stored for one (1) month (or according to local regulations).

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

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

8. WHAT RIGHTS DO CANDIDATES HAVE REGARDING THE PROCESSING OF THEIR PERSONAL DATA?

All candidates may exercise the following rights [1]

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

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

5. **Right to erasure**: Candidates may request that their personal data be erased, particularly if it is no longer necessary for the performed processing. The data controller must erase personal data promptly, except in the cases provided for in the Regulation;

6. **Right to restrict processing**: Candidates 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 circumstances defined by the GDPR [2.]

7. **Right of opposition**: Candidates 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;

8. **Right to portability**: Whenever personal data is processed after obtaining the candidate's consent or required for the performance of a contract, the candidates concerned may ask to receive their personal data provided to the data controller, in a widely-used and structured electronic format. This right to portability can be exercised only if the data processing is operated under candidate's consent.

The controller undertakes to examine requests submitted by candidates within the time limits specified in the GDPR. If a request is obviously baseless or excessive, the data controller does not necessarily have to respond positively and will notify the candidate of the reason for rejection within the time limits.

[1] Furthermore, candidates whose personal data is processed by a data processor located in France may issue instructions regarding the processing
of their personal data in the event of their death.

[2] It means:

a) if the candidate disputes the accuracy of the processed personal data (for example in case of error related to the candidate's civil status), for a period allowing the controller to verify the accuracy of these data;
b) if the processing is illegal and the candidate objects to the erasure of their data and demands that its use be restricted;
c) if there are no longer any grounds for storing the candidate's personal data but the candidate wishes it to be retained by the controller, for the purpose of exercising or defending their legal rights;
d) if the candidate has opposed processing for the time required in order to check whether the legitimate reasons of the controller should prevail over those of the candidate;

9. CONTACTS

To obtain more information, to get a copy of the appropriate warranties mentioned at the paragraph 5 and to exercise the rights mentioned on the §8, candidates may contact the Human Ressources Department at the Crédit Agricole CIB entity they are applying to or at this email address: **drh.informations@ca-cib.com**.

Candidates may also submit a complaint to the relevant data protection authority if they consider that any personal data processing does not comply with the GDPR. The competent data protection authority, referred to in Article 1.10 of Part 1, shall be the competent national authority listed in Appendix 1.

10. CHARTER APPLICABILITY AND AMENDMENTS

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

The Charter was revised on 16 December 2020

The Charter is available to download from the Crédit Agricole CIB entity's website, at the following address: **www.jobs.ca-cib.com**. It is liable to change, in response to regulatory or processing changes.

APPENDIX 1: LIST OF RELEVANT NATIONAL AUTHORITIES

COUNTRY	DETAILS OF DATA PROTECTION AUTHORITY
FRANCE	**Commission Nationale de l'Informatique et des Libertés - CNIL** 3 Place de Fontenoy, TSA 80715 75334 PARIS CEDEX 07 Tel.: +33 (0)1 53 73 22 22 Website: http://www.cnil.fr/
BELGIUM	**Autorité de Protection des Données** **(previously Commission de la protection de la vie privée)** Rue de la Presse 35 1000 Bruxelles Tel. +32 2 274 48 00 e-mail: contact@apd-gba.be Website: http://www.privacycommission.be/
FINLAND	**Office of the Data Protection** Ombudsman P.O. Box 800, 00521 Helsinki, Finland Tel. +358 10 3666 700 Fax +358 10 3666 735 e-mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi/en/
GERMANY	**Hessischer Datenschutzbeauftragter** Der Hessische Datenschutzbeauftragte, Postfach 3163, 65021 Wiesbaden Tel. +49 611 1408 0 Fax. + 49 611 1408 900 e-mail: poststelle@datenschutz.hessen.de
ITALY	**Garante per la protezione dei dati personali** Piazza di Monte Citorio, 121 00186 Roma Tel. +39 06 69677 1 e-mail: garante@garanteprivacy.it Website: http://www.garanteprivacy.it/
NORWAY	**Datatilsynet** The Data Inspectorate P.O. Box 8177 Dep 0034 Oslo Tel. +47 22 39 69 00 Fax +47 22 42 23 50 e-mail: postkasse@datatilsynet.no
SPAIN	**Agencia de Protección de Datos** C/Jorge Juan, 6 28001 Madrid Tel. +34 91399 6200 Fax +34 91455 5699 e-mail: internacional@agpd.es Website: https://www.agpd.es/

COUNTRY	DETAILS OF DATA PROTECTION AUTHORITY
SWEDEN	**Datainspektionen** Drottninggatan 29 5th Floor Box 8114 104 20 Stockholm Tel. +46 8 657 6100 Fax +46 8 652 8652 e-mail: datainspektionen@datainspektionen.se
UNITED KINGDOM	**The Information Commissioner's Office** Water Lane, Wycliffe House Wilmslow - Cheshire SK9 5AF Tel. +44 1625 545 745 e-mail: international.team@ico.org.uk

Realised by Crédit Agricole Immobilier Services - Production Graphique

CRÉDIT AGRICOLE
CORPORATE & INVESTMENT BANK

Édition 2018