Stand: Februar 2026

Informationen zum Datenschutz für Kollaboration und Kommunikation mittels Microsoft 365

Mit diesen Hinweisen informieren wir Sie über die Verarbeitung Ihrer personenbezogenen Daten mit Microsoft 365. Bei Microsoft 365 handelt es sich – abstrakt betrachtet – um eine Sammlung und Zusammenstellung verschiedenster Werkzeuge der Kollaboration, der Sicherheit, des Datenschutzes, der Verarbeitung von verschiedensten Daten und in der Plattform erstellter Anwendungen. Der Kern dieser Zusammenstellung umfasst vor allem die Werkzeuge

- Exchange Online (E-Mail, Kalender, Adressbuch, Aufgaben),
- OneDrive und SharePoint Online (Speicherung, Verarbeitung, Applikationsplattform) und
- Microsoft Teams (Kollaboration, Chat, Meeting und Telefonie).

Im Rahmen dieses Produktportfolios finden Sie eine genauere Aufstellung der eingesetzten Produkte im Anhang 1 dieses Dokumentes.
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 gehören Applikationen.

1. Wer ist für die Datenverarbeitung verantwortlich?

Verantwortlicher im Sinne des Datenschutzrechts ist der jeweiligen Gesellschaft in der Unternehmensgruppe der **Württembergische Gemeinde-Versicherung a.G.** in Folge WGV genannt.

Württembergische Gemeinde-Versicherung a.G.

Tübinger Str. 55
70178 Stuttgart

Bei datenschutzbezogenen Fragen wenden Sie sich bitte an den Datenschutzbeauftragten der WGV Gruppe:

Tübinger Str. 55
70178 Stuttgart
E-Mail: Datenschutzbeauftragter@wgv.de

Der oben benannte Datenschutzbeauftragte ist der Datenschutzbeauftragte für alle Unternehmen der WGV Gruppe.

WGV Gruppe

Gemeinsamen Verantwortlichkeit nach Art. 26 II 2 der Datenschutz-Grundverordnung (DS-GVO):

- Württembergische Gemeinde-Versicherung a.G.
- WGV-Informatik und Media GmbH
- WGV Versicherung AG
- WGV-Lebensversicherung AG
- WGV Rechtsschutz-Schadenservice GmbH

Weitere Verantwortlichkeit:

- WGV-Beteiligungsgesellschaft mbH
- WGV Holding AG
- Stiftung der Württembergische Gemeinde-Versicherung a.G

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

Zweck der Verarbeitung

Der Zweck der Verarbeitung ist die Bereitstellung eines modernen Arbeitsplatzes mit Microsoft 365 zu einer optimalen Kollaboration und Kommunikation innerhalb und außerhalb der WGV Gruppe. Dazu zählt auch die Bereitstellung, 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.

3. Welche Arten von personenbezogenen Daten werden verarbeitet?

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 M365-Benutzerkonto der WGV Gruppe) sowie nicht User-ID-basierten Vorgängen (Business2Business-User, z. B. externe Personen ohne M365-Benutzerkonto der WGV Gruppe) 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, Transskript 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. **Systemgenerierte 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 notwenige 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 betroffen sein von der Verarbeitung bei Microsoft 365:

Zusammenfassung der Personenkategorien:

- Beschäftigte
- Ehemalige Beschäftigte
- Azubis und Studierende
- Leads
- Kunden/Versicherungsnehmer
- Lieferanten/Dienstleister

5. Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten

Die Rechtsgrundlage für den Betrieb von Microsoft 365:

- 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. c) b) f) DSGVO i.V.m. entsprechenden Verträgen und gesetzlichen Grundlagen wie VVG, DORA;

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). Bei speziellen Aufnahmen, wie zum Beispiel für Trainings und Schulungen oder Werbevideos wird auch einen Modelvertag (Art. 6 Abs. 1 lit. b DSGVO) als Rechtsgrundlage genutzt.

