Technische und Organisatorische Maßnahmen (TOM), des Verlags C.H.BECK im Allgemeinen nach Art. 32 DSGVO, Version 2025-05

Inhaltsverzeichnis

1. Einleitung und Rahmenbedingungen

Die folgenden Festlegungen repräsentieren das Datenschutzkonzept des Verlags C.H.BECK im Allgemeinen (nachfolgend: C.H.BECK).

C.H.BECK legt damit die Standards fest, nach denen die Standorte alle Formen von papiergebundenen und elektronischen Informationen während der Verarbeitung, vom Dateneingang bis zur Vernichtung der Daten, behandeln, schützen und nach der Erbringung der Dienstleistung gemäß der jeweils vereinbarten Anforderung des Kunden vernichten.

Es werden in einzelnen Teilbereichen die entsprechenden Maßnahmen beschrieben, die C.H.BECK durchführt, um einen unzulässigen Umgang mit personenbezogenen Daten und Dokumenten sowie eine unzulässige Verwendung von personenbezogenen Daten gemäß den jeweils gültigen Datenschutzgesetzen zu verhindern und eine entsprechende IT-Sicherheit zu gewährleisten.

1.1. Anwendungsbereich

Die folgenden Festlegungen werden für die gesamte Verarbeitung personenbezogener Daten und somit für alle von C.H.BECK übernommenen Aufträge und Aufgaben eingehalten.
Da aufgrund verschiedenster Auftragsspezifikationen davon auszugehen ist, dass verschiedene Aufträge mit höheren oder niedrigeren Datenschutzstandards verarbeitet werden müssen, ist der Anwendungsbereich der in diesem Dokument definierten Standards durch entsprechende Einzelvereinbarungen mit den Auftraggebern einzuschränken oder zu erweitern. Dies kann insbesondere dann der Fall sein, wenn Subunternehmer an der Leistungserbringung beteiligt sind.

Über diese allgemeinen TOMs hinausgehende Maßnahmen werden in den jeweiligen Verfahrensverzeichnissen geregelt. Weiterhin können die Sicherheitsanforderungen auf Wunsch eines Auftraggebers, erhöht werden, soweit dies in einem Dokument zur entsprechenden Auftragsdokumentation schriftlich vereinbart wird.

1.2. Verantwortlichkeiten Gesamtverantwortung

Gesamtverantwortlich für den IT-Bereich von C.H.BECK, Bereich München, ist die IT-Abteilungsleitung, sowie die der Abteilung übergeordnete kaufmännische Geschäftsführung.

2. Technische und organisatorische Maßnahmen

2.1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

2.1.1. Zutrittskontrolle

Das Ziel einer Zutrittskontrolle ist es, Unbefugten den Zutritt (z.B. zu Datenverarbeitungsanlagen) zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Der Begriff des Zutritts ist dabei räumlich zu verstehen.

Den Zutritt zu unserem Firmengebäude stellen wir durch folgende Maßnahmen sicher:

- Zutritt ist für Gäste nur über zwei Zugänge, die mit Logen besetzt sind, möglich. Dabei ist der Zutritt nur nach Läuten der Glocke und Kontrolle durch die Logen-Mitarbeiter*innen möglich. Fremde Personen müssen sich anmelden und werden in der Loge abgeholt. Sichtbar zu tragende Gäste-Karte werden für die Dauer der Anwesenheit ausgestellt.
- Türsicherungen (elektrische Türöffner) mit Zutrittskarten bzw. Token von außen und im Gebäude
- Außerhalb Öffnungszeiten ist der Zutritt nur mit Zutrittskarten bzw. Token für Mitarbeiter und zugelassene externe Mitarbeiter möglich.
- Protokollierte Vergabe von Zutrittsberechtigungen zum Gebäude inkl. Schlüsselverwaltung und Dokumentation der Schlüsselvergabe
- Entzug der Zutrittsberechtigung nach Ausscheiden
- Perimeter Schutz Standort München
    - Zaunanlagen
    - Gitter vor Fenstern/Türen bei Erreichbarkeit ohne Hilfsmittel
    - Werkschutz und Pförtnerdienst
- Spezielle Schutzvorkehrungen des Serverraums inkl. eigener Zutrittskontrolle

