CEB Data Protection Regulations

The Administrative Council, under the terms of Article X of the Articles of Agreement of the Council of Europe Development Bank,

Considering that due to rapid technological developments and globalisation, International and European legal frameworks with respect to data protection have been updated to ensure high level protection of natural persons;

Considering that the Modernised Convention for the Protection of individuals with regard to the Processing of Personal Data ("Convention 108+") was adopted by the Committee of Ministers of the Council of Europe on 18 May 2018;

Considering that the Regulations on a system for the protection of personal data at the CEB need to be updated and shall be replaced by new CEB Data Protection Regulations;

On the proposal of the Governor, the Staff Committee having been consulted in accordance with Article 6, paragraph 1, of the Regulations on Staff Participation (Appendix I to the Staff Regulations);

Decides:

Chapter I — General Provisions

Article 1 — Object and purpose

In accordance with these Regulations, the Council of Europe Development Bank, hereinafter referred to as "the Bank or the CEB", shall ensure protection of every individual, whatever their nationality or residence, with regard to the processing of their personal data by the CEB or on its behalf, thereby contributing to respect for their human rights and fundamental freedoms, and in particular their right to privacy.

Article 2 — Definitions

For the purposes of these Regulations:

(a) "personal data" means any information relating to an identified or identifiable individual ("data subject"); an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to her or his physical, physiological, mental, economic, cultural or social identity; an individual is not considered identifiable if her or his identification would require unreasonable time, effort or means;

(b) "data processing" means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure, destruction or the carrying out of logical and/or arithmetical operations on such data;

(c) where automated processing is not used, “data processing” means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;

(d) “controller” means any administrative entity, organ, institution or authority within the Bank which alone or jointly with others has the decision-making power with respect to data processing, whether this power derives from a legal designation or factual circumstances;

(e) “recipient” means a natural or legal person, public authority or any other body to whom data are disclosed or made available;

(f) “processor” means a legal or natural person (other than a member of the Bank), public authority or any other body which processes personal data on behalf of the controller;

(g) “internal legal framework” means a system of legally binding instruments such as regulations, rules, policies and procedures defining in particular the Bank’s governance structure, operational aspects of the Bank’s activities, budget and financial management; and conditions of employment by the Bank;

(h) “the data subject’s consent” means any freely given, unambiguous, specific and informed indication, either by a statement or by a clear affirmative action, signifying agreement to the processing of personal data related to them or to individuals for whom they exercise legal authority.

Article 3 — Scope

The present Regulations shall apply to the processing of personal data by the Bank or on its behalf.

Chapter II — Principles for the protection of personal data

Article 4 — Legitimacy of data processing and quality of data

1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.

2. Data processing can be carried out:

(a) on the basis laid down by the CEB legal instruments or internal legal framework where it is necessary for the performance of the Bank’s tasks and activities in furtherance of its purpose as set out in Article II of the Articles of Agreement, including the discharge of its statutory functions; performance of other activities of international cooperation including with other international organisations, and ancillary operations including internal administrative functions;

(b) where it is necessary for compliance with a legal obligation to which the Bank is subject;

(c) on the basis of the data subject’s consent;

(d) where it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(e) where it is necessary in order to protect the vital interests of the data subject or another natural person;

(f) where it is necessary for the purposes of the legitimate interests pursued by the Bank, except where such interests are overridden by the interests or human rights and fundamental freedoms of the data subject.

3. Personal data undergoing processing shall be:

(a) processed lawfully, fairly and in a transparent manner;

(b) collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving, historical, statistical and scientific purposes is compatible with those purposes, subject to appropriate safeguards to be taken by the controller;

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date;

(e) preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.

Article 5 — Processing of special categories of data

The processing of sensitive data such as:

(a) genetic data;

(b) personal data relating to offences, criminal proceedings and convictions, disciplinary proceedings and any related measures;

(c) biometric data uniquely identifying a person;

(d) personal data for the purpose of revealing information relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life;

shall only be carried out where additional appropriate safeguards provided by the Bank's internal legal framework protect against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.

Article 6 — Data security

1. The controller shall take appropriate security measures against risks such as accidental or unauthorised access, destruction, loss, use, modification or disclosure of personal data. Such appropriate measures may be of technical or organisational character and include, as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) measures aimed at ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) measures aimed at restoring the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of the measures.

2. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. Any data breach shall be immediately notified by the controller to the Data Protection Officer. The notification shall, as a minimum:

(a) describe the nature of the personal data breach including, where possible, the categories and estimated number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) describe the likely consequences of the personal data breach;

(c) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

5. The Data Protection Officer shall notify, without delay, the Data Protection Commissioner and the affected data subject(s) of those data breaches which may seriously interfere with their rights and fundamental freedoms.

