

Informationen zum Datenschutz für Microsoft 365

Mit diesen Hinweisen informieren wir Sie über die Verarbeitung Ihrer personenbezogenen Daten durch Microsoft 365. Bei Microsoft 365 handelt es sich – abstrakt betrachtet – um eine Sammlung und Zusammenstellung verschiedenster Werkzeuge und in der Plattform erstellter Anwendungen zum Zwecke der Kollaboration, der Sicherheit, des Datenschutzes und der Verarbeitung von verschiedensten Daten. Der Kern dieser Zusammenstellung umfasst vor allem die Werkzeuge Exchange Online (E-Mail, Kalender, Adressbuch, Aufgaben), SharePoint Online (Speicherung, Verarbeitung, Applikationsplattform) und Microsoft Teams (Kollaboration, Chat, Meeting und Telefonie), sowie Whiteboard als digitales Whiteboard. Ergänzend kommen hinzu Sicherheitswerkzeuge wie die Defender Produktreihe, Intune als App- und Geräteverwaltungswerkzeug.

Diese Datenschutzerklärung umfasst nicht die Drittapplikationen und Schnittstellen Dritter, die an die Microsoft 365 Plattform angebunden wurden. Hierfür verweisen wir auf die gesonderten Datenschutzerklärungen innerhalb der nicht zu Microsoft 365 gehörenden Applikationen.

1. Wer ist für die Datenverarbeitung verantwortlich?

Verantwortlicher im Sinne des Datenschutzrechts ist das jeweilige Unternehmen und die jeweilige Abteilung, die Microsoft 365 einsetzt und Ihre Daten verarbeitet.

Bei datenschutzbezogenen Fragen wenden Sie sich bitte an den Konzern-Datenschutzbeauftragten:

Gesellschaft	Kontakt
Schmitz Cargobull AG	dataprotection@cargobull.com
Preis Ingenieurbüro GmbH	dataprotection@cargobull.com
Schmitz Cargobull Finance GmbH	dataprotection@cargobull.com
Cargobull Parts & Services GmbH	dataprotection@cargobull.com
Cargobull Trailer Store GmbH	dataprotection@cargobull.com
Cargobull Customer Center GmbH	dataprotection@cargobull.com
Cargobull Telematics GmbH	dataprotection@cargobull.com
Schmitz Cargobull Gotha GmbH	dataprotection@cargobull.com
Schmitz Cargobull Nederland B.V.	dataprotection@cargobull.com
Schmitz Cargobull Ibérica S.A	dataprotection@cargobull.com
Schmitz Cargobull Danmark A/S	dataprotection@cargobull.com
Schmitz Cargobull France S.A.R.L.	dataprotection@cargobull.com
Schmitz Cargobull Magyarország Kft.	dataprotection@cargobull.com
Schmitz Cargobull Romania SRL	dataprotection@cargobull.com
Schmitz Cargobull d.o.o. Hrvatska	dataprotection@cargobull.com
Schmitz Cargobull d.o.o. SLOVENIJA	dataprotection@cargobull.com

Schmitz Cargobull d.o.o. Beograd	dataprotection@cargobull.com
Schmitz Cargobull Baltic UAB	dataprotection@cargobull.com
Schmitz Cargobull (UK) Limited	dataprotection@cargobull.com
TSE Trailer-System-Engineering GmbH & Co. KG	dataprotection@cargobull.com
Schmitz Cargobull Austria GmbH	dataprotection@cargobull.com
Schmitz Cargobull Portugal Unipes. Lda	dataprotection@cargobull.com
Schmitz Cargobull Italia S.r.l	dataprotection@cargobull.com
Schmitz Cargobull d.o.o. Sarajevo	dataprotection@cargobull.com
Schmitz Cargobull Belgium BV	dataprotection@cargobull.com
Schmitz Cargobull Makedonien	dataprotection@cargobull.com
Schmitz Cargobull Hellas AE	dataprotection@cargobull.com
Schmitz Cargobull Sverige AB	dataprotection@cargobull.com
Schmitz Cargobull Bulgaria EOOD	dataprotection@cargobull.com
Schmitz Cargobull Treyler Sanayi	dataprotection@cargobull.com
Trailer Engineering AG	dataprotection@cargobull.com
Atlantis Global System S.L.U	dataprotection@cargobull.com
Cargobull Cool GmbH & Co. KG	dataprotection@cargobull.com
Schmitz Cargobull Ukraine GmbH	dataprotection@cargobull.com
Schmitz Cargobull Suomi Oy	dataprotection@cargobull.com
Schmitz Cargobull Eesti OÜ	dataprotection@cargobull.com
Schmitz Cargobull Latvija SIA	dataprotection@cargobull.com
SCB Holding GmbH & Co. KG	dataprotection@cargobull.com
Schmitz Cargobull Schweiz AG	dataprotection@cargobull.com
Schmitz Cargobull Norge AS	dataprotection@cargobull.com
Schmitz Cargobull Logistik und Service GmbH	dataprotection@cargobull.com
CBNA LLC, Cargobull North America	dataprotection@cargobull.com
Schmitz Cargobull Shanghai Co., Ltd	dataprotection@cargobull.com
Schmitz Cargobull SCA LLC	dataprotection@cargobull.com
Schmitz Cargobull Ireland Limited	dataprotection@cargobull.com
KUBIKx GmbH	dataprotection@cargobull.com
Schmitz Cargobull SRL	dataprotection@cargobull.com
Schmitz Cargobull Overseas GmbH	dataprotection@cargobull.com
Schmitz Cargobull KAZ Kazakhstan	dataprotection@cargobull.com
Schmitz Cargobull Michalovce s.r.o.	dataprotection@cargobull.com
Schmitz Cargobull Maroc S.A.R.L.	dataprotection@cargobull.com
Schmitz Finance S.R.L.	dataprotection@cargobull.com
Cargobull Finance Kft.	dataprotection@cargobull.com
Cargobull Finance Polska Sp. z o.o	dataprotection@cargobull.com
Schmitz Cargobull Georgia LLC	dataprotection@cargobull.com
Schmitz Cargobull Albania sh.p.k.	dataprotection@cargobull.com

Die Schmitz Cargobull AG ist für alle Unternehmen und beherrschten Beteiligungen des Schmitz Cargobull Konzern (SCB) datenschutzrechtlich verantwortlich und steuert zentral.

