Auftragsverarbeitung in Rechenzentren – worauf müssen Auftraggeber achten?

Sommerakademie
am 12. September 2022
in Kiel

Heiko Behrendt
0431 988-1212
ULD72@datenschutzzentrum.de
https://www.datenschutzzentrum.de/

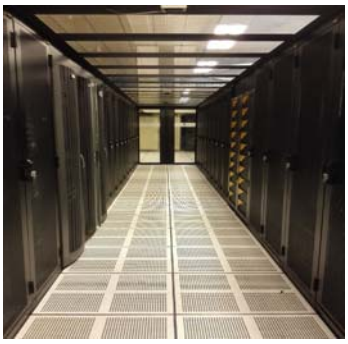
ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Themen

- Rechenzentrum – Infrastruktur
- Regelungen und Nachweise für den Betrieb eines Rechenzentrums
- Vertragsregelungen versus DSGVO
- Garantien des Auftragsverarbeiters
- Mindestanforderungen
- Vertragsinhalte
- Checkliste

Fragen können gerne stets zwischendurch gestellt werden!

Rechenzentrum – Infrastruktur



Quellen: https://pixabay.com/de/photos/serverraum-rechenzentrum-computers-1376349/
https://pixabay.com/de/photos/rechenzentrum-server-computer-286386/

Rechenzentren mit Zettabyte

Im Zeitalter der Digitalisierung steigt die Datenmenge ins Gigantische!

- Das **größte** Rechenzentrum der Welt, betrieben von China Telecom, befindet sich in Langfang (China) und hat eine Fläche von **100 Hektar** mit **hunderttausend Racks** und Platz für bis zu **1,2 Millionen Server**. Das größte Rechenzentrum in **Europa** befindet sich in **Portugal** und hat eine Fläche von **74.322 m²**. Es wird von Telecom betrieben. (Quelle: Wikipedia)
- In **Deutschland** soll es nach Berechnungen ca. **50.000 Rechenzentren** geben. Dazu gehören Rechenzentren von **IT-Dienstleistern (3000)**, Unternehmen die **eigene Rechenzentren** oder kleine IT-Installationen betreiben sowie Rechenzentren aus **Kommunen, Behörden oder Bildungseinrichtungen**. (Quelle: Bitcom Rechenzentren in Deutschland)
- **Mehrere Rechenzentren eines Dienstleisters** werden häufig zu sogenannten **„Cluster-Gruppen"** verbunden.
- Es wird prognostiziert, dass im **Jahr 2025** die globale Datenmenge schon bei **175 Zettabyte** liegen wird. **Ein Zettabyte umfasst rund eine Milliarde Terabyte**. 1 Zettabyte entspricht ca. 250.000.000.000 Milliarden HD-Filmen. (Quelle: https://www.ionos.de/digitalguide/websites/web-entwicklung/speichergroessen/)

Rechenzentren und Dienstleistungen

Welche Unterschiede sind maßgeblich?

Ein Rechenzentrum ist eine **zentrale Einrichtung** bestehend aus Gebäude und Räumen, in denen komplexe leistungsfähige technische Komponenten **für die Datenverarbeitung** untergebracht sind. Es dient der zentralen Datenverarbeitung.

- **Housing**
  Organisationen verwenden i.d.R. **ihre eigene Hard- und Software** und profitieren von der Infrastruktur des Rechenzentrums. Die Administration übernimmt die Organisation selbst.
- **Hosting**
  Organisationen nutzen **Infrastruktur und IT-Komponenten** (Hard- und Software) des Rechenzentrumsdienstleisters, die vom Dienstleister administriert werden.
- **Cloud-Dienste**
  Organisationen nutzen **dynamisch an den Bedarf angepasste** technische Ressourcen als Dienstleistung des Rechenzentrums. Die angebotenen Ressourcen werden meist in **typischen Architekturen**, wie z. B. Bereitstellung von Hard- und Software (Infrastructure as a Service), einer Entwicklungsumgebung (Platform as a Service) oder spezieller Software (Software as a Service) angeboten. Häufig sind die genutzten Komponenten **nicht exakt** abgrenzbar.

Anforderungen für den Rechenzentrumsbetrieb

Sind meine Daten im Rechenzentrum sicher? Worauf muss ich achten?