Article 7 — Transparency of data processing

1. The controller shall inform the data subject, where the latter does not already have the information, of:

(a) its contact details;

(b) the legal basis and the purposes of the intended processing;

(c) the categories of personal data processed;

(d) the recipients or categories of recipients of the personal data, if any;

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

(f) the existence of the right to withdraw consent at any time, where the processing is based on the data subject's consent, without affecting the lawfulness of processing based on consent before its withdrawal;

(g) the existence of any automated decision-making, as well as the significance and the envisaged consequences of such processing for the data subject; and

(h) the means of exercising their rights set out in Article 8 below, as well as any necessary additional information in order to ensure fair and transparent processing of the personal data.

2. Where the personal data are not collected from the data subjects themselves, the controller shall not be required to provide the information referred to in paragraph 1 above where this proves to be impossible or involves disproportionate efforts or is likely to render impossible or seriously impair the achievement of the objectives of the processing.

Article 8 — Rights of the data subject

Every data subject whose personal data is processed by the Bank shall have a right:

1. to obtain, on request, at reasonable intervals and without excessive delay, confirmation of the processing of personal data relating to her or him, the communication in an intelligible form of the data

processed, all available information on their source, on the preservation period as well as any other information that the Bank is required to provide in order to ensure fair and transparent processing of the personal data in accordance with Article 7, paragraph 1;

2. to receive an explanation, on request, of the reasoning underlying data processing where the results of such processing are applied to her or him;

3. to object at any time, on grounds relating to her or his situation, to the processing of personal data concerning her or him; objections shall be deemed unjustified if the Bank demonstrates legitimate grounds for the processing which override her or his interests or rights and fundamental freedoms;

4. to obtain, on request and without excessive delay, rectification or erasure, of such data if these are being or have been processed contrary to the provisions of these Regulations;

5. not to be subject to a decision significantly affecting her or him based solely on an automated processing of data without having her or his views taken into consideration, unless such decision is expressly authorised by the CEB internal legal framework provided that it lays down suitable measures to safeguard the individuals' rights and freedoms and legitimate interests;

6. to have a remedy under Chapter IV of these Regulations where her or his rights under these Regulations have been infringed.

Article 9 — Additional obligations

1. The controller shall take all appropriate measures to ensure, and be able to demonstrate, that the data processing carried out by the controller, or on its behalf by a processor, complies with these Regulations.

2. The controller shall examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

3. The controller shall implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

4. Where a type of processing of personal data is likely to result in a risk to the rights and fundamental freedoms of the data subjects due notably to the nature and volume of the data or the nature, scope and purpose of the processing, the controller shall seek the advice of the Data Protection Officer. The Data Protection Officer shall consult with the Data Protection Commissioner if, in the view of the Data Protection Officer, the risk to the rights and fundamental freedoms of the data subject(s) is particularly high.

5. Where a decision taken by the controller significantly affects a data subject and is based solely on an automated processing of data without having her or his views taken into consideration, the Bank shall provide for suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

6. The controller shall only assign the responsibility of processing of personal data to a processor if the latter provides adequate warranties of compliance with the level of protection of the personal data set forth by these Regulations as well as in the applicable procedures.

7. The carrying out of data processing by a processor on behalf of the Bank shall be governed by a contract or other legal act binding the processor to the Bank and setting out the nature and purpose of the processing, its duration, the type of personal data, the categories of data subjects and the obligations and rights of the Bank and the processor.

8. Each controller 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 processor and the joint controller;

(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 Member States, 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 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 6 (1).

9. The records referred to in paragraph 8 shall be in writing, including in electronic form, and shall be made available to the Data Protection Officer and/or the Data Protection Commissioner on request.

Article 10 — Restrictions

1. The internal legal framework may restrict the application of the provisions of Articles 7 and 8 only when such a restriction respects the essence of the rights and fundamental freedoms of the data subject and constitutes a necessary and proportionate measure to safeguard:

(a) the management of safety and security risks to the Council of Europe Development Bank staff or other individuals involved in the Bank's activities or protection of the important economic interests of the Bank;

(b) the prevention of, or inquiry or investigation into, breaches of the internal legal framework and/or applicable laws and the conduct of disciplinary proceedings;

(c) dispute resolution proceedings;

(d) the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression and access to information.

2. The Bank may restrict the exercise of the provisions specified in Articles 7 and 8 above with respect to data processing which is carried out for archiving purposes in the public interest; scientific or historical research purposes; or statistical purposes and when there is no recognisable risk of infringement of the rights or fundamental freedoms of data subjects. Whenever possible, appropriate safeguards shall be applied such as data minimisation, anonymisation and/or pseudonymisation.

