Vereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen nach §11 BDSG sowie nach Art. 28 und Art. 29 DSGVO

Zwischen

Unternehmensname

Straße

PLZ Stadt

Deutschland

-Auftraggeber-

und

Foxtag GmbH

Kattrepelsbrücke 1

20095 Hamburg

Handelsregister HRB 137778 (Amtsgericht Hamburg)

-Auftragnehmer-

Zusammenfassung

Mit Foxtag können Sie Serviceaufträge Ihren Mitarbeitern übermitteln und diese vor Ort bei Ihren Kunden digital dokumentieren. Wenn Sie Foxtag also nutzen, werden zwangsläufig auch persönliche Daten Ihrer Mitarbeiter (Name, E-Mail Adresse etc.) und Ihrer Kunden (Name, Anschrift, Kontaktdaten etc.) auf der Foxtag-Plattform gespeichert. Für Foxtag hatte der Schutz Ihrer Daten schon immer oberste Priorität. Foxtag verpflichtet sich personenbezogene Daten, die im Zusammenhang mit der Nutzung von Foxtag verarbeitet und genutzt werden, nur für die Zwecke der Erfüllung der Dienstleistung zu verarbeiten und zu nutzen und alle notwendigen Vorkehrungen und Maßnahmen zu treffen, damit das Datengeheimnis und die Datensicherheit jederzeit gewährleistet ist. Diese Vereinbarung zur Auftragsdatenverarbeitung enthält dazu vertiefende Informationen und ist mit dem Inkraftreten der DS-GVO zum 25.05.2018 verpflichtend.

**Inhaltsverzeichnis**

[Zusammenfassung 2](#_Toc514933113)

[Vereinbarung zur Auftragsdatenverarbeitung 4](#_Toc514933114)

[1. Auftragsdatenverarbeitung (Gegenstand und Dauer) 4](#_Toc514933115)

[1.1 Gegenstand und Dauer des Auftrags; Umfang, Art und Zweck der Datenverarbeitung 4](#_Toc514933116)

[1.2 Art der Daten und Kreis der Betroffenen 4](#_Toc514933117)

[1.3 Berichtigung, Löschung und Sperrung von Daten 5](#_Toc514933118)

[1.4 Innerbetriebliche Organisation, Datenschutzbeauftragter und Kontrollmaßnahmen 5](#_Toc514933119)

[1.5 Berechtigung zur Begründung von Unterauftragsverhältnissen 5](#_Toc514933120)

[1.6 Kontrollrechte des Auftraggebers und Duldungs- und Mitwirkungspflichten des Auftragnehmers 5](#_Toc514933121)

[1.7 Mitteilungen über Verstöße gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen 6](#_Toc514933122)

[1.8 Umfang der Weisungsbefugnisse 6](#_Toc514933123)

[1.9 Rückgabe überlassener Datenträger und Löschung gespeicherter Daten nach Beendigung des Auftrags 6](#_Toc514933124)

[1.10 Unterstützung des Auftraggebers (ab 25. Mai 2018) 7](#_Toc514933125)

[1.11 Vertragsanpassung 7](#_Toc514933126)

[2. Technische und organisatorische Maßnahmen 7](#_Toc514933127)

[2.1 Server- und Datenbank-Dienstleister 7](#_Toc514933128)

[2.2 Weitere Dienstleister 8](#_Toc514933129)

[2.3 Zutrittskontrolle 9](#_Toc514933130)

[2.4 Zugangskontrolle 10](#_Toc514933131)

[2.5 Zugriffskontrolle 11](#_Toc514933132)

[2.6 Weitergabekontrolle 12](#_Toc514933133)

[2.7 Eingabekontrolle 13](#_Toc514933134)

[2.8 Auftragskontrolle 13](#_Toc514933135)

[2.9 Verfügbarkeitskontrolle 13](#_Toc514933136)

[2.10 Getrennte Verarbeitung 14](#_Toc514933137)

[2.11 Maßnahmen nach Art. 32 DSGVO (ab 25. Mai 2018) 14](#_Toc514933138)

Vereinbarung zur Auftragsdatenverarbeitung

Die FOXTAG GmbH (im Folgenden "Auftragnehmer") und die oben als Auftraggeber angegebene Firma (im Folgenden "Auftraggeber") haben einen Vertrag über die Nutzung der FOXTAG App und zugehöriger Cloud Services geschlossen (im Folgenden "Vertrag"). Zum Zweck der Erbringung der vertragsgegenständlichen Leistungen durch den Auftragnehmer schließen Auftraggeber und Auftragnehmer (im Folgenden auch "die Parteien") ergänzend die nachfolgende Vereinbarung.