2. Welche personenbezogenen Daten werden verarbeitet und zu welchen Zwecken?

Zweck der Verarbeitung

Der Zweck der Verarbeitung ist die Bereitstellung eines modernen Arbeitsplatzes mittels Microsoft 365, welches eine optimale Lösung für Kollaboration und Kommunikation innerhalb und außerhalb der SCB bietet. Ein weiterer Zweck ist die Bereitstellung und der sichere und reibungslose Betrieb von Microsoft 365 und dessen Werkzeugen.

Unter Kollaboration wird hier beispielsweise die gemeinsame Arbeit an Dateien, die E-Mail-Kommunikation, Besprechungen, Live-Übertragungen und innovative Werkzeuge verstanden.

Die Bereitstellung und der reibungslose Betrieb von Microsoft 365 gehört ebenfalls zu einem der Zwecke, für welche personenbezogene Daten verarbeitet werden. Von dieser Verarbeitung erfasst sind unter anderem die vom System erstellten Protokolle bzw. administrativen Ereignisse (z.B. Log-Dateien über die Anmeldung und Nutzeraktionen) sowie die Metadaten über Anrufe und Besprechungen, welche zu Fehler-, Support-, Statistik- sowie zu Nachweiszwecken genutzt werden. Hierzu wird eine Offenlegung der Informationen an Microsoft vorgenommen, welche durch den Verantwortlichen autorisiert ist, um diesen Betrieb sicherzustellen.

3. Welche Arten von personenbezogenen Daten?

Im Rahmen der Nutzung von Microsoft 365 werden personenbezogenen Daten verarbeitet. Eine Verarbeitung von personenbezogenen Daten kann automatisch erfolgen oder durch Eingabe durch Nutzerinnen und Nutzer.

Personenbezogene Daten werden im Rahmen von User-ID-basierten (mit Microsoft 365-Benutzerkonto der Unternehmen) sowie nicht User-ID-basierten Vorgängen (Business2Business-User, z. B. externe Personen ohne Microsoft 365-Benutzerkonto der Unternehmen) verarbeitet.

Es könnten Daten auch in Drittanbieter Apps verarbeitet werden. Diese sind aktuell deaktiviert.

Zum Zweck der Kollaboration mit bzw. zwischen Usern und Gästen (User-ID-basierte Vorgänge) innerhalb des Tenants sowie des sicheren IT-Betriebes werden von diesen folgenden personenbezogenen Daten verarbeitet:

1. Dokumente und Dateien

Diverse Arten von Dokumenten und Dateien können verarbeitet werden.

2. Kommunikationsdaten des Nutzers

Chat, Videotelefonie, Live-Übertragungen von Ton und ggf. Bild und Bildschirm, Foto

3. Kommunikationsdaten durch das System erzeugt

Zeitpunkt, Ort, Jitter-Wert, Datentransferrate, IP-Adresse, Gerätebezeichnung

- 4. Personenbezogene Basisdaten für den Account (das Benutzerkonto) ergänzbar mit usergenerierten Angaben**
Vorname, Nachname, Adresse, UPN (User principal name; technischer Benutzername), Telefonnummer, Position, Organisation, Mailadresse, Telefon- und Faxnummer
- 5. Authentifizierungsdaten**
Logindaten, Passwort, Benutzername, Zeitpunkt, Ort
- 6. Kontaktinformationen**
Berufliche Kontakt-, Arbeits-, und Organisationsdaten (z.B. Name, E-Mail, Gesellschaft, Personalnummer, ggf. Foto etc.) und private Kontaktinformationen (Private Telefonnummern und Adresse).
- 7. Profilierung**
Risikoprofil im Rahmen der Cybersecurity und IT-Sicherheit (z.B. Identitätsschutz)
- 8. Logfile mit Zugriffen**
Metadaten und Administrative Ereignisse
- 9. System generierte Protokolldaten**
Telemetrie- und Diagnosedaten, die von der Software erstellt werden.
- 10. Geräteinformationen** (einschließlich Informationen zur eingesetzten Software bzw. des genutzten Dienstes)
- 11. Cookies**
Zum Zweck der sicheren und stabilen Bereitstellung der Dienste werden technisch notwendige Cookies eingesetzt. Diese kleinen dem Browser anheftenden Cookies sind zum Beispiel Authentifizierungscookies zum Single-Sign-On.

4. Kategorien der betroffenen Personen

Die folgenden Personen können von der Verarbeitung bei Microsoft 365 betroffen sein:

Zusammenfassung der Personenkategorien

- Beschäftigte
- Ehemalige Beschäftigte
- Freiberufliche MitarbeiterInnen
- BewerberInnen
- Betriebsräte
- Schwerbehindertenvertretung
- DatenschutzmitarbeiterInnen und -koordinatoren
- Auszubildende und Studierende
- Praktikanten
- Kunden
- Leads (zukünftige Kunden)
- Externe (z.B. Dienstleister, Berater, Besucher und weitere Dritte)
- Lieferanten
- Partner und -gesellschaften
- Verbundgesellschaften der Unternehmen

5. Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten

Die Rechtsgrundlage für den Betrieb von Microsoft 365 beruhen auf:

- Beschäftigte Art. 6 Abs. 1 S. 1. lit. b i.V.m. Arbeitsvertrag, i.V.m. Art. 88 DSGVO
- Externe Benutzergruppen Art. 6 Abs. 1 S. 1 lit. b DSGVO i.V.m. entsprechenden Verträgen;

Die Verarbeitungen für Zwecke der IT-Sicherheit (insb. Log-Dateien und Metadaten) sowie Cookies (Cookies und §25 Abs. 2 TTDSG) gründen sich auf Art. 6 Abs. 1 lit. b i.V.m. Arbeitsvertrag. Die von den Verantwortlichen verfolgten berechtigten Interessen umfassen folgende:

- Feststellung missbräuchlicher Nutzung;
- IT-Sicherheit und kontinuierliche Verbesserung der Dienste.

Sollten bei internen Veranstaltungen Bild- und Tonaufnahmen erstellt werden erfolgt dies auf Grundlage von Art. 6 Abs. 1 lit. a) DSGVO (Einwilligung).

6. Verarbeitungen im Einzelnen

6.1. Identitätsmanagement

Im Rahmen des Identitätsmanagements mit Azure Active Directory/Entra-ID (AAD) werden zentral Identitäten, Geräte und Applikationen in Microsoft 365 verarbeitet. Insbesondere werden alle mit Microsoft 365 verknüpften Identitäten mit der Umgebung von Unternehmen, sowie Gäste verarbeitet. Dies ermöglicht den sicheren Zugang und Nutzung diverser Microsoft 365 Applikationen.