Article 11 — Obligations of staff members and other members of the Bank

Staff members and other members of the Bank shall:

1. treat any personal data with utmost care;

2. refrain from any processing of personal data that is not necessary, legitimate and appropriate in the light of their professional duties, these Regulations and the implementing instruments thereof;

3. seek the Data Protection Officer's advice, in a timely manner, where required by these Regulations or the related procedures and guidelines; and act in accordance with the Data Protection Officer's recommendations;

4. cooperate at all times with the Data Protection Officer and the Data Protection Commissioner;

5. identify at her or his level, the risks surrounding personal data protection and promptly inform her or his hierarchical superior and the Data Protection Officer of any circumstances which may result in risks for the protection of personal data.

Article 12 — Transfer of personal data outside the Bank

1. The transfer of personal data outside the Bank to a recipient within a State's jurisdiction or to another international organisation may only take place where the Data Protection Commissioner finds that a level of protection equivalent to that of these Regulations, which are based on the provisions of the Convention 108+, is secured.

2. Such a level of protection can be secured by:

(a) the law of the State or international organisation, including the applicable international treaties or agreements, in particular the fact of being Party to the Convention 108+ and effectively implementing its provisions;

(b) standardised or ad hoc safeguards, approved by the Data Protection Commissioner, provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing of the data, including standard contractual clauses and provisions to be inserted into administrative arrangements between public authorities or bodies.

3. Notwithstanding the provisions of the previous paragraphs, the transfer of personal data may take place if:

(a) the data subject has given her or his explicit consent to the proposed transfer, after being informed of risks arising in the absence of appropriate safeguards, or

(b) the specific interests of the data subject require it in the particular case, for instance in order to protect her or his vital interests, or where she or he is physically or legally incapable of giving consent, or

(c) prevailing legitimate interests, in particular important public interests, require such transfer and it constitutes a necessary and proportionate measure in a democratic society,

(d) the transfer is necessary for the establishment, exercise or defence of legal claims.

4. The Data Protection Commissioner shall be provided with all relevant information concerning the transfers of data subject to ad hoc safeguards referred to in paragraph 2 (b), and, upon request, in paragraph 3.b and 3.c.

Chapter III — Advisory and supervisory authorities

Article 13 — Data Protection Officer

1. The Governor shall designate a Data Protection Officer on the basis of professional qualities, ability to fulfil the tasks referred to in Article 14 below and, in particular, expert knowledge of data protection standards and practices.

2. The Data Protection Officer may be a staff member or fulfil the tasks on the basis of a service contract. The other professional tasks of the Data Protection Officer shall be compatible with their tasks as Data Protection Officer and shall not result in a conflict of interests.

3. The Bank shall publish the contact details of the Data Protection Officer and communicate them to the Data Protection Commissioner.

4. The Governor shall ensure that the Data Protection Officer:

(a) enjoys wide-spread visibility within the Bank;

(b) performs the tasks independently, does not receive any instructions as regards the exercise of their functions and is not dismissed or penalised for performing their tasks;

(c) is provided with the resources necessary to carry out her or his tasks and to access personal data and processing operations.

Article 14 — Tasks of the Data Protection Officer

1. The Data Protection Officer shall be involved, properly and in a timely manner, in all issues involving the Bank which relate to the protection of personal data.

2. The Data Protection Officer shall be entrusted with the following tasks:

(a) to inform and advise the controllers, processors and data subjects of their rights and obligations pursuant to these Regulations and to keep records of such communications;

(b) to ensure that data subjects are informed of their rights and obligations pursuant to these Regulations;

(c) to advise on the implementation, interpretation and application of these Regulations, in particular as to the requirements related to transparency, effective exercise of data subject rights and security of personal data processing;

(d) to advise on the adoption and implementation of the Bank's legal framework in relation to the protection of personal data;

(e) to identify and evaluate the Bank's data processing operations and maintain records thereof;

(f) to monitor the documentation, notification and communication of personal data breaches pursuant to Article 6, paragraph 3 above;

(g) to provide advice and assistance in order to allow the controllers to comply with the obligations under Article 9, paragraph 2 above;

(h) to act as the contact point for and to cooperate with the Data Protection Commissioner on issues related to processing of personal data and to monitor and co-ordinate the response to requests from the latter;

(i) to advise on the processing of personal data referred to in Article 9, paragraph 4 above;

(j) to promote awareness in the Bank of data protection principles, such as rights of data subjects and obligations in the processing of personal data.

Article 15 — Data Protection Commissioner

1. The Data Protection Commissioner shall be an independent supervisory authority overseeing the compliance of personal data processing carried out by the Bank with the provisions of these Regulations. The Data Protection Commissioner shall be nominated by the Governor after consultation of the Staff Committee, on the basis of experience and expert knowledge of data protection standards and practices, and skills required to perform the duties specified in Article 16 below.

2. The term of office of the Data Protection Commissioner shall be four years, and may be renewed once.

3. The Data Protection Commissioner shall act with complete independence and impartiality in performing her or his functions and exercising her or his powers pursuant to the present Regulations and, in doing so, shall neither seek nor accept instructions.

4. The Data Protection Commissioner shall refrain from any action incompatible with her or his functions and powers and shall not, during her or his term of office, engage in any incompatible occupation, whether gainful or not.

5. The operational costs of the Data Protection Commissioner shall be borne by the Bank in accordance with the modalities established by the Governor.

6. The Data Protection Commissioner shall be provided with adequate resources necessary for the effective performance of her or his functions and exercise of her or his powers.

7. The Bank shall assist the Data Protection Commissioner in the performance of her or his functions and in the exercise of her or his powers.

Article 16 — Functions and powers of the Data Protection Commissioner

1. The Data Protection Commissioner shall have the following functions:

(a) to monitor and ensure the application of the provisions of these Regulations;

(b) to examine complaints from data subjects concerning alleged infringement of their rights under the present Regulations and to order remedial action as necessary;

(c) to conduct inquiries into the application of these Regulations, either on her or his own initiative, or in order to examine a complaint from a data subject;

(d) to formulate opinions at the request of the Data Protection Officer or a controller on any matter relating to the implementation of these Regulations;

(e) to make recommendations to a controller who shall subsequently report to the Commissioner on their implementation;

(f) to co-operate with national or international data protection authorities or with data protection authorities of international organisations to the extent necessary for the performance of her or his functions and the exercise of her or his powers.

2. The Data Protection Commissioner shall have the power to:

(a) request from the Bank and access all personal data and all information necessary for the performance of her or his functions and the exercise of her or his powers;

(b) the Bank's premises, including any data processing equipment and means, where there are reasonable grounds for presuming that an activity covered by these Regulations is being carried out there;

(c) impose a temporary or definitive limitation on data processing;

(d) order that processing operations are brought into compliance with the provisions of these Regulations, in particular by rectifying, erasing or destroying all data when they have been processed in contravention of the provisions of these Regulations;

(e) order the Bank to comply with the data subject's requests to exercise her or his rights pursuant to these Regulations;

(f) order the Bank to communicate a personal data breach to the data subject;

(g) order that recipients of disclosed personal data be notified of rectification or erasure of such data by the Bank pursuant to Article 8(4).

Article 17 — Activity report

1. The Data Protection Commissioner shall prepare an annual report outlining her or his activities.

2. The report shall be transmitted to the Governor and made public.

Chapter IV — Remedies and sanctions

Article 18 — Complaints and appeals

1. Any data subject may lodge a complaint with the Data Protection Commissioner if she or he considers that her or his rights under the present Regulations have been contravened.

2. The complaint shall have no suspensive effect on the data processing operation(s) complained of. Nor shall it have a suspensive effect on investigative or any other activities carried out within the framework of the Staff Regulations or other instruments of the internal legal framework.

3. Upon receipt of a complaint, the Data Protection Commissioner shall examine it and shall, within a reasonable period of time and not later than two months from the date of receipt of the complaint, communicate her or his reasoned findings to the Governor. The findings may include ordering any remedial action set out in Article 16, paragraph 2 above. The two-month time-limit may be extended in situations where additional information is required from the data subject with respect to the complaint received.

4. The Data Protection Commissioner's findings shall be final and binding. The Governor shall take a decision in accordance with the findings of the Data Protection Commissioner and notify the decision, together with the findings of the Data Protection Commissioner, to the data subject who lodged the complaint The Governor may decide to award compensation for damages in justified cases.

5. Staff members, former staff members, claimants to their rights, as well as candidates to a competitive recruitment examination may appeal against the Governor's decision to the Administrative Tribunal in accordance with Article XIV of the Staff Regulations.

Article 19 — Disciplinary action

Any failure to comply with the obligations arising from these Regulations, whether intentionally or through negligence on her or his part, shall render a staff member liable to disciplinary action, in accordance with the applicable Staff Regulations and Rules.

Chapter V — Final provisions

Article 20 — Transitional provisions

The Governor shall ensure that processing of personal data already under way on the date these Regulations enter into force are brought into conformity with these Regulations within a period of two years.

Article 21 — Publication and entry into force

These Regulations shall be published on the CEB's website and enter into force on 1 July 2022.