

Datenschutzrichtlinie und -programm der Deka

Stand: 09/2026, Version 1.1

..Deka



	Seite
1. Gegenstand und Anwendungsbereich	3
2. Datenschutzhinweise (Data Privacy Policies) und Betroffenenrechte	3
3. Datenschutzmanagement	4
3.1. Prozesse zur Meldung von Datenschutzverletzungen	4
3.2. Verpflichtende Datenschutzbildungen und Sensibilisierung der Mitarbeitenden	5
3.3. Regelmäßige Datenschutzbildungen und Audits	6
3.4. Governance-Strukturen für das Datenschutzmanagement	7
3.5. Berichterstattung an den Vorstand	7
3.6. Sicherheitsvorkehrungen	8
3.7. Verpflichtung und Auditierung von Dienstleistern	8
3.8. Nutzung von Kundendaten	9
4. Kontaktdaten	10
5. Kontinuierliche Weiterentwicklung des Datenschutz-Managementsystems	10

1. Gegenstand und Anwendungsbereich

Für die DekaBank Deutsche Girozentrale (in diesem Dokument „Deka“ genannt) ist der Datenschutz ein zentraler Bestandteil der Geschäftspolitik und unterstützt die Wertschöpfung des Unternehmens. Der Schutz personenbezogener Daten von Kunden und Geschäftspartnern bildet die Basis für deren Vertrauen und trägt maßgeblich zur positiven Reputation der Deka in der Öffentlichkeit bei. Vertrauen und Transparenz sind daher essenzielle Grundpfeiler für den Umgang mit personenbezogenen Daten und stellen zugleich wichtige Unternehmensziele dar.

Um die Anforderungen an den Schutz personenbezogener Daten zu erfüllen und die Vorgaben der Datenschutzgrundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG), des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG) sowie weiterer relevanter Datenschutzvorschriften einzuhalten, wurde ein Datenschutz-Managementsystem etabliert. Dieses bildet eine strukturierte Grundlage, um Datenschutzanforderungen in den Geschäftsprozessen zu integrieren und langfristig zu sichern.

Die Datenschutzrichtlinie und -programm verpflichtet alle Geschäftsbereiche und deren Geschäftstätigkeiten der Deka zur Beachtung und Einhaltung.

2. Datenschutzhinweise (Data Privacy Policies) und Betroffenenrechte

Die Deka informiert die betroffenen Personen in transparenter, verständlicher und leicht zugänglicher Weise über die Verarbeitung ihrer personenbezogenen Daten. Hierzu legt die Deka insbesondere dar,

- welche personenbezogenen Daten verarbeitet werden,
- zu welchen Zwecken und auf welcher Rechtsgrundlage die Verarbeitung erfolgt,
- an welche Empfänger oder Kategorien von Empfängern personenbezogene Daten übermittelt oder diesen bereitgestellt werden,
- nach welchen Kriterien sich die Dauer der Speicherung bzw. die Löschung der Daten bemisst, und
- welche Rechte den betroffenen Personen nach den jeweils anwendbaren datenschutzrechtlichen Vorschriften, insbesondere der Datenschutz-Grundverordnung, zustehen.

Die Erfüllung dieser Informationspflichten erfolgt insbesondere durch die von der Deka bereitgestellten Datenschutzhinweise. Diese sind nach dem jeweiligen Verarbeitungszweck strukturiert und über die unter **www.deka.de/datenschutz** bereitgestellten Links abrufbar. Die in den Datenschutzhinweisen enthaltenen Angaben sind für die Deka verbindlich und bilden die maßgebliche Grundlage für die Information der betroffenen Personen über Art, Umfang und Zwecke der jeweiligen Datenverarbeitung. Dies gilt gleichermaßen für die dort enthaltenen Informationen zu den Betroffenenrechten, insbesondere im Dokument „Ihre Rechte nach der Datenschutz-Grundverordnung“.

Betroffene Personen haben nach Maßgabe der gesetzlichen Vorgaben insbesondere das Recht auf Auskunft über die sie betreffenden personenbezogenen Daten. Darüber hinaus können ihnen – abhängig von den jeweiligen gesetzlichen Voraussetzungen – Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit sowie ein Recht auf Widerspruch gegen bestimmte Verarbeitungen zustehen. Soweit eine Verarbeitung auf einer Einwilligung beruht, besteht zudem das Recht, diese Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen.