Datenkategorien

1-11

weitere Rechtsgrundlagen für den Einsatz

Art. 6 Abs. 1 S. 1 lit. a DSGVO, Art. 88 DSGVO	Bild des/der Beschäftigten
Art. 6 Abs. 1 S. 1 lit. a DSGVO, Art. 88 DSGVO	Lokation des/der Beschäftigten (z.B. bei Verlust des verwalteten Gerätes über Intune, MFA)

6.2. E-Mail, Kalender und Aufgaben

Im Rahmen der Datenverarbeitung in Bezug auf E-Mails, Kalenderdaten und Aufgaben im Speziellen in der Exchange hybriden Umgebung.

Datenkategorien

1,2,3,4,5,6,7,8,9,10

Weitere Rechtsgrundlagen für den Einsatz

Art. 6 Abs. 1 S. 1. lit. b DSGVO i.V.m Arbeitsvertrag oder zukünftigen Arbeitsvertrag	Beschäftigte, BewerberInnen
Art. 6 Abs. 1 S. 1 lit. b DSGVO i.V.m mit den jeweiligen Vertrag	Externe Personen, zur Vertragsverfüllung oder Vertragsanbahnung
Art. 6 Abs. 1 S. 1 lit. b, f DSGVO	Externe Personen, BewerberInnen

6.3. Kommunikation: Chat

Im Rahmen der Chat Kommunikation wird zwischen Beschäftigten und Mitgliedern und auch Gästen kommuniziert. Im Rahmen dessen können neben Chats auch Inhalte wie Dateien geteilt und gemeinsam mit Microsoft Teams bearbeitet werden.

Datenkategorien

1-11

Weitere Rechtsgrundlagen für den Einsatz

Art. 6 Abs. 1 S. 1. lit. b DSGVO i.V.m Arbeitsvertrag oder zukünftigen Arbeitsvertrag	Beschäftigte, BewerberInnen
Art. 6 Abs. 1 S. 1 lit. b, a DSGVO	GeschäftspartnerInnen
Art. 6 Abs. 1 S. 1 lit. a DSGVO	Onlinebewerbungsbespräche mit BewerberInnen = zu Chat
Art. 6 Abs. 1 S. 1 lit. a DSGVO	Externe Personen
Art. 6 Abs. 1 S. 1 lit. a DSGVO, Art. 88 DSGVO	Bild des Beschäftigten, Audiodateien

6.4. Kommunikation: Videokonferenzen

Im Rahmen der Videokonferenzen mit Microsoft Teams wird sowohl Microsoft Teams Besprechungen als auch Microsoft Live Events eingesetzt.

Datenkategorien

1,3,4,5,6,7,9,10,11

Weitere Rechtsgrundlagen für den Einsatz

Art. 6 Abs. 1 S. 1 lit. a, f DSGVO	Onlinebewerbungsbespräche mit BewerberInnen
------------------------------------	--

Art. 6 Abs. 1 S. 1 lit. f DSGVO	Webinare
Art. 6 Abs. 1 S. 1 lit. b, a DSGVO	GeschäftspartnerInnen
Art. 6 Abs. 1 S. 1 lit. a DSGVO Art. 6 Abs. 1 S. 1 lit. f DSGVO	Externe Personen
Art. 6 Abs. 1 S. 1 lit. b, a DSGVO	Anwesenheitsberichte Löschung 90 Tage nach Ende der Besprechung

6.5. Bild im Profil

Mitglieder im Microsoft 365 Tenant haben die Möglichkeit ein Bild in ihrem Profil zu hinterlegen. Dies basiert auf einer Einwilligung. Die Kontrolle über das Bild, sowie dessen Speicherzeitraum liegt in der Hand des Profileigentümers.

Datenkategorien

2

Weitere Rechtsgrundlagen für den Einsatz

Art. 6 Abs. 1 S. 1 lit. a DSGVO	Alle Betroffene
---------------------------------	-----------------

6.6. Zusammenarbeit an Dokumenten und Dateien

Im Rahmen der Zusammenarbeit an Dokumenten und Dateien wird meist SharePoint Online eingesetzt, ob direkt oder im Hintergrund.

Datenkategorien

1,2,4,5,9,10

Weitere Rechtsgrundlagen für den Einsatz

Art. 6 Abs. 1 S. 1 lit. b, a DSGVO	Geschäftspartner/Innen
Art. 6 Abs. 1 S. 1 lit. a, f DSGVO	Externe Personen

6.7. Umfragen

Im Rahmen von Microsoft 365 können mit Forms Umfragen erstellt und durchgeführt werden. Im Rahmen dessen wird pro Umfrage die durchführende Abteilung, der Zweck und die Löschfrist angegeben.

Eine Verarbeitung im SharePoint Online beruht dann je nach Umfrage auf den folgenden Rechtsgrundlagen:

Weitere Rechtsgrundlagen für den Einsatz

Art. 6 Abs. 1 S. 1. lit. b, a DSGVO bei b i.V.m. Arbeitsvertrag oder zukünftigen Arbeitsvertrag	Beschäftigte, BewerberInnen
Art. 6 Abs. 1 S. 1 lit. b, a DSGVO	Geschäftspartner/Innen
Art. 6 Abs. 1 S. 1 lit. a, f DSGVO	Externe Personen

6.8. Microsoft KI

Im Rahmen der Nutzung von KI findet eine Datenverarbeitung personenbezogener Daten statt. Diese werden nicht zum Training der KI genutzt, sondern können zur Anreicherung oder innerhalb eines Prompts vorkommen. (Microsoft 365 Copilot)

Datenkategorien

1-13

Rechtsgrundlagen

Art. 6 Abs. 1 S. 1. lit. b DSGVO i.V.m. Arbeitsvertrag oder zukünftigen Arbeitsvertrag und Art. 6 Abs. 1 S. 1. lit. a DSGVO	Beschäftigte, BewerberInnen
Art. 6 Abs. 1 S. 1 lit. a DSGVO	Externe Personen
Art. 6 Abs. 1 S. 1 lit. a DSGVO	DienstleisterInnen

6.9. Sicherheitsfunktionen

Im Rahmen der sicheren und stabilen Bereitstellung von Microsoft 365 werden Sicherheitswerkzeuge aus dem Microsoft 365 Paket eingesetzt. Diese sind als Defender bekannt.

