

# Auftragsverarbeitungsvertrag

Der vorliegende Auftragsverarbeitungsvertrag (nachfolgend der „AVV“ bzw. der „Vertrag“ genannt) bildet den Bestandteil der zwischen dem Kunden und Bitrix, Inc, BITRIX24 LIMITED und ihren verbundenen Personen (nachfolgend gemeinsam „Bitrix24“) getroffenen Vereinbarung über die Bereitstellung von Services des Auftragsverarbeiters (gemäß der jeweils gültigen Definition) sowie über die Verarbeitung personenbezogener Daten des Kunden in Übereinstimmung mit den geltenden Datenschutzvorschriften.

Der vorliegende Auftragsdatenverarbeitungsvertrag ist ab dem Datum seines Inkrafttretens wirksam.

Wenn Sie dem Auftragsverarbeitungsvertrag im Namen des Kunden zustimmen, sichern Sie zu, dass Sie: a) rechtlich vollumfänglich befugt sind, den Kunden an diesen Auftragsverarbeitungsvertrag rechtlich zu binden, (b) diesen Auftragsverarbeitungsvertrag gelesen und verstanden haben und (c) im Namen des Kunden diesem Auftragsverarbeitungsvertrag zustimmen. Wenn Sie keine rechtlichen Befugnisse haben, den Kunden rechtlich zu binden, sollen Sie diesem Auftragsverarbeitungsvertrag nicht zustimmen.

## GELTUNGSBEREICH DIESES AUFTRAGSDATENVERARBEITUNGSVERTRAGES

Der vorliegende Auftragsverarbeitungsvertrag gilt nur, soweit die Verarbeitung personenbezogener Daten des Kunden den Datenschutzvorschriften unterliegt, unter anderem wenn:

- (a) die Verarbeitung im Rahmen der Tätigkeiten erfolgt, welche die über die Domainnamen Bitrix24.eu, Bitrix24.de, Bitrix24.it, Bitrix24.pl und Bitrix24.fr registrierten Kunden betreffen. Für weitere Informationen kontaktieren Sie bitte unseren Kundendienst unter <https://helpdesk.bitrix24.de/ticket.php>
- (b) die Verarbeitung im Rahmen der Tätigkeiten einer im EWR ansässigen Niederlassung des Kunden erfolgt und/oder
- (c) der Kunde Dienstleistungen an die im EWR ansässigen betroffenen Personen erbringt.

Wenn das Unternehmen des Kunden, das den vorliegenden Auftragsverarbeitungsvertrag abschließt, den Nutzungsbedingungen von Bitrix24 zugestimmt hat, bildet dieser Auftragsverarbeitungsvertrag eine Ergänzung zu der Vereinbarung und gilt als deren Bestandteil.

Dieser Auftragsverarbeitungsvertrag ersetzt nicht die bisherigen gültigen Vereinbarungen zu deren jeweiligem Gegenstand (einschließlich etwaiger Änderungs- oder Zusatzvereinbarungen zu Datenverarbeitungsverträgen, die sich auf Services des Auftragsverarbeiters beziehen).

Bei Widersprüchen zwischen den Bestimmungen dieses Auftragsverarbeitungsvertrages und den Nutzungsbedingungen (<https://www.bitrix24.eu/terms/>) hat der

Auftragsverarbeitungsvertrag Vorrang. Sofern die Nutzungsbedingungen nicht durch die Bestimmungen dieses Vertrages geändert werden, bleiben sie im vollen Umfang wirksam.

## DIE PARTEIEN VEREINBAREN HIERMIT WAS FOLGT:

### 1. PRÄAMBEL

Dieser AVV legt die von den Parteien getroffenen Vereinbarungen in Bezug auf die Verarbeitung und die Sicherheit personenbezogener Daten des Kunden in Übereinstimmung mit den Datenschutzvorschriften fest.

#### 1.1 DEFINITIONEN UND AUSLEGUNG:

„**Verbundene Personen**“ bezieht sich auf alle Unternehmen, die von Bitrix24 beherrscht werden, von denen Bitrix24 beherrscht wird oder mit denen Bitrix24 unter gemeinsamer Beherrschung steht.

„**Bitrix24**“ bezieht sich auf Bitrix24 LIMITED, Bitrix Inc und ihre verbundenen Unternehmen, die an der Verarbeitung personenbezogener Daten beteiligt sind.

„**Personenbezogene Daten des Kunden**“ bezieht sich auf alle personenbezogenen Daten, die von Bitrix24 im Auftrag des Kunden im Rahmen der Bereitstellung der Services des Auftragsverarbeiters durch Bitrix24 verarbeitet werden.

„**Verletzung des Schutzes personenbezogener Daten**“ bezieht sich auf eine Sicherheitsverletzung bei Bitrix24, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten des Kunden in den von Bitrix24 verwalteten oder auf eine andere Weise kontrollierten Systemen führt. „Verletzung des Schutzes personenbezogener Daten“ bezieht sich nicht auf fehlgeschlagene Versuche oder Aktivitäten, welche die Sicherheit personenbezogener Daten des Kunden nicht gefährden, darunter erfolglose Anmeldeversuche, Pings, Port-Scans, Denial-of-service-Angriffe und sonstige Angriffe auf Netzwerke, Firewalls oder Netzwerksysteme.

„**Datenschutzvorschriften**“ bezieht sich jeweils entsprechend auf: (a) die DSGVO und/oder (b) das Bundesgesetz über den Datenschutz vom 19. Juni 1992 (Schweiz).

„**Datum des Inkrafttretens**“ bezieht sich jeweils entsprechend auf: das Datum, an dem der Kunde auf „Akzeptieren“ geklickt hat oder die Parteien anderweitig diesem Auftragsverarbeitungsvertrag zugestimmt haben.

„**DSGVO**“ bezieht sich auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

„**E-Mail-Adresse für Benachrichtigungen**“ bezieht sich auf die E-Mail-Adresse (falls zutreffend), die vom Kunden über die Benutzeroberfläche der Services des Auftragsverarbeiters oder auf eine andere von Bitrix24 festgelegte Weise angegeben wurde, um bestimmte Benachrichtigungen von Bitrix24 im Zusammenhang mit diesen Auftragsverarbeitungsbedingungen zu erhalten.

„**Personenbezogene Daten**“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar

wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

„**Verarbeitung personenbezogener Daten**“ bedeutet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (wobei „Verarbeitung“ „Verarbeitungsvorgänge“ und „verarbeitet“ die gleiche Bedeutung haben).

„**Sicherheitsmaßnahmen**“ bezieht sich auf die Maßnahmen zum Schutz personenbezogener Daten gegen eine unbeabsichtigte oder unrechtmäßige Vernichtung, unbeabsichtigten Verlust, eine Veränderung oder unbefugte Offenlegung beziehungsweise gegen einen unbefugten Zugang zu personenbezogenen Daten oder gegen alle anderen Formen unrechtmäßiger Verarbeitung gemäß der Beschreibung in der jeweils gültigen Fassung des über den Link im Anhang 2 zu diesem AVV abrufbaren Dokuments (beziehungsweise dessen maßgeblichen Teils, je nachdem welche Services der Kunde von Bitrix24 erwirbt).

„**Services des Auftragsverarbeiters**“ bezieht sich auf die Erbringung von Wartungs- und Supportleistungen sowie Beratungs- und professionellen Dienstleistungen, auf die Bereitstellung von Software als Dienst (Software as a Service) und alle anderen nach dem Vertrag zu erbringenden Leistungen, in Rahmen derer Bitrix24 personenbezogene Daten des Kunden verarbeitet.

