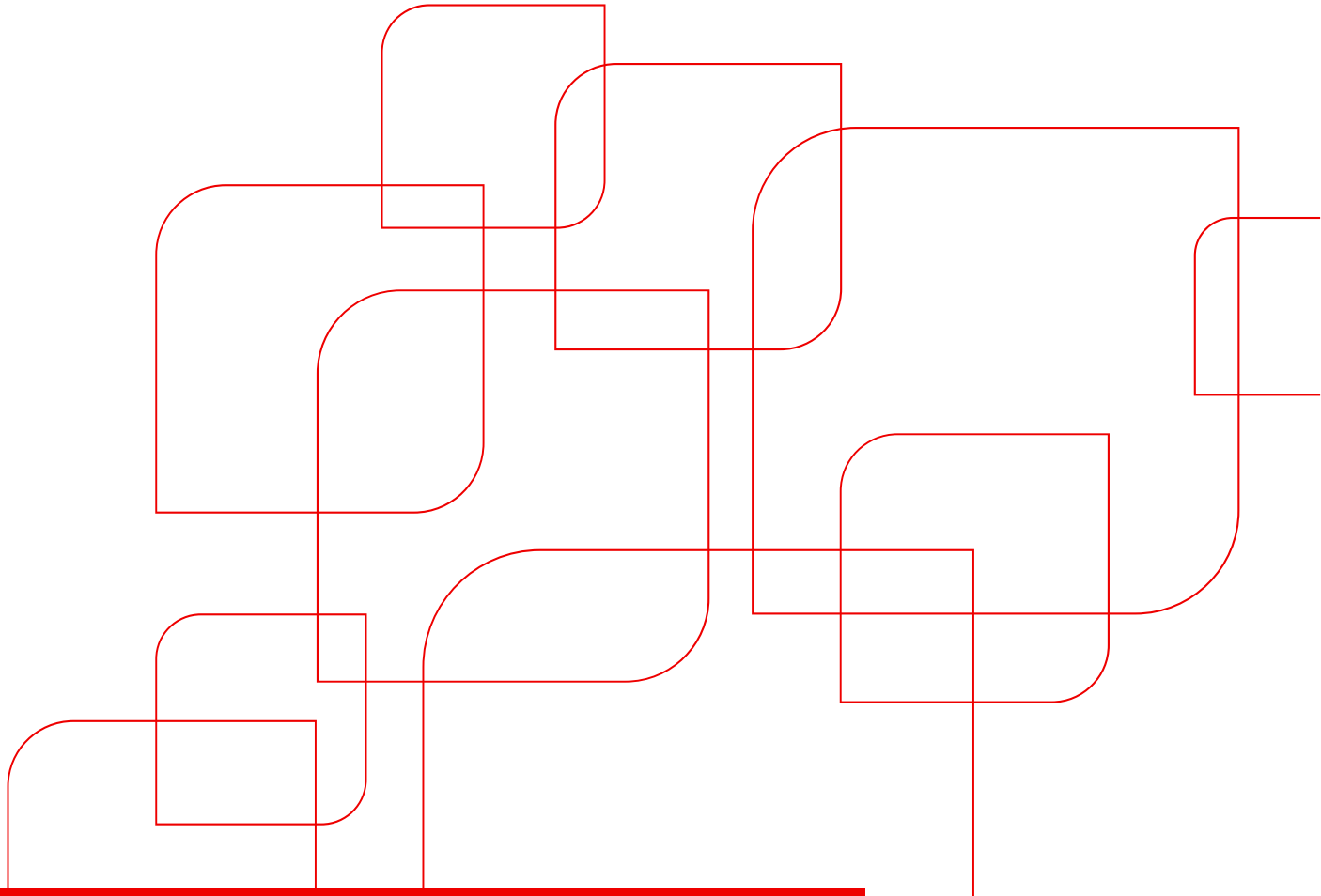

Selbstauskunft über die technischen und organisatorischen Maßnahmen

zur Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten im Auftragsverarbeitungsverhältnis