Die Defender Produkte sollen den modernen Arbeitsplatz rund um Windows und Office, also die Microsoft 365 Umgebung bis zum Endgerät abzusichern. Dazu gehören Cybersecurity Werkzeuge von Antivirus über Antispam und Schutz von Emails und deren Anhängen.

Datenkategorien

1-13

Rechtsgrundlagen

Art. 6 Abs. 1 S. 1. lit. b DSGVO i.V.m. Arbeitsvertrag oder zukünftigen Arbeitsvertrag	Beschäftigte, BewerberInnen
--	-----------------------------

Art. 6 Abs. 1 S. 1 lit. b, e DSGVO	Externe Personen
Art. 6 Abs. 1 S. 1 lit. b, e DSGVO	DienstleisterInnen

6.10. Internationaler Datentransfer

Im Rahmen der Datenverarbeitung kann es zu einem internationalem Datentransfer kommen. Hierbei handelt es sich um Datentransfer im Supportfall und im Falle des Cybersecurity-Vorfalles.

- Rückausnahmen Art. 49 Abs. 1 lit c DSGVO für Zwecke a und f (s. bei "Offenlegung von Daten").
- Rückausnahmen Art. 49 Abs. 1 lit. d DSGVO für Zwecke b, c, d, g, h (s. bei (Offenlegung von Daten)).
- Bei der Verarbeitung im Zwecke der Bereitstellung gilt die DSGVO unmittelbar für Microsoft als Auftragsdatenverarbeiter:
 - Unterauftragsverarbeiter
 - Standarddatenschutzklauseln mit zusätzlichen Absicherungen für die Auftragsverarbeitung

Für **Telemetrie- und Diagnosedaten** wird abgestellt auf den Standard des DPA und den aktuellen EU-Standardvertragsklauseln, Art. 46 Abs. 1 DSGVO für die Verkettung der Microsoft Irland Inc. zu Microsoft Corporation. Es wurde durch Konfiguration die Sammlung und Verarbeitung von Telemetrie- und Diagnosedaten auf ein Minimum reduziert und auch die Speicherung in der Umgebung reduziert. Ab Ende 2024 werden diese Daten nur noch in Europa verarbeitet und es besteht für personenbezogene Daten in diesem Bereich kein Datentransfer in die USA mehr.

Microsoft Corporation

- Standarddatenschutzklauseln mit zusätzlichen Absicherungen für die Auftragsverarbeitung zwischen Microsoft Irland und Microsoft Corporation.
- Seit 10. Juli 2023 gilt ebenso das EU-US Data Privacy Framework als Angemessenheitsbeschluss als Rechtsgrundlage für Microsoft zur Datentransfer in die USA.

7. An welche Empfänger oder Kategorien von Empfängern geben wir Ihre Daten im Rahmen dieser Verarbeitungstätigkeit weiter?

Konzern

Wir geben Ihre Daten bei Bedarf und Grundlage eines Zweckes innerhalb des Konzerns auf Basis einer Auftragsdatenverarbeitung weiter. So wird beispielsweise zentralisiert nur ein Microsoft 365 Tenant eingesetzt und von den Unternehmen und seinen IT-Mitarbeitenden verwaltet.

Auftragsverarbeiter

Wir geben Ihre personenbezogenen Daten auch an von uns beauftragte Dienstleister im Rahmen von Auftragsverarbeitungen weiter (unter anderem z.B. an Microsoft Ireland Operations Ltd.). Diese

umfassen u. a. die durch den Verantwortlichen beauftragte IT-Dienstleister im Rahmen ihrer administrativen Tätigkeiten (z.B. im Rahmen von Support- und Wartungsarbeiten).

Dritte

Externe erhalten im Einzelfall Daten, soweit dies erlaubt und zu den oben genannten Zwecken erforderlich ist. Diese umfassen u. a. die durch den Verantwortlichen beauftragte IT-Dienstleister im Rahmen ihrer administrativen Tätigkeiten (z.B. im Rahmen von Support- und Wartungsarbeiten).

Darüber hinaus übermitteln wir Ihre personenbezogenen Daten, soweit gesetzlich vorgeschrieben, in Einzelfällen an Behörden soweit gesetzlich notwendig.

8. Wie übermitteln wir Daten ins außereuropäische Ausland?

Wir übermitteln Daten auf der Basis von Standardvertragsklauseln in Verbindung mit Auftragsverarbeitungs-Vereinbarungen. Dazu kommt eine Übermittlung der pseudonymisierten Telemetrie- und Diagnosedaten von Microsoft Irland zu Microsoft Corp. auf Basis von EU-Standardvertragsklauseln.

9. Wie lange speichern wir Ihre Daten?

Wir speichern Ihre Daten so lange, wie dies zur Nutzung von Microsoft 365 erforderlich ist bzw. solange ein Zweck oder eine Rechtsgrundlage gegeben ist. Als Cloudbackup wird eine zentrale Backuplösung bei einem deutschen Service-Provider verwendet, um die Microsoft 365 Umgebung (Exchange, SharePoint etc.) zu sichern.

Vom Anwender explizit freigegebene Positionsdaten bzw. Standortdaten werden ausschließlich während der Besprechung verarbeitet. Eine darüber hinaus gehende Speicherung dieser Daten erfolgt nicht.

Metadaten von Anrufen und Besprechungen werden maximal 120 Tage gespeichert (abhängig vom Datum). Auch hier werden die Daten nach Ablauf der Fristen automatisch gelöscht. Eine Anpassung der Fristen für Live Events (120 Tage) und Teams Besprechungen/Anrufe (90) Tage können nicht angepasst werden. Diese werden jedoch für die Stabilität des Systems, Support und auch zur Abwehr von Angriffen in diesem Vektor benötigt. Zugriff haben nur bestimmte berechnigte und überwachte Administratoren.

Protokollierte administrative Ereignisse werden 180 Tage gespeichert und danach automatisch gelöscht.

E-Mails und Anlagen werden im Rahmen der gesetzlichen Aufbewahrungsfristen aufbewahrt und sodann gelöscht, wenn keine anderen Zwecke vorhanden sind.

