
Datenschutzrichtlinie

Anwendungsbereich

Diese Datenschutzrichtlinie behandelt alle Informationen, die die firstcolo GmbH im Rahmen der von Kunden beauftragten Produkte und Services verarbeitet, sofern keine anderen spezifischeren Richtlinien gelten. Unsere Services umfassen Cloud-Services (firstcolo Cloud, firstkube, VMware Cloud, Proxmox Cloud), Managed Services (Managed Hosting, Cloud management, Microsoft Services, Nextcloud, DaaS), Storage Services (Cloud Storage Services, Storage on Demand) und soweit anwendbar Hardware Services (Dedicated Server) und Colocation & Housing (Colocation, Private Cage).

Diese Datenschutzrichtlinie konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den Allgemeinen Geschäftsbedingungen des Auftragnehmers (**firstcolo GmbH**) und aus dem daraus entstandenen Einzelvertrag mit dem Auftraggeber (nachstehend „**Kunden**“) ergeben. Der Auftragnehmer erbringt für den Auftraggeber auf der Grundlage des bestehenden Servicevertrags die dort näher bezeichneten Leistungen. Die Regelungen dieser Richtlinie gehen den Regelungen des Servicevertrages und sonstiger Absprachen zwischen den Vertragsparteien vor, sofern und soweit dies erforderlich ist, um das geltende Datenschutzrecht einzuhalten. Diese Vereinbarung findet Anwendung auf alle Tätigkeiten bei deren Durchführung der Auftragsverarbeiter, Mitarbeiter des Auftragsverarbeiters oder durch den Auftragsverarbeiter nach Maßgabe dieser Richtlinie beauftragte Empfänger Zugriff auf personenbezogene Daten, des Auftraggebers erhalten und / oder solche personenbezogenen Daten für den Auftraggeber in dessen Auftrag verarbeiten, insbesondere erheben, speichern und verwenden. Verpflichtungen des Auftragsverarbeiters aufgrund gesetzlicher Vorschriften oder behördlicher oder gerichtlicher Anordnungen bleiben von dieser Vereinbarung unberührt.

Gegenstand, Spezifizierung und Dauer der Auftragsverarbeitung

Gegenstand und Dauer der Auftragsverarbeitung

Der Auftragsverarbeiter verarbeitet nach Abschluss eines Rahmen- oder Zusatzvertrages unter Umständen personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieser Richtlinie. Aus dem Rahmenvertrag ergeben sich Gegenstand und Dauer der Auftragsverarbeitung.

Räumlicher Anwendungsbereich

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Art der Daten

Abhängig von den im Rahmen- oder Zusatzvertrag gebuchten Services, ergeben sich die Art der Daten, die Art und Zweck der Datenverarbeitung und die Kategorien der betroffenen Personen.

Generell

Zur Rechnungsstellung und Bearbeitung von Kundentickets wird ein Kundenaccount mit den notwendigen Stammdaten und Zahlungsinformationen angelegt. Weitere Mitbenutzeraccounts können eigenständig durch den Hauptaccountnutzer angelegt werden.

Diese Daten, sowie im Rahmen von Kundentickets bereitgestellte Informationen werden von uns entsprechend den gesetzlichen Vorgaben gespeichert und danach anonymisiert.

Cloud Services und Storage Services

Die Art der Daten umfasst alle Inhalte, die der Kunde in den zur Verfügung gestellten Services

speichert. Es findet kein direkter Zugriff seitens firstcolo auf die Daten statt. Eine indirekte Verarbeitung personenbezogener Daten kann ggf. erfolgen durch:

- Log-Auswertung von API-Endpunkten zur Absicherung der Systeme, Erkennen von Angriffen, Sicherstellen der korrekten Funktionalität der Endpunkte
- Backups der Openstack-Umgebung zur Sicherung der Daten zur Wiederherstellung bei einem Systemausfall
- Log-Auswertung Firewall und Web-Proxy zur Absicherung der Systeme, erkennen von Angriffen, sicherstellen der korrekten Funktionalität der Firewall
- Log-Auswertung DNS-Server zur Absicherung der Systeme, erkennen von Angriffen, sicherstellen der korrekten Funktionalität der DNS-Server

Bei Beendigung der Vertragslaufzeit werden alle verbliebenen Daten des Kunden unwiederbringlich gelöscht.

