clearstream | DEUTSCHE BÖRSE GROUP

Datenschutz- und Datensicherheitskonzept

Technische und organisatorische Maßnahmen

Für Kunden der Clearstream Banking Frankfurt

Dokumentennummer: 7236

Januar 2019

Vorbehaltlich gegenteiliger Angabe erfolgen alle Zeitangaben in Mitteleuropäischer Zeit (MEZ).

Vorwort

Dieses Dokument beschreibt die als verbindlich festgelegten technischen und organisatorischen Maßnahmen im Zusammenhang von durchgeführten Auftragsverarbeitungsvorgängen zwischen Verantwortlichen/Auftraggeber und Auftragsverarbeiter/Auftragnehmer der Clearstream Banking AG und gibt dadurch Informationen zum gültigen Datenschutz- und Datensicherungskonzept.

Geltungsbereich

Die beschriebenen technischen und organisatorischen Maßnahmen gelten für Clearstream Banking AG.

Leerseite

Inhalt

Leerseite

1. Datenschutz- und Datensicherheitskonzept

Der im Folgenden beschriebene Maßnahmenkatalog beschreibt technische und organisatorische Einzelmaßnahmen, die nach Art. 24 Abs. 1 EU-DS-GVO für die Auftragsverarbeitung getroffen wurden.

Clearstream Banking AG kommt der in der EU-DS-GVO festgelegten Verpflichtung nach, die Datenverarbeitung personenbezogener Daten durch angemessene, technische und organisatorische Maßnahmen abzusichern und personenbezogene Daten nach Möglichkeit zu anonymisieren oder zu pseudonymisieren. Alle getroffenen Maßnahmen müssen dabei das Risiko des jeweiligen Datenverarbeitungsvorgangs berücksichtigen und dem Stand der Technik entsprechen. Dabei soll die Wirksamkeit der Maßnahme insbesondere den Schutzzielen Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit Rechnung tragen. Die Integration von Datenschutzmaßnahmen, Informationssicherheit sowie weiterer Maßnahmen zur Sicherung der Datenverarbeitungsvorgänge unterstützt dies.

Begriffsdefinition Schutzwerte:

- **Vertraulichkeit:** Schutz der Daten, Informationen und Programmen vor unberechtigten Zugriffen und unbefugter Preisgabe.
- **Integrität:** Sachliche und fachliche Korrektheit und Vollständigkeit aller Informationen und Daten während der Verarbeitung.
- **Verfügbarkeit:** Informationen, Daten, Applikationen, IT Systeme und IT Netze stehen für die Verarbeitung zur Verfügung.
- **Belastbarkeit:** Bezeichnet als ein Aspekt der Verfügbarkeit und damit die Widerstandsfähigkeit von Informationen, Daten, Applikationen, IT Systemen und IT Netzen im Störfall, Fehlerfall oder bei hoher Belastung.

Leerseite

2. Vertraulichkeit

Zum Schutz der Vertraulichkeit werden technische und organisatorische Maßnahmen getroffen, die dazu geeignet sind die Vertraulichkeit zu schützen. Dabei wird der Stand der Technik, Art, Umfang, Umstände, Zwecke der Verarbeitung, Kosten der Implementierung, Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt. Folgende Maßnahmen schützen die Vertraulichkeit personenbezogener Daten:

2.1 Zutrittskontrolle

Es sind Maßnahmen getroffen, die Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet bzw. genutzt werden, verwehrt. Dies erfolgt durch:

2.1.1 Objektsicherung

- Das Betriebsgelände und die Gebäude werden durch Sicherheitspersonal, 24/7 h überwacht.
- Das Rechenzentrum – und damit die Hardware, Server oder Komponenten – ist ein eigener abgesicherter Bereich, der von den normalen Büroräumen getrennt ist.
- Das Öffnen der Türen wird zusätzlich technisch überwacht.
- Es werden Kontrollpatrouillen durchgeführt.
- Es sind Wartungsverträge für technische Überwachungsanlagen vorhanden.
- Es erfolgt eine Ausweiskontrolle durch das Sicherheitspersonal.
- Der Zutritt wird protokolliert.
- Zutritt wird nur Befugten durch Überprüfung und nach Feststellung der Identität gewährt.

2.1.2 Sicherheitszonen

Das Rechenzentrum ist ein von den Büroräumen getrennter Bereich mit strikter Zutrittsbeschränkung und Überwachung (Closed-Shop).

