

Geltungsbereich	2
Verantwortliche und Datenschutzbeauftragte	3
Allgemeine Hinweise	5
Cloud-Dienste	5
Management, Organisation und Hilfswerkzeuge.....	6
Kommunikation via Messenger	6
Single-Sign-On-Anmeldung.....	7
Videokonferenzen, Onlinemeetings, Webinare und Bildschirm-Sharing.....	9
Meldung schädlicher Anrufe in Microsoft Teams	10
Bezug von Applikationen über Appstores	10
Künstliche Intelligenz (KI)	11
Dienstanbieter.....	12
Für den Verband.....	12
Für die Einrichtungen	12
Berechtigte Interessen	12
Ihre Rechte und weitere Informationen zum Datenschutz.....	13

Geltungsbereich

Diese Datenschutzerklärung gilt für alle Beschäftigten der Verbandsfamilie.

- Genoverband e.V. (im Folgenden Verband)
- AWADO GmbH Wirtschaftsprüfungsgesellschaft
- AWADO Bankenberatung GmbH
- AWADO Mittelstandsberatung GmbH
- AWADO Kommunikationsberatung GmbH
- AWADO Rechtsanwaltsgesellschaft GmbH
- GenoAkademie GmbH & Co. KG
- GenoHotel GmbH
- GenoPersonalConsult GmbH
- Genossenschaftlicher Arbeitgeberverband Norddeutschland e. V.

Alle Unternehmen zusammen werden im Folgenden „Verbandsfamilie“ genannt. Alle übrigen Unternehmen der Verbandsfamilie werden im Folgenden „Einrichtungen“ genannt. Soweit nicht ausdrücklich erwähnt, gelten die nachfolgenden Ausführungen für alle Unternehmen der Verbandsfamilie.

Sie gelten außerdem für externe Nutzer, insbesondere Mitglieder, Kunden, Geschäfts- und Vertragspartner, Interessenten, Dienstleister und Lieferanten der Verbandsfamilie.

Verantwortliche und Datenschutzbeauftragte

Verantwortlicher im Sinne der Datenschutz-Grundverordnung ist jeweils das Unternehmen der Verbandsfamilie, das über die Zwecke und Mittel der konkreten Verarbeitung personenbezogener Daten entscheidet. Die Kontaktdaten der Unternehmen und ihrer Datenschutzbeauftragten, soweit benannt, lauten:

Genoverband e.V.

Kontakt: Wilhelm-Haas-Platz, 63263 Neu-Isenburg; Telefon: 069 6978-0; E-Mail: kontakt@genoverband.de.

Datenschutzbeauftragter: Genoverband e.V. – Datenschutzbeauftragter –, Wilhelm-Haas-Platz, 63263 Neu-Isenburg; E-Mail: datenschutz@genoverband.de.

AWADO Bankenberatung GmbH

Kontakt: Wilhelm-Haas-Platz, 63263 Neu-Isenburg; Telefon: 069 6978-3349; E-Mail: bankenberatung@awado-gruppe.de.

Datenschutzbeauftragter: AWADO Bankenberatung GmbH – Datenschutzbeauftragter –, Wilhelm-Haas-Platz, 63263 Neu-Isenburg; E-Mail: datenschutz@awado-gruppe.de.

AWADO GmbH Wirtschaftsprüfungsgesellschaft

Kontakt: Wilhelm-Haas-Platz, 63263 Neu-Isenburg; Telefon: 069 6978-3349; E-Mail: info@awado-gruppe.de.

Datenschutzbeauftragter: AWADO GmbH Wirtschaftsprüfungsgesellschaft – Datenschutzbeauftragter –, Wilhelm-Haas-Platz, 63263 Neu-Isenburg; E-Mail: datenschutz@awado-gruppe.de.

AWADO Kommunikationsberatung GmbH

Kontakt: Ludwig-Erhard-Allee 20, 40227 Düsseldorf; Telefon: 0211 16091-4900; E-Mail: akb@awado-gruppe.de.

Datenschutzbeauftragter: AWADO Kommunikationsberatung GmbH – Datenschutzbeauftragter –, Ludwig-Erhard-Allee 20, 40227 Düsseldorf; E-Mail: datenschutz@awado-gruppe.de.

AWADO Mittelstandsberatung GmbH

Kontakt: Linkstraße 12, 10785 Berlin; Telefon: 030 264727079; E-Mail: info-amb@awado-gruppe.de.

Datenschutzbeauftragter: AWADO Mittelstandsberatung GmbH – Datenschutzbeauftragter –, Linkstraße 12, 10785 Berlin; E-Mail: datenschutz@awado-gruppe.de.

AWADO Rechtsanwaltsgesellschaft GmbH

Kontakt: Wilhelm-Haas-Platz, 63263 Neu-Isenburg; Telefon: 069 6978-3385; E-Mail: info@awado-rag.de.

Datenschutzbeauftragter: AWADO Rechtsanwaltsgesellschaft GmbH – Datenschutzbeauftragter –, Wilhelm-Haas-Platz, 63263 Neu-Isenburg; E-Mail: datenschutz@awado-gruppe.de.

GenoAkademie GmbH & Co. KG

Kontakt: Raiffeisenstraße 10–16, 51503 Rösrath-Forsbach; Telefon: 02205 803-9500; E-Mail: ksc@genoakademie.de.

Datenschutzbeauftragter: GenoAkademie GmbH & Co. KG – Datenschutzbeauftragter –, Raiffeisenstraße 10–16, 51503 Rösrath-Forsbach; E-Mail: datenschutz@genoakademie.de.

GenoHotel Baunatal GmbH

Kontakt: Schulze-Delitzsch-Straße 2, 34225 Baunatal; Telefon: 05601 978-6000; E-Mail: info@genohotel-baunatal.de.

Datenschutzbeauftragter: In den ausgewerteten öffentlich zugänglichen Angaben ist kein gesonderter Kontakt veröffentlicht.

GenoPersonalConsult GmbH

Kontakt: Wilhelm-Haas-Platz, 63263 Neu-Isenburg; Telefon: 069 6978-3129; E-Mail: kontakt@gpconsult.de.

Datenschutzbeauftragter: GenoPersonalConsult GmbH – Datenschutzbeauftragter –, Wilhelm-Haas-Platz, 63263 Neu-Isenburg; E-Mail: datenschutz@genoverband.de.

Genossenschaftlicher Arbeitgeberverband Norddeutschland e. V.

Kontakt: Mailänder Straße 4 a, 30539 Hannover; Telefon: 0511 9574-5500; E-Mail: info@gav-nord.de.

Datenschutzbeauftragter: Ein Datenschutzbeauftragter ist nicht benannt.

Allgemeine Hinweise

Zusätzlich zu unseren bisherigen Datenschutzhinweisen möchten wir Sie an dieser Stelle über den Einsatz von Microsoft 365 informieren. Informationen zu Ihren Rechten und Ansprechpartnern entnehmen Sie bitte den allgemeinen Datenschutzhinweisen Ihres Arbeitgebers.

Bei der Nutzung der M365 werden personenbezogene Daten über Sie verarbeitet. Bitte beachten Sie, dass dieser Datenschutzhinweis Sie nur über die Verarbeitung Ihrer personenbezogenen Daten durch uns informiert, wenn Sie gemeinsam mit uns Anwendungen von Microsoft nutzen oder Daten zu Ihrer Person in der Cloud von Microsoft verarbeiten. Falls Sie Informationen über die Verarbeitung durch Microsoft benötigen, bitten wir Sie die entsprechende Erklärung unter folgendem Link einzusehen.:

<https://privacy.microsoft.com/de-de/privacystatement>

Cloud-Dienste

Wir nutzen über das Internet zugängliche und auf den Servern ihrer Anbieter ausgeführte Softwaredienste (sogenannte "Cloud-Dienste", auch bezeichnet als "Software as a Service") für die Speicherung und Verwaltung von Inhalten (z. B. Dokumentenspeicherung und -verwaltung, Austausch von Dokumenten, Inhalten und Informationen mit bestimmten Empfängern oder Veröffentlichung von Inhalten und Informationen).

In diesem Rahmen können personenbezogenen Daten verarbeitet und auf den Servern der Anbieter gespeichert werden, soweit diese Daten Bestandteil von Verarbeitungsvorgängen durch uns sind. Zu diesen Daten können insbesondere Stammdaten und Kontaktdaten der Nutzer, Daten zu Vorgängen, Verträgen, sonstigen Prozessen und deren Inhalte gehören. Die Anbieter der Cloud-Dienste verarbeiten ferner Nutzungsdaten und Metadaten, die von dort zu Sicherheitszwecken und zur Serviceoptimierung verwendet werden.

Sofern wir mit Hilfe der Cloud-Dienste für andere Nutzer oder öffentlich zugängliche Webseiten Formulare o.a. Dokumente und Inhalte bereitstellen, können die Anbieter Cookies auf den Geräten der Nutzer für Zwecke der Webanalyse oder, um sich Einstellungen der Nutzer (z. B. im Fall der Mediensteuerung) zu merken, speichern.

- **Verarbeitete Datenarten:** Bestandsdaten (z. B. Namen, Adressen); Kontaktdaten (z. B. E-Mail, Telefonnummern); Inhaltsdaten (z. B. Eingaben in Onlineformularen); Nutzungsdaten (z. B. besuchte Webseiten, Interesse an Inhalten, Zugriffszeiten); Meta-, Kommunikations- und Verfahrensdaten (z. B. IP-Adressen, Zeitangaben, Identifikationsnummern, Einwilligungsstatus).
- **Betroffene Personen:** Kunden; Beschäftigte (z. B. Angestellte, Bewerber, ehemalige Mitarbeiter); Interessenten; Kommunikationspartner; Mitglieder; Geschäfts- und Vertragspartner; Dienstleister; Lieferanten.
- **Zwecke der Verarbeitung:** Büro- und Organisationsverfahren; Informationstechnische Infrastruktur (Betrieb und Bereitstellung von Informationssystemen und technischen Geräten (Computer, Server etc.).).
- **Rechtsgrundlagen:** Berechtigte Interessen (Art. 6 Abs. 1 S. 1 lit. f) DSGVO).

Management, Organisation und Hilfswerkzeuge

Wir setzen Dienstleistungen, Plattformen und Software anderer Anbieter (nachfolgend bezeichnet als "Drittanbieter") zu Zwecken der Organisation, Verwaltung, Planung sowie Erbringung unserer Leistungen ein. Bei der Auswahl der Drittanbieter und ihrer Leistungen beachten wir die gesetzlichen Vorgaben.

In diesem Rahmen können personenbezogenen Daten verarbeitet und auf den Servern der Drittanbieter gespeichert werden. Hiervon können diverse Daten betroffen sein, die wir entsprechend dieser Datenschutzerklärung verarbeiten. Zu diesen Daten können insbesondere Stammdaten und Kontaktdaten der Nutzer, Daten zu Vorgängen, Verträgen, sonstigen Prozessen und deren Inhalte gehören.

Sofern Nutzer im Rahmen der Kommunikation, von Geschäfts- oder anderen Beziehungen mit uns auf die Drittanbieter bzw. deren Software oder Plattformen verwiesen werden, können die Drittanbieter Nutzungsdaten und Metadaten zu Sicherheitszwecken, zur Serviceoptimierung oder zu Marketingzwecken verarbeiten. Wir bitten daher darum, die Datenschutzhinweise der jeweiligen Drittanbieter zu beachten.

- **Verarbeitete Datenarten:** Inhaltsdaten (z. B. Eingaben in Onlineformularen); Nutzungsdaten (z. B. besuchte Webseiten, Interesse an Inhalten, Zugriffszeiten); Meta-, Kommunikations- und Verfahrensdaten (z. B. IP-Adressen, Zeitangaben, Identifikationsnummern, Einwilligungsstatus); Kontaktdaten (z. B. E-Mail, Telefonnummern).
- **Betroffene Personen:** Kommunikationspartner; Nutzer (z. B. Webseitenbesucher, Nutzer von Onlinediensten); Kunden; Beschäftigte (z. B. Angestellte, Bewerber, ehemalige Mitarbeiter); Interessenten; Mitglieder; Geschäfts- und Vertragspartner; Dienstleister; Lieferanten.
- **Zwecke der Verarbeitung:** Erbringung vertraglicher Leistungen und Erfüllung vertraglicher Pflichten; Büro- und Organisationsverfahren; Kontaktanfragen und Kommunikation.
- **Rechtsgrundlagen:** Berechtigte Interessen (Art. 6 Abs. 1 S. 1 lit. f) DSGVO).

Kommunikation via Messenger

Wir setzen zu Zwecken der Kommunikation Messenger ein und bitten daher darum, die nachfolgenden Hinweise zur Funktionsfähigkeit der Messenger, zur Verschlüsselung, zur Nutzung der Metadaten der Kommunikation und zu Ihren Widerspruchsmöglichkeiten zu beachten.

Sie können uns auch auf alternativen Wegen, z. B. via Telefon oder E-Mail, kontaktieren. Bitte nutzen Sie die Ihnen mitgeteilten Kontaktmöglichkeiten oder die innerhalb unseres Onlineangebotes angegebenen Kontaktmöglichkeiten.

Im Fall einer Ende-zu-Ende-Verschlüsselung von Inhalten (d. h., der Inhalt Ihrer Nachricht und Anhänge) weisen wir darauf hin, dass die Kommunikationsinhalte (d. h., der Inhalt der Nachricht und angehängte Bilder) von Ende zu Ende verschlüsselt werden. Das bedeutet, dass der Inhalt der Nachrichten nicht einsehbar ist, nicht einmal durch die Messenger-Anbieter selbst. Sie sollten immer eine aktuelle Version der Messenger mit aktivierter Verschlüsselung nutzen, damit die Verschlüsselung der Nachrichteninhalte sichergestellt ist.

Wir weisen unsere Kommunikationspartner jedoch zusätzlich darauf hin, dass die Anbieter der Messenger zwar nicht den Inhalt einsehen, aber in Erfahrung bringen können, dass und wann Kommunikationspartner mit uns kommunizieren sowie technische Informationen zum verwendeten Gerät der Kommunikationspartner und je nach Einstellungen ihres Gerätes auch Standortinformationen (sogenannte Metadaten) verarbeitet werden.

Hinweise zu Rechtsgrundlagen: Sofern wir Kommunikationspartner vor der Kommunikation mit ihnen via Messenger um eine Erlaubnis bitten, ist die Rechtsgrundlage unserer Verarbeitung ihrer Daten deren Einwilligung. Im Übrigen, falls wir nicht um eine Einwilligung bitten und sie z. B. von sich aus Kontakt mit uns aufnehmen, nutzen wir Messenger im Verhältnis zu unseren Vertragspartnern sowie im Rahmen der Vertragsanbahnung als eine vertragliche Maßnahme und im Fall anderer Interessenten und Kommunikationspartner auf Grundlage unserer berechtigten Interessen an einer schnellen und effizienten Kommunikation und Erfüllung der Bedürfnisse unser Kommunikationspartner an der Kommunikation via Messenger. Ferner weisen wir Sie darauf hin, dass wir die uns mitgeteilten Kontaktdaten ohne Ihre Einwilligung nicht erstmalig an die Messenger übermitteln.

Widerruf, Widerspruch und Löschung: Sie können jederzeit eine erteilte Einwilligung widerrufen und der Kommunikation mit uns via Messenger jederzeit widersprechen. Im Fall der Kommunikation via Messenger löschen wir die Nachrichten entsprechend unseren generellen Löschrichtlinien (d. h. z. B., wie oben beschrieben, nach Ende vertraglicher Beziehungen, im Kontext von Archivierungsvorgaben etc.) und sonst, sobald wir davon ausgehen können, etwaige Auskünfte der Kommunikationspartner beantwortet zu haben, wenn kein Rückbezug auf eine vorhergehende Konversation zu erwarten ist und der Löschung keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Vorbehalt des Verweises auf andere Kommunikationswege: Zum Abschluss möchten wir darauf hinweisen, dass wir uns aus Gründen Ihrer Sicherheit vorbehalten, Anfragen über Messenger nicht zu beantworten. Das ist der Fall, wenn z. B. Vertragsinterna besonderer Geheimhaltung bedürfen oder eine Antwort über Messenger den formellen Ansprüchen nicht genügt. In solchen Fällen verweisen wir Sie auf adäquatere Kommunikationswege.

- **Verarbeitete Datenarten:** Kontaktdaten (z. B. E-Mail, Telefonnummern); Nutzungsdaten (z. B. besuchte Webseiten, Interesse an Inhalten, Zugriffszeiten); Meta-, Kommunikations- und Verfahrensdaten (z. B. IP-Adressen, Zeitangaben, Identifikationsnummern, Einwilligungsstatus); Inhaltsdaten (z. B. Eingaben in Onlineformularen).
- **Betroffene Personen:** Kommunikationspartner.
- **Zwecke der Verarbeitung:** Kontaktanfragen und Kommunikation; Direktmarketing (z. B. per E-Mail oder postalisch).
- **Rechtsgrundlagen:** Einwilligung (Art. 6 Abs. 1 S. 1 lit. a) DSGVO); Berechtigte Interessen (Art. 6 Abs. 1 S. 1 lit. f) DSGVO).

Single-Sign-On-Anmeldung

Als "Single-Sign-On" oder "Single-Sign-On-Anmeldung bzw. "-Authentifizierung" werden Verfahren bezeichnet, die es Nutzern erlauben, sich mit Hilfe eines Nutzerkontos bei einem

Anbieter von Single-Sign-On-Verfahren (z. B. einem sozialen Netzwerk), auch bei unserem Onlineangebot, anzumelden. Voraussetzung der Single-Sign-On-Authentifizierung ist, dass die Nutzer bei dem jeweiligen Single-Sign-On-Anbieter registriert sind und die erforderlichen Zugangsdaten in dem dafür vorgesehenen Onlineformular eingeben, bzw. schon bei dem Single-Sign-On-Anbieter angemeldet sind und die Single-Sign-On-Anmeldung via Schaltfläche bestätigen.

Die Authentifizierung erfolgt direkt bei dem jeweiligen Single-Sign-On-Anbieter. Im Rahmen einer solchen Authentifizierung erhalten wir eine Nutzer-ID mit der Information, dass der Nutzer unter dieser Nutzer-ID beim jeweiligen Single-Sign-On-Anbieter eingeloggt ist und eine für uns für andere Zwecke nicht weiter nutzbare ID (sog "User Handle"). Ob uns zusätzliche Daten übermittelt werden, hängt allein von dem genutzten Single-Sign-On-Verfahren ab, von den gewählten Datenfreigaben im Rahmen der Authentifizierung und zudem davon, welche Daten Nutzer in den Privatsphäre- oder sonstigen Einstellungen des Nutzerkontos beim Single-Sign-On-Anbieter freigegeben haben. Es können je nach Single-Sign-On-Anbieter und der Wahl der Nutzer verschiedene Daten sein, in der Regel sind es die E-Mail-Adresse und der Benutzername. Das im Rahmen des Single-Sign-On-Verfahrens eingegebene Passwort bei dem Single-Sign-On-Anbieter ist für uns weder einsehbar, noch wird es von uns gespeichert.

Die Nutzer werden gebeten, zu beachten, dass deren bei uns gespeicherte Angaben automatisch mit ihrem Nutzerkonto beim Single-Sign-On-Anbieter abgeglichen werden können, dies jedoch nicht immer möglich ist oder tatsächlich erfolgt. Ändern sich z. B. die E-Mail-Adressen der Nutzer, müssen sie diese manuell in ihrem Nutzerkonto bei uns ändern.

Die Single-Sign-On-Anmeldung können wir, sofern mit den Nutzern vereinbart, im Rahmen der oder vor der Vertragserfüllung einsetzen, soweit die Nutzer darum gebeten wurden, im Rahmen einer Einwilligung verarbeiten und setzen sie ansonsten auf Grundlage der berechtigten Interessen unsererseits und der Interessen der Nutzer an einem effektiven und sicheren Anmeldesystem ein.

Sollten Nutzer sich einmal entscheiden, die Verknüpfung ihres Nutzerkontos beim Single-Sign-On-Anbieter nicht mehr für das Single-Sign-On-Verfahren nutzen zu wollen, müssen sie diese Verbindung innerhalb ihres Nutzerkontos beim Single-Sign-On-Anbieter aufheben. Möchten Nutzer deren Daten bei uns löschen, müssen sie ihre Registrierung bei uns kündigen.

- **Verarbeitete Datenarten:** Bestandsdaten (z. B. Namen, Adressen); Kontaktdaten (z. B. E-Mail, Telefonnummern); Nutzungsdaten (z. B. besuchte Webseiten, Interesse an Inhalten, Zugriffszeiten); Meta-, Kommunikations- und Verfahrensdaten (z. B. IP-Adressen, Zeitangaben, Identifikationsnummern, Einwilligungsstatus).
- **Betroffene Personen:** Nutzer (z. B. Webseitenbesucher, Nutzer von Onlinediensten).
- **Zwecke der Verarbeitung:** Erbringung vertraglicher Leistungen und Erfüllung vertraglicher Pflichten; Sicherheitsmaßnahmen; Anmeldeverfahren.
- **Rechtsgrundlagen:** Berechtigte Interessen (Art. 6 Abs. 1 S. 1 lit. f) DSGVO).

Videokonferenzen, Onlinemeetings, Webinare und Bildschirm-Sharing

Wir setzen Plattformen und Anwendungen anderer Anbieter (nachfolgend bezeichnet als "Konferenzplattformen") zu Zwecken der Durchführung von Video- und Audio-Konferenzen, Webinaren und sonstigen Arten von Video und Audio-Meetings (nachfolgend zusammenfassend bezeichnet als "Konferenz") ein. Bei der Auswahl der Konferenzplattformen und ihrer Leistungen beachten wir die gesetzlichen Vorgaben.

Durch Konferenzplattformen verarbeitete Daten: Im Rahmen der Teilnahme an einer Konferenz verarbeiten die Konferenzplattformen die im Folgenden genannten personenbezogene Daten der Teilnehmer. Der Umfang der Verarbeitung hängt zum einen davon ab, welche Daten im Rahmen einer konkreten Konferenz gefordert werden (z. B. Angabe von Zugangsdaten oder Klarnamen; bei einmaliger Anmeldung ist der Name frei wählbar) und welche optionalen Angaben durch die Teilnehmer getätigt werden. Neben der Verarbeitung zur Durchführung der Konferenz, können die Daten der Teilnehmer durch die Konferenzplattformen ebenfalls zu Sicherheitszwecken oder Serviceoptimierung verarbeitet werden. Zu den verarbeiteten Daten gehören Daten zur Person (Vorname, Nachname), Kontaktinformationen (E-Mail-Adresse, Telefonnummer), Zugangsdaten (Zugangscode oder Passwörter), Profilbilder, Angaben zur beruflichen Stellung/Funktion, die IP-Adresse des Internetzugangs, Angaben zu den Endgeräten der Teilnehmer, deren Betriebssystem, dem Browser und dessen technischen und sprachlichen Einstellungen, Informationen zu den inhaltlichen Kommunikationsvorgängen, d. h. Eingaben in Chats sowie Audio- und Videodaten, als auch die Nutzung anderer zur Verfügung stehender Funktionen (z. B. Umfragen). Inhalte der Kommunikationen werden in dem durch die Konferenzanbieter technisch bereitgestellten Umfang verschlüsselt. Wenn die Teilnehmer bei den Konferenzplattformen als Benutzer registriert sind, dann können weitere Daten entsprechend der Vereinbarung mit dem jeweiligen Konferenzanbieter verarbeitet werden.

Protokollierung und Aufnahmen: Falls Texteingaben, Teilnahmeergebnisse (z. B. von Umfragen) sowie Video- oder Audioaufnahmen protokolliert werden, wird dies den Teilnehmern im Vorwege transparent mitgeteilt und sie werden – soweit erforderlich – um eine Zustimmung gebeten.

Datenschutzmaßnahmen der Teilnehmer: Bitte beachten Sie zu den Details der Verarbeitung Ihrer Daten durch die Konferenzplattformen deren Datenschutzhinweise und wählen im Rahmen der Einstellungen der Konferenzplattformen, die für Sie optimalen Sicherheits- und Datenschutzeinstellungen. Bitte sorgen Sie ferner für die Dauer einer Videokonferenz für den Daten- und Persönlichkeitsschutz im Hintergrund Ihrer Aufnahme (z. B. durch Hinweise an Mitbewohner, Abschließen von Türen und Nutzung, soweit technisch möglich, der Funktion zur Unkenntlichmachung des Hintergrunds). Links zu den Konferenzräumen sowie Zugangsdaten, dürfen nicht an unberechtigte Dritte weitergegeben werden.

Hinweise zu Rechtsgrundlagen: Sofern neben den Konferenzplattformen auch wir die Daten der Nutzer verarbeiten und die Nutzer um deren Einwilligung in den Einsatz der

Konferenzplattformen oder bestimmter Funktionen bitten (z. B. Einverständnis mit einer Aufzeichnung von Konferenzen), ist die Rechtsgrundlage der Verarbeitung diese Einwilligung. Ferner kann unsere Verarbeitung zur Erfüllung unserer vertraglichen Pflichten erforderlich sein (z. B. in Teilnehmerlisten, im Fall von Aufarbeitung von Gesprächsergebnissen, etc.). Im Übrigen werden die Daten der Nutzer auf Grundlage unserer berechtigten Interessen an einer effizienten und sicheren Kommunikation mit unseren Kommunikationspartnern verarbeitet.

- **Verarbeitete Datenarten:** Bestandsdaten (z. B. Namen, Adressen); Kontaktdaten (z. B. E-Mail, Telefonnummern); Inhaltsdaten (z. B. Eingaben in Onlineformularen); Nutzungsdaten (z. B. besuchte Webseiten, Interesse an Inhalten, Zugriffszeiten); Meta-, Kommunikations- und Verfahrensdaten (z. B. IP-Adressen, Zeitangaben, Identifikationsnummern, Einwilligungsstatus).
- **Betroffene Personen:** Kommunikationspartner; Nutzer (z. B. Webseitenbesucher, Nutzer von Onlinediensten); Abgebildete Personen.
- **Zwecke der Verarbeitung:** Erbringung vertraglicher Leistungen und Erfüllung vertraglicher Pflichten; Kontaktanfragen und Kommunikation; Büro- und Organisationsverfahren.
- **Rechtsgrundlagen:** Berechtigte Interessen (Art. 6 Abs. 1 S. 1 lit. f) DSGVO).

Meldung schädlicher Anrufe in Microsoft Teams

Nutzerinnen und Nutzer können eingehende Anrufe in Microsoft Teams als schädlich (malicious) melden. Im Rahmen einer solchen Meldung werden folgende Daten erfasst:

- **Standardmäßig verfügbar:** Datum und Uhrzeit der Meldung; Name der meldenden Person; Name oder Bezeichnung des gemeldeten Anrufers (kann leer sein); Telefonnummer des gemeldeten Anrufs; Zeitstempel des Anrufbeginns.
- **Nur im Export verfügbar:** Meldungs-ID; Anrufdauer; Teilnehmerliste; Tenant-ID des Anrufers; Domänenname des Anrufers; Telefonnummer, Benutzer-ID und Tenant-ID der meldenden Person.

Der eigentliche Gesprächsinhalt wird nicht erfasst oder gespeichert.

Administratorinnen und Administratoren können die eingereichten Meldungen sowie die zugehörige Risikoeinstufung im Microsoft Admin Center einsehen; **ein Zugriff auf den Gesprächsinhalt erfolgt hierüber nicht.**

Rechtsgrundlage: Rechtsgrundlage der Verarbeitung ist Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Erkennung und Abwehr schädlicher bzw. betrügerischer Anrufe zum Schutz unserer Kommunikationsinfrastruktur und unserer Beschäftigten).

Die Verarbeitung der Meldedaten durch Microsoft erfolgt im Rahmen der bestehenden Auftragsverarbeitung auf Grundlage des mit Microsoft geschlossenen Data Protection Addendums (DPA) sowie unserer Weisungen. Microsoft verarbeitet die Daten ausschließlich zur Bereitstellung des Dienstes, zur Fehlerbehebung sowie zu vertraglich begrenzten Serviceverbesserungen. **Eine Nutzung zu Werbezwecken, zum Nutzerprofiling oder zur allgemeinen Marktforschung findet nicht statt.**

Bezug von Applikationen über Appstores

Der Bezug unserer Applikation erfolgt über spezielle Online-Plattformen, die von anderen Diensteanbietern betrieben werden, an (so genannte "Appstores"). In diesem Zusammenhang gelten zusätzlich zu unseren Datenschutzhinweisen die Datenschutzhinweise der jeweiligen Appstores. Dies gilt insbesondere im Hinblick auf die auf den Plattformen eingesetzten Verfahren zur Reichweitemessung und zum interessenbezogenen Marketing sowie etwaige Kostenpflicht.

- **Verarbeitete Datenarten:** Bestandsdaten (z. B. Namen, Adressen); Zahlungsdaten (z. B. Bankverbindungen, Rechnungen, Zahlungshistorie); Kontaktdaten (z. B. E-Mail, Telefonnummern); Vertragsdaten (z. B. Vertragsgegenstand, Laufzeit, Kundenkategorie); Nutzungsdaten (z. B. besuchte Webseiten, Interesse an Inhalten, Zugriffszeiten); Meta-, Kommunikations- und Verfahrensdaten (z. B. IP-Adressen, Zeitangaben, Identifikationsnummern, Einwilligungsstatus); Inhaltsdaten (z. B. Eingaben in Onlineformularen).
- **Betroffene Personen:** Kunden; Nutzer (z. B. Webseitenbesucher, Nutzer von Onlinediensten).
- **Zwecke der Verarbeitung:** Erbringung vertraglicher Leistungen und Erfüllung vertraglicher Pflichten; Marketing.
- **Rechtsgrundlagen:** Berechtigte Interessen (Art. 6 Abs. 1 S. 1 lit. f) DSGVO).

Künstliche Intelligenz (KI)

Wir setzen Künstliche Intelligenz (KI) ein, wobei personenbezogene Daten verarbeitet werden. Die spezifischen Zwecke und unser Interesse am Einsatz der KI werden nachfolgend genannt. Unter KI verstehen wir entsprechend dem Begriff eines "KI-Systems" gemäß Artikel 3 Nr. 1 der KI-Verordnung ein maschinengestütztes System, das für einen in wechselndem Maße autonomen Betrieb ausgelegt ist, nach seiner Einführung anpassungsfähig sein kann und aus den erhaltenen Eingaben Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen hervorbringt, die physische oder virtuelle Umgebungen beeinflussen können.

Unsere KI-Systeme werden unter strikter Beachtung der gesetzlichen Vorgaben eingesetzt. Diese umfassen sowohl spezifische Regelungen für Künstliche Intelligenz als auch Datenschutzvorgaben. Dabei halten wir insbesondere die Prinzipien der Rechtmäßigkeit, Transparenz, Fairness, menschlichen Kontrolle, Zweckbindung, Datenminimierung und Integrität sowie Vertraulichkeit ein. Wir stellen sicher, dass die Verarbeitung personenbezogener Daten stets auf einer rechtlichen Grundlage erfolgt. Dies kann entweder die Einwilligung der betroffenen Personen oder eine gesetzliche Erlaubnis sein.

Bei der Nutzung externer KI-Systeme wählen wir deren Anbieter (nachfolgend "KI-Anbieter") sorgfältig aus. Entsprechend unseren gesetzlichen Pflichten stellen wir sicher, dass die KI-Anbieter die geltenden Bestimmungen einhalten. Ebenso beachten wir die uns obliegenden Pflichten bei Nutzung oder Betrieb der bezogenen KI-Leistungen. Die Verarbeitung personenbezogener Daten durch uns und die KI-Anbieter erfolgt ausschließlich auf Grundlage einer Einwilligung oder gesetzlichen Berechtigung. Dabei legen wir besonderen Wert auf Transparenz, Fairness und die Wahrung der menschlichen Kontrolle über KI-gestützte Entscheidungsprozesse.

Zum Schutz der verarbeiteten Daten implementieren wir angemessene und robuste technische sowie organisatorische Maßnahmen. Diese gewährleisten die Integrität und Vertraulichkeit der verarbeiteten Daten und minimieren potenzielle Risiken. Durch regelmäßige Überprüfungen der KI-Anbieter und ihrer Leistungen stellen wir die fortlaufende Einhaltung aktueller rechtlicher und ethischer Standards sicher.

Wir setzen KI ausschließlich als unterstützendes Hilfsmittel innerhalb bestehender Verarbeitungstätigkeiten ein. Der Einsatz von KI begründet keinen eigenständigen Verarbeitungszweck. Art, Umfang, Zweck, Speicherdauer und Rechtsgrundlage der Verarbeitung personenbezogener Daten richten sich daher nach der jeweiligen Verarbeitungstätigkeit, in deren Rahmen die KI eingesetzt wird.

Dienstanbieter

Für den Verband

Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland, Mutterunternehmen: Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399 USA; **Rechtsgrundlagen:** Berechtigte Interessen (Art. 6 Abs. 1 S. 1 lit. f) DSGVO); **Website:** <https://microsoft.com/de-de>;

Datenschutzerklärung: <https://privacy.microsoft.com/de-de/privacystatement>,
Sicherheitshinweise: <https://www.microsoft.com/de-de/trustcenter>;

Auftragsverarbeitungsvertrag: <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>; **Grundlage Drittlandübermittlung:** EU-US Data Privacy Framework (DPF), Standardvertragsklauseln (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>).

Für die Einrichtungen

Genoverband e.V., Wilhelm-Haas-Platz, 63263 Neu-Isenburg; **Rechtsgrundlagen:** Berechtigte Interessen (Art. 6 Abs. 1 S. 1 lit. f) DSGVO); **Website:** <https://www.genoverband.de/>,

Datenschutzerklärung: <https://www.genoverband.de/datenschutz/>

Auftragsverarbeitungsvertrag: nicht öffentlich einsehbar

Berechtigte Interessen

Zuverlässigkeit und Stabilität: Microsoft Produkte werden regelmäßig aktualisiert und gewartet.

Produktverbesserung: Die Übermittlung von (ggf. auch) personenbezogenen Daten an Microsoft hilft, die eingesetzten Produkte und Dienste zu analysieren, zu verbessern und zu personalisieren. Dies trägt zu einer positiven Nutzerfahrung sowie zur Abstimmung der Produkte auf die Bedürfnisse des Nutzers bei.

Breite Akzeptanz: Microsoft-Produkte sind weit verbreitet und werden in vielen Unternehmen und Organisationen weltweit genutzt; dadurch ist die internationale Zusammenarbeit effektiv und unkompliziert möglich.

Sicherheit: Microsoft implementiert zahlreiche Funktionen zum Schutz vor Cyber-Bedrohungen. Die Übermittlung von Daten an Microsoft trägt dazu bei, die Sicherheit der Produkte und Dienste zu erhöhen, Sicherheitslücken zu identifizieren und zu schließen.

Technische Unterstützung: Durch die Übermittlung personenbezogener Daten kann der Anbieter technische Probleme des Benutzers identifizieren und lösen.

Skalierbarkeit: Microsoft Produkte sind skalierbar und lassen sich an die Bedürfnisse jeder Unternehmensgröße anpassen.

Kosteneffektivität: Microsoft bietet flexible Preismodelle für seine Produkte und Dienste, die Unternehmen die Optimierung ihrer IT-Ausgaben ermöglichen.

Integrierte Tools: Microsoft bietet integrierte Tools und Funktionen, die Zusammenarbeit und Kommunikation erleichtern, etwa durch die Integration von Office-Anwendungen, Skype for Business und SharePoint.

Hohe Anpassungsfähigkeit: Microsoft-Produkte lassen sich an individuelle Anforderungen anpassen und ermöglichen die Automatisierung von Workflows und Prozessen.

Bekannte Benutzeroberfläche: Microsoft-Produkte verfügen über eine bekannte und einfach zu bedienende Benutzeroberfläche, was die Einarbeitungszeit verkürzt und die Produktivität erhöht.

Umfangreiche Drittanbieter-Integration: Microsoft-Produkte sind offen für Drittanbieter-Integrationen; zahlreiche Anwendungen und Tools sind mit ihnen kompatibel.

Ihre Rechte und weitere Informationen zum Datenschutz

Sie haben das **Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch** und **Datenübertragbarkeit** sowie auf **Beschwerde** bei einer Aufsichtsbehörde. Ob Sie Daten bereitstellen müssen und welche Folgen eine Nichtbereitstellung hat, richtet sich nach den gesetzlichen oder vertraglichen Anforderungen. Eine automatisierte **Entscheidungsfindung einschließlich Profiling findet nicht statt, sofern nicht ausdrücklich anders angegeben.**