

Deka Data Protection Policy and Program

As of: 09/2026, Version 1.1

..Deka



	Page
1. Subject Matter and Scope	3
2. Privacy Notices and Data Subject Rights	3
3. Data Protection Management	4
3.1. Processes for Reporting Personal Data Breaches	4
3.2. Mandatory Data Protection Training and Employee Awareness	5
3.3. Regular Data Protection Analyses and Audits	6
3.4. Governance Structures for Data Protection Management	6
3.5. Reporting to the Board of Management	7
3.6. Security Safeguards	8
3.7. Obligating and Auditing Service Providers	8
3.8. Use of Customer Data	9
4. Contact Information	9
5. Continuous Development of the Data Protection Management System	10

1. Subject Matter and Scope

For DekaBank Deutsche Girozentrale (referred to in this document as “Deka”), data protection is a central component of its business policy and supports the company’s value creation. The protection of the personal data of customers and business partners forms the basis of their trust and contributes significantly to Deka’s positive public reputation. Trust and transparency are therefore essential cornerstones in the handling of personal data and are also important corporate objectives.

In order to meet the requirements for the protection of personal data and to comply with the provisions of the General Data Protection Regulation (GDPR), the German Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG), the German Telecommunications Digital Services Data Protection Act (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz – TDDDG) and other relevant data protection regulations, a data protection management system has been established. This system provides a structured basis for integrating data protection requirements into business processes and safeguarding them over the long term.

The Data Protection Policy and Program obligates all business units of Deka, and their business activities, to observe and comply with it.

2. Privacy Notices and Data Subject Rights

Deka informs data subjects about the processing of their personal data in a transparent, intelligible and easily accessible manner. To this end, Deka sets out, in particular,

- which personal data is processed,
- for which purposes and on which legal basis the processing takes place,
- to which recipients or categories of recipients personal data is transferred or made available,
- the criteria used to determine the storage period or the erasure of the data, and
- which rights data subjects have under the respective applicable data protection laws, in particular the General Data Protection Regulation.

These information obligations are fulfilled in particular through the privacy notices provided by Deka. They are structured according to the respective processing purpose and can be accessed via the links provided at www.deka.de/datenschutz. The information contained in the privacy notices is binding on Deka and forms the authoritative basis for informing data subjects about the nature, scope and purposes of the respective data processing. The same applies to the information on data subject rights contained therein, in particular in the document “Your Rights under the General Data Protection Regulation.”

Subject to the statutory requirements, data subjects have, in particular, the right of access to the personal data concerning them. In addition – depending on the respective statutory conditions – they may have the rights to rectification, erasure, restriction of processing and data portability, as well as a right to object to certain processing. Where processing is based on consent, there is also the right to withdraw such consent at any time with effect for the future.

To exercise their rights, and in the event of questions, requests, concerns or complaints in connection with the processing of their personal data, data subjects may contact the controllers named in the respective privacy notices, the data protection officer named therein, and the competent data protection supervisory authorities.

Deka has an established procedure for handling inquiries and complaints relating to data protection. This procedure provides for clearly defined responsibilities, processing steps and deadlines in order to ensure that such matters are handled properly, within the applicable deadlines and in a traceable way.

Deka commits to reviewing the privacy notices regularly and whenever circumstances warrant a review, and to updating them where necessary. Material changes that are relevant to data subjects are communicated in an appropriate manner, for example by email, via the website or through other appropriate information channels.

3. Data Protection Management

Deka commits to ensuring compliance with data protection by means of a comprehensive data protection management system.

The data protection management system sets out principles, processes and measures that ensure that personal data is processed by Deka transparently, fairly and in accordance with the statutory data protection provisions (in particular the GDPR), and that data subjects can exercise their rights.

The data protection management system includes policies containing, among other things, the following binding requirements:

3.1. Processes for Reporting Personal Data Breaches

Deka has implemented a clearly defined and documented process for detecting, assessing, reporting and following up on personal data breaches. The purpose of this process is to identify personal data breaches without undue delay, assess them appropriately and initiate the measures required under the applicable data protection provisions within the applicable deadlines.