2.1.3 Art der Zutrittskontrolle

- Es erfolgt eine automatische Ausweiskontrolle durch persönliche Zutrittskarten und Aufzeichnung der Anwesenheit durch Chipkartenleser.
- Die Sicherung der Büros erfolgt durch kontrollierte Schlüsselregelung.
- Der Empfang ist während der Kernzeiten besetzt und empfängt Besucher.
- Notausgänge sind gegen missbräuchliche Benutzung gesichert.

2.1.4 Regelung der Zutrittsberechtigungen

- Zutrittsberechtigungen sind restriktiv ausgestaltet und werden auf Grundlage entsprechender Berechtigungsverfahren erteilt.
- Es erfolgt eine Festlegung befugter Personen mit Bezug auf Sicherheitszonen (z. B. Rechenzentrum).
- Besucher und Externe müssen sich am Empfang anmelden und werden abgeholt und begleitet.
- Es bestehen Regelungen für das Ausscheiden von Mitarbeitern oder den internen Stellen- bzw. Berechtigungswechsel.

- Es bestehen Regelungen / Folgemaßnahmen bei Verlust von Ausweisen, Schlüsseln usw.
- Wartungs- und Reparaturpersonal wird beaufsichtigt.
- Eine Revisionsfähigkeit von Vergabe und Entzug der Zutrittsberechtigungen ist gegeben.

2.2 Zugangskontrolle zu Datenverarbeitungssystemen

Es wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Dies erfolgt durch:

2.2.1 Regelung der Zugangsberechtigungen

- Zugangsberechtigungen werden Nutzern auf Grundlage von Berechtigungsverfahren erteilt.
- Es erfolgt eine Vergabe von persönlicher Benutzerkennung und persönlichem Initialkennwort.
- Der Zugang erfolgt erst nach vorheriger Anmeldung (Login) mit Authentisierung (Benutzerkennung, Kennwort oder auch Token-Device).
- Die Bildschirmsitzung wird durch Bildschirmschoner mit Kennwort nach einem festgelegten Zeitraum automatisch geschützt und kann darüber hinaus manuell gesperrt werden.
- Maßnahmen zur Passwortsicherheit (Länge, Komplexität und Aufbewahrung) und Regelungen für die Verwendung von Passwörtern sind getroffen.
- Regelungen bei Verlust (Vergessen) von Passwörtern oder auch Token-Device sind getroffen.
- Eine Regelung, die ein Need-to-know und ein Need-to-do Prinzip für Berechtigungsverfahren zwingend vorsieht, ist getroffen.
- Administratoren-Konten werden ausschließlich für eng begrenzte Tätigkeiten genutzt.
- Regelungen für das Ausscheiden bzw. den Stellenwechsel von Berechtigten sind getroffen.
- Die Trennung der Verbindung bei wiederholten Fehlversuchen oder Zeitüberschreitungen ist gegeben.
- Inaktive Verbindungen werden nach einer definierten Wartezeit (time-out) automatisch geschlossen.
- Eine getrennte Infrastruktur für Besucher ist vorhanden.
- Nutzer können nur gemäß den ihnen erteilten Berechtigungen auf personenbezogenen Daten zugreifen (durch Rollenvergabe, funktionale User etc.).
- Personenbezogene Daten werden im Ruhezustand RACF (Resource Access Control Facility) geschützt gespeichert.
- Unbefugte Zugriffsversuche werden entdeckt (z. B. Protokollierung der Systemnutzung) und entsprechend untersucht.

2.2.2 Zusätzliche Maßnahmen beim Fernzugang

- Personen, die zur Anmeldung von außerhalb befugt sind, werden festgelegt.
- Eine Netzzugangssicherung durch Hard- und Softwaremaßnahmen ist gegeben.
- Unbefugter Zugriff aus dem Internet wird durch den Einsatz von Firewalls verhindert.
- Unbefugte Zugriffsversuche können entdeckt werden (Intrusion Detection).
- Schutz bestehender Sitzungen gegen Übernahme durch andere Nutzer (Session Hijacking) ist gegeben.

2.2.3 Protokollierung von Zugängen

- Der Zugang zu Datenverarbeitungssystemen und Arbeitsplatzrechnern wird protokolliert (z. B. in Logdatei).
- Die Benutzung der Datenverarbeitungssysteme ist nachweisbar (Protokollierung der Zugänge).
- Eine Protokollierung der Remotezugänge am (SSL) VPN-Gateway findet statt.
- Eine Protokollierung der Vergabe / Änderung von Zugangsberechtigungen findet statt.
- Eine regelmäßige Auswertung der Protokolle findet statt.