- Organisationsstrukturen – **Personal, fachliches Know-how, Standorte**
- Perimeterschutz
- Schutz der Gebäude- und Rauminfrastruktur
- Technische Komponenten für die Datenverarbeitung – Server, SAN, Switches, Firewalls
- **Zugangs- und Zugriffskontrolle** – Berechtigungsmanagement, Protokollierung, Revision
- Klimatisierung
- Strom und Notstrom
- Netzverkabelung, Netzanbindung, Datenkommunikation
- Überwachung, Monitoring
- **Mandantentrennung**
- Notfallmanagement
- Brandschutz
- **Datensicherung**
- …

Quellen: https://pixabay.com/de/photos/apfel-imac-ipad-arbeitsplatz-606761/
https://pixabay.com/de/illustrations/vpn-virtuelles-privates-netzwerk-4328341/
https://pixabay.com/de/photos/serverraum-rechenzentrum-computers-1376349/

Regelungen nach dem Stand der Technik

Als Indikator und Auswahlkriterium!

- **DIN EN 50600** – Vorgaben für die Planung, den Neubau und den Betrieb eines Rechenzentrums
  - Teil 1: Allgemeine Konzepte
  - Teil 2-1: Gebäudekonstruktion
  - Teil 2-2: Stromversorgung und Stromverteilung
  - Teil 2-3: Regelung der Umgebungsbedingungen
  - Teil 2-4: Infrastruktur der Telekommunikationsverkabelung
  - Teil 2-5: Sicherungssysteme
  - Teil 3-1: Informationen für das Management und den Betrieb
  - …

Welche Regelungen setzt das Rechenzentrum für den Schutz der Daten um?

Wie hoch ist das Schutzniveau?

Entspricht es den Anforderungen des Auftraggebers?

- **ISO 27001** – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (nativ oder IT-Grundschutz)
- **Trusted Site Infrastructure (TSI)** – Standard für Rechenzentren des TÜViT
- **IT-Grundschutz-Kompendium BSI** – OPS.2.1 Outsourcing und OPS.2.2 Cloud-Nutzung
- **C5:2020** – Kriterienkatalog Cloud Computing des BSI

- **DSGVO** – Datenschutz-Grundverordnung i.V.m. dem Standard-Datenschutzmodell
- Bereichsspezifische Datenschutzregelungen z. B. § 75c SGB V IT-Sicherheit in Krankenhäusern
- …

Nachweise für den Betrieb des Rechenzentrums

Wie hoch lege ich die Messlatte an Sicherheit?

- Darstellung der **Organisationsstrukturen** und der **Geschäftsprozesse**
- **Personelle Ressourcen** für Datenschutz- und Informationssicherheit
- **Leitlinien** zur Zielerreichung von Datenschutz und Informationssicherheit
- Beschreibung der **technischen Umgebung**, Server, virtualisierte Umgebung, Speichersysteme, Router, Switches, Firewalls, Administrations- und Monitoringsysteme
- **Schutzniveau mit Gefährdungs-** und **Risikoanalyse** des Rechenzentrums
- **Konzepte** für Notstrom, Brandschutz, Datensicherung, Löschung, Virenschutz etc.
- Darstellung der **Netzstrukturen** und der Netzanschlüsse
- **Technische und organisatorische Maßnahmen,** z. B. auf der Basis von IT-Grundschutz
- **Verfügbarkeitsanforderungen**, z. B. Tier-Klassifikationssystem des Uptime Institute
- Notfallplan, **Notfallkonzept,** z. B. Business Impact Analyse
- **Richtlinien** für die Administration der technischen Komponenten
- **Verzeichnis** über im Auftrag eines Verantwortlichen durchgeführte Tätigkeiten
- **Zertifizierung** anerkannter Standards, z. B. ISO 27001
- …

Vertragsregelungen // DSGVO

Quellen: https://pixabay.com/de/photos/gesch%c3%a4ft-unterschrift-vertrag-962354/
https://pixabay.com/de/illustrations/dsgvo-datenschutz-sicherheit-4263955/

Mängel bei Auftragsverarbeitungen

Wie sieht die Praxis häufig aus (allgemein)?

- Die **Überprüfung** der **Garantien** bzw. die **Eignungsfeststellung** des Auftragsverarbeiters wird häufig nicht durchgeführt.
- Inwieweit der Auftragsverarbeiter vereinbarte **Vertragsregelungen** datenschutzkonform umsetzt, ist nicht **bekannt** und wird auch nicht regelmäßig **kontrolliert**.
- Auftragsverarbeiter werden **ohne** Vertragsgrundlage beauftragt, persb. Daten zu verarbeiten.
- Verträge werden **dezentral** von den Abteilungen abgeschlossen und verwaltet. Es fehlt dem Verantwortlichen der **Überblick**, welche Auftragsverarbeitungen bestehen.
- Die Verträge sind bezüglich der **Anforderungen** des Verantwortlichen nicht standardisiert. Die Aufnahme von **Vertragsinhalten** nach Art. 28 DSGVO ist unvollständig.
- **Technische und organisatorische Maßnahmen** (TOM) sind im Vertrag zu allgemein formuliert. Ein Bezug auf **Gefährdungen** und **Risiken** fehlt.
- Die **Prüffähigkeit** der im Vertrag festgelegten TOMs ist nur sehr eingeschränkt möglich, weil eine **Dokumentation der infrastrukturellen und technischen Gegebenheiten** des Auftragsverarbeiters fehlt bzw. nicht vollständig vorgelegt werden kann.