2.1.2. Zugangskontrolle

Das Ziel einer Zugangskontrolle ist es, mit Hilfe geeigneter Maßnahmen zu verhindern, dass Unbefugte in Datenverarbeitungsanlagen und -systeme, mit denen personenbezogene Daten verarbeitet oder genutzt werden, eindringen oder diese nutzen können.
Um den Zugang zu unserem Netzwerk zu schützen, haben wir folgende Maßnahmen getroffen:

- Benutzerverwaltung zur Anmeldung
- Kontrollmechanismen zur User-Verwaltung
- Individueller Benutzername und Passwort
- Passwortregelung (Anzahl Zeichen, Sonderzeichen, Historie, keine Zeichenfolgen)
- Multi-Faktor-Authentifizierung
- Mobile Device Management
- Einsatz sicherer Übertragungstechnik (VPN-Einwahl, Publik-Key-Infrastruktur)
- Segmentierung von Netzwerken nach Schutzbedürftigkeit

- Einsatz von Virenscanner und Firewall
- Zusätzlicher System-Log-In für bestimmte Anwendungen
- Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)

2.1.3. Zugriffskontrolle

Das Ziel einer Zugriffskontrolle ist es, zu gewährleisten, dass ausschließlich die zur Benutzung der Datenverarbeitungssysteme Berechtigen auf die ihrer Zugriffsberechtigung unterliegenden personenbezogene Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung,
Nutzung und nach der Speicherung nicht unbefugt gelesen, vervielfältigt, verändert oder entfernt werden können. Um unerlaubte Tätigkeiten innerhalb der Systeme von C.H.BECK außerhalb der eingeräumten Berechtigungen zu verhindern, haben wir folgende Maßnahmen getroffen:

- Rechtevergabe nach Rollen/Organisationseinheiten
- Verwaltung von Berechtigungen
- Differenzierte Berechtigungen
- Profile
- Genehmigungsroutine
- Verschlüsselung von USB-Datenträgern, externen Festplatten und Laptops sowie der Daten selbst auf sonstigen Wechseldatenträgern (z.B. CD, DVD)
- Verwaltung der Zugriffsrechte durch Administrator
- Datenschutzkonforme Entsorgung von Datenträgern und Papier
- Vier-Augen-Prinzip
- Aufgabenbezogene Berechtigungsprofile
- Passwort-Identifikation

2.1.4. Trennungskontrolle

Das Ziel des Trennungsgebots ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten ebenfalls getrennt voneinander verarbeitet werden.
Um sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden, haben wir die folgenden Maßnahmen getroffen:

- Funktionstrennung durch mandantenfähige Systeme
- Berechtigungsvergabe nach Rollen
- Getrennte Datenbanken
- Trennung von Entwicklungs-, Test- und Produktivsystemen
- Getrennte elektronische Laufwerk pro Organisationeinheit

2.1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- Pseudonymisierung mittels einer eindeutigen Identifikationsnummer (ID).

2.2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.2.1. Weitergabekontrolle

Das Ziel einer Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, vervielfältigt, verändert oder entfernt werden können, und dass überprüft sowie festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zu Datenübertragung vorgesehen ist.
Folgende Maßnahmen haben wir in Bezug auf die Weitergabe von personenbezogenen Daten getroffen:

- Sichere Aufstellung von Servern und SAN (Sicherheitsbereich)/ NAS
- Unternehmenseigene Domain zur E-Mail-Kommunikation (intern)
- Einsatz einer Cloud-E-Mail Security Applikation
- Einsatz von sicheren Cloud Lösungen
- Weitergabe an Dritte nur nach Prüfung der Rechtsgrundlage
- Schriftliche Festlegung der Weitergabe in Drittländer
- Sichere Übertragung von Datenlieferungen (SFTP, VPN)
- Gesichertes WLAN
- Trennung Gäste WLAN und internes WLAN
- SSL-Verschlüsselung bei Web-access
- Beschränkung des zur Übermittlung befugten Personenkreises
- Nutzung von KI-Systemen für betriebliche Zwecke ist nur nach intern festgelegten Richtlinien und unter Beachtung eines Risikobewertungs- und Freigabeprozesses erlaubt; die Eingabe von Daten in KI-Systeme unterliegt unternehmensinternen Verwendungsvorgaben