Zur Wahrnehmung ihrer Rechte sowie bei Fragen, Anliegen, Bedenken oder Beschwerden im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten können sich betroffene Personen an die in den jeweiligen Datenschutzhinweisen benannten Verantwortlichen, an den dort genannten Datenschutzbeauftragten sowie an die zuständigen Datenschutzaufsichtsbehörden wenden.

Die Deka verfügt über ein etabliertes Verfahren zur Bearbeitung von Anfragen und Beschwerden mit Datenschutzbezug. Dieses Verfahren sieht klar definierte Zuständigkeiten, Bearbeitungsschritte und Fristen vor, um eine ordnungsgemäße, fristgerechte und nachvollziehbare Bearbeitung entsprechender Anliegen sicherzustellen.

Die Deka verpflichtet sich, die Datenschutzhinweise regelmäßig sowie anlassbezogen zu überprüfen und bei Bedarf zu aktualisieren. Wesentliche Änderungen, die für die betroffenen Personen von Bedeutung sind, werden in geeigneter Weise kommuniziert, beispielsweise per E-Mail, über die Website oder über sonstige angemessene Informationskanäle.

3. Datenschutzmanagement

Die Deka verpflichtet sich mit einem umfassenden Datenschutz-Managementsystem die Einhaltung des Datenschutzes sicherzustellen.

Das Datenschutz-Managementsystem legt Grundsätze, Prozesse und Maßnahmen dar, die sicherstellen, dass personenbezogene Daten durch die Deka transparent, fair und im Einklang mit den gesetzlichen Bestimmungen zum Datenschutz (insbesondere der DSGVO) verarbeitet werden und Betroffene ihre Rechte wahrnehmen können.

Das Datenschutz-Management-System beinhaltet Richtlinien, u.a. mit folgenden verbindlichen Vorgaben:

3.1. Prozesse zur Meldung von Datenschutzverletzungen

Die Deka hat einen klar definierten und dokumentierten Prozess zur Erkennung, Bewertung, Meldung und Nachbearbeitung von Datenschutzverletzungen implementiert. Dieser Prozess dient dazu, Datenschutzverletzungen unverzüglich zu identifizieren, angemessen zu bewerten und die nach den anwendbaren datenschutzrechtlichen Vorgaben erforderlichen Maßnahmen fristgerecht einzuleiten.

Der Prozess umfasst insbesondere folgende Bestandteile:

■ Identifikation und Erstbewertung von Datenschutzverletzungen

Datenschutzrelevante Vorfälle werden nach festgelegten Kriterien erfasst, dokumentiert und einer ersten fachlichen Bewertung unterzogen. Dabei wird insbesondere geprüft, ob eine Verletzung des Schutzes personenbezogener Daten im Sinne der Datenschutz-Grundverordnung vorliegt.

■ Risikobewertung für betroffene Personen

Im Rahmen der weiteren Bewertung wird ermittelt, ob und in welchem Umfang durch den Vorfall ein Risiko oder ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bestehen kann. Hierbei werden insbesondere Art, Umfang, Sensibilität und Menge der betroffenen Daten, die Anzahl der betroffenen Personen, mögliche Folgen des Vorfalls sowie bereits ergriffene technische und organisatorische Schutzmaßnahmen berücksichtigt.

■ Meldung an die zuständige Datenschutzaufsichtsbehörde

Soweit eine Meldepflicht besteht, erfolgt die Meldung an die zuständige Datenschutzaufsichtsbehörde innerhalb der gesetzlich vorgesehenen Fristen. Die Deka stellt sicher, dass die hierfür erforderlichen Informationen unverzüglich zusammengetragen, bewertet und in geeigneter Form an die Aufsichtsbehörde übermittelt werden.

■ Benachrichtigung betroffener Personen

Sofern nach der gesetzlichen Bewertung eine Benachrichtigung der betroffenen Personen erforderlich ist, erfolgt diese ohne unangemessene Verzögerung. Die Benachrichtigung enthält die gesetzlich erforderlichen Informationen, insbesondere eine Beschreibung der Art der Datenschutzverletzung, mögliche Folgen sowie die ergriffenen oder vorgeschlagenen Maßnahmen zur Begrenzung nachteiliger Auswirkungen.

■ Einleitung von Abhilfe- und Begrenzungsmaßnahmen

Die Deka ergreift angemessene technische, organisatorische und prozessuale Maßnahmen, um die Auswirkungen einer Datenschutzverletzung zu begrenzen, weitere Beeinträchtigungen zu vermeiden und die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten wiederherzustellen.