„**Unterauftragsverarbeiter**“ bezieht sich auf Dritte, die von Bitrix24 zum Zwecke der Bereitstellung bestimmter Services des Auftragsverarbeiters und der damit verbundenen technischen Unterstützung einen logischen Zugang zu personenbezogenen Daten des Kunden erhalten und zu ihrer Verarbeitung ermächtigt werden.

„**Vertragslaufzeit**“ bezieht sich auf den Zeitraum zwischen dem Datum des Inkrafttretens und der Beendigung der Bereitstellung der Services des Auftragsverarbeiters an den Kunden durch Bitrix24.

Die in diesem AVV verwendeten Begriffe „**Verantwortlicher**“, „**betroffene Person**“, „**personenbezogene Daten**“, „**Verarbeitung**“, „**Auftragsverarbeiter**“ und „**Aufsichtsbehörde**“ haben die ihnen in der DSGVO zugewiesene Bedeutung.

## 2. VERARBEITUNG VON PERSONENBEZOGENEN DATEN

### 2.1 Verantwortlichkeiten und Einhaltung gesetzlicher Vorschriften; Genehmigung.

2.1.1 Pflichten des Auftragsverarbeiters und des Verantwortlichen. Die Parteien sind sich einig und erklären sich damit einverstanden, dass:

(a) Im Anhang 1 zu den Standardvertragsklauseln der Gegenstand und die Einzelheiten zu der Verarbeitung personenbezogener Daten des Kunden festgelegt sind;

(b) Bitrix24 in Bezug auf personenbezogene Daten des Kunden der Auftragsverarbeiter gemäß den Datenschutzvorschriften ist;

(c) Der Kunde in Bezug auf personenbezogene Daten des Kunden der Verantwortliche oder gegebenenfalls Auftragsverarbeiter gemäß den Datenschutzvorschriften ist;

(d) Jede Partei verpflichtet ist, die ihr gemäß den Datenschutzvorschriften obliegenden Pflichten hinsichtlich der Verarbeitung personenbezogener Daten des Kunden zu erfüllen;

(e) Der Kunde verpflichtet ist, personenbezogene Daten im Rahmen seiner Nutzung oder Inanspruchnahme der Services in Übereinstimmung mit den in den Datenschutzvorschriften festgelegten Anforderungen zu verarbeiten. Der Kunde gewährleistet ferner, dass die von ihm mit der Verarbeitung personenbezogener Daten beauftragten Unterauftragsverarbeiter die Datenschutzvorschriften einhalten. Der Kunde trägt die alleinige Verantwortung für die Genauigkeit, Qualität und Rechtmäßigkeit personenbezogener Daten und der vom Kunden für die Erhebung personenbezogener Daten eingesetzten Mittel.

2.2 Genehmigung durch externe Verantwortliche. Wenn der Kunde der Auftragsverarbeiter ist, sichert der Kunde gegenüber Bitrix24 zu, dass die Handlungen des Kunden, welche die personenbezogenen Daten des Kunden betreffen, und die vom Kunden beauftragten Unterauftragsverarbeiter, darunter die Beauftragung von Bitrix24 als einen weiteren Auftragsverarbeiter, von dem entsprechenden Verantwortlichen genehmigt worden sind.

2.3 Die Parteien sind sich einig, dass Bitrix24 beziehungsweise die Unternehmen der Bitrix24-Guppe verpflichtet sind, bei der Beauftragung von Unterauftragsverarbeitern die im nachstehenden Abschnitt 7 „Unterauftragsverarbeiter“ festgelegten Anforderungen einzuhalten.

2.4 Durch den Abschluss dieses Auftragsverarbeitungsvertrages weist der Kunde Bitrix24 an, personenbezogene Daten des Kunden ausschließlich in Übereinstimmung mit den geltenden gesetzlichen Vorschriften zu bearbeiten: (a) um Services des Auftragsverarbeiters bereitzustellen und die damit verbundene technische Unterstützung zu leisten; (b) wie im Rahmen der Nutzung der Services des Auftragsverarbeiters durch den Kunden (einschließlich in den Einstellungen und anderen Funktionen der Services des Auftragsverarbeiters) sowie der damit verbundenen technischen Unterstützung weiter festgelegt; (c) wie in diesem Auftragsverarbeitungsvertrag bestimmt und (d) wie in den schriftlichen Anweisungen des Kunden, die von Bitrix24 zum Zwecke dieses Auftragsverarbeitungsvertrages als maßgebliche Anweisungen akzeptiert wurden, näher dokumentiert.

2.5 Löschung nach Ablauf der Vertragslaufzeit. Nach Ablauf der Vertragslaufzeit ist Bitrix24 gemäß den Anweisungen des Kunden verpflichtet, alle personenbezogenen Daten des Kunden (einschließlich vorhandener Kopien) aus den Systemen von Bitrix24 in Übereinstimmung mit den geltenden gesetzlichen Vorschriften zu löschen. Bitrix24 wird dieser Anweisung sobald wie billigerweise möglich, spätestens jedoch nach 90 Tagen, nachkommen, wenn kraft gesetzlicher Vorschriften der Vereinigten Staaten, der EU oder eines EU-Mitgliedsstaates keine Pflicht zur Speicherung dieser Daten vorgesehen ist.

2.5.1 Löschung des Accounts

Bleibt eine Bitrix24-Instanz, welche auf einem kostenlosen Tarif läuft (egal, ob darauf zurückgesetzt oder ursprünglich kostenlos erstellt), im Laufe von 30 Tagen inaktiv, wird sie archiviert, und kann nur durch einen Administrator wiederhergestellt werden (es muss also ein Nutzer mit den administrativen Zugriffsrechten sein).

Zur Wiederherstellung des Accounts reicht, dass ein Administrator sich einloggt.

Wird sich kein Administrator im Laufe von weiteren 15 Tagen im Account einloggen, wird die Bitrix24-Instanz komplett gelöscht.

### 3. LAUFZEIT DIESES AVV

Dieser AVV ist ab dem Datum des Inkrafttretens wirksam und bleibt ungeachtet des Ablaufs der Vertragslaufzeit weiterhin gültig, bis alle personenbezogenen Daten des Kunden durch Bitrix24 wie in diesem AVV festgelegt gelöscht werden. Die Löschung der Daten bewirkt eine automatische Beendigung des AVV.

### 4. RECHTE BETROFFENER PERSONEN

4.1 Wenn der Kunde im Rahmen seiner Nutzung oder Inanspruchnahme der Services keine Möglichkeit zur Berichtigung, Korrektur, Einschränkung oder Löschung personenbezogener Daten, wie in den Datenschutzvorschriften festgelegt, hat, ist Bitrix24 (unter Berücksichtigung der Verarbeitungsart personenbezogener Daten des Kunden und gegebenenfalls gemäß Artikel 11 der DSGVO) verpflichtet, durch die Bereitstellung entsprechender Funktionen im Rahmen der Services des Auftragsverarbeiters den Kunden dabei zu unterstützen, dessen Pflicht zur Beantwortung von Anträgen betroffener Personen nachzukommen. Dies umfasst gegebenenfalls auch die Pflicht des Kunden zur Beantwortung von Anträgen im Rahmen der Wahrnehmung von in Kapitel III der DSGVO festgelegten Rechten durch betroffene Personen.