6. Verarbeitungen in Einzelnen

Identitätsmanagement

Im Rahmen des Identitätsmanagements mit Azure Active Directory (AAD) werden zentral Identitäten, Geräte und Applikationen zentral in Microsoft 365 verarbeitet. Insbesondere werden alle mit Microsoft 365 verknüpften Identitäten mit der Umgebung der WGV Gruppe 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 Beschäftigen
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)
Art. 6 Abs. 1 S. 1 lit. c) b) f) DSGVO i.V.m. entsprechenden Verträgen, § 34 VVG, DORA	Externe Benutzergruppen und Verwaltung von B2B

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 mit dem Beschäftigungsverhältnis (Art. 88 DSGVO)	Beschäftigte, BewerberInnen
Art. 6 Abs. 1 S. 1 lit. b) DSGVO	Externe Personen, zur Vertragsverfüllung oder Vertragsanbahnung
Art. 6 Abs. 1 S. 1 lit. b) DSGVO	Externe Personen und Beschäftigte von Unternehmen

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 mit dem Beschäftigungsverhältnis	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), f) DSGVO	Externe Personen
Art. 6 Abs. 1 S. 1 lit. a) DSGVO, Art 88 DSGVO	Bild des Beschäftigen, Audiodateien

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. b DSGVO mit dem Beschäftigungsverhältnis	Beschäftigte, BewerberInnen
Art. 6 Abs. 1 S. 1 lit. a) DSGVO	Onlinebewerbungsbespräche mit BewerberInnen
Art. 6 Abs. 1 S. 1 lit. b), a) DSGVO	GeschäftspartnerInnen
Art. 6 Abs. 1 S. 1 lit. a), bzw. f) DSGVO Art. 6 Abs. 1 S. 1 lit. a) DSGVO	Externe Personen und Personen von externen Unternehmen
Art. 6 Abs. 1 S. 1 lit. b), a) DSGVO	Anwesenheitsberichte Löschung 90 Tage nach Ende der Besprechung

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) DSGVO mit dem Beschäftigungsverhältnis	Beschäftigte, BewerberInnen
Art. 6 Abs. 1 S. 1 lit. b), a) DSGVO	Geschäftspartner/Innen
Art. 6 Abs. 1 S. 1 lit. a) DSGVO	Externe Personen
Art. 6 Abs. 1 S. 1 lit. a) DSGVO	Beschäftigte im Bilderupload

Kommunikation: Townhall Meeting

Im Rahmen der größeren Videokonferenzen als Live Stream mittels Microsoft Teams werden wenige personenbezogene Daten verarbeitet.

Art. 6 Abs. 1 S. 1. lit. b) DSGVO mit dem Beschäftigungsverhältnis	Beschäftigte, BewerberInnen
Art. 6 Abs. 1 S. 1 lit. b), a) DSGVO in Verbindung mit dem Dienstleistungs- oder Werkvertrag	Geschäftspartner/Innen
Art. 6 Abs. 1 S. 1 lit. a), f) DSGVO	Externe Personen

Kommunikation: Aufnahme von Besprechungen

Eine Aufnahme von Besprechungen beinhaltet die Aufnahme von Video, Audio und auch die direkte Transkription der Besprechung.

Art. 6 Abs. 1 S. 1. lit. b), a) DSGVO i.V. mit dem Beschäftigungsverhältnis	Beschäftigte, BewerberInnen
Art. 6 Abs. 1 S. 1 lit. b), a) DSGVO	Geschäftspartner/Innen
Art. 6 Abs. 1 S. 1 lit. a) DSGVO	Externe Personen
Art. 6 Abs. 1 S. 1. lit. a) DSGVO (Einwilligung)	Alle Betroffene

Kommunikation: Besprechungen mit sensiblen Datenklassen

Im Rahmen der sicheren verschlüsselten Videokonferenzen kann es zu der Verarbeitungen von sensiblen Daten der Art 9,10 DSGVO kommen. Dies gilt beispielsweise für Wiedereingliederung, Mitarbeitergespräche, Gespräche mit Versicherungsnehmern und Compliance-, sowie Rechtsschutzfälle.

Art. 6 Abs. 1 S. 1. lit. a) DSGVO, Art. 9 Abs. 2 lit. a DSGVO	Beschäftigte
Art. 6 Abs. 1 S. 1 lit. a) DSGVO , Art. 9 Abs. 2 lit. a DSGVO	Geschäftspartner/Innen
Art. 6 Abs. 1 S. 1 lit. a) DSGVO , Art. 9 Abs. 2 lit. a DSGVO	Kunden/Versicherungsnehmer

Werkzeuge für Beschäftige zur Unterstützung des Arbeitsalltages

Im Rahmen der Microsoft 365 Nutzung werden Werkzeuge zur Unterstützung der Arbeitsorganisation bereitgestellt. Diese können vom Beschäftigten ein und ausgeschaltet werden.