2.3 Zugriffskontrolle / Benutzerkontrolle

Es ist 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. Dies erfolgt durch:

2.3.1 Berechtigungskonzept

- Regelungen für die Vergabe und die Verwaltung von Zugriffsberechtigungen sind getroffen.
- Individuelle Zugriffsrechte und Benutzergruppen sind gebildet.
- Die Verwaltung der Benutzergruppen erfolgt in einem zentralen Verzeichnisdienst.
- Vergebene Berechtigungen werden regelmäßig überprüft.

2.3.2 Zugriffsschutz

- Einsatz von Verschlüsselungsroutinen sowie die Möglichkeit zur Dateiverschlüsselung ist gegeben.
- Die Verschlüsselung von mobilen Endgeräten ist gegeben.
- Netzzugriffssicherungen sind eingerichtet.
- Es werden nur freigegebene Hard- und Software verwendet.
- Netzkomponenten sind gesichert.
- Das Netzwerk ist segmentiert.
- Eine Trennung von Test- und Produktivumgebung erfolgt.
- Kritische Dienste unterliegen einem Monitoring.
- Es erfolgt eine Beschränkung der freien Abfragemöglichkeiten (SQL-Query) von Datenbanken.
- Eine sichere Entsorgung von Informationen (zertifiziert nach DIN 66399) ist gewährleistet.

2.3.3 Aufbewahrung bei Verwendung von Datenträgern

- Die Aufbewahrung von Datenträgern ist geregelt.
- Verschlüsselte Datenträger stehen zur Verfügung.
- Es erfolgt keine Reparatur von Datenträgern, sondern eine sichere Löschung/Vernichtung (nach DIN 66399).
- Eine Festlegung der zur Datenträgerentnahme befugten Personen erfolgt.
- Festplatten sind hardwareverschlüsselt.

2.4 Trennungskontrolle

Es ist zu gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können. Dies erfolgt durch folgende Maßnahmen:

- Die eingesetzte Software und Ablagestruktur ist mandantenfähig.
- Es erfolgt eine logische Trennung der Daten.
- Es gibt innerbetriebliche Vorgaben für die Datenerhebung und -verarbeitung.

3. Integrität

Sachliche und fachliche Korrektheit und Vollständigkeit aller Informationen und Daten während der Verarbeitung von personenbezogenen Daten wird gewährleistet. Die Identifikation und Korrektur unzulässiger Änderungen muss gewährleistet sein. Folgende Kontrollen stellen die Integrität der personenbezogenen Daten sicher:

3.1 Weitergabekontrolle / Übertragungskontrolle

Unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport ist zu verhindern. Dies geschieht wie folgt:

3.1.1 Regelung der elektronischen Übertragung

- Eine Datenübertragung findet in geschützten Netzwerken statt.
- Externe Netzwerke werden exklusiv genutzt (VPN, Standleitung).
- Filtermechanismen verhindern Verbindungen von und zu unzulässigen DV-Systemen (Firewall).
- Es gibt die Möglichkeit Daten zu verschlüsseln (z. B. S-MIME, PGP) und verschlüsselt zu übertragen (z. B. SSL, TLS).
- Eine Authentisierung erfolgt bei E-Mails (digitale Signatur).

3.1.2 Regelung bei der Speicherung auf Wechseldatenträgern

Eine Speicherung von personenbezogenen Daten auf Wechseldatenträgern ist grundsätzlich nicht vorgesehen. Im Ausnahmefall werden ausschließlich verschlüsselte mobile Datenträger verwendet:

- Personenbezogene Daten werden auf Datenträgern (Bänder oder USB Sticks etc.) ausschließlich in einem zutrittsgesicherten zentralen Rechenzentrum gespeichert und verwahrt.
- Private Datenträger sind in Geschäftsräumen grundsätzlich verboten; anlassbezogene Ausnahmen werden nur auf Antrag genehmigt.

3.1.3 Regelungen des Transports von Datenträgern

- Datenträger mit personenbezogenen Daten sind beim Transport von unbefugtem Zugriff, Beschädigung und Verlust geschützt.
- Transport von Datenträgern mit personenbezogenen Daten erfolgt ausschließlich durch betriebszugehörige Boten, gesicherte Transportverhältnisse oder eine sonstige sichere Versendeform.
- Datenträger sind stets verschlüsselt.
- Papierentsorgung erfolgt mittels Aktenvernichter und/oder durch Entsorgungsfirma.