Die von Sicherheitswerkzeugen und von sonstigen, der IT-Sicherheit dienenden Werkzeugen verarbeiteten personenbezogenen Daten werden für 180 Tage aufbewahrt und dann der Löschung zugeführt. In Einzelfällen und bei Sicherheitsvorfällen kann es dazu kommen, dass einige Daten länger aufbewahrt werden, um den Vorfall zu untersuchen und zukünftige zu unterbinden.

Unter bestimmten Umständen müssen Ihre Daten auch länger aufbewahrt werden, beispielsweise im Zusammenhang mit einer entsprechenden behördlichen oder gerichtlichen Anordnung in Form eines sog. Litigation Hold, welches ein Verbot der Datenlöschung für die Dauer des Verfahrens beinhaltet.

10. Technisch-organisatorische Maßnahmen

Im Rahmen der Verarbeitung ihrer personenbezogenen Daten haben wir eine Risikoanalyse für die Verarbeitung durchgeführt und darauf beruhend risiko-angepasste technische und organisatorische Maßnahmen eingeführt. Diese Maßnahmen werden regelmäßig geprüft und den bestehenden Risiken angepasst.

Unter anderem haben wir folgenden Maßnahmen ergriffen:

- Datenklassifikation
- Monitoring und Überwachung der Umgebung
- Deaktivierung der Feedback-Funktion
- Einschränkung der Funktionen der verbundenen und optional verbundenen Dienste
- Vertragliche Maßnahmen und Zusatzverträge

Die Unternehmen hat ein integriertes Managementsystem für Datenschutz und Informationssicherheit implementiert und lässt dieses auf Grundlage der ISO 27001 bzw. dem Branchen-TISAX Level 2 bis 3 in den jeweiligen Gesellschaften, die zertifiziert wurden und regelmäßig extern auditieren werden.

Microsoft Entra ID (früher: Azure Active Directory (AAD)) und Single-sign-on (SSO)

Azure Active Directory (neu: Microsoft Entra ID) (ADD) wird insbesondere als Identitätssystem von Microsoft eingesetzt. Dieses ermöglicht es den Zugriff zu Anwendungen, Dateien und zu Geräten nach dem Need-to-Know-Prinzip zu steuern und zu überwachen. Darüber hinaus setzen wir MFA zur Absicherung der Accounts ein. Des Weiteren ermöglicht ADD eine automatische Anmeldung auf von Unternehmen verwalteten Geräten.

11. Welche Datenschutzrechte haben Sie?

Im Folgenden enumerieren wir die Ihnen nach dem Datenschutzrecht zustehenden Rechte, die Sie gegenüber dem Verantwortlichen jederzeit unentgeltlich geltend machen können.

Wie Sie den Datenschutzbeauftragten und den Verantwortlichen erreichen, erfahren Sie unter Punkt 1.

Auskunftsrecht: Sie haben das Recht, von uns Auskunft über die Verarbeitung Ihrer personenbezogenen Daten zu erhalten.

Berichtigungsrecht: Sie haben das Recht, von uns die Berichtigung Sie betreffender unrichtiger bzw. unvollständiger personenbezogener Daten zu verlangen.

Recht auf Löschung: Sie haben das Recht, bei Vorliegen der in Art. 17 DSGVO genannten Voraussetzungen, die Löschung Ihrer Daten zu verlangen. Danach können Sie beispielsweise die

Löschung Ihrer Daten verlangen, soweit diese für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Außerdem können Sie die Löschung verlangen, wenn wir Ihre Daten auf der Grundlage Ihrer Einwilligung verarbeiten und Sie diese Einwilligung später widerrufen.

Recht auf Einschränkung der Verarbeitung: Sie haben das Recht, die Einschränkung der Verarbeitung Ihrer Daten zu verlangen, wenn die Voraussetzungen des Art. 18 DSGVO vorliegen. Dies ist beispielsweise der Fall, wenn Sie die Richtigkeit Ihrer Daten bestreiten. Für die Dauer der Überprüfung der Richtigkeit der Daten können Sie dann die Einschränkung der Verarbeitung verlangen.

Recht auf Datenübertragbarkeit: Sofern die Datenverarbeitung auf der Grundlage einer Einwilligung oder einer Vertragserfüllung beruht und diese zudem unter Einsatz einer automatisierten Verarbeitung erfolgt, haben Sie das Recht, Ihre Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese an einen anderen Datenverarbeiter zu übermitteln.

Widerrufsrecht: Sofern die Datenverarbeitung auf einer Einwilligung beruht, haben Sie das Recht, die Datenverarbeitung im Rahmen einer Einwilligung mit Wirkung für die Zukunft jederzeit kostenlos zu widerrufen.

Beschwerderecht: Sie haben außerdem das Recht, sich bei einer Aufsichtsbehörde für den Datenschutz über die Verarbeitung Ihrer Daten zu beschweren.

Widerspruchsrecht: Betroffene Personen haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit der Datenverarbeitung zu widersprechen, soweit diese auf der Rechtsgrundlage „berechtigtes Interesse“ beruht. Sofern betroffene Personen von ihrem Widerspruchsrecht Gebrauch machen, wird die Verarbeitung ihrer Daten eingestellt, es sei denn es können - gemäß den gesetzlichen Vorgaben - zwingende schutzwürdige Gründe für die Weiterverarbeitung nachgewiesen werden, welche den Rechten der betroffenen Personen überwiegen.

Data Privacy Information for Microsoft 365

AI-generated translation – the German version shall prevail.

This notice informs you about the processing of your personal data in connection with Microsoft 365. Microsoft 365 is, in general terms, a collection of tools and applications provided on the platform for collaboration, security, data protection and the processing of different types of data. The core services include Exchange Online (email, calendar, address book and tasks), SharePoint Online (storage, processing and application platform), Microsoft Teams (collaboration, chat, meetings and telephony) and Whiteboard as a digital whiteboard. In addition, security tools such as the Microsoft Defender product line and Intune for app and device management are used.

This Privacy Statement does not cover third-party applications or third-party interfaces connected to the Microsoft 365 platform. Please refer to the separate privacy notices within applications that are not part of Microsoft 365.

12. Who is responsible for data processing?

The controller within the meaning of data protection law is the respective company and department that uses Microsoft 365 and processes your data.