Art. 6 Abs. 1 S. 1. lit. a) DSGVO	Beschäftigte, BewerberInnen

Sachbearbeitung und Schadensregulierung

Die Sachbearbeitung im Versicherungswesen umfasst die sorgfältige Prüfung und Bearbeitung von Kundenanfragen sowie die Verwaltung aller relevanten Vertragsunterlagen. Dazu gehört auch die Erstellung neuer Versicherungsverträge, bei der individuelle Risiken bewertet und passende Tarife ausgewählt werden. Im Schadenfall übernimmt die Schadensregulierung die Bewertung eingereichter Schadensmeldungen, prüft Anspruchsgrundlagen und sorgt für eine schnelle und transparente Abwicklung, so dass Kundinnen und Kunden zuverlässig unterstützt werden.

Art. 6 Abs. 1 S. 1. lit. b) i.V.m. Arbeitsvertrag, i.V.m. Art 88 DSGVO	Beschäftigte
Externe Benutzergruppen Art. 6 Abs. 1 S. 1 lit. c) b) f) DSGVO i.V.m. entsprechenden Verträgen und iVm VVG, DORA	Kunden und Externe

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 Antivir über Antispam und Schutz von Emails und deren Anhängen.

Datenkategorien

1-11

Rechtsgrundlagen

Art. 6 Abs. 1 S. 1. lit. b), f) DSGVO	Beschäftigte, Bewerberinnen
Art. 6 Abs. 1 S. 1 lit. b), f) DSGVO	Externe Personen
Art. 6 Abs. 1 S. 1 lit. b), f) DSGVO	DienstleisterInnen

Desweiteren stellen wir in der Rechtsgrundlage Art. 6 Abs. 1 S. 1 lit. c DSGVO in Verbindung mit DORA und VAIT auf eine gesetzliche Pflicht hin zur Nachvollziehbarkeit, Cyberabwehr und Sicherheit der IT-Anwendung im Versicherungsbetrieb für alle Betroffenengruppen ab.

Defender für Endpunkt

Microsoft Defender für Endpunkt ist eine Endpunkt-Sicherheitsplattform für Unternehmen, die Unternehmensnetzwerken dabei helfen soll, erweiterte Bedrohungen zu verhindern, zu erkennen, zu untersuchen und auf Sie zu reagieren.“

Defender for Office 365

Microsoft Defender for Office 365 ist ein cloudbasierter E-Mail-Filterdienst, der Ihre Organisation vor erweiterten Bedrohungen für E-Mail- und Zusammenarbeitstools wie Phishing, Kompromittierung geschäftlicher E-Mails und Malwareangriffe schützt. Defender for Office 365 bietet auch Untersuchungs-, Hunting- und Wartungsfunktionen, mit denen Sicherheitsteams Bedrohungen effizient identifizieren, priorisieren, untersuchen und darauf reagieren können.

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-Vorfalls.

- 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) e), 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 im Tenant reduziert. Ab Ende 2023 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
- TIA

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

Sofern eine Rechtsgrundlage oder Einwilligung zur Weitergabe Ihrer Daten existiert, werden Ihre Daten nur denjenigen Stellen zur Verfügung gestellt, die diese zur Erfüllung der oben genannten Zwecke benötigen. Dabei handelt es sich vorwiegend um Stellen innerhalb unseres Unternehmens eingesetzte Dienstleister (z.B. interne IT-Dienstleister und an Microsoft Ireland Operations Ltd.), Erfüllungsgehilfen sowie Gesellschaften innerhalb des Konzernverbundes. Sämtliche Empfänger sind ihrerseits zur Einhaltung des Datenschutzes verpflichtet.

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

Wir übermitteln Daten auf der Basis von Standardvertragsklauseln in Verbindung mit Vereinbarungen zur Auftragsverarbeitung. Dazu kommt eine Übermittlung der pseudonymisierten Telemetrie- und Diagnosedaten von Microsoft Irland zu Microsoft Corp. auf Basis von EU-Standardvertragsklauseln. Im Übrigen erfolgt keine Weitergabe an Empfänger in Drittländern, die kein der DSGVO entsprechendes Datenschutzniveau gewähren.

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 von Microsoft Irland zu Microsoft Corp. (USA) auf Basis von EU-Standardvertragsklauseln im Rahmen der pseudonymisierten Telemetrie- und Diagnosedaten, sowie Support und IT-Security Fälle. Für den Support wurde extra das Verfahren Customer Lockbox aktiviert, um einen Zugriff zu minimieren und zu kontrollieren.

9. Wie lange speichern wir Ihre Daten?

Wir speichern Ihre Daten so lange, wie dies zur Nutzung von Microsoft 365 erforderlich ist bzw. wir ein berechtigtes Interesse an der weiteren Speicherung haben. Hierzu zählt auch eine Speicherung nach gesetzlichen Verpflichtungen, wie § 147 AO und § 238 HGB, die durch Aufbewahrungsregeln bis zu 10 Jahre eingehalten werden.