4.2 Bitrix24 ist verpflichtet, den Kunden in dem gesetzlich zulässigen Umfang über die von betroffenen Personen gestellten Anträge auf Zugang zu, Berichtigung, Korrektur, Einschränkung und Löschung personenbezogener Daten dieser Personen beziehungsweise auf Wahrnehmung sonstiger in der DSGVO vorgesehener Rechte umgehend zu informieren. Bitrix24 ist nicht berechtigt, Anträge betroffener Personen ohne eine schriftliche Einwilligung des Kunden zu beantworten. Dies gilt nicht für eine Bestätigung, dass der Antrag den Kunden betrifft. Bitrix24 kooperiert mit dem Kunden und unterstützt ihn bei der Beantwortung von Anträgen betroffener Personen auf Zugang zu deren personenbezogenen Daten beziehungsweise auf Wahrnehmung sonstiger Rechte gemäß der DSGVO, sofern dies rechtlich zulässig ist und sofern der Kunde im Rahmen seiner Nutzung oder Inanspruchnahme der Services keinen Zugang zu diesen personenbezogenen Daten hat.

### 5. MITARBEITER

5.1 Bitrix24 stellt sicher, dass ihre an der Verarbeitung personenbezogener Daten beteiligten Mitarbeiter über den vertraulichen Charakter personenbezogener Daten informiert sind, eine entsprechende Schulung zu ihren Aufgaben erhalten haben und den Geheimhaltungspflichten in dem im Anhang zu diesem AVV festgelegten Umfang unterliegen, wobei diese Pflichten auch nach der Beendigung der Beschäftigung dieser Personen bei Bitrix Inc fortbestehen.

5.2 Bitrix Inc stellt sicher, dass der Zugang der Unternehmen der Bitrix24 Gruppe zu personenbezogenen Daten ausschließlich denjenigen Beschäftigten vorbehalten ist, die einen solchen Zugang zum Zwecke der Vertragserfüllung benötigen.

## 6. DATENSICHERHEIT

6.1 Bitrix24 bietet administrative, technische und organisatorische Garantien zum Schutz der Sicherheit, Vertraulichkeit und Integrität personenbezogener Daten. Diese Maßnahmen sind im Anhang 2 zu diesem AVV beschrieben.

6.2 Sicherheitsmaßnahmen bei Bitrix24. Bitrix24 ist verpflichtet, die im Anhang 2 zu diesem AVV beschriebenen technischen, physischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten des Kunden gegen eine unbeabsichtigte oder unrechtmäßige Vernichtung, einen unbeabsichtigten oder unrechtmäßigen Verlust, eine unbeabsichtigte oder unrechtmäßige Veränderung oder unbefugte Offenlegung beziehungsweise gegen einen unbefugten Zugang umzusetzen und aufrechtzuerhalten. Die Sicherheitsmaßnahmen gemäß Anhang 2 zu diesem AVV umfassen unter anderem die Maßnahmen: (a) zur Sicherstellung fortlaufender Vertraulichkeit, Integrität, Verfügbarkeit und Stabilität von Systemen und Services von Bitrix24; (b) zur raschen Wiederherstellung des Zugangs zu personenbezogenen Daten bei einer Verletzung des Schutzes personenbezogener Daten sowie (c) zur regelmäßigen Wirksamkeitsüberprüfungen. Bitrix24 ist berechtigt, die Sicherheitsmaßnahmen von Zeit zu Zeit zu verbessern oder zu ändern, vorausgesetzt, dass solche Verbesserungen und Änderungen zu keiner Verschlechterung der allgemeinen Sicherheit der Services des Auftragsverarbeiters führen.

6.3 Befolgung von Sicherheitsmaßnahmen durch die Mitarbeiter von Bitrix24. Bitrix24 trifft angemessene Vorkehrungen zur Sicherstellung der Befolgung von Sicherheitsmaßnahmen durch ihre Mitarbeiter, Auftragnehmer und Unterauftragsverarbeiter in dem für ihren Tätigkeitsbereich angemessenen Umfang. Dies beinhaltet, dass alle zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder im entsprechenden Umfang gesetzlicher Verpflichtung zur Vertraulichkeit gemäß der Beschreibung im Anhang 2 zu diesem AVV unterliegen.

6.4 Unterstützung durch Bitrix24 bei Sicherheitsmaßnahmen. Der Kunde erklärt sich damit einverstanden, dass Bitrix24 den Kunden bei der Einhaltung von Pflichten des Kunden betreffend die Sicherheit personenbezogener Daten und betreffend Verletzungen des Schutzes personenbezogener Daten, unter anderem gegebenenfalls von Pflichten des Kunden gemäß Artikel 32 bis einschließlich Artikel 34 der DSGVO unterstützt, indem sie:

(a) die Sicherheitsmaßnahmen in Übereinstimmung mit dem Anhang 2 zu diesem AVV umsetzt und aufrechterhält;

(b) die Bestimmungen des Abschnitts 5 (Verletzungen des Schutzes personenbezogener Daten) einhält und

(c) dem Kunden die Sicherheitsdokumentation zur Verfügung stellt.

## 7. UNTERAUFTRAGSVERARBEITER

7.1 Zustimmung zur Beauftragung von Unterauftragsverarbeitern. Der Kunde gestattet Bitrix24 ausdrücklich die Beauftragung externer Unterauftragnehmer im Zusammenhang

mit der Bereitstellung von Services (abrufbar auch unter Bitrix24 Infrastruktur und Unterauftragsverarbeiter). Bitrix24 hat mit jedem der Unterauftragsverarbeiter eine schriftliche Vereinbarung geschlossen, in der die Pflichten zum Schutz von Kundendaten in mindestens dem gleichen Umfang wie in diesem AVV festgelegt sind, sofern dies für die Art der von diesem Unterauftragsverarbeiter erbrachten Leistungen angemessen ist.

7.2 Verzeichnis derzeitiger Unterauftragsverarbeiter und Benachrichtigung über neue Unterauftragsverarbeiter. Bitrix24 stellt dem Kunden das aktuelle Verzeichnis der Unterauftragsverarbeiter für die im Anhang 1 zu diesem AVV aufgeführten Leistungen zur Verfügung. Das Verzeichnis der Unterauftragsverarbeiter beinhaltet die Angaben zur Identität der Unterauftragsverarbeiter und ihrem Standort und kann vom Kunden auf der Website von Bitrix24 eingesehen werden (abrufbar auch unter Bitrix24 Infrastruktur und Unterauftragsverarbeiter).

7.3 Anforderungen an die Beauftragung von Unterauftragsverarbeitern. Bei der Beauftragung von Unterauftragsverarbeitern verpflichtet sich Bitrix24:

(a) anhand einer schriftlichen Vereinbarung sicherzustellen, dass:

(i) der Unterauftragsverarbeiter ausschließlich dann auf die personenbezogenen Daten des Kunden zugreifen und diese nutzen kann, wenn dies zur Erfüllung der ihm im Rahmen des Unterauftrages übertragenen Pflichten erforderlich ist, und sich dabei an die Nutzungsbedingungen (einschließlich dieses AVV) hält;

(ii) der Unterauftragsverarbeiter den in Artikel 28(3) der DSGVO festgelegten Datenschutzbestimmungen unterliegt, wenn die Verarbeitung personenbezogener Daten des Kunden in den Anwendungsbereich der DSGVO fällt;

(b) für die Einhaltung aller im Rahmen des Unterauftrages dem Unterauftragsverarbeiter übertragenen Pflichten sowie für alle dessen Handlungen und unterlassenen Handlungen im vollen Umfang zu haften.

7.4 Widerspruchsrecht gegen Beauftragung neuer Unterauftragsverarbeiter.

Im Falle einer Beauftragung neuer Unterauftragsverarbeiter während der Vertragslaufzeit und sofern die DSGVO auf die Verarbeitung personenbezogener Daten des Kunden Anwendung findet, verpflichtet sich Bitrix24, den Kunden spätestens 10 Tage bevor der neue Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten des Kunden beginnt, über die Beauftragung (mit Angabe zu der Firma und dem Sitz des entsprechenden Unterauftragsverarbeiters sowie zu den von ihm zu erbringenden Leistungen) zu benachrichtigen, indem er eine E-Mail an die E-Mail-Adresse für Benachrichtigungen versendet.

