Deka Data Protection Policy and Programme

Version 1.0 – as of: 02 January 2026

1. Scope

This data protection programme defines the principles, processes and measures ensuring that Deka processes personal data transparently, fairly and in accordance with the laws on data protection (in particular the EU General Data Protection Regulation (GDPR)) and that data subjects are able to exercise their rights.

This document is binding on all business divisions and their operations of DekaBank Deutsche Girozentrale (hereinafter referred to as "**Deka**").

2. Data privacy policies and rights of data subjects

Deka explains transparently

- what data Deka processes,
- for what purposes Deka processes such data,
- to whom the data is transmitted or made available,
- how long the data is stored, and
- what rights data subjects have.

Such information is provided in data privacy policies, the contents of which are mandatory for Deka. The data privacy policies are available at www.deka.de/datenschutz (see the links to the general and special data privacy policies provided there); these policies, as well as the document entitled "Your Rights under the General Data Protection Regulation" (also linked there), are binding on Deka.

The rights of data subjects under the data privacy policies include the right to have access to their data and the right to demand correction or erasure of their data.

If they have any requests, concerns or complaints, data subjects may contact the data controllers referred to in the data privacy policies, the data protection officer specified therein or the competent data protection authorities.

Deka has an established complaints process with clearly defined deadlines for the processing of requests and complaints relating to data privacy.

Deka will review and, where required, update the data privacy policies on a regular basis and inform data subjects about any material changes, e.g. by email or on the Deka website.

3. Data protection management

Deka undertakes to ensure data protection compliance by implementing a comprehensive data protection management system (DPMS). The DPMS contains policies that provide for binding standards, including, without limitation thereto:

3.1. Processes for reporting data breaches

Deka has implemented a clearly defined process for reporting data breaches, including:

- identification and risk assessment of data breaches,
- reporting to the competent data protection authorities within the deadlines provided for by law, and
- informing the data subjects, where necessary.

3.2. Mandatory data protection training and employee awareness

All employees of Deka undergo mandatory data protection training on a regular basis on topics such as the GDPR, secure data processing and prevention of data breaches.

Deka carries out communication initiatives on a regular basis to raise awareness among employees for data protection issues, e.g. in the form of workshops or informational campaigns.

3.3. Regular data protection analysis and audits

Deka conducts data protection analysis measures, risk assessments (e.g. by way of data protection impact assessment (DPIA) as well as other privacy impact assessments (PIA)) and audits on a regular basis to ensure data protection compliance.

3.4. Governance structures for data protection management

Deka has implemented clearly defined governance structures, including:

- appointment of an independent data protection officer, and
- clearly defined internal responsibilities and processes for compliance with data protection obligations.

3.5. Reporting to the management board

Deka's management board is informed about the status of the data protection management system on a regular basis, including about:

- results of audits and risk assessments,
- risk reporting of data breaches, and
- process implementation in the event of data protection initiatives.

3.6. Protection measures

Deka undertakes to implement appropriate safeguards and measures for the protection of personal data, in particular technical and organisational measures to ensure a level of security appropriate to the risk, including pseudonymisation and encryption (e.g. SSL/TLS), measures ensuring the confidentiality, integrity, availability and resilience of Deka's systems, measures ensuring that personal data can be restored in the event of incidents, and regular tests, assessments and evaluations of the effectiveness of these measures, in particular for the protection against accidental or unlawful destruction, loss or alteration or unauthorised disclosure of, or access to, personal data.

3.7. Service providers bound by data protection obligations

Deka requires all service providers processing personal data on behalf of Deka to ensure an appropriate, equivalent level of data protection. This is ensured by contractual terms and audits.

4. Contact details

Deka's contact details, e.g. if data subjects want to make a request for information, correction or erasure, are as follows:

DekaBank Deutsche Girozentrale
Große Gallusstr. 14
60315 Frankfurt am Main
Telephone +49 (0) 69 71 47 – 652
Email: service@deka.de

Deka's data protection officer can be contacted (e.g. for complaints or concerns) at:

DekaBank Deutsche Girozentrale
Data Protection Officer
Große Gallusstr. 14
60315 Frankfurt am Main
Email: datenschutz@deka.de

5. Implementation and review

This data protection programme will be reviewed at least once a year and updated if required.