# Auftragsdatenverarbeitung (Gegenstand und Dauer)

## Gegenstand und Dauer des Auftrags; Umfang, Art und Zweck der Datenverarbeitung

### Der Auftragnehmer erhebt, verarbeitet und nutzt die zum Zweck der Erbringung der vertragsgegenständlichen Leistungen übergebenen Daten im Wege der weisungsgebundenen Auftragsdatenverarbeitung (§ 11 BDSG, ab 25. Mai 2018: Art. 28 DSGVO) für den Auftraggeber. Der Auftraggeber bleibt "Herr der Daten" und behält die volle Kontrolle über die vom Auftragnehmer zu erhebenden, zu verarbeitenden und zu nutzenden Daten. Im Verhältnis der Parteien stehen sämtliche vom Auftragnehmer für den Auftraggeber erhobenen, verarbeiteten oder genutzten Daten ausschließlich dem Auftraggeber zu; ein Zurückbehaltungsrecht des Auftragnehmers besteht hieran nicht.

### Der Gegenstand des Auftrags ergibt sich aus dem Vertrag. Der Auftragnehmer wird im Rahmen der Auftragsdatenverarbeitung (§ 11 BDSG, ab 25. Mai 2018: Art. 28 DSGVO) für die Dauer des Vertrages und soweit aufgrund nachvertraglicher Pflichten erforderlich darüber hinaus personenbezogene Daten erheben, verarbeiten und/oder nutzen. Dies erfolgt ausschließlich für den Auftraggeber und auf der Basis dieser Vereinbarung, der vom Auftraggeber erteilten Weisungen, der gesetzlichen Vorgaben und zur Erfüllung der übertragenen Aufgaben. Der Umfang, die Art und der Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den Auftragnehmer sind in den Vertragsdokumenten beschrieben.

## Art der Daten und Kreis der Betroffenen

Betroffen sind alle zur Verwaltung der Anlagen und Gegenstände vorgehaltenen personenbezogenen Daten, wie etwa Personenstammdaten, Vertragsstammdaten, Rechnungsdaten sowie Informationen zu den zugeordneten Objekten, Ansprechpartnern (z.B. Hausmeister für den Objektzugang) Anlagen, Gegenständen und Artikeldaten. Im Rahmen der vertragsgegenständlichen Datenverarbeitung werden möglicherweise vom Auftragnehmer insbesondere personenbezogene Daten über

* die Kunden oder Ansprechpartner des Auftraggebers, deren Kontaktdaten (Name, Anschrift, Telefonnummer(n), Mailadresse(n)), mit ihnen vereinbarte Termine und die digitalisierte Unterschriften des Kunden oder eines Vertreters zu den einzelnen durchgeführten Serviceleistungen wie z.B. Wartungen sowie ggf. Abrechnungsinformationen
* die Namen der vom Auftraggeber eingesetzten Mitarbeiter, deren Kontaktdaten (Firmen-Anschrift, Telefonnummer(n), Mailadresse(n)), die Zuordnung zu einzelnen Serviceaufträgen wie Installations-, Wartungs-, Störungsbehebungs- oder Reparaturaufträgen sowie die digitalisierte Unterschrift des Mitarbeiters zur Bestätigung der ergänzten Eingaben und
* die vom Auftraggeber betreuten Objekte, Anlagen und Gegenstände sowie deren Zuordnung zu den Kunden des Auftraggebers als Eigentümer oder Verwalter (insbesondere betreffend der Standorte, Anzahl, Servicebedürftigkeit und Wartungszustand einschließlich Prüfergebnisse, Messdaten, Mängel, getauschte Teile, Anmerkungen, Fotos und betriebsrelevante Informationen wie Pläne, Fehlercodes, Handbücher, etc. bezüglich der Anlagen und Gegenstände)

erhoben, verarbeitet und genutzt. Im Übrigen ergeben sich die Art der Daten und der Kreis der Betroffenen aus den Vertragsdokumenten.

## Berichtigung, Löschung und Sperrung von Daten

Der Auftragnehmer ist verpflichtet, auf Aufforderung durch den Auftraggeber die von ihm erhobenen, verarbeiteten und/oder genutzten Daten zu berichtigen, zu löschen und/oder zu sperren.

## Innerbetriebliche Organisation, Datenschutzbeauftragter und Kontrollmaßnahmen

### Der Auftragnehmer stellt sicher, dass sein Personal über die Bedeutung des Datenschutzes sowie die sich aus dem BDSG (ab 25. Mai 2018: der DSGVO) und sonstigen Vorschriften über den Datenschutz ergebenden Pflichten belehrt und schriftlich auf die Einhaltung des § 5 BDSG verpflichtet ist (ab 25. Mai 2018: schriftlich zur Einhaltung der Vertraulichkeit und des Art. 29 DSGVO verpflichtet haben) und dass Daten, die dem Datenschutz unterliegen, nur nach Maßgabe der einschlägigen rechtlichen Anforderungen verarbeitet werden. Der Auftragnehmer verpflichtet sich, nur solchen Mitarbeitern Zugang zu den Informationen und Daten der Auftraggeber zu gewähren, die unmittelbar mit der Leistungserbringung im Rahmen dieses Vertrags betraut sind. In datenschutzrechtlichen Fragen ist bei der Foxtag GmbH folgender Ansprechpartner benannt: Dirk Thiede.