Der Kunde kann der Beauftragung eines neuen Unterauftragsverarbeiters widersprechen, indem er Bitrix24 innerhalb von fünf (5) Werktagen nach dem Erhalt einer von Bitrix24 versandten Mitteilung umgehend schriftlich benachrichtigt. Sollte der Kunde der Beauftragung eines neuen Unterauftragsverarbeiters widersprechen, wird Bitrix24 angemessene Anstrengungen unternehmen, um dem Kunden geänderte Services zur Verfügung zu stellen oder eine wirtschaftlich vertretbare Änderung der Konfiguration oder der Nutzung der Services durch den Kunden zu empfehlen, bei der keine Verarbeitung personenbezogener Daten durch den abgelehnten neuen Unterauftragsverarbeiter



stattfindet. Dies darf jedoch nicht dazu führen, dass der Kunde dadurch unverhältnismäßig benachteiligt wird. Ist Bitrix24 nicht in der Lage, eine solche Änderung innerhalb eines angemessenen Zeitraums, spätestens jedoch innerhalb von dreißig (30) Tagen zu bewirken, kann der Kunde den entsprechenden Auftrag mittels einer schriftlichen Mitteilung an Bitrix24 stornieren. Dies gilt ausschließlich für diejenigen Services, die von der Bitrix24 nur mit Hinzuziehung des abgelehnten neuen Unterauftragsverarbeiters bereitgestellt werden können. Bitrix24 erstattet dem Kunden alle vorausbezahlten Gebühren für die stornierten Services für die verbleibende Laufzeit des Auftrages ab der Wirksamkeit der Stornierung, ohne dass der Kunde eine Vertragsstrafe für eine solche Stornierung zahlen muss.

## 8. VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN.

8.1 Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten. Sollte Bitrix24 Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erlangen, ist Bitrix24 verpflichtet: (a) den Kunden über die Verletzung des Schutzes personenbezogener Daten umgehend zu benachrichtigen, und (b) angemessene Maßnahmen zur Minimierung der Schäden und zum Schutz personenbezogener Daten des Kunden unverzüglich zu ergreifen.

8.2 Angaben zu einer Verletzung des Schutzes personenbezogener Daten. Eine Benachrichtigung hat, sofern möglich, Einzelheiten zu der Verletzung des Schutzes personenbezogener Daten zu enthalten. Dies umfasst unter anderem die Maßnahmen zur Minimierung etwaiger Risiken und die Empfehlungen von Bitrix24 an den Kunden zum Umgang mit der Verletzung des Schutzes personenbezogener Daten.

8.3 Übersendung der Benachrichtigung. Bitrix24 nimmt die Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten an die E-Mail Adresse für Benachrichtigungen oder nach eigenem Ermessen von Bitrix24 (unter anderem wenn der Kunde keine E-Mail-Adresse angegeben hat) auf einem anderen direkten Kommunikationsweg (z.B. telefonisch oder bei einem persönlichen Gespräch) vor. Die Pflicht zur Angabe der E-Mail-Adresse für Benachrichtigungen obliegt alleine dem Kunden und er hat sicherzustellen, dass die E-Mail-Adresse für Benachrichtigungen aktuell und gültig ist.

8.4 Pflicht zur Benachrichtigung Dritter. Der Kunde trägt die alleinige Verantwortung für die Einhaltung der für den Kunden geltenden gesetzlichen Bestimmungen betreffend die Benachrichtigungspflicht sowie für die Einhaltung von Pflichten zur Benachrichtigung Dritter im Zusammenhang mit etwaigen Verletzungen des Schutzes personenbezogener Daten.

8.5 Keine Schuldanerkennung seitens Bitrix24. Eine Benachrichtigung über oder eine Reaktion auf eine Verletzung des Schutzes personenbezogener Daten seitens Bitrix24 gilt nicht als eine Schuldanerkennung oder Anerkennung einer Haftung seitens Bitrix24 in Bezug auf die Verletzung des Schutzes personenbezogener Daten.

## 9. ÜBERPRÜFUNG DER EINHALTUNG DES AVV

9.1 Um die Einhaltung ihrer Pflichten aus diesem AVV durch Bitrix24 nachzuweisen, sowie auf Anfrage des Kunden ist Bitrix24 verpflichtet, ausführlichere Informationen über die im Anhang 2 zu diesem AVV beschriebenen Sicherheitsmaßnahmen bereitzustellen.

9.2 Auf Anfrage des Kunden und vorbehaltlich der in diesem AVV festgelegten Vertraulichkeitspflichten ist Bitrix24 verpflichtet, dem Kunden, bei dem es sich um keinen Wettbewerber von Bitrix24 handelt (bzw. einem unabhängigen externen Prüfer des Kunden, bei dem es sich um keinen Wettbewerber von Bitrix24 handelt) Informationen bezüglich der Einhaltung der in diesem AVV festgelegten Pflichten und der Umsetzung der im Anhang 2 zu diesem AVV angeführten Sicherheitsmaßnahmen vorzulegen. Der Kunde kann bei Bitrix24 eine Vor-Ort-Überprüfung der für den Schutz personenbezogener Daten maßgeblichen Architektur, Systeme und Verfahren an Standorten, an denen personenbezogene Daten gespeichert werden, beantragen. Der Kunde ist verpflichtet, Bitrix24 die von Bitrix24 oder von ihren Unterauftragsverarbeitern für solche Vor-Ort-Überprüfungen aufgewendete Zeit zu vergüten. Die Vergütung richtet sich nach den bei Bitrix24 geltenden Sätzen für professionelle Dienstleistungen, die dem Kunden auf Anfrage vorgelegt werden. Vor dem Beginn einer solchen Vor-Ort-Überprüfung bestimmen der Kunde und Bitrix24 im beiderseitigen Einvernehmen neben dem von dem Kunden zu zahlenden Erstattungssatz den Umfang, den Zeitpunkt und die Dauer der jeweiligen Überprüfung. Alle Erstattungssätze müssen angemessen sein und die von Bitrix24 oder ihren externen Unterauftragsverarbeitern aufgewendeten Ressourcen berücksichtigen. Der Kunde benachrichtigt Bitrix24 unverzüglich über etwaige im Rahmen einer Überprüfung festgestellte Verstöße.

## 10. DATENSCHUTZ-FOLGEABSCHÄTZUNG

Auf Anfrage des Kunden unterstützt Bitrix24 den Kunden bei der Sicherstellung der Einhaltung aller Pflichten des Kunden in Bezug auf Datenschutz-Folgeabschätzungen und die vorherige Konsultation, einschließlich (gegebenenfalls) der Pflichten des Kunden gemäß Artikeln 35 und 36 der DSGVO, sofern der Kunde anderweitig keinen Zugang zu den maßgeblichen Informationen hat und sofern solche Informationen Bitrix24 vorliegen. Bitrix24 bietet dem Kunden angemessene Unterstützung bei der Zusammenarbeit mit der Aufsichtsbehörde bei der Erfüllung deren Aufgaben an.

## 11. DATENÜBERMITTLUNGEN

1.1 In den meisten Fällen werden die über die Domainzonen Bitrix24.eu, Bitrix24.de, Bitrix.it, Bitrix24.pl und Bitrix24.fr erhobenen Daten durch BITRIX24 LIMITED, die ihren Sitz in der Republik Zypern hat, innerhalb des Europäischen Wirtschaftsraums verarbeitet und in der Europäischen Union, nämlich in Frankfurt, Deutschland, in den Datenzentren von Amazon Web Services gehostet. Diese Datenzentren entsprechen im vollen Umfang den Bestimmungen der DSGVO

<https://aws.amazon.com/premiumsupport/knowledge-center/gdpr-compliance/>

11.2 Für weitere Informationen über die Datenverarbeitungsvorgänge betreffend die über die Domainnamen Bitrix24.com, Bitrix24.in, Bitrix24.tr, Bitrix24.cn registrierten Kunden kontaktieren Sie bitte unseren Kundendienst. Weitere Informationen zu den Datenverarbeitungsstandorte finden sich unter <https://helpdesk.bitrix24.de/ticket.php>.