2.2.2. Eingabekontrolle

Das Ziel einer Eingabekontrolle ist es, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten in die Systeme und Anlagen zur Datenverarbeitung eingegeben, verändert oder entfernt worden sind.
Die Nachvollziehbarkeit innerhalb der Datenverwaltungen stellen wir wie folgt sicher:

- Protokollierung der Eingabe personenbezogener Daten
- Systemseitige Protokollierungen
- Funktionelle Verantwortlichkeiten

2.3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DS-GVO)

2.3.1. Verfügbarkeitskontrolle

Das Ziel der Verfügbarkeitskontrolle ist es, zu gewährleisten, dass personenbezogene Daten gegen die Zerstörung oder Verlust physisch sowie auch logisch geschützt sind.

- Back-Up Verfahren

- Unterbrechungsfreie Stromversorgung (USV)
- Aufbewahrungsmodalitäten von Back-Ups (Safe, getrennter Brandabschnitt, etc.)
- Virenschutz /Firewall
- Brand- und Löschwasserschutz
- Geeignete Archivierungsräumlichkeiten
-

2.3.2. rasche Wiederherstellung

- IT-Notfallmanagement
- Inkl. zugehöriger Wiederherstellungs- und -anlaufpläne

2.4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

2.4.1. Allgemein

Allgemeine Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management
- Externe IT-Risikoevaluierung
- Konzept für eine Datenschutzpanne

2.4.2. Auftragskontrolle

Das Ziel einer Auftragskontrolle im Sinne von Art. 28 DS-GVO ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend des Auftrags und den Weisungen des Auftragsgebers verarbeitet werden können.

- Vertragliche Regelungen gemäß Art. 28 DS-GVO (Auftragsdatenverarbeitung)
- Unteraufträge nur bei gleichwertigem Schutzniveau
- Prüfung und Dokumentation beim Auftragnehmer getroffener Maßnahmen
- Verpflichtung der Mitarbeiter von Auftragnehmern auf das Datengeheimnis

3. Begleitende Dokumente zu den technisch-organisatorischen Maßnahmen

Die Verarbeitung der personenbezogenen Daten erfolgt unter anderem auf Servern in von C.H.BECK beauftragten Rechenzentren. C.H.BECK hat alle erforderlichen datenschutzrechtlichen Verträge mit den Rechenzentrumsbetreibern abgeschlossen.

4. Weitere Maßnahmen

Sämtliche Beschäftigten von C.H.BECK, die personenbezogenen Daten verarbeiten, sind in Schriftform zur Wahrung der Vertraulichkeit verpflichtet. Die Beschäftigten werden im Umgang mit personenbezogenen Daten geschult.

5. Schlussbestimmung

Der Datenschutz unterliegt bei C.H.BECK einem kontinuierlichen Verbesserungsprozess und wird an die jeweiligen aktuellen und gültigen Datenschutzbestimmungen angepasst. Eine Aktualisierung des Dokuments findet fortlaufend statt.

Änderungshistorie

Version	Datum	Bearbeiter	Änderung
1.0	29. Mai.2018	Scheit, Rauch, Tetter, Siewert, Stach	Einstellung von §11 DBSG nach Art. 32 DS-GVO
1.1	30.Jänner 2019	Helfrich	Redaktionelle Bearbeitung
2.0	1. Dezember 2022	Scheit, Tetter, Stach, Bischoff	Aktualisierung und Ergänzungen 2022
2025-05	30. Mai 2025	Scheit, Stach, Fallenstein, Schulte, Knott	Aktualisierung und Erweiterung zu KI-Aspekten