x-cellent technologies GmbH

Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO

Version	*V.1.0*
Autor	*Susanne Rothermel*
Besitzer des Dokuments	*Susanne Rothermel*
Genehmigt von	
Datum der Genehmigung	
Überprüfung	*Jährlich*
Datum der nächsten Überprüfung	
Status des Dokuments	*Final*
Vertraulichkeitsstufe	*Öffentlich*
Dokument Kontakt	susanne.rothermel@x-cellent.com
Anwendbarkeit	Anlage zu AV-Verträgen, Information an Kunden

Versionshistorie:

Datum	Version	Erstellt von	Beschreibung der Änderung
18.05.2026	V1	Susanne Rothermel	Initiale Erstellung des Dokumentes

Genehmigungsstufe	Rolle	Datum/Version	Name
Freigabe	DSB	29.5.2026, V1.0	Ext. DSB, Fa. Dataguard

Inhalt

1. Gegenstand und Zweck der TOM

Die nachfolgenden technisch-organisatorischen Maßnahmen (TOM) beschreiben, wie x-cellent technologies personenbezogene Daten als Auftragsverarbeiter gemäß Art. 28 DSGVO schützt.

Die Umsetzung dieser Maßnahmen erfolgt im Rahmen eines nach ISO/IEC 27001 zertifizierten Informationssicherheitsmanagementsystems. Die Maßnahmen werden regelmäßig überprüft und bei Bedarf weiterentwickelt.

Das vorliegende Dokument dient der transparenten Darstellung der umgesetzten Maßnahmen und stellt eine abstrahierte Beschreibung ohne technische Detailtiefe dar. Es ist als Anlage zu Auftragsverarbeitungsverträgen vorgesehen.

Detaillierte Informationen zu einzelnen Sicherheitsmaßnahmen können bei Bedarf im Rahmen von Sicherheitsprüfungen bereitgestellt werden. Kontakt: datenschutz@x-cellent.com

2. Anwendungsbereich

Diese technisch-organisatorischen Maßnahmen gelten für sämtliche Verarbeitungen personenbezogener Daten, die x-cellent technologies im Auftrag des Verantwortlichen durchführt.

Der Anwendungsbereich umfasst insbesondere:

- Mitarbeitende und sonstige Personen, die mit der Verarbeitung personenbezogener Daten betraut sind
- die eingesetzten IT-Systeme und Anwendungen
- organisatorische und technische Prozesse der Datenverarbeitung
- eingesetzte Unterauftragsverarbeiter

Die TOM gelten unabhängig davon, ob die Verarbeitung in eigenen oder fremden Rechenzentren sowie vor Ort oder im Rahmen von Remote-Zugriffen erfolgt.

3. Grundsätze der Datensicherheit

Die Umsetzung der technisch-organisatorischen Maßnahmen erfolgt nach einem risikobasierten Ansatz unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung.

Die Maßnahmen orientieren sich an folgenden Grundsätzen:

- **Vertraulichkeit:** Schutz personenbezogener Daten vor unbefugtem Zugriff
- **Integrität:** Schutz vor unbefugter oder unbeabsichtigter Veränderung
- **Verfügbarkeit:** Sicherstellung der Zugänglichkeit und Wiederherstellbarkeit personenbezogener Daten

Die Angemessenheit der Maßnahmen wird regelmäßig überprüft und bei Bedarf angepasst.

4. Technisch-organisatorische Maßnahmen im Einzelnen

4.1. Zutrittskontrolle (physischer Zugang)

Der Zugang zu Räumlichkeiten und Einrichtungen, in denen personenbezogene Daten verarbeitet werden, ist auf berechtigte Personen beschränkt.

Unbefugten wird der Zutritt durch organisatorische und technische Maßnahmen verwehrt. Besucher erhalten nur in Begleitung Zugang zu sensiblen Bereichen.

4.2. Zugangskontrolle (IT-Systeme)

Der Zugang zu IT-Systemen, auf denen personenbezogene Daten verarbeitet werden, ist durch geeignete Authentifizierungsverfahren geschützt.

