Allgemeine Geschäftsbedingungen über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 und 29 DSGVO

Die Allgemeinen Geschäftsbedingungen gelten für die Vertragslaufzeit für „EDoc“ zwischen dem Kunden und der

EDEKABANK AG
New-York-Ring 6
22297 Hamburg

in weiterer Folge auch **„Auftragsverarbeiter“ oder „Auftragnehmer“** genannt, beide Parteien gemeinsam werden auch **„Vertragsparteien“** genannt.

1. Allgemeines

Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen nach dem Vertrag über die Nutzung der Dokumentenmanagement-Software „EDoc“ (nachfolgend **„Hauptvertrag“**). Dazu ist es erforderlich, dass der Auftragsverarbeiter personenbezogene Daten verarbeitet, für die der Verantwortliche im Sinne des Datenschutzrechts verantwortlich ist.

2. Wesentliche Inhalte der Auftragsverarbeitung

2.1. Gegenstand der Verarbeitung

Gegenstand der Verarbeitung ist die Bereitstellung eines cloudbasierten Dokumentenmanagementsystems durch den Auftragnehmer. Näheres zum Gegenstand der Auftragsverarbeitung ergibt sich aus dem Hauptvertrag.

2.2. Dauer der Verarbeitung

Die Dauer der Verarbeitung richtet sich nach der Laufzeit des Hauptvertrags.

2.3. Zweck und Art der Verarbeitung

Die Verarbeitung der personenbezogenen Daten erfolgt für den Zweck der Speicherung von Daten und Dokumenten in einer Cloudumgebung. Näheres zu Art und Zweck der Verarbeitung ergibt sich aus dem Hauptvertrag.

2.4. Art der personenbezogenen Daten

Personenbezogene Daten, welche sich aus den hochgeladenen Dokumenten ergeben.

2.5. Kategorien der von der Datenverarbeitung betroffenen Personen

- Kunden
- Lieferanten
- Beschäftigte

2.6. Ort der Verarbeitung

Die Verarbeitung von Daten durch den Auftragsverarbeiter erfolgt ausschließlich im Gebiet von Mitgliedstaaten der Europäischen Union. Eine Datenverarbeitung außerhalb dieses Gebiets, auch im Wege der Gewährung des Zugriffs auf Auftragsdaten an Personen außerhalb dieses Gebiets, bedarf der vorherigen schriftlichen Zustimmung des Verantwortlichen. Die Zustimmung darf nicht willkürlich verweigert werden. Eine Datenverarbeitung in Ländern, die nicht Mitgliedstaat der Europäischen Union sind (nachfolgend **„Drittstaaten“**), darf nur unter der weiteren Bedingung erfolgen, dass die Voraussetzungen der Artikel 44, 45, 46 oder Artikel 49 DSGVO erfüllt sind.

3. Verarbeitung auf Weisung

3.1. Grundsatz

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf (durch den Hauptvertrag, diesen Vertrag über die Auftragsverarbeitung oder individuell) erteilte Weisung des Verantwortlichen, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche hat das Recht, jederzeit ergänzende Weisungen zu erteilen. Mündliche Weisungen wiederholt der Verantwortliche unverzüglich in Textform.

3.2. Erteilung und Empfang von Weisungen

Der Verantwortliche teilt dem Auftragsverarbeiter die weisungsberechtigte(n) Person(en) schriftlich mit. Die Mitteilung wird Gegenstand dieses Vertrages. Für den Fall, dass sich die weisungsberechtigte(n) Person(en) beim Verantwortlichen ändern, wird der Verantwortliche dies dem Auftragsverarbeiter unverzüglich schriftlich mitteilen.

Der Auftragsverarbeiter teilt dem Verantwortlichen die Person(en), die zum Empfang von Weisungen des Verantwortlichen berechtigt sind, auf Nachfrage schriftlich mit.

3.3. Dokumentationspflicht

Der Auftragsverarbeiter hat die Weisung des Verantwortlichen hinreichend zu dokumentieren. Die elektronische Form der Dokumentation genügt.

3.4. Informationspflicht bei Zweifeln an der Rechtmäßigkeit der Weisung

Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darüber informieren, wenn eine vom Verantwortlichen erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Die Beurteilung der Zulässigkeit der Datenverarbeitung durch den Verantwortlichen ist für den Auftragsverarbeiter bindend.
Die Vertragsparteien haften einander für Schäden, die ihnen aus einer Durchführung oder einer Aussetzung der Durchführung entstehen, die auf einer rechtlichen Fehleinschätzung der anderen Partei beruht.

4. Verpflichtung zur Vertraulichkeit und zur Einhaltung des Datenschutzes

Der Auftragsverarbeiter setzt bei der Durchführung der Leistungen nur Beschäftigte ein, die (i) entweder vertraglich zur Vertraulichkeit verpflichtet wurden oder gesetzlich zur Verschwiegenheit verpflichtet sind und (ii) zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

5. Sicherheit der Datenverarbeitung

5.1. Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos im Sinne von Artikel 32 Abs. 1 DSGVO zu berücksichtigen. Die konkreten technischen und organisatorischen Maßnahmen werden in Anlage 1 aufgelistet. Sie unterliegen dem technischen Fortschritt und der Weiterentwicklung.

5.2. Wesentliche Änderungen, die die Integrität, Vertraulichkeit, Belastbarkeit oder Verfügbarkeit der Maßnahmen beeinträchtigen können, bedürfen der Zustimmung des Verantwortlichen. Der Verantwortliche darf die Zustimmung nicht unbillig verweigern. Das durch die mit diesem Vertrag vereinbarten Maßnahmen gewährleistete Schutzniveau darf nicht unterschritten werden. Änderungen sind hinreichend zu dokumentieren. Der Verantwortliche kann jederzeit eine aktuelle Beschreibung der vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen anfordern.

6. Unterauftragsverhältnisse

6.1. Eigenmächtige Inanspruchnahme von Unterauftragnehmern

Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO in Anspruch zu nehmen. Der Auftragsverarbeiter hat den Verantwortlichen mindestens zwei Wochen vorher über jede Inanspruchnahme oder Ersetzung eines weiteren Auftragsverarbeiters zu informieren. Der Verantwortliche kann der Inanspruchnahme oder Ersetzung eines weiteren Auftragsverarbeiters ohne Nennung eines Grundes binnen einer Frist von zwei Wochen schriftlich widersprechen. Dem Auftragsverarbeiter steht für den Fall der Nichterteilung der Genehmigung ein Sonderkündigungsrecht des zugrunde liegenden Dienstleistungsvertrages und dieser Vereinbarung zu.

Die in der Anlage 2 benannten „weiteren Auftragsverarbeiter“ sind zum Zeitpunkt des Vertragsabschlusses zur Erbringung der Auftragsverarbeitung beauftragt.

6.2. Modalitäten des Unterauftrags

Der Auftragsverarbeiter darf weitere Auftragsverarbeiter nur in Anspruch nehmen, wenn der weitere Auftragsverarbeiter in demselben Umfang vertraglich gegenüber dem Auftragsverarbeiter zur Einhaltung des Datenschutzes verpflichtet ist, wie der Auftragsverarbeiter gegenüber dem Verantwortlichen aus diesem Vertrag. Der Vertrag zwischen dem Auftragsverarbeiter und dem weiteren Auftragsverarbeiter muss insbesondere hinreichende Garantien dafür bieten, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Der Auftragsverarbeiter hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren. Dem Verantwortlichen sind der Auftragsvertrag bzw. die relevanten Auszüge auf Anfrage in Kopie zu übermitteln.

Der Auftragsverarbeiter hat den weiteren Auftragsverarbeiter sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen dem Verantwortlichen und dem Auftragsverarbeiter getroffenen Vereinbarungen einhalten kann. Der Auftragsverarbeiter hat sich insbesondere vorab und regelmäßig während der Vertragsdauer zu vergewissern, dass der weitere Auftragsverarbeiter die nach den Vorgaben der DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragsverarbeiter zu dokumentieren und auf Anfrage dem Verantwortlichen zu übermitteln.

Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen dafür, dass die weiteren Auftragsverarbeiter ihren Datenschutzpflichten nachkommen, die ihm durch den Verantwortlichen im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

6.3. Abgrenzung

Nicht als Unterauftragsverhältnisse sind Dienstleistungen anzusehen, die der Auftragsverarbeiter bei Dritten als reine Nebenleistung in Anspruch nimmt, um seine geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt, Post- und Kurierdienste, Transportleistungen und Bewachungsdienste. Der Auftragsverarbeiter ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen getroffen wurden, um den Schutz personenbezogener Daten des Verantwortlichen zu gewährleisten. Wartungs- und Pflegeleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen aus diesem Vertrag genutzt werden.

7. Unterstützung des Verantwortlichen bei der Erfüllung von Betroffenenrechten

7.1. Soweit eine Mitwirkungsleistung des Auftragsverarbeiters für die Wahrung von Betroffenenrechten durch den Verantwortlichen erforderlich ist, wird der Auftragsverarbeiter die jeweils erforderlichen Mitwirkungsleistungen nach Weisung des Verantwortlichen erbringen.

7.2. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragsverarbeiter geltend machen.

8. Unterstützung des Verantwortlichen bei der Erfüllung eigener Pflichten

8.1. Der Auftragsverarbeiter unterstützt den Verantwortlichen in dem jeweils erforderlichen Umfang dabei, die dem Verantwortlichen obliegenden Pflichten,

- ein dem Risiko angemessenes Schutzniveau zu gewährleisten,
- die Verletzung des Schutzes personenbezogener Daten an Aufsichtsbehörden unverzüglich und möglichst binnen 72 Stunden zu melden,
- den in Bezug auf eine Verletzung Betroffenen zu benachrichtigen,
- eine Datenschutz-Folgenabschätzung durchzuführen und ggf. vor Verarbeitung die zuständige Aufsichtsbehörde zu konsultieren,

zu erfüllen.

8.2. Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen vertragliche Vereinbarungen und/oder die erteilten Weisungen des Verantwortlichen, der durch ihn oder Dritte erfolgt ist und der einen Bezug zu dieser Auftragsverarbeitung hat, unverzüglich in schriftlicher Form mitzuteilen, wobei Textform genügt. Eine mündliche Mitteilung ist in Textform nachzuholen. Der Auftragsverarbeiter dokumentiert die Verletzungen einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen.

8.3. Der Verantwortliche und der Auftragsverarbeiter arbeiten gem. Artikel 31 DSGVO auf Anfrage der Aufsichtsbehörde mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Der Auftragsverarbeiter ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Verantwortlichen gemäß Artikel 31 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Verantwortlichen zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die dafür erforderlich sind, dass der Verantwortliche den Nachweis darüber erbringen kann, dass er seine datenschutzrechtlichen Pflichten als Verantwortlicher einhält.

8.4. Der Auftragsverarbeiter wirkt bei der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten im Sinne von Artikel 30 Abs. 1 DSGVO durch den Verantwortlichen mit. Er hat dem Verantwortlichen die erforderlichen Angaben in geeigneter Weise mitzuteilen. Insbesondere wird er dem Verantwortlichen einen Auszug aus seinem Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 Abs. 2 DSGVO mitteilen, damit dieser sein Verzeichnis von Verarbeitungstätigkeiten erstellen kann.

8.5. Ferner wird der Auftragsverarbeiter den Verantwortlichen – sofern rechtlich zulässig – unverzüglich darüber informieren, wenn eine Aufsichtsbehörde bei dem Auftragsverarbeiter Kontrollhandlungen oder Maßnahmen unternimmt, die sich auf diese Auftragsverarbeitung beziehen.

9. Löschung und Rückgabe

9.1. Der Auftragsverarbeiter hat nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten sowie Unterlagen, sonstige Daten und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung bzw. Aufbewahrung besteht. Gleiches gilt für Test- und Ausschussmaterial. Die Daten des Auftragsverarbeiters sind unwiederbringlich datenschutzgerecht zu löschen. Eine unwiderrufliche physische Löschung ist zu protokollieren. Dies betrifft auch etwaige Datensicherungen beim Auftragsverarbeiter. Der Auftragsverarbeiter hat die Löschung in geeigneter Weise zu dokumentieren. Bestehen gesetzliche Aufbewahrungspflichten, hat die Löschung der Daten nach Ende der Aufbewahrungspflicht zu erfolgen. Ein angemessenes Löschkonzept ist zu dokumentieren.

9.2. Vor Abschluss der Erbringung der Vertragsleistungen darf der Auftragsverarbeiter nicht mehr benötigte Daten erst nach vorheriger Zustimmung durch den Verantwortlichen löschen. Die Zustimmung zur Löschung kann auch durch eine Einigung der Vertragsparteien auf ein Löschkonzept erteilt werden.

9.3. Der Verantwortliche hat das Recht, die vollständige und vertragsgemäße Rückgabe oder Löschung der Daten beim Auftragsverarbeiter zu kontrollieren. Dies kann auch nach vorheriger Anmeldung mit angemessener Frist durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragsverarbeiters erfolgen.

10. Ermöglichung von Kontrollen und Zurverfügungstellung von Informationen

10.1. Der Verantwortliche hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen, um die Einhaltung der gesetzlichen Vorschriften zum Datenschutz, der zwischen den Vertragsparteien getroffenen vertraglichen Regelungen und der Weisungen des Verantwortlichen durch den Auftragsverarbeiter jederzeit im erforderlichen Umfang zu kontrollieren.

10.2. Der Auftragsverarbeiter ist dem Verantwortlichen gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle erforderlich ist.

10.3. Der Verantwortliche kann eine Einsichtnahme in die vom Auftragsverarbeiter für den Verantwortlichen verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen. Der Verantwortliche kann hierzu nach vorheriger Anmeldung mit angemessener Frist die Kontrolle in der Betriebsstätte des Auftragsverarbeiters zu den jeweils üblichen Geschäftszeiten vornehmen. Der Verantwortliche wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragsverarbeiters durch die Kontrollen nicht unverhältnismäßig zu stören. Für hierdurch verursachte Aufwände kann der Auftragsverarbeiter eine angemessene Vergütung verlangen, soweit die Kontrolle nicht wegen eines Gesetzes- oder Vertragsverstoßes durch den Auftragsverarbeiter erforderlich wurde. Der Auftragsverarbeiter wird dem Verantwortlichen vorab eine Kosteninformation zukommen lassen.

10.4. Der Auftragsverarbeiter kann die Einhaltung der technischen und organisatorischen Maßnahmen durch geeignete Bestätigungen, wie z. B. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Revision, Datenschutzbeauftragter) nachweisen.

11. Kündigung

Die Kündigung richtet sich nach dem Hauptvertrag.

12. Schlussbestimmungen

12.1. Sollte das Eigentum des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu informieren. Der Auftragsverarbeiter wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

12.2. Nebenabreden bedürfen der Textform, es sei denn, sie betreffen die Beauftragung weiterer Auftragnehmer, die der Schriftform bedürfen (siehe Ziffer 6). Entsprechendes gilt auch für die Änderung oder Aufhebung dieser Klausel.

12.3. Sollten einzelne Teile dieses Vertrages unwirksam sein, berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlagen:
Beschreibung der technischen und organisatorischen Maßnahmen gemäß Ziff. 5 (Anlage 1)
Vorab genehmigte weitere Auftragsverarbeiter (Anlage 2)

Anlage 1 – Technisch-organisatorische Maßnahmen

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau im Hinblick auf die erforderliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer zu gewährleisten.

Die Parteien haben das erforderliche Schutzniveau gemeinsam ermittelt (Artikel 32 Abs. 1 DSGVO). Die Parteien sind zu dem Ergebnis gekommen, dass das Risiko der Verarbeitung als hoch einzustufen ist und daher auch ein hohes Schutzniveau einzuhalten ist.

