Datenschutzrichtlinie

Stand: März 2024

Inhalt

1 Einführung

Diese Datenschutzrichtlinie legt fest, wie Glassomer GmbH (im Folgenden "Unternehmen" genannt) personenbezogene Daten erhebt, verwendet, speichert und schützt. Das Unternehmen verpflichtet sich zur Einhaltung der Datenschutz-Grundverordnung (DSGVO) und aller einschlägigen deutschen Datenschutzgesetze.

2 Verantwortliche Stelle

Die für die Verarbeitung Verantwortliche im Sinne der DSGVO ist:

Bastian E. Rapp, Chief Information (CIO) Glassomer GmbH, In den Kirchenmatten 54, cio@glassomer.com.

3 Zweck der Datenverarbeitung

Das Unternehmen verarbeitet personenbezogene Daten ausschließlich für legitime und rechtmäßige Zwecke. Die Erfassung und Nutzung von personenbezogenen Daten erfolgen transparent und nachvollziehbar, gemäß der vorliegenden Datenschutzrichtlinie. Das Unternehmen stellt sicher, dass die Grundsätze der Datenminimierung und Zweckbindung gemäß DSGVO gewahrt werden.

3.1 Verarbeitungszwecke

Personenbezogene Daten werden nur zu vorab festgelegten, rechtlich zulässigen und offen kommunizierten Zwecken erhoben. Diese Zwecke werden den betroffenen Personen transparent mitgeteilt, sei es durch Datenschutzinformationen, Datenschutzerklärungen oder andere geeignete Mittel. Das Unternehmen informiert die betroffenen Personen klar und deutlich über die Zwecke, für die ihre Daten erhoben und verarbeitet werden.

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich für die Erfüllung der festgelegten Zwecke. Es werden nur die Daten erhoben, die für die Erreichung dieser Zwecke erforderlich sind, und es findet keine weitere Verarbeitung statt, die nicht mit den kommunizierten Zwecken vereinbar ist.

Beispielhafte Verarbeitungszwecke können sein:

- Bereitstellung und Verbesserung unserer Produkte oder Dienstleistungen
- Kommunikation mit Kunden, Lieferanten und anderen Geschäftspartnern
- Verwaltung von Kundenbeziehungen, einschließlich Kundenbetreuung, -support und -service
- Abwicklung von Bestellungen, Verträgen und Zahlungen
- Personalmanagement, einschließlich Bewerbungsverfahren, Mitarbeiteradministration und Gehaltsabrechnung
- Einhaltung rechtlicher Verpflichtungen, einschließlich steuerlicher und buchhalterischer Aufzeichnungen
- Gewährleistung der Sicherheit unserer Systeme und Daten sowie Bekämpfung von Betrug und Missbrauch
- Marktforschung, Analyse und Entwicklung neuer Produkte oder Dienstleistungen
- Erfüllung von behördlichen Anfragen und rechtlichen Verpflichtungen

Das Unternehmen aktualisiert seine Datenschutzerklärung regelmäßig, um sicherzustellen, dass alle Verarbeitungszwecke klar und aktuell kommuniziert werden. Diese transparente Kommunikation über die Zwecke der Datenverarbeitung trägt dazu bei, das Vertrauen der betroffenen Personen zu stärken und die Einhaltung der Datenschutzgesetze zu gewährleisten.

3.2 Einwilligung

Sofern die Verarbeitung personenbezogener Daten auf der Einwilligung der betroffenen Personen basiert, legt das Unternehmen großen Wert darauf, dass diese Einwilligung freiwillig, informiert und eindeutig erfolgt. Vor der Einholung der Einwilligung werden den betroffenen Personen transparente Informationen über den Verarbeitungszweck, die Art der verarbeiteten Daten, die Identität des Verantwortlichen sowie etwaige Empfänger der Daten zur Verfügung gestellt.

Die Einwilligung wird spezifisch für den jeweiligen Verarbeitungszweck eingeholt und nicht durch die bloße Akzeptanz allgemeiner Geschäftsbedingungen oder Datenschutzrichtlinien erlangt. Das Unternehmen stellt sicher, dass die betroffenen Personen die Möglichkeit haben, ihre Einwilligung ohne negative Auswirkungen zu verweigern oder zu widerrufen.