■ Dokumentation und Nachbereitung

Alle Datenschutzverletzungen werden nachvollziehbar dokumentiert. Dies umfasst insbesondere den Sachverhalt, die Bewertung der Risiken, die getroffenen Entscheidungen, etwaige Meldungen und Benachrichtigungen sowie die ergriffenen Abhilfemaßnahmen. Die Dokumentation dient zugleich dem Nachweis der Einhaltung datenschutzrechtlicher Anforderungen.

■ Identifikation von Verbesserungsbedarfen

Im Anschluss an die Bearbeitung eines Vorfalls erfolgt eine Analyse möglicher Ursachen und struktureller Schwachstellen. Daraus abgeleitete Verbesserungsmaßnahmen fließen in das Datenschutz-Managementsystem bzw. Datenschutzprogramm der Deka ein, um künftige Datenschutzverletzungen möglichst zu vermeiden und die Wirksamkeit bestehender Schutzmaßnahmen fortlaufend zu erhöhen.

Durch diesen Prozess stellt die Deka sicher, dass Datenschutzverletzungen rechtzeitig erkannt, rechtlich bewertet, ordnungsgemäß gemeldet und wirksam nachbearbeitet werden. Die Einhaltung gesetzlicher Fristen, insbesondere der Meldepflichten gegenüber Datenschutzaufsichtsbehörden, wird durch definierte Zuständigkeiten, Eskalationswege und Verfahrensvorgaben unterstützt.

3.2. Verpflichtende Datenschutzzschulungen und Sensibilisierung der Mitarbeitenden

Awareness für Datenschutz ist ein wesentlicher Bestandteil des Datenschutzmanagements der Deka und bildet die Grundlage für die rechtskonforme, verantwortungsvolle und sichere Verarbeitung personenbezogener Daten. Sie trägt dazu bei, datenschutzrechtliche Anforderungen wirksam in die Geschäftsprozesse und die tägliche Arbeit der Mitarbeitenden zu integrieren sowie Risiken für die Rechte und Freiheiten betroffener Personen frühzeitig zu erkennen und zu vermeiden.

Ziel der Datenschutzzschulungen und Sensibilisierungsmaßnahmen ist es, bei den Mitarbeitenden ein kontinuierliches Datenschutzbewusstsein zu schaffen, datenschutzkonformes Verhalten nachhaltig im Arbeitsalltag zu verankern und eine gelebte Datenschutzkultur innerhalb der Deka zu fördern. Die Mitarbeitenden sollen befähigt werden, personenbezogene Daten unter Beachtung der geltenden datenschutzrechtlichen Vorgaben, insbesondere der Datenschutz-Grundverordnung, sachgerecht, zweckgebunden und vertraulich zu verarbeiten.

Ein Schwerpunkt liegt in der Sensibilisierung der Mitarbeitenden für den rechtmäßigen und sorgfältigen Umgang mit personenbezogenen Daten. Dies umfasst sowohl die Vermittlung grundlegender datenschutzrechtlicher Kenntnisse als auch praxisorientierte Hinweise zu typischen Verarbeitungssituationen, Vertraulichkeitspflichten, Datenminimierung, Zweckbindung, Speicherbegrenzung, Betroffenenrechten sowie zum Umgang mit Datenschutzanfragen und möglichen Datenschutzverletzungen.

Neben rechtlichen Grundlagen werden auch organisatorische und prozessuale Anforderungen vermittelt, um Datenschutzrisiken frühzeitig zu erkennen und angemessen darauf zu reagieren. Hierzu zählen insbesondere interne Meldewege, Zuständigkeiten, Dokumentationsanforderungen sowie Vorgaben zum Umgang mit tatsächlichen oder vermuteten Datenschutzverletzungen. Dadurch wird sichergestellt, dass Mitarbeitende ihre Verantwortung im Datenschutz kennen und datenschutzrelevante Sachverhalte rechtzeitig adressieren können.

Zur Förderung des Datenschutzbewusstseins setzt die Deka auf verpflichtende Schulungen, Workshops, E-Learning-Module sowie ergänzende Kommunikations- und Sensibilisierungsmaßnahmen. Diese Formate werden flexibel, praxisnah und zielgruppenspezifisch ausgestaltet. Je nach Aufgabenbereich, Funktion und Art des Umgangs mit personenbezogenen Daten können weiterführende oder vertiefende Schulungsinhalte vorgesehen werden.