11.3 Internationale Datenübermittlungen. Vorbehaltlich geeigneter Garantien gemäß Artikel 46 der DSGVO (siehe Ziff. 11.3.1, 11.3.2) darf Bitrix24 personenbezogene Daten des Kunden in den Vereinigten Staaten von Amerika und in der Russischen Föderation verarbeiten.

### 11.3.1 Einhaltung der Rahmenvereinbarungen für den EU-USA-, UK-US- und den Schweiz-USA-Datenschutzschild.

Bitrix24 hält sich an die Bestimmungen der zwischen den USA und der EU, der Schweiz und dem Vereinigten Königreich vereinbarten Datenschutzschild-Vereinbarungen, die von dem US-amerikanischen Handelsministeriums für die Erfassung, Nutzung und Aufbewahrung der aus der EU und der Schweiz in die Vereinigten Staaten übermittelten personenbezogenen Daten festgelegt wurden. Das Unternehmen hat bestätigt, dass es sich an die in dem Datenschutzschild festgelegten Grundsätze der Informationspflicht und Wahlmöglichkeit, Verantwortlichkeit für die Weitergabe, Sicherheit, Datenintegrität und Zweckbindung, des Auskunftsrechts sowie an die Grundsätze des Rechtsschutzes, der Durchsetzung und Haftung hält. Bei Widersprüchen zwischen den Bestimmungen dieser Datenschutzrichtlinie und den Grundsätzen des Datenschutzschildes haben die Grundsätze des Datenschutzschildes Vorrang. Weitere Informationen zum Datenschutzschild-Programm und unserer Zertifizierung finden Sie unter <https://www.privacyshield.gov>. Die Einhaltung der Bestimmungen des Datenschutzschildes durch das Unternehmen wird von der US-amerikanischen Federal Trade Commission überwacht.

In Übereinstimmung mit den im Datenschutzschild festgelegten Grundätzen ist Bitrix24 verpflichtet, den Beschwerden im Zusammenhang mit der Erfassung und Nutzung Ihrer personenbezogenen Daten nachzugehen. Bürger aus der EU und der Schweiz, die Nachfragen oder Beschwerden zu unserer Datenschutzschild-Richtlinie haben, werden gebeten, sich zuerst an Bitrix24 unter [privacy@bitrix24.com](mailto:privacy@bitrix24.com) zu wenden.

Die lokalen Datenschutzbehörden des Kunden in der EU treten als Ihre unabhängigen Beschwerdestellen für die aus der EU übermittelten Daten auf.

Bitrix24 hat sich ferner verpflichtet, mit dem von den EU-Datenschutzbehörden und dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) eingerichteten Gremium bei ungeklärten Datenschutzschild-Beschwerdefällen betreffend die aus der EU und der Schweiz übermittelten Daten zusammenzuarbeiten.

Unter bestimmten Umständen, die auf der Datenschutzschild-Webseite unter <https://www.privacyshield.gov/article?id=ANNEX-I-introduction> näher beschrieben sind, hat der Kunde auch das Recht, ein verbindliches Schiedsverfahren zu beantragen, wenn andere Streitbeilegungsmöglichkeiten ausgeschöpft wurden. Dabei kann Bitrix24 für rechtswidrige Weitergabe an Dritte von den nach dem Datenschutzschild erhaltenen personenbezogenen Informationen zur Verantwortung gezogen werden.

11.3.2 Die Sicherheit von Daten und Rechten betroffener Personen gemäß der DSGVO bei den Datenverarbeitungsvorgängen in der Russischen Föderation und in den USA wird durch die angemessenen Garantien nach Artikel 46 der DSGVO, insbesondere die von der Europäischen Kommission im Einklang mit dem Prüfverfahren angenommenen Standarddatenschutzklauseln gewährleistet. Die Europäische Kommission hat bestimmt, dass die Standarddatenschutzklauseln hinreichende Garantien für den Datenschutz bei grenzübergreifend zu übermittelten Daten bieten. Sie sind berechtigt, Informationen über diese vertraglichen Garantien zu erhalten (kontaktieren Sie dazu bitte unseren Datenschutzbeauftragten).

## 12. ANWENDBARES RECHT

12.1 Dieser AVV (einschließlich sämtlicher außervertraglichen Sachverhalte und Verpflichtungen, die sich daraus ergeben oder im Zusammenhang damit stehen) unterliegt den gesetzlichen Vorschriften der Republik Zypern und ist in Übereinstimmung damit auszulegen.

12.1 Für alle Streitigkeiten, Widersprüche, Gerichtsverfahren und Ansprüche zwischen den Parteien im Zusammenhang mit diesem Vertrag (einschließlich sämtlicher außervertraglichen Sachverhalte und Verpflichtungen, die sich daraus ergeben oder im Zusammenhang damit stehen) sind die zypriotischen Gerichte zuständig.

12.3 Für die in Ziffer 11.3.2 angeführten Datenübermittlungen in die Länder außerhalb des EWR, die durch die Verantwortlichen in der EU an die Auftragsverarbeiter außerhalb der EU vorgenommen werden und die durch angemessene Garantien gemäß Artikel 46 der DSGVO, speziell durch die von der Europäischen Kommission im Einklang mit dem Prüfverfahren angenommenen Standarddatenschutzklauseln geschützt sind, sowie für Kunden, sofern die Verarbeitung im Rahmen der Tätigkeit einer Niederlassung in einem anderen Land des EWR als der Republik Zypern erfolgt, und/oder Kunden, welche Leistungen an betroffene Personen in einem anderen Land des EWR als der Republik Zypern erbringen, gilt die Aufsichtsbehörde in der Republik Zypern als die federführende Aufsichtsbehörde gemäß Artikel 56 der DSGVO.

Die Aufsichtsbehörde der einzigen Niederlassung von Bitrix24 im EWR, die zuständig ist, als federführende Aufsichtsbehörde für grenzüberschreitende Verarbeitung durch den Auftragsverarbeiter in Übereinstimmung mit dem in Artikel 60 der DSGVO festgelegten Verfahren aufzutreten, ist die Aufsichtsbehörde in der Republik Zypern.

### 13. ÄNDERUNGEN DIESES AVV

13.1 Bitrix24 ist berechtigt, Änderungen an diesem AVV vorzunehmen, wenn diese Änderung:

- (a) durch diesen AVV ausdrücklich gestattet ist;
- (b) die Änderung der Firma oder der Rechtsform der juristischen Person betrifft;
- (c) notwendig ist, um die geltenden gesetzlichen Bestimmungen, Vorschriften, einen gerichtlichen Beschluss oder eine von einer Regulierungs- oder Regierungsbehörde erlassene Richtlinie einzuhalten, oder
- (d) wenn diese Änderung: (i) zu keiner Verschlechterung der allgemeinen Sicherheit der Services des Auftragsverarbeiters führt; (ii) zu keiner Erweiterung des Umfangs beziehungsweise Beseitigung der Beschränkungen für die Verarbeitung personenbezogener Daten des Kunden führt und (iii) nach vernünftiger Auffassung von Bitrix24 keine sonstigen erheblichen negativen Auswirkungen auf die Rechte des Kunden aus diesem AVV hat.