The process comprises, in particular, the following elements:

■ Identification and initial assessment of personal data breaches

Data protection-relevant incidents are recorded and documented according to defined criteria and subjected to an initial expert assessment. This includes, in particular, examining whether a personal data breach within the meaning of the General Data Protection Regulation has occurred.

■ Risk assessment for data subjects

As part of the further assessment, it is determined whether, and to what extent, the incident may result in a risk or a high risk to the rights and freedoms of natural persons. In particular, the nature, scope, sensitivity and volume of the data concerned, the number of data subjects affected, the possible consequences of the incident, and the technical and organizational safeguards already in place are taken into account.

■ Notification to the competent data protection supervisory authority

Where a notification obligation exists, the competent data protection supervisory authority is notified within the statutory deadlines. Deka ensures that the information required for this purpose is gathered and assessed without undue delay and transmitted to the supervisory authority in an appropriate form.

■ Communication to data subjects

Where, based on the statutory assessment, communication to the data subjects is required, it is made without undue delay. The communication contains the information required by law, in particular a description of the nature of the personal data breach, its possible consequences, and the measures taken or proposed to mitigate adverse effects.

■ Initiation of remedial and mitigation measures

Deka takes appropriate technical, organizational and procedural measures to limit the effects of a personal data breach, to prevent further harm, and to restore the confidentiality, integrity and availability of personal data.

■ Documentation and follow-up

All personal data breaches are documented in a traceable manner. This includes, in particular, the facts, the risk assessment, the decisions taken, any notifications and communications, and the remedial measures taken. The documentation also serves as evidence of compliance with data protection requirements.

■ Identification of areas for improvement

Following the handling of an incident, possible causes and structural weaknesses are analyzed. Improvement measures derived from this analysis are incorporated into Deka's data protection management system or data protection program in order to avoid future personal data breaches as far as possible and to continuously increase the effectiveness of existing safeguards.

Through this process, Deka ensures that personal data breaches are detected in a timely manner, legally assessed, properly reported and effectively followed up. Compliance with statutory deadlines, in particular the notification obligations vis-à-vis data protection supervisory authorities, is supported by defined responsibilities, escalation paths and procedural requirements.

3.2. Mandatory Data Protection Training and Employee Awareness

Data protection awareness is an essential component of Deka's data protection management and forms the basis for the lawful, responsible and secure processing of personal data. It helps to integrate data protection requirements effectively into business processes and employees' day-to-day work and to identify and avoid risks to the rights and freedoms of data subjects at an early stage.

The aim of the data protection training and awareness measures is to create ongoing data protection awareness among employees, to embed data protection-compliant conduct sustainably in everyday work, and to foster a lived data protection culture within Deka. Employees are to be enabled to process personal data appropriately, in a purpose-limited manner and confidentially, in compliance with the applicable data protection requirements, in particular the General Data Protection Regulation.

One focus is on raising employees' awareness of the lawful and careful handling of personal data. This includes both conveying basic knowledge of data protection law and providing practical guidance on typical processing situations, confidentiality obligations, data minimization, purpose limitation, storage limitation, data subject rights, and the handling of data protection inquiries and potential personal data breaches.

In addition to the legal fundamentals, organizational and procedural requirements are also conveyed in order to identify data protection risks at an early stage and respond to them appropriately. These include, in particular, internal reporting channels, responsibilities, documentation requirements and rules for handling actual or suspected personal data breaches. This ensures that employees are aware of their responsibilities in data protection and can address data protection-relevant matters in a timely manner.

To promote data protection awareness, Deka relies on mandatory training courses, workshops, e-learning modules and supplementary communication and awareness measures. These formats are designed to be flexible, practical and tailored to specific target groups. Depending on the area of responsibility, function and nature of the handling of personal data, more advanced or in-depth training content may be provided.

Data protection awareness measures address current and practice-relevant topics and use suitable internal communication channels such as intranet articles, newsletters, internal notices, guidelines or information campaigns in order to reach a broad target group and to strengthen attention to data protection topics on a lasting basis.

Participation in mandatory data protection training is documented and tracked. In this way, Deka ensures that employees are regularly informed about their data protection obligations and that the planned training measures are carried out in a traceable manner.