For data protection-related questions, please contact the Group Data Protection Officer:

Company	Contact
Schmitz Cargobull AG	dataprotection@cargobull.com
Price Ingenieurbüro GmbH	dataprotection@cargobull.com
Schmitz Cargobull Finance GmbH	dataprotection@cargobull.com
Cargobull Parts & Services GmbH	dataprotection@cargobull.com
Cargobull Trailer Store GmbH	dataprotection@cargobull.com
Cargobull Customer Center GmbH	dataprotection@cargobull.com
Cargobull Telematics GmbH	dataprotection@cargobull.com
Schmitz Cargobull Gotha GmbH	dataprotection@cargobull.com
Schmitz Cargobull Nederland B.V.	dataprotection@cargobull.com
Schmitz Cargobull Ibérica S.A	dataprotection@cargobull.com
Schmitz Cargobull Danmark A/S	dataprotection@cargobull.com
Schmitz Cargobull France S.A.R.L.	dataprotection@cargobull.com
Schmitz Cargobull Hungary Ltd.	dataprotection@cargobull.com
Schmitz Cargobull Romania SRL	dataprotection@cargobull.com
Schmitz Cargobull d.o.o. Croatia	dataprotection@cargobull.com
Schmitz Cargobull d.o.o. SLOVENIJA	dataprotection@cargobull.com
Schmitz Cargobull d.o.o. Beograd	dataprotection@cargobull.com
Schmitz Cargobull Baltic UAB	dataprotection@cargobull.com
Schmitz Cargobull (UK) Limited	dataprotection@cargobull.com

TSE Trailer-System-Engineering GmbH & Co. KG	dataprotection@cargobull.com
Schmitz Cargobull Austria GmbH	dataprotection@cargobull.com
Schmitz Cargobull Portugal Unipes. Lda	dataprotection@cargobull.com
Schmitz Cargobull Italia S.r.l	dataprotection@cargobull.com
Schmitz Cargobull d.o.o. Sarajevo	dataprotection@cargobull.com
Schmitz Cargobull Belgium BV	dataprotection@cargobull.com
Schmitz Cargobull Macedonia	dataprotection@cargobull.com
Schmitz Cargobull Hellas AE	dataprotection@cargobull.com
Schmitz Cargobull Sverige AB	dataprotection@cargobull.com
Schmitz Cargobull Bulgaria EOOD	dataprotection@cargobull.com
Schmitz Cargobull Treyler Sanayi	dataprotection@cargobull.com
Trailer Engineering AG	dataprotection@cargobull.com
Atlantis Global System S.L.U	dataprotection@cargobull.com
Cargobull Cool GmbH & Co. KG	dataprotection@cargobull.com
Schmitz Cargobull Ukraine GmbH	dataprotection@cargobull.com
Schmitz Cargobull Suomi Oy	dataprotection@cargobull.com
Schmitz Cargobull Eesti OÜ	dataprotection@cargobull.com
Schmitz Cargobull Latvija SIA	dataprotection@cargobull.com
SCB Holding GmbH & Co. KG	dataprotection@cargobull.com
Schmitz Cargobull Schweiz AG	dataprotection@cargobull.com
Schmitz Cargobull Norge AS	dataprotection@cargobull.com
Schmitz Cargobull Logistik und Service GmbH	dataprotection@cargobull.com
CBNA LLC, Cargobull North America	dataprotection@cargobull.com
Schmitz Cargobull Shanghai Co., Ltd	dataprotection@cargobull.com
Schmitz Cargobull SCA LLC	dataprotection@cargobull.com
Schmitz Cargobull Ireland Limited	dataprotection@cargobull.com
KUBIKx GmbH	dataprotection@cargobull.com
Schmitz Cargobull SRL	dataprotection@cargobull.com
Schmitz Cargobull Overseas GmbH	dataprotection@cargobull.com
Schmitz Cargobull KAZ Kazakhstan	dataprotection@cargobull.com
Schmitz Cargobull Michalovce s.r.o.	dataprotection@cargobull.com
Schmitz Cargobull Maroc S.A.R.L.	dataprotection@cargobull.com
Schmitz Finance S.R.L.	dataprotection@cargobull.com
Cargobull Finance Ltd.	dataprotection@cargobull.com
Cargobull Finance Polska Sp. z o.o	dataprotection@cargobull.com
Schmitz Cargobull Georgia LLC	dataprotection@cargobull.com
Schmitz Cargobull Albania sh.p.k.	dataprotection@cargobull.com

Schmitz Cargobull AG is responsible under data protection law for all companies and controlled shareholdings of the Schmitz Cargobull Group (SCB) and manages them centrally.

13. What personal data is processed and for what purposes?

Purpose of processing

The purpose of processing is to provide a modern workplace based on Microsoft 365, offering an effective solution for collaboration and communication within and outside SCB. Another purpose is to deploy and operate Microsoft 365 and its tools securely and reliably.

Collaboration here means, for example, working together on files, e-mail communication, meetings, live broadcasts and innovative tools.

The provision and reliable operation of Microsoft 365 is also one of the purposes for which personal data is processed. This processing includes, among other things, system-generated logs and administrative events, such as log files relating to logins and user actions, as well as metadata on calls and meetings used for troubleshooting, support, statistical and verification purposes. For this purpose, information is disclosed to Microsoft, which is engaged by the controller to ensure operation of the service.

14. What types of personal data?

Personal data is processed when Microsoft 365 is used. The processing of personal data may occur automatically or through input by users.

Personal data is processed both in user-ID-based operations, using Microsoft 365 user accounts of the companies, and in non-user-ID-based operations, for example in business-to-business scenarios involving external persons without a company Microsoft 365 user account.

Data may also be processed in third-party apps. These are currently disabled.

For the purpose of collaboration with or between users and guests within the tenant, and to ensure secure IT operations, the following personal data is processed by the tenant in user-ID-based processes:

12. Documents and files

Various types of documents and files can be processed.

13. User's Communication Data

Chat, video telephony, live audio broadcasts and, where applicable, video, screen sharing and photos

14. Communication data generated by the system

Time, location, jitter value, data transfer rate, IP address, device designation

15. Basic personal data for the user account, which may be supplemented by user-generated data

First name, last name, address, UPN (User Principal Name), telephone number, position, organisation, email address, telephone and fax number

16. Authentication data

Login data, password, username, time, location

17. Contact

information

Professional contact, work and organizational data (e.g. name, e-mail, company, personnel number, photo if applicable, etc.) and private contact information (private telephone numbers and address).