Betroffene Personen haben das uneingeschränkte Recht, ihre Einwilligung jederzeit zu widerrufen. Der Widerruf hat keine Auswirkungen auf die Rechtmäßigkeit der Verarbeitung vor dem Widerruf.

Um sicherzustellen, dass die Einwilligung den Anforderungen der Datenschutzgrundverordnung (DSGVO) entspricht, verwendet das Unternehmen eindeutige Einwilligungsformulare oder andere klar erkennbare Einwilligungsmittel und dokumentiert die Einholung der Einwilligung gemäß den gesetzlichen Anforderungen.

Die Einhaltung dieser Grundsätze gewährleistet, dass die Verarbeitung personenbezogener Daten im Einklang mit den Bestimmungen der DSGVO und anderen geltenden Datenschutzgesetzen erfolgt.

3.3 Vertragsdurchführung

Personenbezogene Daten werden verarbeitet, wenn dies zur Erfüllung vertraglicher Verpflichtungen erforderlich ist. Dies umfasst die Verarbeitung von Daten, um Produkte oder Dienstleistungen bereitzustellen, Verträge zu erfüllen oder auf Anfrage vorvertragliche Maßnahmen durchzuführen.

3.4 Gesetzliche Verpflichtungen

Das Unternehmen verarbeitet personenbezogene Daten, um rechtlichen Verpflichtungen nachzukommen. Hierzu gehören unter anderem die Erfüllung von steuerlichen und buchhalterischen Pflichten gemäß den geltenden Gesetzen und Vorschriften. Dies umfasst die Aufbewahrung und Dokumentation von Daten, die für steuerliche Zwecke erforderlich sind, sowie die Erstellung von Berichten und Abrechnungen gemäß den gesetzlichen Anforderungen.

Darüber hinaus kooperiert das Unternehmen mit behördlichen Anfragen und erfüllt alle rechtlichen Verpflichtungen, die sich aus nationalen und internationalen Gesetzen und Vorschriften ergeben. Dies kann die Zusammenarbeit mit Aufsichtsbehörden, Strafverfolgungsbehörden oder anderen staatlichen Stellen beinhalten, um Anfragen zu beantworten, Untersuchungen durchzuführen oder gesetzliche Anforderungen zu erfüllen.

Die Verarbeitung personenbezogener Daten zur Erfüllung gesetzlicher Verpflichtungen erfolgt im Rahmen der jeweiligen rechtlichen Grundlage und unter Berücksichtigung der Datenschutzprinzipien der DSGVO und anderer anwendbarer Datenschutzgesetze. Das Unternehmen stellt sicher, dass die Daten nur für die jeweiligen gesetzlich vorgeschriebenen Zwecke verwendet werden und die erforderlichen Sicherheitsmaßnahmen getroffen werden, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu gewährleisten.

Die Einhaltung dieser gesetzlichen Verpflichtungen ist von entscheidender Bedeutung für das Unternehmen und unterstreicht unser Engagement für die Einhaltung der geltenden Gesetze und Vorschriften sowie für den Schutz der Rechte und Interessen der betroffenen Personen.

3.5 Legitime Interessen

Sofern erforderlich und gesetzlich zulässig, behält sich das Unternehmen das Recht vor, personenbezogene Daten auf Grundlage seiner legitimen Interessen zu verarbeiten. Dabei wird stets eine sorgfältige Interessenabwägung vorgenommen, um sicherzustellen, dass die Rechte und Interessen der betroffenen Personen angemessen berücksichtigt werden.

Die Verarbeitung personenbezogener Daten auf der Grundlage legitimer Interessen kann verschiedene Zwecke umfassen, wie beispielsweise:

- Gewährleistung der Sicherheit und Integrität der Systeme und Daten des Unternehmens
- Prävention von Betrug, Missbrauch oder rechtswidrigem Verhalten
- Verbesserung der Qualität, Sicherheit und Leistung von Produkten oder Dienstleistungen
- Durchführung von Marktanalysen, Kundenprofilierungen oder Marketingaktivitäten
- Wahrung rechtlicher Ansprüche oder Durchsetzung von Vertragsbedingungen

Bei der Verarbeitung personenbezogener Daten auf Grundlage legitimer Interessen achtet das Unternehmen darauf, dass die Verarbeitung im Einklang mit den Datenschutzprinzipien der DSGVO steht und die Auswirkungen auf die betroffenen Personen minimiert werden. Insbesondere werden die Grundsätze der Datenminimierung, Zweckbindung und Transparenz beachtet.