Die Nutzung erfolgt ausschließlich über personalisierte Benutzerkonten. Unbefugte Systemnutzung wird durch geeignete organisatorische und technische Maßnahmen verhindert.

4.3. Zugriffskontrolle

Der Zugriff auf personenbezogene Daten ist auf diejenigen Personen beschränkt, die diesen zur Erfüllung ihrer Aufgaben benötigen (need to know).

Die Vergabe und der Entzug von Zugriffsrechten erfolgen nach definierten Berechtigungs- und Rollenmodellen und werden regelmäßig überprüft.

4.4. Weitergabekontrolle

Personenbezogene Daten werden bei der Übertragung gegen unbefugte Kenntnisnahme geschützt.

Die Weitergabe von personenbezogenen Daten an Dritte erfolgt ausschließlich im Rahmen der vertraglich vereinbarten Zwecke und unter Einsatz geeigneter Sicherheitsmaßnahmen.

4.5. Eingabekontrolle und Nachvollziehbarkeit

Durch geeignete organisatorische und technische Maßnahmen wird sichergestellt, dass die Eingabe, Veränderung und Löschung personenbezogener Daten in angemessenem Umfang nachvollziehbar sind.

Änderungen an Daten und Systemen werden durch geeignete organisatorische und technische Maßnahmen gesteuert und in angemessenem Umfang dokumentiert sowie vor unbefugter Manipulation geschützt.

4.6. Verfügbarkeitskontrolle und Wiederherstellbarkeit

Zur Sicherstellung der Verfügbarkeit personenbezogener Daten werden geeignete Maßnahmen zur Datensicherung und Wiederherstellung eingesetzt.

Diese Maßnahmen dienen dazu, personenbezogene Daten vor Verlust zu schützen und eine zeitnahe Wiederherstellung nach Störungen oder technischen Zwischenfällen zu ermöglichen.

4.7. Trennungsgebot/Mandantentrennung

Personenbezogene Daten, die zu unterschiedlichen Zwecken verarbeitet werden, sind logisch oder organisatorisch voneinander getrennt.

Eine unzulässige Vermischung von Daten aus unterschiedlichen Verarbeitungskontexten wird durch geeignete Maßnahmen verhindert.

5. Einsatz von Unterauftragsverarbeitern

Soweit Unterauftragsverarbeiter eingesetzt werden, erfolgt dies ausschließlich unter Beachtung der Vorgaben aus Art. 28 DSGVO.

Unterauftragsverarbeiter werden sorgfältig ausgewählt, vertraglich verpflichtet und hinsichtlich der von ihnen eingesetzten technisch-organisatorischen Maßnahmen überprüft.

6. Umgang mit Datenschutzverletzungen

x-cellent technologies hat Verfahren implementiert, um Datenschutzverletzungen zu erkennen, zu bewerten und zu behandeln. Im Falle einer Verletzung des Schutzes personenbezogener Daten wird der Verantwortliche unverzüglich informiert, sodass dieser seinen gesetzlichen Melde- und Informationspflichten nachkommen kann.

7. Überprüfung und Weiterentwicklung der TOM

Die technisch-organisatorischen Maßnahmen entsprechen dem Stand der Technik zum Zeitpunkt der Erstellung. Sie werden regelmäßig sowie anlassbezogen überprüft und bei Bedarf angepasst.

Dies umfasst insbesondere die Berücksichtigung technischer Weiterentwicklungen, organisatorischer Änderungen sowie neuer oder geänderter Risiken für personenbezogene Daten.

Mitarbeitende werden regelmäßig im Hinblick auf Datenschutz und Informationssicherheit sensibilisiert.

8. Ergänzende Anlage: TOM-Checkliste (Übersicht)

Die nachfolgende TOM-Checkliste dient der übersichtlichen Darstellung der umgesetzten technisch-organisatorischen Maßnahmen gemäß Art. 32 DSGVO.

Die Checkliste ergänzt die vorstehenden Beschreibungen und stellt eine strukturierte Zusammenfassung ohne technische Detailtiefe dar.