Auswahl eines Auftragsverarbeiters

Welche Regelungen sind zu beachten?

- Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend **Garantien** dafür bieten, dass **geeignete technische und organisatorische Maßnahmen** so durchgeführt werden, dass die Verarbeitung **im Einklang mit den Anforderungen dieser Verordnung** erfolgt und den **Schutz der Rechte der betroffenen Person gewährleistet (Art. 28 Abs. 1 DSGVO)**.
- Der Auftragsverarbeiter nimmt **keinen weiteren Auftragsverarbeiter** ohne vorherige gesonderte **oder allgemeine schriftliche Genehmigung** des Verantwortlichen in Anspruch **(Art. 28 Abs. 2 DSGVO)**.
- Die **Vertragsregelungen** mit dem Auftragsverarbeiter zur Einhaltung des Datenschutzes orientieren sich an den **Vorgaben des Art. 28 Abs. 3 DSGVO**. Hierzu gehören u. a.
  - den **Gegenstand** und die Dauer der Verarbeitung,
  - Art und Zweck der Verarbeitung,
  - die Art der personenbezogenen Daten,
  - die Kategorien betroffener Personen und
  - die **Pflichten und Rechte** des Verantwortlichen

  festzulegen. Ferner sind alle gemäß Art. 32 DSGVO **erforderlichen Maßnahmen** zu bestimmen.

Garantien (Eignung) des Auftragsverarbeiters

Erwägungsgrund 81 zu Art. 28 DSGVO

- Dem **Auftraggeber bzw. dem Verantwortlichen** wird **vor Auftragsvergabe** zunächst eine **Prüfung** der **Eignung** des Auftragsverarbeiters auferlegt.
- Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter im Namen des Verantwortlichen vorzunehmende **Verarbeitung eingehalten** werden, sollte ein Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, **nur Auftragsverarbeiter heranziehen**, die insbesondere im Hinblick auf
  - **Fachwissen,** z. B. Know-how, Kenntnisse im Bereich der beauftragten Dienstleistung
  - **Zuverlässigkeit,** z. B. Größe und Maßstäbe des Unternehmens
  - **Ressourcen,** z. B. Vertretung, Beständigkeit, Redundanz

  hinreichende **Garantien** dafür bieten, dass **technische und organisatorische Maßnahmen** auch für die Sicherheit der Verarbeitung getroffen werden, die den Anforderungen dieser Verordnung genügen **(Erwägungsgrund 81)**.
- In der DSGVO ist nicht geregelt, **wie** die Prüfung der **Garantien** bzw. der **Eignung** des Auftragsverarbeiters durchgeführt werden soll. Gleichwohl sollte der Verantwortliche das festgelegte **Prüfverfahren nachweisen** können.

Mindestanforderungen für die Auswahl eines AV

Vom Verantwortlichen vorab festzulegen!

Unabhängig von der Kritikalität der geplanten Dienstleistung (vgl. „ein dem Risiko angemessenes Schutzniveau", Art. 32 DSGVO) anzuwenden!

Beispiele für Mindestanforderungen:

- Ein **Datenschutzmanagement muss** implementiert sein!
- Die Bestellung eines **Datenschutzbeauftragten muss** intern oder extern (mit Vertretung) umgesetzt sein!
- Eine (regelmäßige) **Überprüfung und Kontrolle** durch den Verantwortlichen (Auftraggeber) **muss** gewährleistet sein!
- Die **Sensibilisierung der Beschäftigten** (Schulungskonzept, Vertraulichkeitsverpflichtung) **muss** umgesetzt sein!
- Eine ausreichende **Dokumentation** der Geschäftsprozesse, Infrastruktur, IT-Einsatz, Netz und TOMs **muss** vorgelegt werden!
- Ein **Verfahren** über die regelmäßige **Überprüfung und Bewertung** der Wirksamkeit der TOMs **muss** beim Auftragsverarbeiter implementiert sein!
- Ein **Datenschutzvorfall- und Notfallmanagement muss** vorhanden sein!
- ...

Ergänzende Anforderungen für die Auswahl eines AV

Vom Verantwortlichen vorab festzulegen!

In Abhängigkeit von hoher Kritikalität der geplanten Dienstleistung anzuwenden!