The training and awareness measures are reviewed regularly and adjusted as necessary. Feedback and evaluation processes serve to assess the effectiveness of the measures and to identify potential for improvement. This continuous optimization ensures that the data protection awareness measures meet current legal, regulatory and organizational requirements and that employees remain continuously prepared for their role in data protection.

3.3. Regular Data Protection Analyses and Audits

Deka has implemented appropriate organizational and procedural measures to continuously ensure, and be able to demonstrate, compliance with data protection requirements, in particular the GDPR and the respective applicable national data protection provisions.

To this end, Deka regularly carries out data protection analyses, data protection risk assessments, data protection impact assessments pursuant to Art. 35 GDPR, other privacy impact assessments, and risk-based audits and control measures. The results are documented, assessed and — where necessary — translated into appropriate technical and organizational measures.

Deka's data protection officer performs the duties of the role independently and without being bound by instructions. The data protection officer continuously monitors compliance with data protection requirements and internal data protection policies and advises the responsible departments on the assessment and implementation of necessary data protection measures.

Before new processing activities are introduced or existing processing activities are materially changed, Deka uses bindingly defined processes to ensure that a data protection assessment is carried out. This includes, in particular, reviewing the lawfulness, purpose limitation, data minimization, storage limitation, transparency, and integrity and confidentiality of the processing.

Data protection requirements are already taken into account in the design, procurement, development and change phases of systems, applications, products, services and processes. This includes, in particular, the principles of privacy by design and privacy by default pursuant to Art. 25 GDPR, as well as privacy-enhancing technologies and measures such as pseudonymization, access restrictions, role-based authorization concepts, and logging and control mechanisms.

These processes apply both to in-house developments and to the external sourcing of software, products, services and other forms of performance. In this way, Deka ensures that data protection requirements are taken into account, implemented and monitored in a risk-based and traceable manner throughout the entire life cycle of a processing operation.

3.4. Governance Structures for Data Protection Management

Deka has established governance structures for data protection management that ensure the proper, transparent and traceable implementation of data protection requirements. These structures serve to clearly assign responsibilities, define decision-making and escalation paths, and effectively support compliance with the applicable data protection requirements within the organization.

A key component of data protection governance is the appointment of an independent data protection officer. The data protection officer performs the duties of the role in accordance with the statutory requirements and, in particular, works toward compliance with data protection regulations. The data protection officer advises the responsible units and departments on data protection matters, supports data protection-relevant processes and is available as a point of contact for employees, data subjects and supervisory authorities. The independent position of the data protection officer supports the objective performance of the monitoring and advisory function in data protection.

In addition, Deka has clear rules on internal responsibilities, areas of responsibility and processes for fulfilling data protection obligations. These include, in particular, requirements for the lawful processing of personal data, the documentation of processing activities, the handling of data subject rights, the performance of data protection reviews, and the handling of personal data breaches. Defined roles, processes and interfaces ensure that data protection requirements are appropriately integrated into business processes and taken into account in day-to-day operations.

The data protection organization is also integrated into Deka's overarching management and control structures. At Board of Management level, there is clear responsibility for data protection and information security management. The Board member responsible for these areas helps to ensure that data protection and information security are taken into account as essential components of responsible corporate governance and are strategically embedded.

Through these governance structures, Deka creates the organizational prerequisites for effective data protection management. They promote a clear allocation of responsibilities, appropriate monitoring of data protection-relevant processes, and the ongoing development of the data protection organization in line with statutory, regulatory and internal requirements.

3.5. Reporting to the Board of Management

Deka's Board of Management is informed regularly and whenever circumstances warrant such reporting about the status, effectiveness and further development of the data protection management system. Reporting serves to appropriately involve senior management in data protection-relevant steering, monitoring and decision-making processes and to ensure effective data protection governance within Deka.

The regular reporting to the Board of Management covers, in particular, material developments, risks, measures and control activities relating to the processing of personal data. These include, among others:

■ Results of audits, controls and risk assessments

The Board of Management receives information on relevant results of internal and external reviews, audits, control activities and data protection-related risk assessments. This includes, in particular, identified weaknesses, identified needs for action, recommended measures, and the implementation status of agreed improvement measures.