Datenschutzbezogene Awareness-Maßnahmen greifen aktuelle und praxisrelevante Themen auf und nutzen geeignete interne Kommunikationskanäle wie beispielsweise Intranetbeiträge, Newsletter, interne Hinweise, Leitfäden oder Informationskampagnen, um eine breite Zielgruppe zu erreichen und die Aufmerksamkeit für Datenschutzthemen dauerhaft zu stärken.

Die Teilnahme an verpflichtenden Datenschutzs Schulungen wird dokumentiert und nachgehalten. Hierdurch stellt die Deka sicher, dass Mitarbeitende regelmäßig über ihre datenschutzrechtlichen Pflichten informiert werden und die vorgesehenen Schulungsmaßnahmen nachvollziehbar durchgeführt werden.

Die Schulungs- und Sensibilisierungsmaßnahmen werden regelmäßig überprüft und bei Bedarf angepasst. Feedback- und Evaluationsprozesse dienen dazu, die Wirksamkeit der Maßnahmen zu bewerten und Verbesserungspotenziale zu identifizieren. Diese kontinuierliche Optimierung stellt sicher, dass die Datenschutz-Awareness-Maßnahmen aktuellen rechtlichen, regulatorischen und organisatorischen Anforderungen entsprechen und die Mitarbeitenden fortlaufend auf ihre Rolle im Datenschutz vorbereitet bleiben.

3.3. Regelmäßige Datenschutzanalysen und Audits

Die Deka hat angemessene organisatorische und prozessuale Maßnahmen implementiert, um die Einhaltung der datenschutzrechtlichen Anforderungen, insbesondere der DSGVO und der jeweils anwendbaren nationalen Datenschutzvorschriften, fortlaufend sicherzustellen und nachweisen zu können.

Hierzu führt die Deka regelmäßig Datenschutzanalysen, Datenschutz-Risikobewertungen, Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO, sonstige Privacy Impact Assessments sowie risikoorientierte Audits und Kontrollmaßnahmen durch. Die Ergebnisse werden dokumentiert, bewertet und — soweit erforderlich — in angemessene technische und organisatorische Maßnahmen überführt.

Der Datenschutzbeauftragte der Deka nimmt seine Aufgaben unabhängig und weisungsfrei wahr. Er überwacht fortlaufend die Einhaltung der datenschutzrechtlichen Vorgaben sowie der internen Datenschutzrichtlinien und berät die verantwortlichen Fachbereiche bei der Bewertung und Umsetzung erforderlicher Datenschutzmaßnahmen.

Vor der Einführung neuer oder der wesentlichen Änderung bestehender Verarbeitungstätigkeiten stellt die Deka durch verbindlich definierte Prozesse sicher, dass eine datenschutzrechtliche Bewertung erfolgt. Dabei werden insbesondere Rechtmäßigkeit, Zweckbindung, Datenminimierung, Speicherbegrenzung, Transparenz sowie Integrität und Vertraulichkeit der Verarbeitung geprüft.

Datenschutzanforderungen werden bereits in der Konzeptions-, Beschaffungs-, Entwicklungs- und Änderungsphase von Systemen, Anwendungen, Produkten, Dienstleistungen und Prozessen berücksichtigt. Dies umfasst insbesondere die Grundsätze Privacy by Design und Privacy by Default gemäß Art. 25 DSGVO sowie datenschutzfördernde Technologien und Maßnahmen wie Pseudonymisierung, Zugriffsbeschränkungen, rollenbasierte Berechtigungskonzepte, Protokollierungs- und Kontrollmechanismen.

Diese Prozesse gelten sowohl für Eigenentwicklungen als auch für den Fremdbezug von Software, Produkten, Dienstleistungen und sonstigen Leistungen. Dadurch stellt die Deka sicher, dass Datenschutzanforderungen risikoorientiert, nachvollziehbar und über den gesamten Lebenszyklus einer Verarbeitung hinweg berücksichtigt, umgesetzt und überwacht werden.

3.4. Governance-Strukturen für das Datenschutzmanagement

Die Deka verfügt über etablierte Governance-Strukturen für das Datenschutzmanagement, die eine ordnungsgemäße, transparente und nachvollziehbare Umsetzung datenschutzrechtlicher Anforderungen sicherstellen. Diese Strukturen dienen dazu, Verantwortlichkeiten eindeutig zuzuweisen, Entscheidungs- und Eskalationswege festzulegen sowie die Einhaltung der geltenden Datenschutzvorgaben innerhalb der Organisation wirksam zu unterstützen.

