COUNCIL OF EUROPE DEVELOPMENT BANK
BANQUE DE DEVELOPPEMENT DU CONSEIL DE L'EUROPE

Annual Report of the Data Protection Commissioner

1 October 2022 - 31 December 2023

ANNUAL REPORT OF THE DATA PROTECTION COMMISSIONER FOR 2023

Contents

Billy Hawkes

January 2024

Summary

This is my first report as Data Protection Commissioner. It covers the period from my appointment on 1 October 2022 to 31 December 2023. The main focus of my activity during this 15-month period has been on working with the Data Protection Officer (DPO) to ensure full compliance with the requirements of the Regulations when the transition period for implementation expires on 1 July 2024. I believe that the Bank is substantially compliant with the high standards it has set itself in the revised Regulations. My findings on the one substantive complaint I dealt with did not show any element of non-compliance, based on a rigorous examination of all aspects of the Bank's processing of staff data, the main category of personal data processed by the Bank. Going forward, the Bank is well placed to be able to demonstrate, as a member of the Council of Europe family, that it will continue to meet the high standards expected of it in an area where the Council has been a major standard-setter.

Introduction

1. This is my first report as Data Protection Commissioner. It covers the period from my appointment on 1 October 2022 to 31 December 2023. It is prepared in accordance with Article 17 of the CEB Data Protection Regulations which state that the Commissioner *shall prepare an annual report outlining her or his activities. The report shall be transmitted to the Governor and made public*.
2. The main focus of my activity during this 15-month period has been on working with the Data Protection Officer (DPO) to ensure full compliance with the requirements of the Regulations.
3. I visited the Bank's headquarters in Paris on 8 occasions. In the course of these visits, I met the Governor of the Bank as well as directors and senior managers. All assured me of their commitment to the Bank living up to the high standards of data protection set out in its Data Protection Regulations, which in turn reflected the leading role of the Council of Europe in promoting the highest standards in this area. I also had a meeting (over Zoom) with the Staff Committee and participated in a stakeholder meeting with the Administrative Tribunal.

CEB Data Protection Regulations

4. The Regulations entered into force on 1 July 2022, following approval by the Administrative Council. Article 20 provides for a two-year transition period to bring processing activities into conformity with the Regulations. The Regulations replaced an earlier system of data protection which entered into force in 2008.
5. The Regulations provide for a comprehensive system of protection of personal data within the Bank, modelled closely on the provisions of the Council of Europe's *Modernised Convention for the Protection of individuals with regard to the Processing of Personal Data* ("Convention 108+") and the *Council of Europe Regulations on the Protection of Personal Data*. They involve a strengthening of governance arrangements for data protection, notably by replacing an internal committee with an external independent commissioner.
6. Accountability for compliance rests with *data controllers*. A *controller* is defined in Article 2 as *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*.

Role of Commissioner

7. Articles 15 and 16 provide for the appointment and functions of the Commissioner (DPC). Article 15.3 provides that the 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. Article 16 sets out that the 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.*

8. The Regulations provide the Commissioner with extensive powers of investigation and enforcement in relation to personal data processed by the Bank.

Role of Data Protection Officer

9. Articles 13 and 14 provide for the appointment and functions of a *Data Protection Officer* (DPO). During the period covered by this report, the DPO appointed by the Governor was Nicolas BOUGOT, who combined the DPO function with his role as Chief Information Security Officer (CISO). I am satisfied that this combination of functions meets the requirements of Article 13.2 that *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.* Mr Bougot hold a professional qualification in data protection, awarded by the University of Maastricht.

10. The DPO provides support and advice to data controllers and data subjects to ensure correct implementation of the Regulations. The DPO also acts as the main contact point for the Data Protection Commissioner.

Categories of Personal Data

11. Article 9.8 of the Regulations imposes an obligation on each data controller to maintain a record of processing activities under its responsibility containing 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).*

12. In preparation for the entry into force of the new Regulations, the DPO, with the assistance of a consultant, had drawn up a detailed Record of Processing Activity (ROPA) describing the different categories of data processed by the Bank. The DPO has arranged to update the ROPA, which now constitutes a comprehensive record of personal data processed by the Bank, to be reviewed and updated regularly. One aspect that requires some further work is that covered by Article 9.8 (f): *the envisaged time limits for erasure of the different categories of data*

13. The ROPA shows that the main category of personal data processed by the Bank is the data of its employees and contractors. This can include *special categories of data* as defined in Article 5, such as personal data relating to health and to disciplinary proceedings. Other categories include contact details of persons within entities that the Bank deals with in its role as a borrower and lender of funds. The nature of the Bank's activities does not require the collection of personal data of the ultimate beneficiaries of its loans.
14. The Bank uses a number of external agencies to perform specialised tasks such as provision of payroll services. Each such arrangement is covered by a contract as required by Article 9.7. The DPO has carried out a review of these contracts and, in a small number of cases, some enhancements may be desirable when contracts are being renewed.

Transparency

15. Article 7 of the Regulations requires that a data 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.*

16. A comprehensive note was issued to all staff of the Bank on 27 November 2023 giving the information listed above, including the roles of the DPO and DPC. The note is also on the Bank's Intranet.

Promotion of Awareness

17. Article 14.2 (j) of the Regulations assigns as one of the tasks of the *DPO to promote awareness in the Bank of data protection principles, such as rights of data subjects and obligations in the processing of personal data*. The Bank's intranet includes a page dedicated to data protection which includes guides and a video on the subject. The DPO has delivered targeted training to staff dealing with HR data, the main category of personal data processed by the Bank. He has also provided detailed advice on data security and on the use of AI tools by bank staff.