■ Risk reporting on personal data breaches and data protection risks

Personal data breaches and other relevant data protection-related risks are assessed within the existing reporting and escalation channels and, where necessary, reported to the Board of Management. Reporting covers, in particular, the nature and extent of the risks identified, possible effects on data subjects and on Deka, remedial and mitigation measures taken, and any notification or communication obligations toward supervisory authorities or data subjects.

■ Status of implementation of data protection-relevant processes and initiatives

The Board of Management is informed about the implementation, further development and effectiveness of key data protection processes and data protection initiatives. These include, in particular, measures to strengthen the data

protection management system, implement regulatory requirements, improve internal procedures, and sustainably embed data protection requirements in Deka's business processes.

Reporting is carried out in an appropriate form and with an appropriate level of detail to enable the Board of Management to make a well-founded assessment of the data protection situation, existing risks and necessary measures. On this basis, the Board of Management can appropriately fulfill its steering and oversight responsibility with regard to effective data protection management.

The regular involvement of the Board of Management ensures that data protection risks are addressed transparently, necessary measures are prioritized, and the continuous development of the data protection management system is supported at management level.

3.6. Security Safeguards

Deka commits to implementing appropriate technical and organizational measures to protect personal data and to continuously adapting them to the respective risk situation. These include, in particular, measures to ensure the confidentiality, integrity, availability and resilience of systems, for example through encryption, role- and rights-based authorization management, access controls, firewalls, malware protection, intrusion detection systems and structured vulnerability management.

In addition, Deka ensures recoverability in the event of technical or security-related incidents through backup and emergency procedures, defined incident and crisis management processes, and clear responsibilities. The effectiveness of the safeguards is regularly reviewed through controls, audits, evaluations and feedback processes and adjusted as necessary. Furthermore, binding security requirements, training, awareness measures and target group-specific awareness activities promote an appropriate level of security awareness among employees and help protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access.

3.7. Obliging and Auditing Service Providers

Deka obligates service providers, suppliers, business partners and other third parties that process personal data on behalf of Deka or obtain access to Deka's data, systems or processes to comply with an appropriate level of data protection and information security that meets Deka's requirements.

Before an engagement and before any processing of personal data begins, a risk-based review of the respective service provider is carried out. This covers, in particular, data protection requirements, information security requirements, and technical and organizational measures. It is examined whether the service provider offers the necessary guarantees for data protection-compliant and secure processing and meets Deka's regulatory, contractual and internal security requirements.

Personal data is processed by service providers exclusively on the basis of binding contractual arrangements, in particular data processing agreements pursuant to Art. 28 GDPR, where applicable, as well as supplementary agreements on information security, control rights, notification obligations, emergency and recovery measures, and compliance with Deka's internal requirements. In this context, Deka specifies appropriate technical and organizational measures for data security, in particular for protection against unauthorized access, loss, alteration, disclosure or other unlawful processing.

Compliance with these requirements is monitored through contractually agreed control and audit rights, regular risk-based reviews, self-assessments, audits and other control measures. The relevant review and audit intervals are determined by Deka's internal requirements and by the nature, scope, criticality and risk profile of the respective service.

Where a service provider uses further subcontractors or sub-service providers, it is contractually obligated to pass on accordingly the data protection, information security and control requirements agreed with Deka. The use of sub-

service providers is subject to the agreed transparency, review and approval requirements and to appropriate integration into Deka's risk and control management.

3.8. Use of Customer Data

Deka processes customer data exclusively for specified, explicit and lawful purposes. Customer data is used, in particular, where this is necessary for the establishment, performance or termination of a contractual relationship or where another legal basis permits or requires the processing. This includes, in particular, regulatory and supervisory obligations, for example in connection with know-your-customer checks, anti-money laundering, sanctions list screening, tax requirements and other statutory documentation and verification obligations.

Customer data is processed for purposes other than those originally intended only if there is a separate legal basis for doing so. This is the case, in particular, if the customer has given express consent or if the further processing is compatible with the purposes for which the data was originally collected. In such cases, Deka examines whether the statutory requirements regarding purpose limitation, transparency and proportionality are met.

Where customer data is to be used beyond the mere performance of a contract, Deka provides customers with transparent and tiered consent options. This enables customers to decide for themselves whether, and to what extent, their data may be processed, for example, for advisory, information, analysis or marketing purposes. As a rule, consent is given on a voluntary basis and in accordance with the opt-in principle.