Das hohe Schutzniveau wird durch diese Maßnahmen eingehalten:

1. Vertraulichkeit (Artikel 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle
  Unter Zutrittskontrolle versteht man Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

  In der EDEKABANK AG getroffene Maßnahmen:

  - Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)
  - Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
  - Türsicherungen (elektrische Türöffner, Zahlenschloss, Code-Schloss etc.)
  - Werkschutz, Pförtner
  - Alarmanlage
  - Videoüberwachung
  - Mitarbeiter- und Berechtigungsausweise

- Zugangskontrolle
  Unter Zugangskontrolle versteht man Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

  In der EDEKABANK AG getroffene Maßnahmen:

  - (sichere) Kennwörter,
  - automatische Sperrmechanismen
  - Zwei-Faktor-Authentifizierung
  - Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
  - Kennwortverfahren (Min. 12 Zeichen lang und Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen)
  - BIOS-Passwörter
  - Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität
  - Elektronische Dokumentation sämtlicher Passwörter und Verschlüsselung dieser
  - Dokumentation zum Schutz vor unbefugten Zugriff
  - Sicherstellung, dass genutzte Datenträger verschlüsselt sind

- Zugriffskontrolle
  Unter Zugriffskontrolle versteht man Maßnahmen, die geeignet sind, zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

  In der EDEKABANK AG getroffene Maßnahmen:

  - Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
  - Protokollierung von Zugriffen
  - Differenzierte Berechtigungen/ Rollen
  - Dokumentation von Berechtigungen
  - Genehmigungsroutine
  - Verschlüsselung von Laptops
  - Segregation of Duties

- Trennungskontrolle
  Unter Trennungskontrolle versteht man Maßnahmen, die geeignet sind, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

  In der EDEKABANK AG getroffene Maßnahmen:

  - Getrennte Datenbanken
  - Zugriffsberechtigungen
  - Trennung durch Zugriffsregelungen

- Pseudonymisierung (Artikel 32 Abs. 1 lit. a DSGVO; Artikel 25 Abs. 1 DSGVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

2. Integrität (Artikel 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
  Unter Weitergabekontrolle versteht man Maßnahmen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

  In der EDEKABANK AG getroffene Maßnahmen:

  - Verschlüsselung
  - Virtual Private Networks (VPN)
  - Protokollierung
  - Gesichertes WLAN
  - SSL-Verschlüsselung bei Web-access
  - Regelungen zur Datenträgervernichtung, etc.

- Eingabekontrolle
  Unter Eingabekontrolle versteht man Maßnahmen, die geeignet sind, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

  In der EDEKABANK AG getroffene Maßnahmen:

  - Zugriffsrechte
  - Systemseitige Protokollierungen
  - Differenzierte Berechtigungen/ Rollen

3. Verfügbarkeit und Belastbarkeit (Artikel 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle
  Unter Verfügbarkeitskontrolle versteht man Maßnahmen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Rasche Wiederherstellbarkeit (Artikel 32 Abs. 1 lit. c DSGVO).

  In der EDEKABANK AG getroffene Maßnahmen:

  - Backup-Strategie/ Ausfallpläne und Wiederherstellungspläne
  - unterbrechungsfreie Stromversorgung (USV)
  - Virenschutz
  - Firewall

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Artikel 32 Abs. 1 lit. d DSGVO; Artikel 25 Abs. 1 DSGVO)

- Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt.
- Es bestehen Organisationsanweisungen zum Datenschutz.
- Mitarbeiter sind zum Datenschutz informiert und geschult sowie zur Einhaltung der Vertraulichkeit verpflichtet.
- Dokumentation und Prüfung von Datenschutzvorfällen
- Die EDEKABANK AG führt das erforderliche Verzeichnis der Verarbeitungstätigkeiten als Auftragsverarbeitern
- Es werden nur die gemäß Vorgaben des Auftraggebers erforderlichen Daten verarbeitet.
- Die Verträge mit weiteren Auftragnehmern gemäß Art. 28 Abs. 4 DSGVO (Verarbeitung personenbezogener Daten im Auftrag) enthalten die vorgeschriebenen Angaben und Vereinbarungen.
- Die Verträge mit weiteren Auftragnehmern enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers
- Die Verträge mit weiteren Auftragnehmern enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
- Sorgfältige Auswahl und Kontrolle weiterer Auftragnehmer.

Anlage 2 – Weitere Auftragsverarbeiter

Folgende „weitere Auftragsverarbeiter“ sind zum Zeitpunkt des Vertragsabschlusses zur Erbringung der Auftragsverarbeitung beauftragt:

1. Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland; Cloud Services