13.2 Benachrichtigung über die Änderungen. Sollte Bitrix24 beabsichtigen, diesen AVV zu ändern, wird Bitrix24 spätestens 30 Tage (bzw. einen entsprechend kürzeren Zeitraum, der kraft geltender gesetzlicher Bestimmungen, Vorschriften, eines gerichtlichen Beschlusses oder einer von einer Regulierungs- oder Regierungsbehörde erlassenen Richtlinie notwendig ist) vor dem Inkrafttreten der Änderung den Kunden darüber in Kenntnis setzen,

indem Bitrix24 entweder: (a) eine E-Mail an die E-Mail-Adresse für Benachrichtigungen versendet oder (b) den Kunden über die Benutzeroberfläche der Services des Auftragsverarbeiters darauf hinweist. Widerspricht der Kunden einer solchen Änderung, ist der Kunde berechtigt, den Vertrag durch eine schriftliche Erklärung gegenüber Bitrix24 zu kündigen, die spätestens 30 Tage nachdem Bitrix24 ihn über die Änderung benachrichtigt zu erfolgen hat.

## Anhang 1

### GEGENSTAND UND EINZELHEITEN ZUM GEGENSTAND DER DATENVERARBEITUNG

Betroffene Personen. Die übermittelten personenbezogenen Daten umfassen folgende Kategorien betroffener Personen:

1. betroffene Personen, über die Bitrix24 im Rahmen der Bereitstellung von Services des Auftragsverarbeiters personenbezogene Daten erhebt, und/oder
2. betroffene Personen, deren personenbezogene Daten im Rahmen der Bereitstellung von Services des Auftragsverarbeiters von dem Kunden, auf dessen Anweisung oder in dessen Auftrag an Bitrix24 übermittelt werden.

Sie umfassen:

- Mitarbeiter, einschließlich ehrenamtlicher Mitarbeiter, Vertreter, Zeitarbeitnehmer und Aushilfskräfte
- Kunden und Auftraggeber (einschließlich deren Mitarbeiter)
- Lieferanten (einschließlich deren Mitarbeiter)
- Gesellschafter oder Träger
- Antragsteller, Korrespondenzpartner und Frageteller
- Berater, Gutachter und sonstige Sachverständige

Datenkategorien. Die übermittelten personenbezogenen Daten betreffen folgende Datenkategorien:

- persönliche Daten, einschließlich Informationen, welche die betroffene Person und ihre persönlichen Merkmale kennzeichnen, unter anderem der Name und die Kontaktinformationen;
- Kommunikationsmetadaten;
- Mitarbeiterdaten, unter anderem gegebenenfalls die Arbeitszeit und der Standort (vorbehaltlich der Nutzerzustimmung im Rahmen der Zeiterfassung);

- persönliche Unterlagen, die von einer Behörde zu Identifizierungszwecken ausgestellt wurden, unter anderem Kopien der Passdaten;
- bereitgestellte Waren und Dienstleistungen und die damit zusammenhängenden Informationen, einschließlich der Angaben zu bereitgestellten Waren und Dienstleistungen, ausgestellten Lizenzen sowie Verträgen;
- Angaben zu dem Land, der Stadt, dem Bundesstaat und der Region;
- Online-Identifizierungsmerkmale;
- Gerätekennungen;
- persönliche Bilder;
- Angaben zu Lebensgewohnheiten und sozialen Verhältnissen.

Besondere Datenkategorien (falls zutreffend):

Verarbeitungsvorgänge. Auf die personenbezogenen Daten finden folgende grundlegende Verarbeitungsvorgänge Anwendung (bitte auflisten):

- IT, digitale, technische oder Telekommunikationsleistungen, unter anderem Bereitstellung von Technologieprodukten und Dienstleistungen, Telekommunikations- und Netzwerkdiensten, digitalen Dienstleistungen, Hosting, Cloud- und Kundendienstleistungen und Softwarelizenzierung. Dies umfasst unter anderem:
- das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, das Abfragen, die Verwendung, die Offenlegung, das Löschen oder die Vernichtung personenbezogener Daten des Kunden zum Zwecke der Bereitstellung von Services und der damit verbundenen technischen Unterstützung an den Kunden in Übereinstimmung mit diesem Auftragsverarbeitungsvertrag. Zu den Services zählen: Social Intranet, Projektmanagement und Aufgaben, Chat und Video, Dokumentationsmanagement und Bitrix24.Drive, Kalender, E-Mail, CRM, Webseiten, Open Channels, Kontaktzentren, Telefonie, Zeitmanagement, CRM-Marketing, Arbeitsabläufe, eCommerce, Box-Version.

## Anhang 2

### SICHERHEITSMASSNAHMEN

Bitrix24 verpflichtet sich, die in diesem Anhang 2 festgelegten Sicherheitsmaßnahmen umzusetzen und aufrechtzuerhalten. Bitrix24 ist berechtigt, die Sicherheitsmaßnahmen von Zeit zu Zeit zu verbessern oder zu ändern, vorausgesetzt, dass solche Verbesserungen und Änderungen zu keiner Verschlechterung der allgemeinen Sicherheit der Services des Auftragsverarbeiters führen.

#### 1. WICHTIGSTE DATENSCHUTZGRUNDSÄTZE BEI BITRIX24

- 1.1 Alle IT-Systeme von Bitrix24 sind gegen einen unbefugten Zugang geschützt.
- 1.2 Alle IT-Systeme von Bitrix24 werden ausschließlich in Übereinstimmung mit den maßgeblichen Unternehmensrichtlinien verwendet.
- 1.3 Alle Mitarbeiter von Bitrix24 und alle Dritten, die befugt sind, die IT-Systeme zu nutzen, einschließlich unter anderem Unterauftragsverarbeitern, haben sicherzustellen, dass sie mit diesen Richtlinien vertraut sind und diese zu jedem Zeitpunkt befolgen.
- 1.4 Alle direkten Vorgesetzten haben sicherzustellen, dass alle unterstellten und weisungsgebundenen Mitarbeiter und Unterauftragsverarbeiter diese Richtlinien gemäß Absatz 2.3. stets befolgen und einhalten.
- 1.5 Alle auf den IT-Systemen gespeicherten Daten werden sicher und im Einklang mit den maßgeblichen Bestandteilen der EU-Datenschutzverordnung 2016/679 („DSGVO“) und allen anderen derzeit geltenden und in Zukunft zu verabschiedenden Datenschutzvorschriften verwaltet.
- 1.6 Allen auf den IT-Systemen gespeicherten Daten werden entsprechend ihrer Vertraulichkeitsstufe eingeordnet. Alle einer Vertraulichkeitsstufe eingeordneten Daten werden entsprechend ihrer Klassifizierung behandelt.
- 1.7 Alle auf den IT-Systemen gespeicherten Daten stehen ausschließlich denjenigen Nutzern zur Verfügung, die den Zugang zu ihnen aus legitimen Gründen benötigen.
- 1.8 Alle auf den IT-Systemen gespeicherten Daten sind gegen einen unbefugten Zugang und gegen eine unrechtmäßige Verarbeitung geschützt.
- 1.9 Alle auf den IT-Systemen gespeicherten Daten sind gegen den Datenverlust und die Datenbeschädigung geschützt.
- 1.10 Alle Verletzungen des Schutzes personenbezogener Daten auf den IT-Systemen oder von den darauf gespeicherten Daten werden gemeldet und anschließend von der IT-Abteilung untersucht.