### Der Auftragnehmer ist im Rahmen des § 38 Abs. 3 BDSG (ab 25. Mai 2018: Art. 31 DSGVO) verpflichtet, gegenüber der Aufsichtsbehörde Auskünfte richtig, vollständig und rechtzeitig zu erteilen. Er wird Maßnahmen der Aufsichtsbehörde gem. § 38 Abs. 4 BDSG dulden sowie vollziehbare Anordnungen gem. § 38 Abs. 5 BDSG erfüllen (ab 25. Mai 2018: Maßnahmen der Aufsichtsbehörde nach Art. 58 zu dulden und zu erfüllen).

## Berechtigung zur Begründung von Unterauftragsverhältnissen

Der Auftragnehmer ist berechtigt, für die Erbringung seiner Leistungen Subunternehmer einzuschalten. Er wird lediglich zuverlässige Subunternehmer beauftragen und dafür sorgen, dass sich die Weisungen und Rechte des Auftraggebers entsprechend § 11 BDSG (ab 25. Mai 2018: Art. 28 DSGVO) auch im Verhältnis zu den Subunternehmern durchsetzen lassen. Der Auftragnehmer ist insbesondere verpflichtet, beauftragte Subunternehmer schriftlich oder – ab 25. Mai 2018 – in einem elektronischen Format (vgl. Art. 28 Abs. 9 DSGVO) zu allen Punkten dieses Vertragsanhanges zu verpflichten.

Der Auftragnehmer wird mit Inkrafttreten der DSGVO den Auftraggeber über jede ab 25. Mai 2018 beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von die datenverarbeitungsrelevanten Subunternehmern informieren und dem Auftraggeber die Gelegenheit zum Einspruch gegen derartige Ernennungen oder Änderungen geben. Ein solches Einspruchsrecht besteht, wenn objektiv zu befürchten ist, dass der Auftragsnehmer durch die Ernennung seine mit Blick auf den Datenschutz vereinbarten Pflichten nicht erfüllen wird. Im Übrigen steht dem Auftragnehmer im Falle eines Einspruchs durch den Auftraggeber das Recht zu, den Vertrag außerordentlich mit einer Frist von einem Monat zu kündigen.

## Kontrollrechte des Auftraggebers und Duldungs- und Mitwirkungspflichten des Auftragnehmers

### Der Auftragnehmer ist verpflichtet, die nach dem Gesetz erforderlichen Kontrollen des Auftraggebers, Einsichtnahmen in Dokumente sowie Anfertigung von Kopien zu dulden und an allen für die Erfüllung der gesetzlichen Kontrollrechte erforderlichen Maßnahmen angemessen mitzuwirken. Der Auftraggeber ist berechtigt, die Ausführung der einschlägigen Datenschutzbestimmungen, der datenschutzrechtlichen Regelungen dieses Vertrags, seiner Weisungen sowie der Datensicherungsmaßnahmen hinsichtlich der Verarbeitung seiner Daten zu kontrollieren. Die Kontrollrechte umfassen auch ein Einsichtsrecht in die Prüfungsberichte der zuständigen Aufsichtsbehörde für den Datenschutz.

### Kontrollmaßnahmen in den Betriebsräumen dürfen nur erfolgen, wenn eine angemessene Ausübung der Kontrolle nicht auf anderem Wege, insbesondere durch Fragebögen, durch die Anforderung von Prüfergebnissen oder durch Einschaltung von sachverständigen Dritten durchführbar ist. Ohne wichtigen Grund dürfen sie nur während der Betriebszeiten stattfinden, sie erfordern eine rechtzeitige vorherige Ankündigung dem Auftragnehmer gegenüber.

### Die Kontrollmaßnahmen werden ausschließlich vom betrieblichen Datenschutzbeauftragten – ersatzweise vom Geschäftsführer – des Auftraggebers oder einer von diesem beauftragten Person vorgenommen. Sofern der Datenschutzbeauftragte des Auftraggebers bei der Wahrnehmung seiner Kontrollaufgaben geheime Informationen über den Auftragnehmer erhält, die über das zur Erfüllung seiner Aufgaben erforderliche Maß hinausgehen, ist er zur Geheimhaltung verpflichtet.

## Mitteilungen über Verstöße gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen

### Stellt der Auftragnehmer Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Datenschutzvorschriften oder gegen die in diesem Vertrag genannten datenschutzrelevanten Verpflichtungen fest, so hat er dies dem Auftraggeber unverzüglich, spätestens innerhalb von 72 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis, mitzuteilen und das weitere Verfahren mit dem Auftraggeber abzustimmen.

### Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich nach Kenntnisnahme des relevanten Ereignisses und stimmt das weitere Verfahren mit dem Auftraggeber ab.

## Umfang der Weisungsbefugnisse

### Der Auftragnehmer wird Weisungen des Auftraggebers, welche sich auf die Beachtung der Vorschriften des BDSG (ab 25. Mai 2018: der DSGVO) oder sonstiger einschlägiger datenschutzrechtlicher Vorschriften beziehen, beachten. Er wird die bei der Leistungserbringung vom Auftraggeber erhaltenen Daten ausschließlich nach den Weisungen des Auftraggebers erheben, verarbeiten und nutzen. Der Auftraggeber wird sein Weisungsrecht durch die Geschäftsführung oder durch von ihr schriftlich Beauftragte ausüben. Weisungen erfolgen grundsätzlich schriftlich, mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich bestätigen.

### Der Auftragnehmer informiert den Auftragsverarbeiter unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen das BDSG (ab 25. Mai 2018: gegen die DSGVO) oder gegen andere Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten verstößt.

## Rückgabe überlassener Datenträger und Löschung gespeicherter Daten nach Beendigung des Auftrags

Nach Beendigung des Vertrags (einschließlich – soweit zutreffend – nachvertraglicher Pflichten) wird der Auftragnehmer die für den Auftraggeber erhobenen, verarbeiteten und/oder genutzten Daten wie Anlagen und Komponenten, Artikeldaten und Prüfprotokolle und Berichte dem Auftraggeber herausgeben. Darüber hinaus steht dem Auftraggeber das Recht zu, diese Herausgabe jederzeit auch vor Vertragsende zu verlangen. Weitergehende gesetzliche Löschungsverpflichtungen und Löschungsansprüche bleiben unberührt. Dies gilt nicht, wenn nach dem Recht der Europäischen Union oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

## Unterstützung des Auftraggebers (ab 25. Mai 2018)

### Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte nach Kapitel III der DSGVO nachzukommen.

### Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten nach Art. 32 DSGVO (Technische und Organisatorische Maßnahmen), Art. 33 DSGVO (Meldung von Datenschutzverletzungen an die Aufsichtsbehörde), Art. 34 DSGVO (Benachrichtigung der Betroffenen Personen im Falle von Datenschutzverletzungen), Art. 35 und 36 DSGVO (Datenschutzfolgenabschätzung und Konsultation mit der Aufsichtsbehörde).

### Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zur Verfügung, die der Auftragnehmer benötigt, um nachzuweisen, dass er die Pflichten nach Art. 28 DSGVO (Auftragsdatenverarbeitung) einhält.

## Vertragsanpassung

Die Parteien verpflichten sich, diese Vereinbarung und insbesondere die Anforderungen an die nach Ziff. 2 dieser Vereinbarung an geänderte gesetzliche Anforderungen und/oder Veränderungen im Stand der Technik im gegenseitigen Einvernehmen an die geänderten Gegebenheiten anzupassen.

# Technische und organisatorische Maßnahmen

Zur Gewährleistung der Sicherheit und Vertraulichkeit der Daten, die dem Datenschutz unterliegen, wird der Auftragnehmer die erforderlichen technischen und organisatorischen Maßnahmen, insbesondere die durch § 9 BDSG (ab 25. Mai 2018: Art. 32 DSGVO) und die sonstigen einschlägigen anwendbaren rechtlichen Rahmenbedingungen festgelegten Maßnahmen, treffen und aufrechterhalten. Insbesondere umfasst dies die im Folgenden aufgeführten Maßnahmen durch Foxtag selbst oder dem von Foxtag genutzten Dienstleister.

Foxtag nutzt zur Zeit folgende Dienstleister:

## Server- und Datenbank-Dienstleister

Amazon Web Services (AWS). Beauftragt für: Bereitstellen der Server-Infrastruktur (Hosting)

Foxtag nutzt Server von AWS, dem weltgrößten Anbieter von Cloudhosting-Lösungen, am Standort Frankfurt. Die AWS Cloudhosting-Lösungen erfüllen höchste Sicherheitsanforderungen.

Der Hostingpartner ist nach höchsten Standards zertifiziert:

* DIN ISO/IEC 27001:2013 (IT-Sicherheitsmanagement)
* PCI DSS-konform (Payment Card Industry Data Security Standard)
* ISO 9001:2008 (Qualitätsmanagement)
* ISO 27018:2014 (Informationssicherheitsstandard)
* SOC1 / SOC2 /SSAE 16/ISAE 3402 (Prüfung durch unabhängige Dritte)
* BSI C5-Testat
* PCI Level 1

Aktuelle Angaben zum Sicherheitskonzept von AWS finden sich unter: <https://aws.amazon.com/de/region-frankfurt/>.