Customer data is disclosed or made available to third parties for advertising purposes only if the customer has given prior express consent or if another statutory permission applies. Without an appropriate legal basis, customer data is not transferred to third parties for third-party advertising purposes.

For advertising communications by email or telephone, Deka generally obtains the customer's prior consent. Where an email address has been collected in the context of an existing customer or contractual relationship and is to be used for Deka's own advertising information, Deka informs the customer of this at the time the address is collected and points out the existing right to object.

Customers may object at any time, with effect for the future, to the use of their data for direct marketing purposes, in particular by email, telephone or mail. Likewise, consent that has been given may be withdrawn at any time. The withdrawal or objection does not affect the lawfulness of the processing carried out up to that point. Deka ensures that customers' corresponding preferences are taken into account without undue delay and implemented in the relevant systems.

4. Contact Information

For questions regarding the processing of personal data and for asserting data subject rights under data protection law, in particular the rights of access, rectification, erasure, restriction of processing, data portability or objection, data subjects may contact Deka.

DekaBank Deutsche Girozentrale
Große Gallusstraße 14
60315 Frankfurt am Main
Phone: +49 69 7147-652
Email: service@deka.de

In addition, data subjects may contact Deka's data protection officer directly with questions, concerns or complaints in connection with the processing of their personal data.

DekaBank Deutsche Girozentrale
Data Protection Officer

Große Gallusstraße 14
60315 Frankfurt am Main
Email: datenschutz@deka.de

The above contact options are available, in particular, for matters relating to the exercise of data subject rights and for data protection-related reports, complaints or other inquiries.

5. Continuous Development of the Data Protection Management System

Deka commits to continuously developing its data protection management system and adapting it to statutory, regulatory, organizational and procedural requirements. The continuous improvement process is a central element in this regard, serving to continuously strengthen the effectiveness of data protection management and to ensure a traceable, sustainable and legally compliant implementation of data protection requirements.

Through regular reviews and adjustments of data protection-relevant processes, measures and controls, Deka ensures that the data protection management system meets the respective applicable requirements and can respond appropriately to new developments. In particular, findings from personal data breaches, internal and external reviews, audits, risk analyses, control activities, complaints, data subject requests, and regulatory or organizational changes are taken into account.

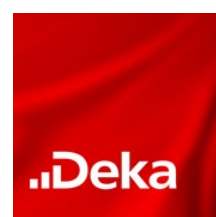
The methodology and implementation of the continuous improvement process are based on a structured procedural model, in particular the PDCA cycle — Plan, Do, Check, Act. This approach enables the systematic planning, implementation, review and adjustment of data protection-related measures and processes. In this way, it is ensured that data protection is not merely implemented through isolated measures, but is permanently integrated into the relevant business processes and continuously optimized.

The aim of the continuous improvement process is the ongoing development and sustainable strengthening of Deka's data protection management system. To this end, all relevant processes, measures and controls are regularly reviewed, assessed and adjusted as necessary. This is intended to identify data protection risks at an early stage, manage them appropriately, and effectively protect the rights and freedoms of data subjects.

To ensure the effectiveness of the data protection management system, Deka uses suitable control and review mechanisms across all relevant data protection processes. These serve the structured and traceable monitoring of data protection-related requirements and support the ongoing assessment of the appropriateness and effectiveness of the measures implemented.

The results of controls, reviews and other assessment tools are evaluated as part of the continuous improvement process and translated into specific optimization measures. In doing so, identified needs for action are prioritized, responsibilities are assigned and implementation progress is tracked. Relevant findings, progress and measures are communicated to the respective responsible internal stakeholders and taken into account in ongoing processes.

Through this structured improvement approach, Deka ensures that its data protection management system is continuously developed, effectively monitored and adapted to changing conditions. This supports sustainable data protection governance and ongoing compliance with data protection requirements within Deka.



DekaBank
Deutsche Girozentrale
Große Gallusstraße 14
60315 Frankfurt am Main
Postfach 11 05 23
60040 Frankfurt

Telefon: (0 69) 7147 - 0
Telefax: (0 69) 7147 - 1376
www.deka.de