Ein wesentlicher Bestandteil der Datenschutz-Governance ist die Benennung eines unabhängigen Datenschutzbeauftragten. Der Datenschutzbeauftragte nimmt seine Aufgaben nach Maßgabe der gesetzlichen Anforderungen wahr und wirkt insbesondere auf die Einhaltung der datenschutzrechtlichen Vorschriften hin. Er berät die verantwortlichen Stellen und Fachbereiche in Datenschutzfragen, begleitet datenschutzrelevante Prozesse und steht als Ansprechpartner für Mitarbeitende, betroffene Personen sowie Aufsichtsbehörden zur Verfügung. Seine unabhängige Stellung unterstützt eine objektive Wahrnehmung der Kontroll- und Beratungsfunktion im Datenschutz.

Darüber hinaus bestehen innerhalb der Deka klare Regelungen zu internen Verantwortlichkeiten, Zuständigkeiten und Prozessen zur Erfüllung datenschutzrechtlicher Pflichten. Diese umfassen insbesondere Vorgaben zur rechtmäßigen Verarbeitung personenbezogener Daten, zur Dokumentation von Verarbeitungstätigkeiten, zur Bearbeitung von Betroffenenrechten, zur Durchführung datenschutzrechtlicher Prüfungen sowie zum Umgang mit Datenschutzverletzungen. Durch definierte Rollen, Prozesse und Schnittstellen wird sichergestellt, dass datenschutzrechtliche Anforderungen angemessen in Geschäftsprozesse integriert und im operativen Betrieb berücksichtigt werden.

Die Datenschutzorganisation ist zudem in die übergeordneten Leitungs- und Kontrollstrukturen der Deka eingebunden. Auf Vorstandsebene besteht eine klare Verantwortlichkeit für die Themen Datenschutz und Informationssicherheitsmanagement. Das hierfür zuständige Vorstandsmitglied trägt dazu bei, dass Datenschutz und Informationssicherheit als wesentliche Bestandteile einer verantwortungsvollen Unternehmensführung berücksichtigt und strategisch verankert werden.

Durch diese Governance-Strukturen schafft die Deka die organisatorischen Voraussetzungen für ein wirksames Datenschutzmanagement. Sie fördern eine klare Verantwortungszuordnung, eine angemessene Überwachung datenschutzrelevanter Prozesse sowie die fortlaufende Weiterentwicklung der Datenschutzorganisation im Einklang mit gesetzlichen, regulatorischen und internen Anforderungen.

3.5. Berichterstattung an den Vorstand

Der Vorstand der Deka wird regelmäßig und anlassbezogen über den Status, die Wirksamkeit und die Weiterentwicklung des Datenschutz-Managementsystems informiert. Die Berichterstattung dient der angemessenen Einbindung der Unternehmensleitung in datenschutzrelevante Steuerungs-, Überwachungs- und Entscheidungsprozesse sowie der Sicherstellung einer wirksamen Datenschutz-Governance innerhalb der Deka.

Die regelmäßige Information des Vorstands umfasst insbesondere wesentliche Entwicklungen, Risiken, Maßnahmen und Kontrollhandlungen im Zusammenhang mit der Verarbeitung personenbezogener Daten. Hierzu zählen unter anderem:

■ Ergebnisse von Audits, Kontrollen und Risikobewertungen

Der Vorstand erhält Informationen über relevante Ergebnisse aus internen und externen Prüfungen, Audits, Kontrollhandlungen sowie datenschutzbezogenen Risikobewertungen. Dies umfasst insbesondere festgestellte Schwachstellen, identifizierte Handlungsbedarfe, empfohlene Maßnahmen sowie den Status der Umsetzung vereinbarter Verbesserungsmaßnahmen.

■ Risikoberichterstattung zu Datenschutzverletzungen und Datenschutzrisiken

Datenschutzverletzungen und sonstige relevante datenschutzbezogene Risiken werden im Rahmen der bestehenden Berichts- und Eskalationswege bewertet und, soweit erforderlich, an den Vorstand berichtet. Die Berichterstattung umfasst insbesondere Art und Umfang der festgestellten Risiken, mögliche Auswirkungen auf betroffene Personen und die Deka, ergriffene Abhilfe- und Begrenzungsmaßnahmen sowie etwaige Melde- oder Benachrichtigungspflichten gegenüber Aufsichtsbehörden oder betroffenen Personen.