3.1.4 Regelungen der Entsorgung von Datenträgern

Datenträger werden datenschutzgerecht entsorgt und durch die Entsorgungsfirma vernichtet.

3.2 Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies erfolgt durch folgende Maßnahmen:

- Zuständigkeiten für Dateneingabe einschließlich Vertretungsregelungen sind durch Berechtigungsvergabe festgelegt.
- Protokollierung aller Eingaben, Veränderungen oder Löschungen von Daten, so dass Urheber, Zeitpunkt und Inhalt der Änderung nachvollzogen werden können.
- Relevante Benutzeraktivitäten werden aufgezeichnet (Absender, Zeitstempel und Änderungsinhalt).
- Protokollauswertungssysteme werten die erfassten Protokolle aus.

4. Verfügbarkeit und Belastbarkeit / Wiederherstellbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten vor der Gefahr einer zufälligen Zerstörung oder einem Verlust abgesichert sind. Hierfür sind folgende Maßnahmen getroffen worden:

4.1 Erstellung und Verwahrung von Sicherheitskopien

- Ein dokumentiertes Datensicherungskonzept liegt vor.
- Eine kontrollierte und regelmäßige Sicherung der Dateien und Datenbanken erfolgt.
- Tests der Datensicherung werden regelmäßig durchgeführt und dokumentiert.
- Die Datensicherung ist geschützt vor unberechtigten Zutritt, Zugang und Zugriff.
- Datensicherungsträger werden getrennt von den Originaldaten sicher an besonders geschützten Orten gelagert.

4.2 Gewährleistung des laufenden Betriebes

Der laufende Betrieb ist durch folgende technische und organisatorische Maßnahmen sichergestellt:

- Schichtbetrieb
- Kapazitätsplanung und -monitoring

4.2.1 Ausfallsicherheit

Vollständig redundantes Sysplex (System processing complex) (mindestens 99,9% Verfügbarkeit)

4.2.2 Unterbrechungsfreie Stromversorgung

- Eine unterbrechungsfreie Stromversorgung (USV) mit ausreichender Kapazität ist dem Rechenzentrum vorgeschaltet.
- Die ordnungsgemäße Funktionsfähigkeit wird durch regelmäßige Tests sichergestellt.
- Die Tests werden dokumentiert.

4.2.3 Brandschutz

- Flächendeckende Brandmeldeanlagen und / oder Brandfrühest-Erkennungsanlagen Betrieb (je nach Location) sind vorhanden.
- CO_2-Handlöscher sind im Rechenzentrum vorhanden.
- Auf eine Brandlastreduzierung wird geachtet.

4.2.4 Klimatisierung

- Redundante Klimatisierungssysteme im Rechenzentrum sind vorhanden.
- Mehrere Klimamodule zur optimalen Kälteverteilung sind vorhanden.
- Eine Leckagewarnung mit Weiterleitung auf die ständig besetzte Stelle des Wachdienstes ist vorhanden.

- Eine Temperaturüberwachung mit Weiterleitung auf die ständig besetzte Stelle des Wachdienstes ist vorhanden.
- Es erfolgt eine Benachrichtigung der verantwortlichen Mitarbeiter (IT-Operations, IT-Leitung) durch den Wachdienst bei Auslösung.
- Wartungsverträge sind vorhanden.

4.2.5 Anbindung Internet

Eine redundante Internetanbindung ist vorhanden.

4.3 Maßnahmen zum betrieblichen Katastrophenschutz

- Ein Notfallhandbuch (mit Zuständigkeiten) ist erstellt und gepflegt.
- Eine Notfallorganisation ist etabliert.
- Notfallübungen werden durchgeführt und dokumentiert.

4.4 Organisatorische Maßnahmen

- Sicherheitsrichtlinien sowie sicherheits- und datenschutzspezifische Arbeitsanweisungen existieren, wurden verkündet und werden kontrolliert.
- Vorgaben für Verfahrens- und Programmdokumentation sind vorhanden.
- Eingesetzte Hard- und Software ist vorhanden und betriebsbereit, um die Originaldaten aus den Kopien mittels der Back-up Geräte herzustellen.
- Die Betriebsbereitschaft wird regelmäßig überprüft.
- DV-Systeme werden vor Inbetriebnahme gemäß definierter Verfahren gehärtet und damit auf höheres Sicherheitsniveau gehoben.
- Ein Business Continuity Management ist etabliert.
- Ein Failover Procedure ist definiert.
- Das Vorhandensein ausreichender Personalressourcen ist gewährleistet.
- Die Anwender werden geschult.
- Ein Informationssicherheitsbeauftragter ist bestellt.
- Regelungen für die Dateihaltung (zentrale Sicherung) liegen vor.
- Daten werden erst nach Ablauf der definierten Aufbewahrungsfristen gelöscht.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Durch interne Prozesse und Abläufe, insbesondere auf organisatorischer Ebene, muss die Wirksamkeit der umgesetzten Maßnahmen überprüft, bewertet und evaluiert werden.