18. Profiling

Risk profile in the context of cybersecurity and IT security (e.g. identity protection)

19. Log file with accesses

Metadata and administrative events

20. System-generated log data

Telemetry and diagnostic data generated by the software.

21. Device information (including information about the software or service used)

22. Cookies

Technically necessary cookies are used to provide the services securely and reliably. These small cookies, which are stored in the browser, include authentication cookies for single sign-on, for example.

15. Categories of data subjects

The following people may be affected by Microsoft 365 processing:

Summary of the categories of data subjects

- Employees
- Former employees
- Freelancers
- Applicants
- Works councils
- Representatives for severely disabled employees
- Data protection staff and coordinators
- Trainees and students
- Interns
- Customers
- Leads (future customers)
- External parties (e.g. service providers, consultants, visitors and other third parties)
- Suppliers
- Partners and companies
- Affiliated companies

16. Legal basis for processing personal data

The legal basis for the operation of Microsoft 365 is based on:

- Employees Art. 6 para. 1 sentence 1. lit. b in conjunction with employment contract, in conjunction with Art. 88 GDPR
- External user groups Art. 6 para. 1 sentence 1 lit. b GDPR in conjunction with corresponding contracts;

Processing for IT security purposes, in particular log files and metadata, as well as technically necessary cookies under Section 25 para. 2 TTDSG, is based on Art. 6 para. 1 lit. b GDPR in conjunction with the employment contract. The legitimate interests pursued by the controllers include the following:

- Detection of misuse;
- IT security and continuous improvement of services.

If image and sound recordings are made at internal events, this is done on the basis of Art. 6 para. 1 lit. a) GDPR (consent).

17. Processing in detail

17.1. Identity Management

As part of identity management with Microsoft Entra ID, formerly Azure Active Directory (AAD), identities, devices and applications are processed centrally in Microsoft 365. In particular, all identities associated with Microsoft 365 in the companies' environment, as well as guest identities, are processed. This enables secure access to and use of various Microsoft 365 applications.

Data categories

1-11

Additional legal bases for use

Art. 6 para. 1 sentence 1 lit. a GDPR, Art. 88 GDPR	Employee photo
Art. 6 para. 1 sentence 1 lit. a GDPR, Art. 88 GDPR	Location of the employee(s) (e.g. in the event of loss of the managed device via Intune, MFA)

17.2. Email, Calendar, and Tasks

This includes, in particular, data processing related to emails, calendar data and tasks in the Exchange hybrid environment.

Data categories

1,2,3,4,5,6,7,8,9,10

Additional legal bases for use

Art. 6 para. 1 sentence 1 lit. b GDPR in conjunction with employment contract or future employment contract	Employees, applicants
Art. 6 para. 1 sentence 1 lit. b GDPR in conjunction with the respective contract	External persons, for contract performance or contract initiation
Art. 6 para. 1 sentence 1 lit. b, f GDPR	External persons, applicants

17.3. Communication: Chat

Chat communication enables communication between employees, members and guests. In addition to chats, content such as files can also be shared and jointly edited in Microsoft Teams.

Data categories

1-11

Additional legal bases for use

Art. 6 para. 1 sentence 1 lit. b GDPR in conjunction with employment contract or future employment contract	Employees, applicants
Art. 6 para. 1 sentence 1 lit. b, a GDPR	Business partners
Art. 6 para. 1 sentence 1 lit. a GDPR	Online application interviews with applicants via chat
Art. 6 para. 1 sentence 1 lit. a GDPR	External persons
Art. 6 para. 1 sentence 1 lit. a GDPR, Art. 88 GDPR	Employee photo, audio files

6.4. Communication: Video conferences

Microsoft Teams meetings and Microsoft Live Events are used for video conferences.

Data categories

1,3,4,5,6,7,9,10,11

Additional legal bases for use

Art. 6 para. 1 sentence 1 lit. a, f GDPR	Online application interviews with applicants
Art. 6 para. 1 sentence 1 lit. f GDPR	Webinars
Art. 6 para. 1 sentence 1 lit. b, a GDPR	Business partners
Art. 6 para. 1 sentence 1 lit. a GDPR Art. 6 para. 1 sentence 1 lit. f GDPR	External persons
Art. 6 para. 1 sentence 1 lit. b, a GDPR	Attendance reports Deletion 90 days after the meeting ends

17.4. Image in profile

Members of the Microsoft 365 tenant may add a photo to their profile. This is based on consent. Control over the photo and its retention period remains with the profile owner.

Data categories

2

Additional legal bases for use

Art. 6 para. 1 sentence 1 lit. a GDPR	All data subjects
---------------------------------------	-------------------

17.5. Collaborate on documents and files

SharePoint Online is usually used for collaboration on documents and files, either directly or in the background.

Data categories

1,2,4,5,9,10

Additional legal bases for use

Art. 6 para. 1 sentence 1 lit. b, a GDPR	Business partners
Art. 6 para. 1 sentence 1 lit. a, f GDPR	External persons

17.6. Surveys

Microsoft Forms can be used within Microsoft 365 to create and conduct surveys. For each survey, the department conducting the survey, the purpose and the deletion period are specified.

Depending on the survey, processing in SharePoint Online is then based on the following legal bases:

Additional legal bases for use

Art. 6 para. 1 sentence 1. lit. b, a GDPR in the case of b in conjunction with the employment contract or future employment contract	Employees, applicants
Art. 6 para. 1 sentence 1 lit. b, a GDPR	Business partners
Art. 6 para. 1 sentence 1 lit. a, f GDPR	External persons

6.8. Microsoft AI

When AI is used, personal data may be processed. This data is not used to train the AI, but may be processed for enrichment purposes or as part of a prompt. (Microsoft 365 Copilot)

Data categories

1-13

Legal basis

Art. 6 para. 1 sentence 1 lit. b GDPR in conjunction with the employment contract or future employment contract and Art. 6 para. 1 sentence 1 lit. a GDPR	Employees, applicants
---	-----------------------

Art. 6 para. 1 sentence 1 lit. a GDPR	External persons
Art. 6 para. 1 sentence 1 lit. a GDPR	Service providers

17.7. Security features

Security tools from the Microsoft 365 suite are used as part of the secure and reliable provision of Microsoft 365. These tools are known as Microsoft Defender products.

The Defender products are intended to secure the modern workplace, from Windows and Office to the Microsoft 365 environment and end-user devices. This includes cybersecurity tools ranging from antivirus and antispam protection to protection for emails and attachments.