■ Status der Umsetzung datenschutzrelevanter Prozesse und Initiativen

Der Vorstand wird über die Implementierung, Weiterentwicklung und Wirksamkeit wesentlicher Datenschutzprozesse und Datenschutzinitiativen informiert. Dazu gehören insbesondere Maßnahmen zur Stärkung des Datenschutz-Managementsystems, zur Umsetzung regulatorischer Anforderungen, zur Verbesserung interner Verfahren sowie zur nachhaltigen Verankerung datenschutzrechtlicher Vorgaben in den Geschäftsprozessen der Deka.

Die Berichterstattung erfolgt in geeigneter Form und mit angemessener Detailtiefe, um dem Vorstand eine fundierte Beurteilung der Datenschutzlage, bestehender Risiken und erforderlicher Maßnahmen zu ermöglichen. Auf dieser Grundlage kann der Vorstand seiner Steuerungs- und Überwachungsverantwortung im Hinblick auf ein wirksames Datenschutzmanagement angemessen nachkommen.

Durch die regelmäßige Einbindung des Vorstands wird sichergestellt, dass Datenschutzrisiken transparent adressiert, notwendige Maßnahmen priorisiert und die kontinuierliche Weiterentwicklung des Datenschutz-Managementsystems auf Leitungsebene unterstützt werden.

3.6. Sicherheitsvorkehrungen

Die Deka verpflichtet sich, angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten umzusetzen und fortlaufend an die jeweilige Risikolage anzupassen. Hierzu zählen insbesondere Maßnahmen zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, etwa durch Verschlüsselung, ein rollen- und rechtebasiertes Berechtigungsmanagement, Zugriffskontrollen, Firewalls, Malware-Schutz, Intrusion-Detection-Systeme sowie ein strukturiertes Schwachstellenmanagement.

Darüber hinaus stellt die Deka durch Backup- und Notfallverfahren, definierte Prozesse des Vorfalls- und Krisenmanagements sowie klare Verantwortlichkeiten die Wiederherstellungsfähigkeit bei technischen oder sicherheitsrelevanten Zwischenfällen sicher. Die Wirksamkeit der Schutzmaßnahmen wird regelmäßig durch Kontrollen, Audits, Evaluationen und Feedback-Prozesse überprüft und bei Bedarf angepasst. Ergänzend fördern verbindliche Sicherheitsvorgaben, Schulungen, Awareness-Maßnahmen und zielgruppenspezifische Sensibilisierungen ein angemessenes Sicherheitsbewusstsein der Mitarbeitenden und tragen dazu bei, personenbezogene Daten vor unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff zu schützen.

3.7. Verpflichtung und Auditierung von Dienstleistern

Die Deka verpflichtet Dienstleister, Lieferanten, Geschäftspartner sowie sonstige Dritte, die personenbezogene Daten im Auftrag der Deka verarbeiten oder Zugriff auf Daten, Systeme oder Prozesse der Deka erhalten, zur Einhaltung eines angemessenen und den Anforderungen der Deka entsprechenden Datenschutz- und Informationssicherheitsniveaus.

Vor der Beauftragung und vor Aufnahme einer Verarbeitung personenbezogener Daten erfolgt eine risikoorientierte Prüfung des jeweiligen Dienstleisters. Diese umfasst insbesondere datenschutzrechtliche Anforderungen, Vorgaben zur Informationssicherheit und technische und organisatorische Maßnahmen. Dabei wird geprüft, ob der Dienstleister die erforderlichen Garantien für eine datenschutzkonforme und sichere Verarbeitung bietet und die regulatorischen, vertraglichen und internen Sicherheitsanforderungen der Deka erfüllt.

Die Verarbeitung personenbezogener Daten durch Dienstleister erfolgt ausschließlich auf Grundlage verbindlicher vertraglicher Regelungen, insbesondere durch Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO, soweit einschlägig, sowie ergänzender Vereinbarungen zu Informationssicherheit, Kontrollrechten, Meldepflichten, Notfall- und Wiederherstellungsmaßnahmen sowie zur Einhaltung interner Vorgaben der Deka. Die Deka gibt hierbei angemessene technische und organisatorische Maßnahmen zur Datensicherheit vor, insbesondere zum Schutz vor unbefugtem Zugriff, Verlust, Veränderung, Offenlegung oder sonstiger unrechtmäßiger Verarbeitung.

Die Einhaltung dieser Anforderungen wird durch vertraglich vereinbarte Kontroll- und Auditrechte, regelmäßige risikoorientierte Überprüfungen, Self-Assessments, Audits sowie sonstige Kontrollmaßnahmen überwacht. Die maßgeblichen Prüf- und Auditintervalle richten sich nach internen Vorgaben der Deka sowie nach Art, Umfang, Kritikalität und Risikogehalt der jeweiligen Dienstleistung.