## Weitere Dienstleister

2.2.1 Clever Reach. Beauftragt für: Versand von E-Mails

Die Firma CleverReach unter der Websiteadresse „https://cleverreach.de/“ eine webbasierte eigenständige E-Mail-Marketing-Software an. Diese wird durch die Firma CleverReach GmbH & Co. KG, Mühlenstr. 43, 26180 Rastede/Germany, betrieben. Foxtag benutzt Clever Reach für den Versand des Kundennewsletters, der über neuerungen und Veränderungen von Foxtag informiert.

Weitere Informationen zum Datenschutz von Clever Reach unter <https://www.cleverreach.com/de/funktionen/datenschutz/eu-dsgvo/>

2.2.2 Postmark beauftragt für: Versand von automatisierten System-E-Mails

Postmark wird von der Firma Wildbit, LLC, 225 Chestnut Street, Philadelphia, PA, 19106 betrieben. Foxtag nutzt Postmark für den automatiserten Versand von E-Mail von der Foxtag-Plattform wie z.B. den Versand von Berichten oder Benachrichtigungen über zugewiesene Serviceaufträgen per E-Mail an Servicetechniker.

Weiter Informationen zum Datenschutz von Postmark unter <https://postmarkapp.com/eu-privacy>

2.2.3 Pipedrive beauftragt für: Verwaltung von Kunden und Interessenten

Pipedrive ist ein Verkaufsmanagement-Tool, das kleine Verkaufsteams bei der Verwaltung komplizierter und langwieriger Verkaufsprozesse unterstützen soll. Foxtag verwaltet mit Pipdedrive Kunden- und Interessentendaten und speichert dabei u.a. Namen und Kontaktdaten sowie Informationen zum Unternehmen, den aktuellen Stand des Kontaktes und die Kontakthistorie bspw. bezogen auf den Verkaufprozesses oder die bestehenden Kundenbeziehung. Pipedrive wird durch die Firma Pipedrive Inc, 460 Park Ave SouthNew York, NY 10016, USA betrieben.

Weitere Informationen zum Datenschutz von Pipedrive unter https://support.pipedrive.com/hc/de/articles/360000335129-Pipedrive-und-DSGVO

2.2.4 Billomat beauftragt für: Rechnungsstellung

Billomat ist eine Buchhaltungssoftware und Rechnungsprogramm. Foxtag verwendet Billomat zur Rechnungstellung an seine Kunden. Es werden Kundendaten wie Name, Adresse und Kontaktdaten sowie Zahlbeträge und Bezahlstatus gespeichert. Billomat wird von der Billomat GmbH & Co. KG, Barbiergasse 6, 90443 Nürnberg betrieben.

Weitere Informationen zum Datenschutz von Billomat unter [https://www.billomat.com/magazin/billomat-und-dsgvo/#](https://www.billomat.com/magazin/billomat-und-dsgvo/)

2.2.5 G Suite von Google beauftragt für: Office-Software sowie Datei-Verwaltung und -Speicherung (z.B. Mails, Kalender und Dokumente)

G Suite stellt eine vollumfängliche Kommunikations- und Kollaborationsplattform mitsamt Office-Umgebung aus der Cloud zur Verfügung. Foxtag nutzt G Suite als Office-Software sowie zur Datei-Verwaltung und -Speicherung und erledigt damit tägliche Arbeitsprozesse wie E-Mails schreiben und lesen, Kalendereinträge verwalten, Dokumente erstellen und ablegen, etc.. G Suite wird bereitgestellt und betrieben von Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. Google sichert die Einhaltung der Datenschutz-Grundverordnung in allen Google-Cloud-Diensten zu.

Weitere Informationen zum Datenschutz und der Einhaltung der DSGVO von Google Cloud Diensten und G Suite unter <https://www.google.com/intl/de_at/cloud/security/gdpr/>

2.2.6 iCloud von Apple beauftragt für: Verwaltung Kontakte, Kalender, E-Mail

iCloud ist ein Online-Dienst des Unternehmens Apple Inc., Infinite Loop, Cupertino, CA 95014, USA mit dem Daten gespeichert und zwischen Geräten synchronisiert werden können. icloud ist in jedem Apple Gerät imtegriert, also auch i Phones, iPads und Mac-Rechnern. Foxtag benutzt Apple Geräte und die vefügbaren Programme wie bspw. Mails, Kontakte und Kalender für die tägliche Büroarbeit und Kommunikation.

Auf den von Foxtag verwendete Geräten wurden Software-Updates durchgeführt. Diese Updates stimmen laut apple mit der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union überein.

Weitere Informationen zum Datenschutz und der Einhaltung der DSGVO von Apple siehe unter

* [apple.com/de/privacy](https://www.apple.com/de/privacy/)
* <https://www.apple.com/de/privacy/approach-to-privacy/>
* <https://www.apple.com/legal/privacy/de-ww/>
* <https://www.apple.com/de/business/docs/iOS_Security_Guide.pdf>

## Zutrittskontrolle

Maßnahmen, die sicherstellen, dass Unbefugte keinen Zutritt (räumlich) zu den Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden.

Der Auftragnehmer wird Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren. Hierzu wird der Auftragnehmer insbesondere:

### Maßnahmen von AWS: Die Datenverarbeitung/-Speicherung bei AWS findet in den Räumen von AWS Frankfurt statt. Das Rechenzentrum befinden sich an einem geheimen Ort und verfügen über ein striktes Sicherheitskonzept.

### Bis auf die vereinbarten Zutrittsmöglichkeiten der Administratoren und Moderatoren ist Mitarbeitern des Auftragnehmers ein Zutritt zu den  Rechenzentren, in denen Daten des Auftraggebers gespeichert werden, unmöglich. Eine Datenverarbeitung außerhalb des Rechenzentrums erfolgt nicht. Bei der Dokumentation der obigen Zutrittskontrolle werden die technischen und organisatorischen Maßnahmen der Datenverarbeitung bei AWS in Frankfurt beschrieben.

### Das Rechenzentrum von Amazon erfüllt die DIN ISO/IEC 27001 und 27018-Zertifizierung und ermöglicht Zutritt nur für autorisiertes Fachpersonal des Rechenzentrums

### Zu den eingesetzten Maßnahmen zählen unter anderem:

### Video-Überwachung der Umgebung und der Data-Centers

### Bewegungssensoren, Intrusion-Detection Systeme und Werkschutz

### Einteilung in Sicherheitszonen / Sperrbereiche

### Personenkontrolle durch Pförtner bzw. Werkschutz

### Elektronisch gesicherter Zugang (Zwei Faktor Authentifizierung)

### Vollständige Dokumentation und regelmäßige Prüfung des Zutritts

### Weitere Informationen zu den Sicherheitsprozessen des Amazon Webservices Rechenzentrums finden Sie hier:

### http://aws.amazon.com/de/security/

### https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

### https://cert.webtrust.org/pdfs/soc3\_amazon\_web\_services.pdf

### https://d0.awsstatic.com/whitepapers/compliance/AWS\_Risk\_and\_Compliance\_White paper.pdf

### Maßnahmen von Foxtag: Mitarbeitern des Auftragnehmers wird ein Sicherheits-Schlüssel für das Büro ausgehändigt. Jeder einzelne unterschreibt bei Erhalt der Schlüssel, dass er keinen der Schlüssel an Dritte weiterreicht und es unverzüglich meldet, sollte er seine Schlüssel verlieren.

## Zugangskontrolle

Maßnahmen, die sicherstellen, dass Datenverarbeitungssysteme nicht von Unbefugten genutzt werden können. Gemeint ist hiermit im Gegensatz zur Zutrittskontrolle das Verhindern des Eindringens in das EDV-System seitens unbefugter Personen, insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Sowie Maßnahmen die sicherstellen, dass der Versuch des unbefugten Zugangs nicht unbemerkt bleibt.

Der Auftragnehmer ist verpflichtet, zu verhindern, dass seine Datenverarbeitungssysteme von Unbefugten genutzt werden können. Hierzu wird der Auftragnehmer insbesondere:

* den Zugriff auf die Daten des Auftraggebers mit Zugangsdaten schützen und ihn dadurch sowohl nach innen als auch nach außen nur befugten Personen ermöglichen.
* alle Computersysteme mit personalisierten Benutzernamen und Passwörtern schützen
* den Zugang zu den Kunden-Accounts mit der Erfordernis zur Eingabe von personalisierten Benutzernamen und Passwörtern schützen. Dies gilt für den Zugriff auf die Daten über den Web zugänglichen Kunden-Account als auch für die zur Auftragsdurchführung verwendetete Foxtag App.
* verdächtige Anmeldeversuche zu analysieren und unterbinden. Das können beispielsweise mehrfach falsche Passworteingaben, Zugriffe mit IP-Adressen außerhalb Europas oder von verdächtigen Browsern/Endgeräten sein.
* die Daten verschlüsselt auf den Datenbank-Servern des Hostings-Anbieter (Subunternehmen) ablegen unter Verwendung eines verschlüsselten Dateisystems (encryption at rest)
* die Daten zu 100% verschlüsselt zwischen Datenbank und mobilem Endgerät (mit installierter Foxtag App) übertragen (TLS 1.2, SSLlabs-Bewertung: A)
* die Daten auf den mobilen Endgeräten mit installierter Foxtag App in gesicherten, paswortgeschützten Bereichen speichern

Die Daten werden auf der bei AWS betriebenen Plattform verarbeitet. Der Zugang zu den Daten erfolgt nur über die vorgesehenen Funktionen (Administrationsoberflächen, Webanwendungen) für berechtigte Personen.

Sämtliche Mitarbeiter von Foxtag und AWS sind vertraglich zur Geheimhaltung verpflichtet sowie dazu, die jeweils unternehmensinternen Sicherheitsbestimmungen zu beachten. Diese sehen vor, den Bildschirm bei Verlassen des Arbeitsplatzes zu sperren. Zudem werden insbesondere auch bei den Dienstleistern von Foxtag unter anderem folgende Sicherheitsmechanismen eingesetzt:

* Kennwortrichtlinien und Verfahren (Mindestlänge, Qualität, regelmäßiger Wechsel des Kennworts)
* Sicherung von Notebooks und Datenspeichern durch hardwareseitige Verschlüsselung
* Protokollierung aller wesentlichen Administrationstätigkeiten und Transaktionen
* Technische und Organisatorische Verfahren bei Incidents und Angriffen

## Zugriffskontrolle

Maßnahmen, die sicherstellen, dass die zur Benutzung der Datenverarbeitungsanlagen befugten Personen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und unbefugtes Lesen, Kopieren, Verändern verhindert wird, insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Sowie Maßnahmen die sicherstellen, dass der Versuch des unbefugten Zugriffs nicht unbemerkt bleibt.

Der Auftragnehmer wird dafür sorgen, 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 oder entfernt werden können. Hierzu wird der Auftragnehmer insbesondere:

* über ein Berechtigungskonzept regeln, dass nur befugte Personen Zugriff auf die Daten und Systeme erlangen. Weitere Informationen zum Berechtigungskonzept und der Nutzerverwaltung finden Sie in der Foxtag Nutzerhilfe unter <http://help.foxtag.de/category/T1XEym7S2P-firmenweite-einstellungen-und-nutzerverwaltung>
* Ein Login-Verfahren zur Anmeldung in den Foxtag-Account und in die App nutzen mit E-Mail-Adresse des Nutzers und Passwort. Für einen Login in die Foxtag-App kann zusätzlich im eingeloggten Bereich des Foxtag-Accounts ein QR-Code angezeigt und genutzt werden. Für den Login und die Login-Daten gilt:
  + E-Mail-Adressen sind im Foxtag-System immer eindeutig und können jeweils nur für ein Nutzkonto verwendet verwendet werden.
  + Passwörter werden bei Foxtag verschlüsselt üertragen und verschlüsselt gespeichert
  + Die letzten Logins werden gespeichert
  + Fehlgeschlagene Anmeldeversuche werden gespeichert
  + Speicherung verwendete Geräte, Betriebssysteme und Versionen der Apps
  + Foxtag analysiert und unterbindet verdächtige Anmeldeversuche. Das können beispielsweise mehrfach falsche Passworteingaben, Zugriffe mit IP-Adressen außerhalb Europas oder von verdächtigen Browsern/Endgeräten sein
* die Datenübertragung zu 100% verschlüsseln (TLS 1.2, SSLlabs-Bewertung: A)
* sicherstellen, dass Mitarbeiter von Foxtag keinen Zugriff auf die vom Auftraggeber gespeicherten Daten haben. Dabei gelten folgende Ausnahmen:
  + Foxtag wird vom Auftraggeber beauftragt (bspw. manueller Import von Daten)
  + Foxtag Kundenservice-Mitarbeitern wird vom Auftraggeber der Zugang zum Account des Auftraggebers für Service-Zwecke gewährt
  + Zugriff von technischem Personal von Foxtag zum Zweck einer Störungsbehebung
  + Erfassung statistischer Daten zu Abrechnungszwecken oder zur Weiterentwicklung der Plattform
* die Auftraggeber verpflichten, als Nutzer reale Personen anzulegen und diese korrekt zu benennen (Vorname und Nachname für jeden Nutzer).
* die Auftraggeber verpflichten, ihre Zugangsdaten geheim zu halten und entsprechend sichere Passwörter zu wählen, um einen Missbrauch durch Dritte zu vermeiden.

Der Zugang zur Datenverarbeitungsanlage ist durch das Rechenzentrum von Amazon Webservices geregelt. Weiter Informationen zum DIN ISO/IEC 27001 zertifizierten Rechenzentrum finden Sie hier:

http://aws.amazon.com/de/security/

Und ein Whitepaper hier: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

## Weitergabekontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während  des Transportes oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Der Auftragnehmer wird dafür sorgen, dass personenbezogene Daten bei elektronischer Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Auftragnehmer wird dafür sorgen, dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Die Weitergabekontrolle wird durch den Auftragnehmer durch den Einsatz der folgenden Lösungen sichergestellt:

* Die Datenübertragung zwischen Foxtag Server und App erfolgt zu 100% verschlüsselt (TLS 1.2, SSLlabs-Bewertung: A)
* Die vom Auftraggeber gespeicherten Daten werden von Foxtag unter keinen Umständen an Dritte weitergegeben. Zugriffsberechtigungen werden ausschließlich vom Kunden selbst vergeben.
* Bis auf die mit dem Auftraggeber vereinbarten Zugriffsmöglichkeiten (vergleiche Punkt 2.3) ist Mitarbeitern des Auftragnehmers ein Zugriff auf Daten des Auftraggebers unmöglich.

Die Wege der Datenübermittlung über das Internet bzw. per E-Mail werden mit dem Auftraggeber individuell vereinbart, z.B. die Übertragung von Import-Dateien seitens des Auftraggebers per E-Mail.

Automatisch erstellte Protokolle über ausgefgühte Arbeiten und Prüfungen enthalten neben den Prüfergebnissen und ausgeführten Arbeiten den Name und Unterschrift des durchführenden Technikers oder Prüfers sowie Name und Unterschrift des Kunden oder des Ansprechpartners vor Ort. Das Protokoll wir automatisch im Kunden-Account des Auftraggebers gespeichert. Zudem vergibt der Auftraggeber E-Mail-Adressen (interne Mitarbeiter und berechtigte Dritte), an die eine E-Mail mit einem Download-Link zum Protokoll gesendet wird.

Einer Speicherung, Weitergabe, Transport auf mobilen Datenträgern erfolgt nicht

## Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Der Auftragnehmer wird dafür sorgen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert und/oder entfernt worden sind. Die Eingabekontrolle erfolgt dabei insbesondere durch:

* Eine Datenlöschung durch den Auftraggeber nur als eingeloggter Nutzer möglich ist entsprechend der bereitgestellten Funktionalitäten im Webportal und in der App.
* Regelung, dass Mitarbeiter des Auftragnehmers nur im Rahmen der Vereinbarung mit dem Auftraggeber und im Rahmen ihrer Funktion Zugriff auf die erforderlichen Daten (vergleiche Punkt 2.3) haben.
* Eine Datenlöschung seitens des Auftragnehmers ausschließlich durch technischem Personal mit Administratorrechten möglich ist sowie durch im Account des Auftraggebers eingeloggten Mitarbeitern, denen der Auftraggeber zuvor Zugangsrechte zu ihrem Account gewährt hat.

## Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Der Auftragnehmer wird dafür sorgen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Die Auftragskontrolle erfolgt dabei insbesondere durch:

* Eindeutige Vertragsgestaltung
* Klare Verantwortlichkeiten und Zugriffsmöglichkeiten für die beteiligten Mitarbeiter
* Mit Subauftragnehmern wurden Auftragsdatenverarbeitungsvereinbarungen abgeschlossen, mit denen die Anforderungen des Auftraggebers an den Auftragnehmer auch den Subauftragnehmern übertragen werden.

## Verfügbarkeitskontrolle

Maßnahmen zur Datensicherung (physikalisch/ logisch) gegen zufällige Zerstörung oder Verlust

Der Auftragnehmer trägt dafür Sorge, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Die Verfügbarkeitskontrolle erfolgt dabei insbesondere durch:

* Hochverfügbare Datenbanken (Replication auf physisch getrennte Standby-Systeme)
* Tägliche Backups
* Versionierter Dateispeicher

Die Plattform wird bei AWS über mehrere Verfügbarkeitszonen betrieben. Durch das Verteilen der Plattform über mehrere Verfügbarkeitszonen bleibt das System bei den meisten Ausfallarten, einschließlich Naturkatastrophen oder Systemausfällen, stabil.

<http://aws-de-media.s3.amazonaws.com/images/Region%20Frankfurt/AWS_Security_Whitepaper-german_final.pdf>

## Getrennte Verarbeitung

Der Auftragnehmer stellt durch geeignete technische, personelle und organisatorische Maßnahmen sicher, dass die Vertraulichkeit der übermittelten Daten auch gegenüber anderen Auftraggebern gewahrt wird und jeder Auftraggeber nur Zugriff auf seine Daten hat. Der Auftragnehmer verpflichtet sich, alle Kundendaten zweckgebunden zu verarbeiten und gegenüber Daten anderer Kunden abzuschotten.

## Maßnahmen nach Art. 32 DSGVO (ab 25. Mai 2018)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten treffen der Auftragnehmer und der Auftraggeber geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

### die Verschlüsselung personenbezogener Daten. Dies erfolgt insbesondere durch:

* die nach Ziff. 2.2 vorgesehene Verschlüsselung.

### Maßnahmen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Dies erfolgt insbesondere durch

* die nach Ziff. 2.1 bis 2.8 vorgesehenen Maßnahmen
* Vorhalten einer hinreichenden Leistungsreserve im Rechenzentrum / Einsatz leicht skalierbarer Hosting-Lösungen / o.ä.. nach Ziffer 2.7

### Maßnahmen, um die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Dies erfolgt insbesondere durch

* das nach Ziff. 2.7 vorgesehene Backup

### Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, den \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Hamburg, den \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Auftraggeber FOXTAG GmbH / Auftragnehmer