Finanz Informatik GmbH & Co. KG (Finanz Informatik oder FI genannt)

Version 3.0

finanz informatik

Selbstauskunft über die technischen und organisatorischen Maßnahmen

1. Allgemeine Angaben des Auftragnehmers

1.1 Name des Unternehmens

Firmenbezeichnung	

1.2 Anschrift des Unternehmens

Land	
Ort	
Postfach	
Straße und Hausnummer	

1.3 Ansprechpartner/in

Name	
E-Mail	

1.4 Datenschutzbeauftragte/r

Name	
E-Mail	

1.5 Kurze Beschreibung der durchzuführenden Aufgabe/Verarbeitung:

1.6 Kategorien betroffener Personen*

☐ Kunden	☐ Externe	☐ Gremien
☐ Interessenten	☐ Lieferanten	☐ Organmitglied
☐ Gläubiger	☐ Besucher	☐ Beschäftigte FI
☐ Wirtschaftlich Berechtigter	☐ Bewerber	☐ Beschäftigte Institute

☐ Weitere (bitte ausführen)

*) Natürliche Personen

1.7 Art der personenbezogenen Daten

☐ Personenstammdaten	☐ Zahlungs-/Umsatzdaten	☐ Lohn und Gehalt
☐ Kontakt- und Kommunikationsdaten	☐ Vorgänge/Einzeltätigkeiten	☐ Ausbildung und Qualifikation
☐ Identifikationsdaten	☐ Lebens-/Konsumverhalten	☐ Nutzungsverhalten
☐ Vertragsstammdaten	☐ Sicherheiten	☐ Bildaufzeichnungen
☐ Vertragsdetails	☐ Wirtschaftliche Verhältnisse	☐ Tonaufzeichnungen

☐ Weitere personenbezogene Daten (Bitte detailliert aufführen)

1.8 Erfüllungsort

☐ In den Räumen des Auftraggebers

☐ In den Räumen des Auftragnehmers

☐ Bei dem Subunternehmer (bitte Firma und Staat nennen):

1.9 In welchen Staaten wird die Datenverarbeitung (inkl. Fernzugriff) durchgeführt?

☐ In Deutschland bzw.

☐ innerhalb der EU/EWR oder

☐ in einem Drittland auf Basis eines Angemessenheitsbeschlusses (Art. 45 DSGVO) in:

☐ in einem Drittland auf Basis geeigneter Garantien (Art. 46 DSGVO) in:

☐ in einem Drittland auf Grundlage einer Ausnahme (Art. 49 DSGVO) in:

☐ **Nicht relevant** aus anderen Gründen (bitte nennen)

1.10 Offenlegung von Daten an Empfänger in Drittländern

☐ Es erfolgt **keine** Offenlegung von personenbezogene Daten an Empfänger in Drittländern i. S. Art. 44 ff, DSGVO

Der Auftragnehmer legt personenbezogene Daten ggü. Empfängern in Drittländern offen und hat dafür die folgenden Anforderungen gemäß Art. 44 ff. DSGVO erfüllt:

a) Angaben zur Drittlandübermittlung

Staat	
ins Drittland übermittelte personenbezogene Daten	
Verarbeitungsaufgabe im Drittland	

b) Erlaubnisgrundlagen für Drittlandübermittlung:

- ☐ Angemessenheitsbeschluss liegt vor
- ☐ Standardvertragsklauseln wurden abgeschlossen (Transfer Impact Analyse liegt vor)
- ☐ Grundsätzliche oder die weiteren Ausnahmen nach Art. 49 DSGVO sind erfüllt (bitte nennen und nachweisen)

Selbstauskunft über die technischen und organisatorischen Maßnahmen

2. Vertraulichkeit (Art. 32 Abs. 1 b DSGVO)

2.1 Zutrittskontrolle, folgende Maßnahmen sind zum Schutz vor unbefugtem Zutritt zu den Datenverarbeitungsanlagen implementiert:

☐ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)	☐ Werkschutz, Pförtner	☐ Regelmäßige Überprüfung der vergebenen Berechtigungen für Hoch-Sicherheitszonen (Rezertifizierung)
☐ Türsicherungen (elektrische Türöffner, Zahlenschloss, Sicherheitsschließzylinder, etc.)	☐ Alarmanlage	☐ Spezielle Schutzvorkehrungen des Serverraums (Vereinzelungsschleusen für RZ-Zugang, baulicher Schutz gegen diverse Angriffsarten)
☐ Sicherheitstüren / -fenster	☐ Videoüberwachung	☐ Mitarbeiter- und Berechtigungsausweise
☐ Gitter vor Fenstern/Türen im Bereich der Rechenzentrumsgebäude (RZ-Gebäude)	☐ Schutzzonen nach Zwiebelschalenprinzip (höchste Stufe im Inneren) mit Berechtigungsprüfung an jedem Übergang	☐ PIN-Eingabe außerhalb Regelarbeitszeit bei Gebäudezugang bzw. dauerhaft bei besonders gesicherten Arealen (z. B. RZ und RZ-Technik)
☐ Zaunanlagen (im Bereich RZ-Gebäude)	☐ Zutrittsregelungen in Abhängigkeit zur Schutzzone (SZ)	☐ Besucherregelung (zum Beispiel: Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)
☐ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe	☐ Berechtigungsvergabe für Zutritt in Hoch-Sicherheitszonen nur nach vorheriger Prüfung der Berechtigung durch Führungskraft und Flächenverantwortlichen	

☐ **Nicht relevant** (bitte begründen)

☐ **Sonstiges** (bitte beschreiben)

2.2 **Zugangskontrolle**, folgende Maßnahmen sind zum Schutz vor unbefugtem Zugang zu den Datenverarbeitungssystemen implementiert:

☐ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk	☐ Autorisierungsprozess für Zugangsberechtigungen	☐ Berücksichtigung des Minimalprinzips bei der Rollenvergabe („need to know“)
☐ Single Sign On	☐ BIOS-Passwörter	☐ Kennwortverfahren
☐ Protokollierung des Zugangs	☐ Verwendung zusätzlicher Benutzerkennungen für administrative Tätigkeiten	☐ Automatische Sperrung des Zugangs zu Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
☐ Autorisierungsprozess für Berechtigungen	☐ Erstellung und Verwaltung von Benutzerprofilen sowie Rechte- und Rollenkonzepte	☐ Funktionstrennung im Berechtigungsmanagement „Segregation of Duties (SoD)" (Definition von SoD-Klassen und Führung einer SoD-Matrix)

☐ **Nicht relevant** (bitte begründen

☐ **Sonstiges** (bitte beschreiben)

2.3 **Zugriffskontrolle**, folgende Maßnahmen sind zum Schutz vor unbefugtem Zugriff auf personenbezogene Daten implementiert:

- ☐ Verwaltung und Dokumentation von differenzierten Berechtigungen
- ☐ Erstellung und Verwaltung von Benutzerprofilen sowie Rechte- und Rollenkonzepte
- ☐ Funktionstrennung im Berechtigungsmanagement „Segregation of Duties (SoD)" (Definition von SoD-Klassen und Führung einer SoD-Matrix)
- ☐ Auswertungen/Protokollierungen von Datenverarbeitungen
- ☐ Verschlüsselung von Datenträgern
- ☐ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
- ☐ Autorisierungsprozess für Berechtigungen
- ☐ „Mobile Device Management-System“
- ☐ Nicht reversible Löschung von Daten auf Datenträgern, sofern diese der vorgegebenen Löschanforderungen unterliegen
- ☐ Genehmigungsroutinen für die Beantragung von Zugriffsrechten
- ☐ Vier-Augen-Prinzip u.a. im Berechtigungsmanagement
- ☐ **Nicht relevant** (bitte begründen)

- ☐ **Sonstiges** (bitte beschreiben)

2.4 **Trennungskontrolle**, folgende Maßnahmen stellen sicher, dass die Mandantentrennung bei zu unterschiedlichen Zwecken erhobenen personenbezogenen Daten eingehalten wird:

- ☐ Speicherung der Datensätze in logisch oder physikalisch nach Mandanten getrennten Datenbanken oder in separaten Tabellen pro Mandant innerhalb einer Datenbank
- ☐ Getrennte Datenverarbeitung in separaten Prozessen mit differenzierenden Zugriffsregelungen pro Mandant
- ☐ Nutzung anwendungsspezifischer Trennungs- oder Berechtigungsmechanismen (falls erforderlich)
- ☐ Zugriffsberechtigungen pro Mandant nach funktioneller Zuständigkeit
- ☐ Trennung von Entwicklungsumgebung, Testumgebung und Produktionsumgebung
- ☐ **Nicht relevant** (bitte begründen)

- ☐ **Sonstiges** (bitte beschreiben)

2.5 **Pseudonymisierung (Art. 32 Abs. 1 a, Art. 25 Abs. 1 DSGVO**), Maßnahmen, um unbefugte oder unrechtmäßige Datenverarbeitung zu verhindern, indem Identifikationsmerkmale bestimmter oder bestimmbarer Personen durch Kennzeichen ersetzt werden und die Zuordnung zur betroffenen Person nicht ohne zusätzliche Informationen möglich ist. Die Verarbeitung der ursprünglichen Identifikationsmerkmale muss getrennt erfolgen und es sind zusätzliche technische und organisatorische Maßnahmen zu gewährleisten.

- ☐ Maßnahmen werden gemäß vorstehender Beschreibungen umgesetzt.
- ☐ Es erfolgt keine Pseudonymisierung von Daten.
- ☐ **Nicht relevant**, weil zur Aufgabenerfüllung ausschließlich Systeme des Auftraggebers genutzt werden.
- ☐ **Sonstiges** (bitte beschreiben)

2.6 **Weitergabekontrolle**, es ist sichergestellt, dass personenbezogene Daten der Finanz Informatik GmbH & Co. KG bzw. dessen Kunden bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

☐ Verschlüsselung (je nach Empfängerkreis) von Email bzw.- Email-Anhängen	☐ Physikalische Transportsicherung	☐ Regelung zum Umgang mit mobilen Speichermedien
☐ Verschlüsselung des Speichermediums von Laptops	☐ Verpackungs- und Versandvorschriften	☐ Protokollierung von Datenübertragung oder Datentransport
☐ Gesicherter File Transfer	☐ Gesichertes WLAN	☐ Protokollierung von lesenden Zugriffen
☐ Gesicherter Datentransport	☐ „Mobile Device Management-System“	☐ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten
☐ Verschlüsselung von Datenträgern	☐ „Data Loss Prevention (DLP)-System“	☐ Verwendung von abgesicherten Weitverkehrs-Netzwerkverbindungen (WAN)

☐ **Nicht relevant** (bitte begründen)

☐ **Sonstiges** (bitte beschreiben)

2.7 **Eingabekontrolle**, durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer als Auftragsverarbeiter oder Unterauftragsverarbeiter personenbezogene Daten der Finanz Informatik GmbH & Co. KG bzw. dessen Kunden personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- ☐ Zugriffsrechte
- ☐ Sicherheits-/Protokollierungssoftware
- ☐ „Data Loss Prevention (DLP)-System“
- ☐ Systemseitige Protokollierungen
- ☐ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- ☐ Dokumenten Management System (DMS) mit Änderungshistorie
- ☐ Mehraugenprinzip
- ☐ **Nicht relevant** (bitte begründen)

- ☐ **Sonstiges** (bitte beschreiben)

3. Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit (Art. 32 Abs. 1 b und c DSGVO)

3.1 Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

☐ Sicherheitskonzept für Software- und IT-Anwendungen	☐ Spiegeln von Festplatten	☐ Virenschutz
☐ Back-Up und Restore Verfahren	☐ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)	☐ Firewall
☐ Aufbewahrungsprozess für Back-Ups (Datensicherungen werden in zwei Kopien in zwei unterschiedlichen RZ-Lokationen abgelegt)	☐ Geeignete Archivierungsräumlichkeiten für Papierdokumente	☐ Notfallplan
☐ Gewährleistung der Datenspeicherung im gesicherten Netzwerk	☐ Brand- und/oder Löschwasserschutz des Serverraums	☐ Erfolgreiche Notfallübungen
☐ Bedarfsgerechtes Einspielen von Sicherheitsupdates	☐ Klimatisierter Serverraum	☐ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)

☐ **Nicht relevant** (bitte begründen)

☐ **Sonstiges** (bitte beschreiben)

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

4.1 Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

☐ Leitbild zum Datenschutz	☐ Bestellung eines Datenschutzbeauftragten	☐ Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
☐ Richtlinien zum Datenschutz	☐ Verpflichtung der Mitarbeiter auf das Datengeheimnis und Bankgeheimnis	☐ Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)
☐ Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit	☐ Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten	☐ Ext. Prüfung/Auditierung der Informationssicherheit (im Rahmen von z. B. ISO 27001-Zertifizierung, Prüfung gemäß IDW PS 951 o. ä.)

☐ **Nicht relevant** (bitte begründen)

☐ **Sonstiges** (bitte beschreiben)

4.2 Incident-Response-Management, folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse sichergestellt sind:

- ☐ Prozess zur standardisierten Meldung, Bearbeitung und Dokumentation von (potentiellen) Datenschutzverletzungen
- ☐ Meldeprozess für Datenschutzverletzungen nach Art. 4 Nr. 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- ☐ Meldeprozess für Datenschutzverletzungen nach Art. 4 Nr. 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)
- ☐ **Nicht relevant** (bitte begründen)

- ☐ **Sonstiges** (bitte beschreiben)

5. Privacy by Design und Privacy by Default (Art. 25 DSGVO)

5.1 Bereits bei der Konzeption von Anwendungen und Prozessen sind nur diejenigen personenbezogenen Daten zu betrachten, die für den Verarbeitungszweck benötigt werden. Die Gesamtkonzeption muss bereits die Grundsätze des Datenschutzes berücksichtigen. Hierbei ist nicht nur die Technik zu betrachten, sondern auch die datenschutzorientierte, prozessuale Gestaltung von Verarbeitungstätigkeiten.

Die Default-Einstellungen sind sowohl bei den standardisierten Voreinstellungen bei der Planung und Entwicklung von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert. Wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben bzw. von Eingabemöglichkeiten (z. B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden (z. B. hinsichtlich des Umfangs der Verarbeitung). Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden können) oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt.

☐ Ja, solche Maßnahmen werden umgesetzt

☐ Nein, solche Maßnahmen werden nicht umgesetzt.

☐ **Nicht relevant** (bitte begründen)

☐ **Sonstiges** (bitte beschreiben)

5.2 **Auftragskontrolle**, durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

☐ Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers	☐ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer	☐ Dokumentiertes Verfahren zur Auswahl des Dienstleisters
☐ Prozess zur Erteilung und/oder Befolgung von Weisungen	☐ Unabhängige Auditierung der Weisungsgebundenheit	☐ Standardisiertes Vertragsmanagement zur Vor- und Nachkontrolle der Dienstleister
☐ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern	☐ Verpflichtung der Mitarbeiter auf das Datengeheimnis	
☐ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung	☐ Formalisiertes Auftragsmanagement	

☐ **Nicht relevant** (bitte begründen)

☐ **Sonstiges** (bitte beschreiben)