5.1 Datenschutz-Management

Die umfangreichen Pflichten und Anforderungen der EU-DS-GVO erfordern eine ganzheitliche Strategie nach einem strukturierten Ansatz und ein entsprechendes Managementsystem. Alle Elemente, die für die Sicherstellung des Datenschutzes erforderlich sind, unterliegen der systematischen Koordination des Datenschutz-Managements. Hierzu zählen folgende Maßnahmen:

- Die Datenschutzorganisation ist etabliert.
- Über die Datenschutzstrategie wird ein strukturierter Ansatz verfolgt.
- Etablierte Prozesse sehen die Einbindung des Datenschutzbeauftragten vor.
- Datenschutzrelevante Richtlinien und Arbeitsanweisungen werden verkündet und die Einhaltung kontrolliert.
- Formalisierte Freigabeverfahren für neue DV-Verfahren und bei wesentlichen Änderungen in Altverfahren sind vorhanden.

5.2 Incident-Response-Management

Um im Bedarfsfall eines Vorfalls reagieren zu können, sind einschlägige Meldewege zu definieren und Verantwortlichkeiten festzulegen. Hierzu sind folgende Maßnahmen getroffen worden:

- Mitarbeiter sind entsprechend geschult.
- Meldestellen und Meldewege für (Sicherheits-)Vorfälle sind definiert.
- Geordnete Behandlung ist sichergestellt.
- Dokumentation wird gepflegt.
- Gewonnene Erfahrungswerte fließen in die weitere Ausgestaltung und Verbesserung der Prozesse ein.

5.3 Datenschutzfreundliche Voreinstellungen

Durch Voreinstellungen ist sicherzustellen, dass personenbezogene Daten nur nach dem jeweiligen bestimmten Verarbeitungszweck verarbeitet werden. Dies gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang der Verarbeitung, die Speicherfrist und die Zugänglichkeit. Folgende Maßnahmen wurden umgesetzt:

- Durch kontinuierlichen Sensibilisierungs- und Schulungsprozess im Rahmen des Datenschutzmanagements sind die Mitarbeiter behutsam im Umgang mit personenbezogenen Daten und berücksichtigen den datenschutzrechtlichen Grundsatz der Datenminimierung im Rahmen der Entwicklung von technischen und geschäftlichen Prozessen.

5.4 Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Es erfolgt keine Auftragsverarbeitung im Sinne von Art. 28 EU-DS-GVO ohne entsprechende Weisung des Auftraggebers. Hierzu sind folgende Maßnahmen getroffen:

- Ein interner Prozess stellt sicher, dass notwendige Verträge zur Auftragsdatenverarbeitung abgeschlossen werden.
- Ein schriftlicher Vertrag zwischen Auftraggeber und Auftragnehmer liegt jeweils vor.
- Der Auftraggeber erteilt dem Auftragnehmer Weisungen in Schriftform.
- Der Auftragnehmer hat ausreichende betriebsinterne Anweisungen aufgrund des Auftrags und der damit verbundenen Weisungen des Auftraggebers sichergestellt.
- Ausreichende Maßnahmen zur Einhaltung des Datenschutzes durch einen möglichen Unterauftragnehmer können auch durch den Auftraggeber geprüft werden.
- Wenn beim Auftragnehmer eine Prüfung durch die Aufsichtsbehörde stattgefunden hat, so kann der Auftraggeber den Prüfbericht verlangen; gleiches gilt für Prüfungen bei möglichen Unterauftragnehmern.

Kontakt

www.clearstream.com

Veröffentlicht von

Clearstream Banking Frankfurt

Eingetragene Adresse
Clearstream Banking AG, Frankfurt
Mergenthalerallee 61
D - 65760 Eschborn
Deutschland

Postanschrift
Clearstream Banking AG, Frankfurt
D - 60485 Frankfurt/Main
Deutschland

Januar 2019

Dokumentnummer: 7236