Sofern ein Dienstleister weitere Unterauftragnehmer oder Subdienstleister einsetzt, wird er vertraglich verpflichtet, die mit der Deka vereinbarten Datenschutz-, Informationssicherheits- und Kontrollanforderungen entsprechend weiterzugeben. Der Einsatz von Subdienstleistern unterliegt den vereinbarten Transparenz-, Prüf- und Zustimmungserfordernissen sowie einer angemessenen Einbindung in das Risiko- und Kontrollmanagement der Deka.

3.8. Nutzung von Kundendaten

Die Deka verarbeitet Kundendaten ausschließlich zu festgelegten, eindeutigen und rechtmäßigen Zwecken. Eine Nutzung erfolgt insbesondere, soweit dies zur Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses erforderlich ist oder eine sonstige gesetzliche Grundlage die Verarbeitung erlaubt oder vorschreibt. Hierzu zählen insbesondere regulatorische und aufsichtsrechtliche Verpflichtungen, etwa im Zusammenhang mit Know-Your-Customer-Prüfungen, der Geldwäscheprävention, Sanktionslistenprüfungen, steuerrechtlichen Vorgaben sowie sonstigen gesetzlichen Dokumentations- und Nachweispflichten.

Eine Verarbeitung von Kundendaten zu anderen als den ursprünglich vorgesehenen Zwecken erfolgt nur, sofern hierfür eine gesonderte Rechtsgrundlage besteht. Dies ist insbesondere der Fall, wenn der Kunde ausdrücklich eingewilligt hat oder wenn die weitere Verarbeitung mit den ursprünglichen Erhebungszwecken vereinbar ist. Die Deka prüft in diesen Fällen, ob die gesetzlichen Anforderungen an Zweckbindung, Transparenz und Verhältnismäßigkeit eingehalten werden.

Soweit Kundendaten über die reine Vertragserfüllung hinaus genutzt werden sollen, stellt die Deka den Kunden transparente und abgestufte Einwilligungsmöglichkeiten zur Verfügung. Kunden können dadurch selbst bestimmen, ob und in welchem Umfang ihre Daten beispielsweise für Beratungs-, Informations-, Analyse- oder Marketingzwecke verarbeitet werden dürfen. Die Einwilligungen erfolgen grundsätzlich auf freiwilliger Basis und nach dem Opt-In-Prinzip.

Eine Weitergabe oder Überlassung von Kundendaten an Dritte zu Werbezwecken erfolgt ausschließlich, wenn der Kunde hierin zuvor ausdrücklich eingewilligt hat oder eine andere gesetzliche Erlaubnis besteht. Ohne eine entsprechende Rechtsgrundlage werden Kundendaten nicht für fremde Werbezwecke an Dritte übermittelt.

Für werbliche Ansprachen per E-Mail oder Telefon holt die Deka grundsätzlich eine vorherige Einwilligung des Kunden ein. Soweit eine E-Mail-Adresse im Rahmen einer bestehenden Kunden- oder Vertragsbeziehung erhoben wurde und für eigene werbliche Informationen genutzt werden soll, informiert die Deka den Kunden bereits bei Erhebung der Adresse hierüber und weist auf das bestehende Widerspruchsrecht hin.

Kunden können der Nutzung ihrer Daten für Zwecke der Direktwerbung, insbesondere per E-Mail, Telefon oder Post, jederzeit mit Wirkung für die Zukunft widersprechen. Ebenso können erteilte Einwilligungen jederzeit widerrufen werden. Der Widerruf oder Widerspruch hat keine Auswirkungen auf die Rechtmäßigkeit der bis dahin erfolgten Verarbeitung. Die Deka stellt sicher, dass entsprechende Präferenzen der Kunden unverzüglich berücksichtigt und in den relevanten Systemen umgesetzt werden.

4. Kontaktdaten

Für Fragen zur Verarbeitung personenbezogener Daten sowie zur Geltendmachung datenschutzrechtlicher Betroffenenrechte, insbesondere auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch, können sich betroffene Personen an die Deka wenden.

DekaBank Deutsche Girozentrale
Große Gallusstraße 14
60315 Frankfurt am Main
Telefon (0 69) 71 47 – 652
E-Mail: service@deka.de

Darüber hinaus können sich betroffene Personen bei Fragen, Bedenken oder Beschwerden im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten unmittelbar an den Datenschutzbeauftragten der Deka wenden.