Vom Anwender explizit freigegebene Positionsdaten bzw. Standortdaten werden ausschließlich während der Nutzung zur Verfügung gestellt. Weiterhin werden die Daten im Falle eines Verlusts von Hardware in Kenntnis der Nutzerinnen und Nutzern benötigt. Eine weitere Speicherung der Daten erfolgt nicht.

Metadaten von Anrufen und Besprechungen werden maximal 180 Tage gespeichert (abhängig vom Datum). Auch hier werden die Daten nach Ablauf der Fristen automatisch gelöscht.

Für Schulungen und Meetings über Microsoft Teams Besprechungen werden je nach Bedarf Teilnehmerberichte generiert, die nach 90 Tagen gelöscht werden.

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

Soweit ein Referent im Rahmen eines „Teams Live Events“ die Bild- und Tonaufzeichnung aktiviert, wird diese maximal 120 Tage nach der Veranstaltung gespeichert. Dies gilt auch für die Metadaten des Live Events, die dann automatisch gelöscht werden. Eine frühere Löschung ist auf Antrag des jeweils betroffenen Referenten möglich und wird vom Organisator des Events durchgeführt.

Bei „Teams Live Events“ werden eingereichte Fragen der Teilnehmer maximal 120 Tage nach der Veranstaltung gespeichert. Fragen können auch anonym gestellt werden. Die Daten werden vollständig als Teil der Aufzeichnung des jeweiligen Events aufbewahrt und zusammen mit der Aufzeichnung gelöscht.

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

Personenbezogene Daten, die in Sicherheitswerkzeugen und der IT-Sicherheit dienenden Werkzeugen gespeichert und verarbeitet werden, 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, z.B. wenn im Zusammenhang mit einem behördlichen oder gerichtlichen Verfahren ein sog. Litigation Hold (d.h. ein Verbot der Datenlöschung für die Dauer des Verfahrens) angeordnet wird (z. B. §§ 195ff. BGB).

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
- Pseudonymisierung von Berichten und Reports
- Automatisches Löschen von Daten in vordefinierten Zyklen

Die WGV hat ein Managementsystem für Datenschutz und Informationssicherheit implementiert und lassen dieses auf Grundlage der ISO 27001 regelmäßig extern auditieren.

11. Welche Datenschutzrechte haben Sie?

Im Folgenden informieren wir Sie über die Ihnen nach dem Datenschutzrecht zustehenden Rechte, die Sie gegenüber dem Verantwortlichen und dem jeweiligen Datenschutzbeauftragten jederzeit unentgeltlich geltend machen können.

Jede betroffene Person hat das Recht auf Auskunft nach Art. 15 DSGVO, das Recht auf Berichtigung nach Art. 16 DSGVO, das Recht auf Löschung nach Art. 17 DSGVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO, das Recht auf Widerspruch aus Art. 21 DSGVO, sowie das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO. Beim Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen nach §§ 34 und 35 BDSG. Darüber hinaus besteht ein Beschwerderecht bei der zuständigen Datenschutzaufsichtsbehörde (Art. 77 DSGVO i. V. m. § 19 BDSG).

Eine erteilte Einwilligung in die Verarbeitung personenbezogener Daten können Sie jederzeit uns gegenüber widerrufen. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die vor der Geltung der DSGVO, also vor dem 25. Mai 2018 uns gegenüber erteilt worden sind. Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

Gibt es Ihrerseits eine Pflicht zur Bereitstellung von Daten?

Im Rahmen unserer Geschäftsbeziehung müssen Sie diejenigen personenbezogenen Daten bereitstellen, die für die Aufnahme und Durchführung einer Geschäftsbeziehung und die Erfüllung der damit verbundenen vertraglichen Pflichten erforderlich sind oder zu deren Erhebung wir gesetzlich verpflichtet sind.

Information über Ihr Widerspruchsrecht nach Art. 21 DSGVO

Einzelfallbezogenes Widerspruchsrecht

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 e) DSGVO (Datenverarbeitung im öffentlichen Interesse) und Art. 6 Abs. 1 f) DSGVO (Datenverarbeitung auf Grundlage einer Interessenabwägung) erfolgt, Widerspruch einzulegen. Legen Sie Widerspruch ein, werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten, es sie denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Recht und Freiheiten überwiegen, oder die Verarbeitungsdienst der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Die für uns zuständige Datenschutzaufsichtsbehörde ist:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg
Lautenschlagerstraße 20
70173 Stuttgart

Telefon: 0711 615541-0
Telefax: 0711 615541-15

E-Mail: poststelle@lfdi.bwl.de