Data categories

1-13

Legal basis

Art. 6 para. 1 sentence 1 lit. b GDPR in conjunction with employment contract or future employment contract	Employees, applicants
Art. 6 para. 1 sentence 1 lit. b, e GDPR	External persons
Art. 6 para. 1 sentence 1 lit. b, e GDPR	Service providers

17.8. International data transfer

Data processing may involve international data transfers, particularly in the context of support services and cybersecurity incidents.

- Derogations under Art. 49 (1) (c) GDPR for purposes a and f (see "Disclosure of data").
- Derogations under Art. 49 (1) (d) GDPR for purposes b, c, d, g, h (see "Disclosure of data").
- In the case of processing for the purpose of provision, the GDPR applies directly to Microsoft as a data processor:
 - Sub-processors
 - Standard contractual clauses with additional safeguards for processing on behalf of the controller

Telemetry **and diagnostic data** are processed on the basis of the Data Processing Addendum and the current EU standard contractual clauses pursuant to Art. 46 para. 1 GDPR for the transfer from Microsoft Ireland Inc. to Microsoft Corporation. The collection and processing of telemetry and diagnostic data has been reduced to a minimum through configuration, and storage within the environment has also been limited. From the end of 2024, this data will only be processed in Europe and personal data in this area will no longer be transferred to the USA.

Microsoft Corporation

- Standard contractual clauses with additional safeguards for processing on behalf of the controller between Microsoft Ireland and Microsoft Corporation.
- Since July 10, 2023, the EU-US Data Privacy Framework has also been the legal basis for Microsoft to transfer data to the USA as an adequacy decision.

7. With which recipients or categories of recipients do we share your data as part of this processing activity?

Group

Where necessary and based on a defined purpose, we share your data within the group on the basis of commissioned data processing. For example, one Microsoft 365 tenant is used centrally and managed by the companies and their IT staff.

Processors

We also share your personal data with service providers commissioned by us in the context of processing on behalf of the controller, including, for example, Microsoft Ireland Operations Ltd. These include IT service providers commissioned by the controller for administrative activities, such as support and maintenance work.

Third parties

External parties receive data in individual cases where this is permitted and necessary for the purposes stated above. These include IT service providers commissioned by the controller for administrative activities, such as support and maintenance work.

In addition, we transmit your personal data to authorities in individual cases, to the extent required by law.

18. How do we transfer data outside Europe?

We transfer data on the basis of standard contractual clauses in connection with processing agreements. In addition, pseudonymised telemetry and diagnostic data is transferred from Microsoft Ireland to Microsoft Corp. on the basis of EU standard contractual clauses.

19. How long do we store your data?

We store your data for as long as this is necessary for the use of Microsoft 365 or for as long as a purpose or legal basis exists. A central backup solution hosted by a German service provider is used as a cloud backup for the Microsoft 365 environment, including Exchange and SharePoint.

Position data or location data explicitly shared by the user is processed only during the meeting and is not stored beyond that period.

Metadata from calls and meetings is stored for a maximum of 120 days, depending on the date. This data is automatically deleted after the applicable retention periods have expired. The retention periods for Live Events (120 days) and Teams meetings/calls (90 days) cannot be changed. However, this data is required for system stability, support and protection against attacks using this vector. Access is limited to specific authorised and supervised administrators.

Logged administrative events are stored for 180 days and then automatically deleted.

Emails and attachments are retained within the statutory retention periods and then deleted if no other purpose applies.

The personal data processed by security tools and other IT security tools will be stored for 180 days and then deleted. In individual cases and security incidents, some data may be retained for a longer period of time in order to investigate the incident and prevent future ones.

Under certain circumstances, your data must also be stored for a longer period of time, for example in connection with a corresponding official or court order in the form of a so-called litigation hold, which includes a prohibition on data deletion for the duration of the proceedings.

20. Technical and organisational measures

As part of the processing of your personal data, we have carried out a risk analysis and implemented risk-based technical and organisational measures. These measures are reviewed regularly and adapted to the existing risks.

Among other things, we have taken the following measures:

- Data classification
- Monitoring of the environment
- Deactivation of the feedback function
- Restriction of connected and optional connected services
- Contractual measures and supplementary contracts

The company has implemented an integrated management system for data protection and information security based on ISO 27001 and the industry standard TISAX Level 2 to 3 in the respective companies. These companies have been certified and are audited externally on a regular basis.

Microsoft Entra ID (formerly Azure Active Directory (AAD)) and Single Sign-On (SSO)

Microsoft Entra ID, formerly Azure Active Directory (AAD), is used as Microsoft's identity system. It enables access to applications, files and devices to be controlled and monitored according to the need-to-know principle. We also use MFA to protect accounts. In addition, Microsoft Entra ID enables automatic login on company-managed devices.

21. What data protection rights do you have?

Below, we list the rights to which you are entitled under data protection law and which you may assert against the controller at any time free of charge.

You can find out how to contact the data protection officer and the controller under point 1.

Right of access: You have the right to obtain information from us about the processing of your personal data.

Right to rectification: You have the right to request that we correct any inaccurate or incomplete personal data concerning you.

Right to erasure: You have the right to request the deletion of your data if the conditions specified in Art. 17 GDPR are met. After that, you can, for example, request the deletion of your data if it is no longer necessary for the purposes for which it was collected. You can also request deletion if we process your data on the basis of your consent and you later withdraw this consent.

Right to restriction of processing: You have the right to request the restriction of the processing of your data if the requirements of Art. 18 GDPR are met. This is the case, for example, if you dispute the accuracy of your data. For the duration of the verification of the accuracy of the data, you can then demand the restriction of processing.

Right to data portability: If the data processing is based on consent or performance of a contract and is also carried out using automated processing, you have the right to receive your data in a structured, commonly used and machine-readable format and to transmit it to another data processor.

Right to withdraw consent: If the processing is based on consent, you have the right to withdraw your consent at any time free of charge with effect for the future.

Right to lodge a complaint: You also have the right to lodge a complaint with a data protection supervisory authority regarding the processing of your data.

Right to object: Data subjects have the right to object to data processing at any time on grounds relating to their particular situation, provided that it is based on the legal basis of "legitimate interest". If data subjects make use of their right to object, the processing of their data will be discontinued, unless - in accordance with the legal requirements - compelling legitimate grounds for further processing can be proven which outweigh the rights of the data subjects.