Beispiele für ergänzende Anforderungen (zu prüfen):

- Eine **hohe Verfügbarkeit** der Datenverarbeitung **muss** nachgewiesen werden!
- Die Umsetzung eines anerkannten **Sicherheitsstandards** (ISO 27001, IT-Grundschutz) **muss** erfüllt sein!
- Eine **aktuelle Zertifizierung für Rechenzentren** und eine **DSGVO-Zertifizierung** (wird bald möglich sein) **müssen** nachgewiesen werden!
- Die Datenverarbeitung **muss** an **Standorten** in Deutschland durchgeführt werden!
- Die **Verschlüsselung** der Daten **muss** umgesetzt werden!
- Die **Fernwartung muss** durch namentlich bekanntes Personal des Rechenzentrums-betreibers umgesetzt werden!
- Eine **Mandantentrennung** der Datenverarbeitung **muss** nachgewiesen werden!
- Der Auftragsverarbeiter **muss** die geplante Dienstleistung **ohne** die Beauftragung von **Unter-auftragsverarbeitern** leisten!
- ...

Auftragsverarbeitung auf Basis eines Vertrags

Grundlage für die Einhaltung der DSGVO

- **Vertragsgegenstand**
- **Umfang der Dienstleistung**
- Weisungsbefugnisse des Auftraggebers
- Anforderungen an Personal und IT-Komponenten
- Sicherheit der Datenverarbeitung
- Inanspruchnahme von weiteren Auftragsverarbeitern
- Rechte der betroffenen Personen
- Mitteilungs- und Unterstützungspflichten
- Datenlöschung und Datenrückgabe
- Nachweise und Überprüfungen
- ggf. Kosten für Kontrollen/Audits
- Vertragsdauer und Kündigung
- Haftung
- **Anlage Technische Dokumentation**
- **Anlage TOMs**

Orientierung an Art. 28 Abs. 3 DSGVO!

Die Vertragsregelungen dienen als **Maßstab** für die **Kontrolle** des Auftragsverarbeiters

Erfüllt der Auftragsverarbeiter die im Vertrag festgelegten Regelungen?

Führe ich eine Dokumenten- und/oder eine Vor-Ort-Kontrolle durch?

SOLL IST

Quellen: https://pixabay.com/de/photos/gesch%c3%a4ft-unterschrift-vertrag-962354/
https://pixabay.com/de/photos/serverraum-rechenzentrum-computers-1376349/

Checkliste Auftragsverarbeitung Rechenzentrum

Worauf müssen Auftraggeber insbesondere achten?

- Nach welchen **Kriterien** wird die Eignung des Auftragsverarbeiters/Rechenzentrum festgestellt?
- Verfügt das Rechenzentrum über **ausreichendes Personal** mit gutem Fachwissen?
- Setzt das Rechenzentrum anerkannte **Standards**, z. B. DIN 50600 oder ISO 27001, um?
- Werden vom Rechenzentrum regelmäßig **Audits** zur Überprüfung der TOMs durchgeführt?
- Entspricht der AV-Vertrag den **Anforderungen** des Art. 28 DSGVO?
- Sind die **Datenkommunikationsprozesse** im Rechenzentrum transparent?
- Besteht eine aktuelle **Dokumentation** über die Infrastruktur, die eingesetzte Hard- und Software, die Netzstrukturen und die genutzten Anwendungen?
- Ist das **Schutzniveau** für die Datenverarbeitung im Rechenzentrum festgelegt?
- Werden die im **Vertrag** aufgeführten **technischen und organisatorischen Maßnahmen** vollständig umgesetzt und überprüft?
- Hält das Rechenzentrum sich an die erteilten **Weisungen** des Auftraggebers?
- Hat das Rechenzentrum seine Beschäftigten zur **Vertraulichkeit** verpflichtet?
- Verfügt das Rechenzentrum über ein qualifiziertes **Datenschutzmanagement**?
- Liegt ein **Verzeichnis** über die im Auftrag durchgeführten Verarbeitungstätigkeiten vor?
- Verfügt das Rechenzentrum über ein **Datenschutzvorfall-Management**?
- Wird ein **Unterauftragsverarbeiter** nur mit Genehmigung des Auftraggebers eingesetzt?
- Kann das Rechenzentrum den Auftraggeber bei der Erfüllung seiner **Pflichten**, z. B. bei der Umsetzung einer Datenschutz-Folgenabschätzung, **unterstützen**?
- ...

Vielen Dank für Ihre Aufmerksamkeit!

Heiko Behrendt
ISO 27001 Auditor
0431 9881212
uld72@datenschutzzentrum.de
https://www.datenschutzzentrum.de/

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein