

DAS FINANZBUCH

„DAS FINANZBUCH“ Software GmbH
Argentinerstrasse 21
1040 Wien

Mail • office@freefinance.de
Web • www.freefinance.de

Datenverarbeitungsverzeichnis nach Art 30 Abs 1 DSGVO (Verantwortlicher)

Inhalt

A. Stammdatenblatt	2
B. Datenverarbeitungen/Datenverarbeitungszwecke	2
C. Detailangaben zu Buchhaltung	3
D. Detailangaben zu Erbringung der Services	5
E. Detailangaben zur Sicherheit	7
F. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen	9

A. Stammdatenblatt

Name und Kontaktdaten des (der) für die Verarbeitung (gemeinsam) Verantwortlichen

a. Name und Anschrift

“DAS FINANZBUCH” Software GmbH
Argentinierstrasse 21
1040 Wien

b. E-Mail-Adresse

datenschutz@freefinance.de

c. Name und Kontaktdaten des Datenschutzbeauftragten

Es wird kein Datenschutzbeauftragter benötigt

d. Name und Kontaktdaten des Vertreters des (der) Verantwortlichen

Keiner

B. Datenverarbeitungen/Datenverarbeitungszwecke

1. Zwecke und Beschreibung der Datenverarbeitung

Erfüllung von vertraglichen Pflichten (Art 6 Abs 1 lit b DSGVO):

Um die Services abwickeln zu können speziell auch Betrieb und Wartung durchführen zu können,
und Unterstützung (Support) leisten zu können

Erfüllung von einer rechtlichen Verpflichtung (Art 6 Abs 1 lit c DSGVO):

Zur Erfüllung unserer eigenen Verpflichtungen in Bezug auf Rechnungslegung und Buchhaltung

2. Wurde eine Datenschutz-Folgenabschätzung durchgeführt?

Ja Nein

Wenn Ja, wann?

20.03.2018

C. Detailangaben zu Buchhaltung

1. Kategorien der betroffenen Personen

1 Kunden

2. Rechtsgrundlagen

Erfüllung von einer rechtlichen Verpflichtung (Art 6 Abs 1 lit c DSGVO)

3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten) sind abgelegt

In Datenbank

4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen

a. Kategorien der verarbeiteten Daten und Bekanntgabe, ob sie an Empfänger übermittelt werden

Kategorien der betroffenen Personen- gruppe aus Punkt 1	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO, strafrecht- lich relevant iSd Art 10 DSGVO	Empfänger
1 Kunden	1	Daten zur Person: Steuernummer, UID-Nummer, GLN Nummer, SVA-Nummer	nein	Finanzamt
1 Kunden	2	Daten zur Person: Name, Anschrift, E- Mail, Telefonnummer, Bankverbindung	Nein	

b. Löschungs- und Aufbewahrungsfristen

Daten aus Punkt 4 lit a (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungs- fristen
1	Aufbewahrungsfrist: sieben Jahre nach Ablauf des Kalenderjahres des letzten Geschäftsjahres
2	Aufbewahrungsfrist: sieben Jahre nach Ablauf des Kalenderjahres des letzten Geschäftsjahres

5. Kategorien von Empfängern, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern

a. Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie zB UNO, OSZE)

Empfängerkategorien bzw. Empfänger in Drittstaaten oder Internationalen Organisationen (aus Punkt 4 lit a)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation (Angabe der intern. Organisation)
1	nein	
2	nein	

Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Abs 1 Unterabsatz 1 DSGVO erfolgt (vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Corporate binding rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt):

Nicht zutreffend

D. Detailangaben zu Erbringung der Services

1. Kategorien der betroffenen Personen

1 Kunden

2. Rechtsgrundlagen

Erfüllung von einer rechtlichen Verpflichtung (Art 6 Abs 1 lit c DSGVO)

3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten) sind abgelegt

In Datenbank

4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen

a. Kategorien der verarbeiteten Daten und Bekanntgabe, ob sie an Empfänger übermittelt werden

Kategorien der betroffenen Personen- gruppe aus Punkt 1	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO, strafrecht- lich relevant iSd Art 10 DSGVO	Empfänger
1 Kunden	1	Daten zur Person: Name, Anschrift, E- Mail, Telefonnummer, Bankverbindung, Steuernummer, UID-Nummer, GLN Nummer, SVA-Nummer	nein	

b. Löschungs- und Aufbewahrungsfristen

Daten aus Punkt 4 lit a (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1	Aufbewahrungsfrist: sieben Jahre nach Ablauf des Kalenderjahres des letzten Geschäftsjahres

5. Kategorien von Empfängern, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern

a. Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie zB UNO, OSZE)

Empfängerkategorien bzw. Empfänger in Drittstaaten oder Internationalen Organisationen (aus Punkt 4 lit a)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation (Angabe der intern. Organisation)
1	nein	

Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Abs 1 Unterabsatz 1 DSGVO erfolgt (vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Corporate binding rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt):

Nicht zutreffend

E. Detailangaben zur Sicherheit

1. Kategorien der betroffenen Personen

1 Kunden

2. Rechtsgrundlagen

Erfüllung von einer rechtlichen Verpflichtung (Art 6 Abs 1 lit c DSGVO)

3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten) sind abgelegt

In Datenbank

4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen

a. Kategorien der verarbeiteten Daten und Bekanntgabe, ob sie an Empfänger übermittelt werden

Kategorien der betroffenen Personen-gruppe aus Punkt 1	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO, strafrechtlich relevant iSd Art 10 DSGVO	Empfänger
1 Kunden	1	IP-Adresse	nein	

b. Löschungs- und Aufbewahrungsfristen

Daten aus Punkt 4 lit a (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1	Die IP-Adresse wird 30 Tage nach der Erfassung anonymisiert

5. Kategorien von Empfängern, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern

a. Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie zB UNO, OSZE)

Empfängerkategorien bzw. Empfänger in Drittstaaten oder Internationalen Organisationen (aus Punkt 4 lit a)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation (Angabe der intern. Organisation)
1	nein	

Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Abs 1 Unterabsatz 1 DSGVO erfolgt (vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Corporate binding rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt):

Nicht zutreffend

F. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

a. Vertraulichkeit:

- Absicherung der Server mittels Firewall und Secure administrative host
- Kontinuierliche Updates der Server-Software
- Kontinuierliche Updates der Applikationssoftware
- Absicherung der Datenbank mittels sicheren Passwörtern
- Verwendung von SSL/TLS bei allen Datenübertragungen über das Internet
- Nachvollziehbarkeit der Zugriffe inkl. Exports
- Verschlüsselung der Passwörter

b. Integrität:

- Verwendung von SSL/TLS bei allen Datenübertragungen
- Absicherung der Datenbank durch Integritätsprüfungen
- Protokollierung von administrativen Änderungen

c. Verfügbarkeit und Belastbarkeit:

- Widerkehrende Tests auf Belastbarkeit des Systems
- Überwachungsmechanismen auf Verfügbarkeit des Systems
- Benachrichtigung und Notfallbehandlung bei Ausfällen
- Wiederherstellbarkeit des Systems ist gewährleistet durch Backups

d. Pseudonymisierung und Verschlüsselung:

- Die IP-Adresse wird 30 Tage nach Protokollierung anonymisiert

e. Evaluierungsmaßnahmen:

- Wiederkehrende Tests auf Belastbarkeit und Sicherheit des Systems
- Wiederkehrende Tests der Betriebsumgebung durch den Betreiber
- Wiederkehrende Tests der Systemfunktionen durch den Betreiber
- Automatisierte Sicherheitsprüfung des Systems
- Auditlogs zur Nachvollziehbarkeit von datenschutzrechtlichen- und finanzbuchhalterischen Daten