## **2. SICHERHEITSMASSNAHMEN BEI SOFTWARE**

- 2.1 Sämtliche auf den IT-Systemen verwendeten Softwareanwendungen (einschließlich unter anderem Betriebssystemen, einzelner Softwareanwendungen und Firmware) werden auf dem neuesten Stand gehalten und alle entsprechenden Software-Aktualisierungen, -Korrekturen, -Nachbesserungen und dazwischenliegende Produktaktualisierungen werden durchgeführt.
- 2.2 Beim Feststellen von Sicherheitslücken bei der Software werden diese Sicherheitslücken sofort geschlossen. Andernfalls wird die Software aus den IT-Systemen entfernt, bis die Sicherheitslücke erfolgreich geschlossen werden kann.
- 2.3 Die Mitarbeiter von Bitrix24 dürfen nur mit einer Genehmigung des IT-Managers eigene Software installieren. Dies gilt unabhängig davon, ob diese Software auf einem physischen Datenträger zur Verfügung steht oder heruntergeladen wurde. Alle Softwareanwendungen müssen von dem IT-Manager genehmigt werden und dürfen nur dann installiert werden, wenn die Installation kein Sicherheitsrisiko für die IT-Systeme darstellt und wenn sie gegen keine auf diese Software gegebenenfalls anwendbaren Lizenzverträge verstößt.

## **3. ANTIVIREN-SICHERHEITSMASSNAHMEN**

- 3.1 Die IT-Systeme von Bitrix24 (einschließlich aller Computer und Server) sind durch die geeigneten Antiviren-, Firewall- und sonstige geeignete Internet-Sicherheitssoftware geschützt. Auf allen Softwareanwendungen wurden die neuesten Aktualisierungen und Sicherheitsdefinitionen installiert.
- 3.2 Alle IT-Systeme von Bitrix24 sind durch die Antivirensoftware geschützt und durchlaufen mindestens einmal pro Woche eine vollständige Systemprüfung.
- 3.3 Alle physischen Speichermedien (z.B. USB-Speichersticks oder alle Arten von Datenträgern), die von den Mitarbeitern für die Dateienübermittlungen verwendet werden, werden vor der Übermittlung auf Viren überprüft. Solche Viren-Prüfungen werden von dem Leiter der IT-Abteilung durchgeführt.
- 3.4 Die Mitarbeiter von Bitrix24 dürfen nur mit Genehmigung des IT-Managers die Dateien über Cloud-Speichersysteme übermitteln. Alle von einem Cloud-Speicher heruntergeladenen Dateien werden beim Herunterladen auf Viren geprüft.
- 3.5 Alle an Dritte außerhalb des Unternehmens zu übermittelten Dateien, unabhängig davon, ob sie per E-Mail, auf physischen Datenträgern oder auf andere Weise (z.B. über einen gemeinsamen Cloud-Speicher) bereitgestellt werden, werden vor der Übermittlung im Rahmen des Übermittlungsprozesses auf Viren untersucht.

## **4. SICHERHEITSMASSNAHMEN BEI HARDWARE**

- 4.1 IT-Systeme von Bitrix24 befinden sich in sicher verschlossenen Räumen (die von



befugten Nutzern mit einer Smartcard betreten werden können).

4.2 Alle IT-Systeme, die für die gewöhnliche Nutzung durch die Nutzer nicht vorgesehen sind (einschließlich unter anderem der Server, Netzwerkausstattung und Netzwerkinfrastruktur) befinden sich in abgesicherten klimatisierten Räumen in verschlossenen Schränken, zu denen ausschließlich bestimmte Mitarbeiter der IT-Abteilung Zugang haben).

4.3 Alle von dem Unternehmen bereitgestellten mobilen Geräte (einschließlich unter anderem Laptops, Tablets und Smartphones) werden stets sicher befördert und sorgfältig behandelt.

## **5. ZUGRIFFSSICHERHEIT**

5.1. Die Zugriffsrechte auf alle IT-Systeme werden auf Grundlage der Zuständigkeitsebenen der Mitarbeiter innerhalb der Unternehmensstruktur von Bitrix24 und der Notwendigkeit für die Ausübung ihrer beruflichen Funktionen festgelegt. Die Mitarbeiter erhalten keinen Zugriff auf die IT-Systeme oder elektronische Daten, die begründeterweise zur Ausübung ihrer beruflichen Funktionen nicht erforderlich sind.

5.2 Alle IT-Systeme (und insbesondere mobile Geräte, darunter unter anderem Laptops, Tablets und Smartphones) werden durch ein sicheres Passwort oder den sicheren Zugangscode beziehungsweise durch andere sichere Anmeldeverfahren geschützt, die von der IT-Abteilung für geeignet erklärt und genehmigt wurden.

5.3 Auf alle Passwörter finden folgende Sicherheitsmaßnahmen Anwendung:

- a) Die Passwörter müssen aus mindestens 8 Zeichen bestehen;
- b) Sie müssen eine Kombination aus Groß- und Kleinbuchstaben, Nummern und Symbolen enthalten;
- c) Sie müssen mindestens einmal jede 90 Tage geändert werden;
- d) Sie dürfen mit den vorherigen Passwörtern gleich sein;
- e) Sie dürfen nicht offensichtlich oder leicht zu erraten (z.B. Geburtstage oder andere bedeutungsvolle Daten, Namen, Ereignisse oder Orte, u.s.w.) sein und
- f) Sie müssen von den einzelnen Nutzern selbst erstellt worden sein.

5.4 Alle IT-Systeme mit Bildschirmen und Benutzerinterface-Geräten (z.B. Maus, Tastatur, Touchscreen usw.) werden durch einen mit Passwort geschützten Bildschirmschoner geschützt, der sich nach 5 Minuten der Inaktivität aktiviert.

## **6. SICHERHEIT BEI DATENSPEICHERUNG**

1.1 Alle Daten und insbesondere personenbezogenen Daten werden durch die Verwendung von Passwörtern und der OTP-Autorisierung sicher gespeichert.

1.2 Auf den mobilen Geräten (einschließlich unter anderem Laptops, Tablets und

Smartphones) werden keine personenbezogenen Daten aufbewahrt. Dies gilt unabhängig davon, ob es sich bei dem Gerät um ein Gerät von Bitrix24 handelt oder nicht.

- 1.3 Keine Daten und insbesondere keine personenbezogenen Daten werden auf einen persönlichen Computer oder ein persönliches Gerät des Mitarbeiters übertragen, es sei denn, dass es sich bei dem betreffenden Mitarbeiter um einen im Auftrag von Bitrix24 tätigen Unterauftragsverarbeiter handelt und sich dieser Unterauftragsverarbeiter verpflichtet hat, die Datenschutzrichtlinie des Unternehmens und die DSGVO vollumfänglich einzuhalten.

## **7. DATENSCHUTZ**

7.1 Alle von Bitrix24 erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten (gemäß der DSGVO-Definition) werden streng nach Maßgabe der in der DSGVO festgelegten Grundsätze und Bestimmungen sowie der Datenschutzrichtlinie des Unternehmens erhoben, gespeichert und verarbeitet.

7.2 Alle Nutzer, die für und im Auftrag von Bitrix24 Daten verarbeiten, unterliegen stets den Bestimmungen der Datenschutzrichtlinie des Unternehmens und haben diese einzuhalten. Insbesondere gilt Folgendes:

- a) Alle E-Mails, die vertrauliche oder sensible personenbezogene Daten enthalten, werden durch die Verwendung des TLS SSL-Protokolls verschlüsselt;
- b) Alle E-Mails, die vertrauliche oder sensible personenbezogene Daten enthalten, werden als „vertraulich“ gekennzeichnet;
- c) Vertrauliche und sensible personenbezogene Daten dürfen ausschließlich über gesicherte Netzwerke übermittelt werden; Übermittlungen über ungesicherte Netzwerke sind unter keinen Umständen zulässig;
- d) Alle physisch zu übermittelnden vertraulichen und sensiblen personenbezogenen Daten, einschließlich der Übermittlung auf elektronischen Speichermedien, werden in geeigneten Behältern, die mit als „vertraulich“ beschriftet sind, transportiert.
- e) Werden vertrauliche oder sensible personenbezogene Daten auf einem Computerbildschirm angezeigt und wird der betreffende Computer für einen Zeitraum unbeaufsichtigt gelassen, sind die Mitarbeiter verpflichtet, den Computer und den Bildschirm vor dem Verlassen zu sperren.