DekaBank Deutsche Girozentrale
Datenschutzbeauftragter
Große Gallusstraße 14
60315 Frankfurt am Main
E-Mail: datenschutz@deka.de

Die vorstehenden Kontaktmöglichkeiten stehen insbesondere für Anliegen im Zusammenhang mit der Wahrnehmung von Betroffenenrechten sowie für datenschutzbezogene Hinweise, Beschwerden oder sonstige Anfragen zur Verfügung.

5. Kontinuierliche Weiterentwicklung des Datenschutz-Managementsystems

Die Deka verpflichtet sich, ihr Datenschutz-Managementsystem kontinuierlich weiterzuentwickeln und an gesetzliche, regulatorische, organisatorische sowie prozessuale Anforderungen anzupassen. Der kontinuierliche Verbesserungsprozess bildet hierbei einen zentralen Bestandteil, um die Wirksamkeit des Datenschutzmanagements fortlaufend zu stärken und eine nachvollziehbare, nachhaltige sowie rechtskonforme Umsetzung datenschutzrechtlicher Anforderungen sicherzustellen.

Durch regelmäßige Überprüfungen und Anpassungen der datenschutzrelevanten Prozesse, Maßnahmen und Kontrollen stellt die Deka sicher, dass das Datenschutz-Managementsystem den jeweils geltenden Anforderungen entspricht und angemessen auf neue Entwicklungen reagieren kann. Dabei werden insbesondere Erkenntnisse aus Datenschutzverletzungen, internen und externen Prüfungen, Audits, Risikoanalysen, Kontrollhandlungen, Beschwerden, Betroffenenanfragen sowie regulatorischen oder organisatorischen Änderungen berücksichtigt.

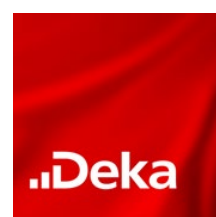
Die Methodik und Umsetzung des kontinuierlichen Verbesserungsprozesses orientiert sich an einem strukturierten Vorgehensmodell, insbesondere am PDCA-Zyklus — Plan, Do, Check, Act. Dieser Ansatz ermöglicht eine systematische Planung, Umsetzung, Überprüfung und Anpassung datenschutzbezogener Maßnahmen und Prozesse. Auf diese Weise wird gewährleistet, dass Datenschutz nicht lediglich punktuell umgesetzt, sondern dauerhaft in die relevanten Geschäftsprozesse integriert und fortlaufend optimiert wird.

Ziel des kontinuierlichen Verbesserungsprozesses ist die laufende Weiterentwicklung und nachhaltige Stärkung des Datenschutz-Managementsystems der Deka. Hierzu werden alle relevanten Prozesse, Maßnahmen und Kontrollen regelmäßig überprüft, bewertet und bei Bedarf angepasst. Dadurch sollen Datenschutzrisiken frühzeitig erkannt, angemessen gesteuert und die Rechte und Freiheiten betroffener Personen wirksam geschützt werden.

Zur Sicherstellung der Wirksamkeit des Datenschutz-Managementsystems setzt die Deka über alle relevanten Datenschutzprozesse hinweg geeignete Kontroll- und Überprüfungsmechanismen ein. Diese dienen der strukturierten und nachvollziehbaren Überwachung datenschutzbezogener Anforderungen und unterstützen die fortlaufende Bewertung der Angemessenheit und Wirksamkeit der implementierten Maßnahmen.

Die Ergebnisse aus Kontrollen, Überprüfungen und sonstigen Bewertungsinstrumenten werden im Rahmen des kontinuierlichen Verbesserungsprozesses ausgewertet und in konkrete Optimierungsmaßnahmen überführt. Dabei werden identifizierte Handlungsbedarfe priorisiert, Verantwortlichkeiten festgelegt und Umsetzungsfortschritte nachgehalten. Relevante Erkenntnisse, Fortschritte und Maßnahmen werden an die jeweils zuständigen internen Stakeholder kommuniziert und in den laufenden Prozessen berücksichtigt.

Durch diesen strukturierten Verbesserungsansatz stellt die Deka sicher, dass ihr Datenschutz-Managementsystem fortlaufend weiterentwickelt, wirksam überwacht und an veränderte Rahmenbedingungen angepasst wird. Dies unterstützt eine nachhaltige Datenschutz-Governance sowie die dauerhafte Einhaltung datenschutzrechtlicher Anforderungen innerhalb der 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