Kategorie	**Maßnahme**	**Umgesetzt**	**Erläuterung**
Zutrittskontrolle (physischer Zugang)	Zutritt zu Betriebs- und Serverräumen ist beschränkt	R	Der physische Zugang zu Räumlichkeiten, in denen personenbezogene Daten verarbeitet oder IT-Systeme betrieben werden, ist auf berechtigte Personen beschränkt. Der Zutritt erfolgt nach definierten organisatorischen Regelungen.
Zutrittskontrolle (physischer Zugang)	Besucherregelungen sind definiert	R	Besucher erhalten ausschließlich kontrollierten Zugang und werden in sensiblen Bereichen begleitet. Unbefugter Zutritt zu Bereichen mit personenbezogenen Daten wird dadurch verhindert.
Zutrittskontrolle (physischer Zugang)	Schutz von Server- und Infrastrukturbereichen	R	Server- und Infrastrukturbereiche sind organisatorisch und räumlich gesichert, sodass ein Zutritt nur durch autorisierte Personen möglich ist.

Kategorie	Maßnahme	Umgesetzt	Erläuterung
Zugangskontrolle (IT-Systeme)	Zugriff auf IT-Systeme nur für berechtigte Nutzer	R	Der Zugriff auf IT-Systeme erfolgt ausschließlich durch berechtigte Nutzer mit personalisierten Benutzerkennungen. Sammel- oder Gemeinschaftskonten werden nicht eingesetzt.
Zugangskontrolle (IT-Systeme)	Geeignete Authentifizierungsverfahren	R	Für den Systemzugang werden geeignete Authentifizierungsverfahren eingesetzt, die dem Stand der Technik entsprechen und einen unbefugten Zugriff verhindern.
Zugangskontrolle (IT-Systeme)	Schutz vor unbefugter Fernzugriffsnutzung	R	Fernzugriffe auf IT-Systeme sind organisatorisch geregelt und technisch abgesichert, sodass ausschließlich autorisierte Zugriffe möglich sind.
Zugriffskontrolle	Rollen- und Berechtigungskonzept	R	Zugriffsrechte auf personenbezogene Daten werden rollen- und aufgabenbezogen vergeben und orientieren sich an den jeweiligen Zuständigkeiten.
Zugriffskontrolle	Prinzip der minimalen Berechtigung	R	Zugriffe werden nach dem Prinzip der minimalen Berechtigung vergeben, sodass Nutzer nur auf diejenigen Daten zugreifen können, die sie zur Erfüllung ihrer Aufgaben benötigen.
Zugriffskontrolle	Entzug von Berechtigungen	R	Bei Änderungen von Aufgaben, Rollen oder beim Ausscheiden von Mitarbeitenden werden Zugriffsrechte zeitnah angepasst oder entzogen.

Kategorie	Maßnahme	Umgesetzt	Erläuterung
Weitergabe	Schutz personenbezogener Daten bei Übertragung	R	Personenbezogene Daten werden bei der Übertragung durch geeignete Maßnahmen vor unbefugter Kenntnisnahme oder Veränderung geschützt.
Weitergabe	Kontrollierte Datenweitergabe	R	Eine Weitergabe personenbezogener Daten erfolgt ausschließlich im Rahmen der vertraglich vereinbarten Zwecke und an berechtigte Empfänger.
Weitergabe	Absicherung externer Übertragungswege	R	Externe Übertragungswege werden durch geeignete organisatorische und technische Maßnahmen abgesichert, um eine unbefugte Kenntnisnahme, Veränderung oder Verlust personenbezogener Daten zu verhindern. Dies umfasst insbesondere Maßnahmen zur Zugriffskontrolle und zur sicheren Übertragung von Daten.
Eingabekontrolle und Nachvollziehbarkeit	Nachvollziehbarkeit von Eingaben und Änderungen	R	Die Eingabe, Veränderung und Löschung personenbezogener Daten ist durch geeignete organisatorische und technische Maßnahmen in angemessenem Umfang nachvollziehbar.
Eingabekontrolle und Nachvollziehbarkeit	Schutz vor unbefugter Manipulation	R	Durch organisatorische und technische Maßnahmen wird verhindert, dass personenbezogene Daten unbefugt verändert oder gelöscht werden.
Eingabekontrolle und Nachvollziehbarkeit	Protokollierung sicherheitsrelevanter Vorgänge	R	Sicherheits- und datenschutzrelevante Vorgänge werden in angemessenem Umfang protokolliert, um eine Nachvollziehbarkeit und Aufklärung von Vorfällen zu ermöglichen.