Data Protection Impact Assessments (DPIA)

18. Article 9.4 of the Regulations obliges data controllers to consult the DPO *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* and for the DPO to consult the DPC in appropriate cases. The DPO has been heavily involved in advising data controllers in the preparation of such DPIAs and has consulted me on two such cases relating to use of external agencies to, respectively, process payroll data and facilitate staff performance.

Data Security

19. Article 6 of the Regulations requires each data controller to *take appropriate security measures against risks such as accidental or unauthorised access, destruction, loss, use, modification or disclosure of personal data*.

20. In view of the sensitive nature of its activities as a bank, the CEB has strict policies governing data security. These cover areas such as access control, authentication, audit, monitoring, alarms, data storage and back up and transmission standards and environment integrity. As the DPO is also the Bank's Chief Information Security Officer, data security is a high priority. My investigation of the complaint detailed below in paragraphs 28-30 allowed me to observe the access controls and other security measures applied to HR data, the main category of personal data processed by the Bank.

Data Breaches

21. Article 6.3 of the Regulations provides that any data breach must be notified by the relevant data controller to the DPO who *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.*
22. On 15 December 2023, the DPO notified me of a data breach that had occurred. This involved a staff member inadvertently being given access to details on a Learning & Development form in respect of fellow-employee. The affected staff member had been informed of the breach, which did not involve the release of sensitive data. I informed the DPO that I was satisfied with the action taken, including the mitigations put in place to avoid a recurrence.

Transfers of Personal Data

23. Article 12.1 of the Regulations provides that *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.* Article 12.2 provides that *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.

24. On 8 November 2022, I issued the following general authorisation, which covers most transfers of personal data outside of the Bank:

In accordance with Article 12.1 of the CEB Data Protection Regulations, and having regard to Article 12.2 (a) of the Regulations, I authorise the transfer of personal data from the Bank to a recipient where that recipient is:

a) within the jurisdiction of a state which is a party to Convention 108+ of the Council of Europe, provided that this Convention has entered into force or

b) within the jurisdiction of a state which is bound by the General Data Protection Regulation (GDPR) of the European Union or

c) within the jurisdiction of a state, or a sector within that state, in respect of which the Commission of the European Union has decided, in accordance with Article 45 of the GDPR, that the state or sector provides an adequate level of protection

Provided always that the personal data has otherwise been processed in accordance with the provisions of the Regulations.

25. On 3 November 2022, I authorised the transfer of personal data from the Bank to OECD in the context of the decision of the Bank to outsource its payroll processing to SIRP, an agency of OECD. In granting

this authorisation, I relied on the assessment of the DPO who had furnished me with a detailed DPIA in respect of the transfers involved.

26. On 15 December 2023, I authorised the transfer of personal data between the Bank and the provider of a publishing software tool based in the USA, in order to facilitate the use of this software in the preparation of the Bank's publications. This transfer was not covered by the general authorisation described above as the US company had not made the necessary binding commitment to comply with the requirements of the EU-US *Privacy Framework*. I granted the authorisation, taking account of minimal risks involved and on condition that the contract between the CEB and the US company included legally-binding and enforceable clauses that secured a level of protection equivalent to that prescribed by the Regulations.

Complaints

27. Article 12.1 of the Regulations provides that *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*. The remaining parts of Article 12 provide that the DPC must examine the complaint and communicate her/his *reasoned findings* to the Governor who must take a decision in accordance with the findings. A complainant may appeal the Governor's decision to the Administrative Tribunal.
28. On 14 September 2022, the Bank received a complaint from a former member of staff, alleging that the Bank had breached the staff member's data protection rights. The complainant contented that, in the course of the member's employment with the Bank, more particularly in relation to the termination of the member's employment, personal data - including special categories of such data - were processed in a manner not compliant with the Regulations. The complaint was transmitted to me on 8 October 2022.
29. My investigation of the complaint involved exchange of correspondence with the complainant and with the Bank and a detailed examination of relevant Bank files held in electronic and physical forms. I was given unfettered access to all such files, including those held by the HR, Legal and Compliance divisions. My examination also permitted me to satisfy myself about the access restrictions and other security measures applied by the Bank to such personal data.
30. I conveyed my findings to the Governor on 31 December 2022. The summary of my findings was: *Having examined the complaint of X, a former employee of the Bank; acting in accordance with Article 18.3 of the CEB Data Protection Regulations; having considered the submissions of the complainant and of the Bank; having examined the relevant files of the Bank; I find that the Bank's processing of the personal data of the complainant by the relevant Data Controllers, during the period of … employment and up to the present date, was carried out in full compliance with the Data Protection Regulations.*
31. My findings were duly communicated to the complainant, who did not avail of the right to appeal to the Administrative Tribunal.
32. On 21 November 2023, I received from the DPO a complaint from a former staff member that his name appeared in response to a Google search on an aspect of his interactions with the Administrative Tribunal, whereas he understood that the Tribunal had granted him anonymity The issue was informally discussed with the Registrar of the Tribunal for the Tribunal to address it.

Conclusion

33. This, my first report as Data Protection Commissioner, shows an organisation that is taking seriously its responsibilities as custodian of personal data. The CEB Data Protection Regulations set the high standard that would be expected of a body that is part of the Council of Europe family, with its distinguished tradition of promoting the highest standards of data protection, viewed as part of the fundamental right

to privacy. The Bank has taken the necessary steps to ensure that it is fully compliant with these Regulations by the end of the transition period on 1 July 2024. Going forward, this focus on substantive compliance will need to continue as new challenges arise in the area of data protection. The DPO, working with his colleagues in the Bank, will have my full support in this important work.