7.3 Alle Anfragen bezüglich des Datenschutzes sind an die Datenschutzbeauftragte, Frau Elena Riazanova (info@quick-gdpr.co.uk), zu richten.

## **8. RECHENZENTREN & NETZWERKSICHERHEIT DES HOSTING-ANBIETERS**

Bitrix24 nutzt die Amazon Web Services zur Speicherung und Analyse von Daten, einschließlich der AWS Cloud Infrastruktur in der Region Europa (Frankfurt) und der Region Europa (Irland).

## **VERFÜGBARKEIT**

AWS kennt alle kritischen Systemkomponenten, die erforderlich sind, um die Verfügbarkeit unseres Systems zu erhalten und den Betrieb im Fall eines Ausfalls wieder aufzunehmen. Kritische Systemkomponenten werden an mehreren, voneinander isolierten Standorten (Availability Zones genannt) gesichert. Jede Availability Zone ist auf einen unabhängigen Betrieb mit hoher Zuverlässigkeit ausgelegt. Die Availability Zones sind vernetzt. Dies ermöglicht Ihnen die Nutzung von Anwendungen, für die ein automatischer, unterbrechungsfreier Failover zwischen den Availability Zones eingerichtet ist. Extrem ausfallsichere Systeme und eine daraus resultierende Serviceverfügbarkeit sind Bestandteil des Systemdesigns. AWS-Kunden profitieren durch den Einsatz von Availability Zones und Datenreplikation von extrem kurzen Wiederherstellungszeiträumen und Wiederherstellungspunktzielen sowie höchstmöglicher Serviceverfügbarkeit.

#### PLAN ZUR AUFRECHTERHALTUNG DES BETRIEBS:

Der AWS-Betriebskontinuitätsplan bestimmt Maßnahmen zur Vermeidung und Verringerung von Störungen durch Umwelteinflüsse. Er enthält betriebliche Details zu den Maßnahmen, die vor, während und nach einem entsprechenden Ereignis ergriffen werden. Der Betriebskontinuitätsplan wird durch Tests gestützt, die auch Simulationen verschiedener Szenarios umfassen. Während und nach diesen Tests dokumentiert AWS die Leistung seiner Mitarbeiter und Prozesse, Korrekturmaßnahmen und die abgeleiteten Erfahrungen zur kontinuierlichen Verbesserung.

#### DATENTRÄGERVERNICHUNG

Medienspeichergeräte, auf denen Kundendaten gespeichert sind, werden von AWS als kritisch eingestuft und deshalb über ihren gesamten Lebenszyklus entsprechend als höchst dringlich behandelt. AWS hat bestehende Normen, wie die Geräte installiert, betrieben und irgendwann zerstört werden, wenn sie nicht mehr verwendet werden. Wenn ein Speichergerät das Ende seines Lebenszyklus erreicht hat, wird es gemäß den in NIST 800-88 beschriebenen Techniken stillgelegt. Medien, auf denen Kundendaten gespeichert wurden, werden erst nach erfolgter Stilllegung aus der Hand von AWS gegeben.

#### INFRASTRUKTURWARTUNG

**Gerätewartung.** AWS überwacht und wartet die elektrischen und mechanischen Geräte präventiv, um den unterbrechungsfreien Betrieb der Systeme in den AWS-Rechenzentren zu gewährleisten. Die Gerätewartung wird von qualifiziertem Personal entsprechend einem dokumentierten Wartungszeitplan durchgeführt.

**Umweltmanagement.** AWS überwacht elektrische und mechanische Systeme und Anlagen, sodass Probleme sofort erkannt werden. Hierfür werden fortlaufend Audit-Tools und Informationen der Gebäudemanagement- und elektrischen Überwachungssysteme ausgewertet. Es werden vorbeugende Wartungen vorgenommen, um eine kontinuierliche Funktionsfähigkeit der Anlagen sicherzustellen.

#### GOVERNANCE UND RISIKO

**Risikomanagement für Rechenzentren.** Das AWS Security Operations Center führt regelmäßig Bedrohungs- und Schwachstellenprüfungen der Rechenzentren durch. Die fortlaufende Bewertung und Abwehr von potenziellen Schwachstellen erfolgt über die Risikobewertungsaktivitäten der Rechenzentren. Diese Bewertung wird zusätzlich zum

Risikobewertungsprozess auf Unternehmensebene durchgeführt, um Risiken für das Unternehmen als Ganzes zu erkennen und zu verwalten. Dabei werden auch regionale behördliche und Umweltrisiken berücksichtigt.

**Sicherheitsbescheinigungen von Dritten.** Durch Prüfungen der AWS-Rechenzentren durch Dritte, wie in unseren Drittanbieterberichten dokumentiert, stellt AWS sicher, dass angemessene Sicherheitsmaßnahmen implementiert wurden, die zum Erwerb von Sicherheitszertifikaten erforderlich sind. Abhängig vom Compliance-Programm und dessen Anforderungen können externe Prüfer die Entsorgung von Medien testen, die Aufzeichnungen der Sicherheitskameras prüfen, die Eingänge und Korridore eines Rechenzentrums beobachten, die elektronischen Zugangskontrollgeräte testen und die Anlagen des Rechenzentrums untersuchen.

### **Netzwerke und Übertragungen.**

**Datenübertragung.** Die Rechenzentren von Bitrix24 sind über private Verbindungen, die durch AWS-Netzwerk-Firewalls geschützt werden vernetzt und ermöglichen sichere Datenübertragungen. Dadurch werden die Vertraulichkeit, Integrität und Verfügbarkeit von Netzwerken geschützt und die Daten können während einer elektronischen Übermittlung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

**Reaktion auf Verletzungen des Schutzes personenbezogener Daten.** Bitrix24 überwacht eine Vielzahl an Kommunikationswegen auf Verletzungen des Schutzes personenbezogener Daten. Das Sicherheitspersonal von Bitrix24 reagiert unverzüglich auf die bekannt gewordenen Verletzungen.

**Externe Angriffsfläche.** Bitrix24 analysiert potentielle Angriffsvektoren und setzt bei den nach außen gerichteten Systemen geeignete herstellereigene Technologien ein, die dafür speziell entwickelt wurden.

**Verschlüsselungstechnologien.** Bitrix24 verwendet eine HTTPS-Verschlüsselung (auch bekannt als SSL bzw. TLS Verbindung).

## **9. SICHERHEIT BEI UNTERAUFTRAGSVERARBEITERN**

Vor einer Beauftragung von Unterauftragsverarbeitern überprüft Bitrix24 die Sicherheit und Datenschutzpraktiken der Unterauftragsverarbeiter. Dadurch wird sichergestellt, dass Unterauftragsverarbeiter über die Sicherheits- und Datenschutzstandards verfügen, die für ihren Zugang zu den Daten und für die von ihnen bereitzustellenden Services angemessen sind. Nach der Bewertung der von einem Unterauftragsverarbeiter ausgehenden Risiken durch Bitrix24 und stets vorbehaltlich der Einhaltung der im Abschnitt 7 festgelegten Anforderungen wird der Unterauftragsverarbeiter aufgefordert, die entsprechenden Sicherheits-, Vertraulichkeits- und Geheimhaltungsvereinbarungen abzuschließen.