Kategorie	Maßnahme	Umgesetzt	Erläuterung
Verfügbarkeitskontrolle und Wiederherstellbarkeit	Regelmäßige Datensicherungen	R	Für personenbezogene Daten bestehen geeignete Verfahren zur regelmäßigen Datensicherung, um Datenverluste zu vermeiden.
Verfügbarkeitskontrolle und Wiederherstellbarkeit	Wiederherstellung bei Störungen	R	Es sind Prozesse definiert, die eine zeitnahe Wiederherstellung personenbezogener Daten nach Störungen oder technischen Zwischenfällen ermöglichen.
Verfügbarkeitskontrolle und Wiederherstellbarkeit	Schutz vor Datenverlust	R	Durch organisatorische und technische Maßnahmen wird das Risiko eines Verlusts personenbezogener Daten angemessen reduziert.
Trennungsgebot/ Mandantentrennung	Trennung nach Verarbeitungszwecken	R	Personenbezogene Daten werden entsprechend ihrem jeweiligen Verarbeitungszweck getrennt verarbeitet.
Trennungsgebot/ Mandantentrennung	Mandantentrennung	R	Durch organisatorische und technische Maßnahmen wird sichergestellt, dass Daten unterschiedlicher Auftraggeber voneinander getrennt sind.
Trennungsgebot/ Mandantentrennung	Schutz vor unzulässiger Datenvermischung	R	Maßnahmen verhindern eine unzulässige Vermischung von Daten aus unterschiedlichen Verarbeitungskontexten.
Unterauftragnehmer	Sorgfältige Auswahl von Unterauftragsverarbeitern	R	Unterauftragsverarbeiter werden vor ihrem Einsatz sorgfältig ausgewählt und im Hinblick auf Datenschutz und Datensicherheit bewertet.

Kategorie	Maßnahme	Umgesetzt	Erläuterung
Unterauftragnehmer	Vertragliche Verpflichtung	R	Unterauftragsverarbeiter werden vertraglich gemäß Art. 28 DSGVO zur Einhaltung geeigneter technisch-organisatorischer Maßnahmen verpflichtet.
Unterauftragnehmer	Prüfung der TOM von Subprozessoren	R	Die Angemessenheit der von Unterauftragsverarbeitern eingesetzten TOM wird risikobasiert überprüft.
Datenschutzverletzungen	Verfahren zur Erkennung von Datenschutzverletzungen	R	Es bestehen definierte Verfahren zur Erkennung, Bewertung und Behandlung von Datenschutzverletzungen.
Datenschutzverletzungen	Information des Verantwortlichen	R	Der Verantwortliche wird im Falle einer Datenschutzverletzung unverzüglich informiert, sodass gesetzliche Meldepflichten eingehalten werden können.
Überprüfung und Weiterentwicklung	Regelmäßige Überprüfung der TOM	R	Die technisch-organisatorischen Maßnahmen werden regelmäßig überprüft, um ihre Wirksamkeit und Aktualität sicherzustellen.
Überprüfung und Weiterentwicklung	Anpassung bei Änderungen oder neuen Risiken	R	Bei organisatorischen oder technischen Änderungen sowie bei neuen Risiken werden die TOM anlassbezogen angepasst.
Überprüfung und Weiterentwicklung	Sensibilisierung von Mitarbeitenden	R	Mitarbeitende werden regelmäßig zu Datenschutz- und Informationssicherheitsanforderungen sensibilisiert.