Managed Services

Die Art der Daten umfasst alle Inhalte, die der Kunde in den zur Verfügung gestellten Services speichert. Es findet kein direkter Zugriff seitens firstcolo auf die Daten statt. Eine indirekte Verarbeitung personenbezogener Daten kann ggf. erfolgen durch:

- Loggen von Systemänderungen. Zur späteren Nachvollziehbarkeit werden bei bestimmten Systemen Änderungen geloggt. Daten wie Nutzer-ID/IP-Adresse in den Logs können ggf. auf natürliche Personen schließen lassen.
- Backups der Managed-Umgebung zur Sicherung der Daten zur Wiederherstellung bei einem Systemausfall
- Bereitstellung von virtuellen Serverlösungen. Es findet keine direkte Verarbeitung von Kundendaten statt, jedoch haben wir im Rahmen der Erstellung und Pflege von Verwaltungssystemen, die dazu dienen vServer an Kunden zu vermieten, einen hohen und direkten Einfluss auf die Verfügbarkeit von den darauf gespeicherten Informationen.
- Bereitstellung von DDoS Lösungen. Es findet keine direkte Verarbeitung von Kundendaten statt, jedoch kann es im Rahmen des Schutzes vor DDoS Angriffen notwendig sein, die Verfügbarkeit einzelner Kundensysteme einzuschränken, um die Erreichbarkeit vieler Systeme zu gewährleisten.

Bei Beendigung der Vertragslaufzeit werden alle verbliebenen Daten des Kunden unwiederbringlich gelöscht.

Colocation & Housing und Hardware Services

Seitens der firstcolo besteht bei diesen Services keine Zugriffsmöglichkeit auf die Daten der Kunden und kein direkter Einfluss auf die verarbeitenden Systeme. Unter keinen Umständen werden Mitarbeiter der firstcolo versuchen sich eigenständig Zugriff auf Server des Kunden oder Mietserver zu verschaffen. Werden defekte Datenträger bei Mietservern ausgetauscht oder Mietserver nach Beendigung der Vertragslaufzeit zurückgegeben, werden die Datenträger genullt und ggf. vernichtet. Es findet keine Auftragsverarbeitung im Sinne der DS-GVO statt.

Sollte ein Kunde explizit die Unterstützung von Fachpersonal für Arbeiten auf Systemebene wünschen, stellt dies eine Erweiterung der bis dahin geschlossenen Serviceleistungen dar und im Rahmen dieser Tätigkeiten gelten die Angaben für „Managed Services“.

Rechte und Pflichten des Auftragnehmers

Einhaltung des geltenden Rechts

Die Pflichten des Auftragnehmers bei der Datenverarbeitung ergeben sich aus dieser Richtlinie und dem anwendbaren Recht. Das anwendbare Recht umfasst insbesondere das Bundesdatenschutzgesetz („**BDSG**“) und die Datenschutz-Grundverordnung („**DS-GVO**“)

Verarbeitung nur nach Weisung

Der Auftragnehmer wird die personenbezogenen Daten des Auftraggebers nur zur Erfüllung der entsprechend bezogenen Serviceleistungen verarbeiten oder auf zusätzlich dokumentierte Weisung des Auftraggebers (Kundenticket).

Weisungsberechtigte Person

Grundsätzlich sind alle Mitarbeiter des Auftraggebers weisungsberechtigt, die Zugriff auf das Ticketsystem des Auftragsverarbeiters haben.

Grundsätzlich sind alle Mitarbeiter des Auftragsverarbeiters weisungsempfangsberechtigt.

Verpflichtung zur Vertraulichkeit

Der Auftragsverarbeiter wird die zur Verarbeitung der personenbezogenen Daten eingesetzten Personen zur Vertraulichkeit verpflichten, soweit diese nicht einer gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

Unterstützung bei der Wahrung der Betroffenenrechte

Der Auftragsverarbeiter wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei dessen Pflichten unterstützen, Anträge auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Personen zu bearbeiten. Wenn sich ein Betroffener hinsichtlich solcher Daten, die der Auftragsverarbeiter im Auftrag des Auftraggebers verarbeitet, zwecks Geltendmachung von Betroffenenrechten unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragsverarbeiter haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

Unterstützung bei der Einhaltung Art. 32 - 36 DS-GVO

Der Auftragsverarbeiter wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und dem Auftragsverarbeiter zur Verfügung stehenden Informationen durch geeignete technische und organisatorische Maßnahmen bei der Einhaltung der in Art. 32-36 DS-GVO genannten Pflichten im Rahmen der eigenen Möglichkeiten unterstützen, insbesondere hinsichtlich der Sicherheit der Verarbeitung, der Datenschutz-Folgeabschätzung und der Konsultation mit Aufsichtsbehörden.

Bestellung eines Datenschutzbeauftragten

Der Auftragsverarbeiter ist zur Bestellung eines Datenschutzbeauftragten verpflichtet. Bei Fragen rund um das Thema Datenschutz kann sich der Kunde direkt an den Datenschutzbeauftragten wenden. Seine Kontaktdaten sind auf der Webseite des Auftragsverarbeiters veröffentlicht.

Meldungen von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Auftraggeber zusammen und unterstützt ihn entsprechend, damit der Auftraggeber seinen Verpflichtungen gemäß den Artikeln 33 und 34 der DS-GVO nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

Technisch-Organisatorische Maßnahmen

Grundsatz

Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragsverarbeiter wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutzgrundverordnung (Art. 32 DS-GVO) genügen.

Ausgestaltung

Der Auftragsverarbeiter hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Änderungen

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Wesentliche Änderungen sind zu dokumentieren. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

Zustimmung des Auftraggebers

Bei Akzeptanz des Servicevertrags durch den Auftraggeber werden die in den "**Technisch-Organisatorische Maßnahmen**" dokumentierten Maßnahmen des Auftragsverarbeiters zur Grundlage der Serviceerbringung.
Subunternehmer

Allgemeine schriftliche Genehmigung

Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Auftraggebers für die Beauftragung von Unterauftragsverarbeitern, die in dieser Datenschutzrichtlinie aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Auftraggeber mindestens vier Wochen im Voraus ausdrücklich in Textform über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Auftraggeber damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Auftraggeber die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann

Bei Vertragsschluss eingeschaltete Subunternehmer

Nur bei den folgenden Services sind Subunternehmer beauftragt:

Managed Services

croit GmbH – Unterstützt bei Bedarf beim Debugging technischer Probleme und erhält im Kontext dieser Arbeiten (und nur für den Zeitraum der Arbeiten) Zugriff auf die CEPH Infrastruktur. Es findet kein direkter Zugriff auf die Daten der Kunden statt.

Sorgfältige Auswahl der Subunternehmer

Der Auftragsverarbeiter hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser zwischen den Vertragsparteien getroffene Vertrag und die gesetzlichen Vorgaben der DS-GVO eingehalten werden können.

Verpflichtung der Subunternehmer

Der Auftragsverarbeiter hat die Verträge mit Subunternehmern so zu gestalten, dass sie den Vorgaben des geltenden Datenschutzrechts und dieser Richtlinie entsprechen. Die Subunternehmer sind vom Auftragsverarbeiter insbesondere zu verpflichten, keine weiteren oder anderen Subunternehmer ohne Einhaltung der Richtlinie zu betrauen. Der Auftragsverarbeiter kontrolliert, ob hinreichende Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass das anwendbare Datenschutzrecht und diese Richtlinie eingehalten werden.

Nebenleistungen

Nicht als Subunternehmerverhältnisse im Sinne der vorstehenden Regelungen sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z.B. Telekommunikationsleistungen, Reinigungsleistungen, Prüfungsleistungen oder unter Umständen auch Wartungsleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers sowie zur Sicherstellung der Vertraulichkeit auch bei fremd vergebenen Nebenleistungen gesetzeskonforme und angemessene vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

Rechte und Pflichten des Auftraggebers

Einhaltung der DS-GVO

Der Auftraggeber ist im Rahmen der Umsetzung dieser Richtlinie für die Einhaltung der Vorgaben der DS-GVO und anderer datenschutzrechtlicher Vorschriften sowie insbesondere dafür verantwortlich, dass die Datenverarbeitung rechtmäßig ist und die gesetzlichen Rechte der betroffenen Personen hinsichtlich ihrer personenbezogenen Daten gewahrt wird.

Informationspflicht

Der Auftraggeber hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

Inspektionen

Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragsverarbeiter darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Verantwortlicher und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragsverarbeiter stehen, hat der Auftragsverarbeiter gegen diesen ein Einspruchsrecht.

Rechtevorbehalt

Der Auftraggeber behält im Verhältnis zum Auftragsverarbeiter sämtliche Rechte an den auf Grundlage dieses Vertrags verarbeiteten personenbezogenen und sonstigen Daten, an überlassenen Datenträgern und überlassenen sowie zur Erfüllung dieses Vertrags geschaffenen Unterlagen. Dem Auftraggeber steht ferner die alleinige Herrschaft über die Daten zu.

Haftung

Der Auftraggeber und der Auftragsverarbeiter haften gegenüber einer betroffenen Person entsprechend der in Art. 82 DS-GVO niedergeschriebenen Regelung. Der Auftragsverarbeiter haftet jedoch nur für Schäden, dessen Eintritt in ihrem Machtbereich waren und nicht für Schäden, die eindeutig dem Auftraggeber zugeordnet werden können. Für Schäden, die eindeutig dem Auftraggeber zugeordnet werden können, haftet der Auftraggeber im vollen Umfang.

Schlussbestimmung

Wirksamkeit

Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder nichtig sein oder infolge Änderung der Gesetzeslage oder durch höchstrichterliche Rechtsprechung oder auf andere Weise ganz oder teilweise unwirksam oder nichtig werden oder weist dieser Vertrag Lücken auf, so sind sich die Vertragsparteien darüber einig, dass die übrigen Bestimmungen dieses Vertrages davon unberührt und gültig bleiben. Für diesen Fall verpflichten sich die Vertragsparteien, unter Berücksichtigung des Grundsatzes von Treu und Glauben an Stelle der unwirksamen Bestimmung, möglichst nahe zu kommen und von der anzunehmen ist, dass die Vertragsparteien sie im Zeitpunkt des Vertragsschlusses vereinbart hätten, wenn sie die Unwirksamkeit oder Nichtigkeit gekannt oder vorhergesehen hätten. Entsprechendes gilt, falls dieser Vertrag eine Lücke enthalten sollte.

Ergänzende Bestimmungen

Sollte diese Richtlinie in einzelnen Punkten im Widerspruch zu den Allgemeinen Geschäftsbedingungen des *Auftragsverarbeiters* stehen, dann erhält die Richtlinie rechtlichen Vorrang vor diesen Dokumenten. Sollten Regelungen fehlen, die wiederum in den Allgemeinen Geschäftsbedingungen zu finden sind, dann gelten deren Regelungen ergänzend zu dieser Richtlinie.

Anwendbares Recht und Gerichtsstand

Es gilt ausschließlich deutsches Recht. Der Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist der Sitz des Auftraggebers.