Die klare Definition und Dokumentation der Verarbeitungszwecke sowie der zugrundeliegenden legitimen Interessen dienen nicht nur der Einhaltung der DSGVO und anderer Datenschutzgesetze, sondern auch der Transparenz gegenüber den betroffenen Personen. Das Unternehmen informiert die betroffenen Personen über die Verarbeitung ihrer Daten auf Grundlage legitimer Interessen in seiner Datenschutzerklärung oder anderen geeigneten Informationsquellen.

4 Datensicherheit

Die Sicherheit und Integrität der verarbeiteten Daten sind von höchster Bedeutung für das Unternehmen Wir setzen uns dafür ein, angemessene technische und organisatorische Maßnahmen zu ergreifen, um die Vertraulichkeit, Verfügbarkeit und Integrität der personenbezogenen Daten sicherzustellen, die wir verarbeiten.

4.1 Zugangskontrolle

Der Zugriff auf personenbezogene Daten ist auf autorisierte Mitarbeiter und Dienstleister beschränkt, die diese Informationen für die Ausführung ihrer Aufgaben benötigen. Alle autorisierten Personen sind zur Vertraulichkeit verpflichtet und werden regelmäßig in Bezug auf Datenschutzbestimmungen und Sicherheitsverfahren geschult.

Der Zugriff auf personenbezogene Daten ist streng auf autorisierte Mitarbeiter und Dienstleister beschränkt, die diese Informationen für die Ausführung ihrer Aufgaben benötigen. Das Unternehmen implementiert geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass nur befugte Personen Zugriff auf personenbezogene Daten haben und dass dieser Zugriff auf das erforderliche Mindestmaß beschränkt ist.

4.1.1 Autorisierung und Schulung

Alle Mitarbeiter und Dienstleister, die Zugriff auf personenbezogene Daten haben, werden vorher autorisiert und erhalten Zugang nur zu denjenigen Daten, die für die Ausführung ihrer spezifischen Aufgaben erforderlich sind. Darüber hinaus sind alle autorisierten Personen verpflichtet, die Vertraulichkeit der Daten zu wahren und sie ausschließlich für die festgelegten Zwecke zu verwenden.

Es wird sichergestellt, dass alle autorisierten Personen regelmäßig in Bezug auf Datenschutzbestimmungen und Sicherheitsverfahren geschult werden. Diese Schulungen umfassen Aspekte wie den sicheren Umgang mit personenbezogenen Daten, die Erkennung von Sicherheitsrisiken und die Meldung von Datenschutzverletzungen.

4.1.2 Überwachung und Protokollierung

Das Unternehmen überwacht und protokolliert den Zugriff auf personenbezogene Daten, um sicherzustellen, dass nur autorisierte Personen auf die Daten zugreifen und um verdächtige Aktivitäten zu erkennen. Jegliche unbefugten Zugriffsversuche oder verdächtige Aktivitäten werden umgehend untersucht, und angemessene Maßnahmen werden ergriffen, um die Sicherheit der Daten zu gewährleisten.

4.1.3 Physische Sicherheit

Für den physischen Schutz von personenbezogenen Daten werden angemessene Sicherheitsmaßnahmen ergriffen, um den unbefugten Zugriff, Diebstahl oder Missbrauch zu verhindern. Dies umfasst Sicherheitsvorkehrungen wie Zugangskontrollen, Überwachungskameras und Sicherheitspersonal an Standorten, an denen personenbezogene Daten gespeichert oder verarbeitet werden. Dies geschieht in einem nach ISO 27001 zertifizierten Rechenzentrum, in welchem die Rechnersysteme des Unternehmens installiert sind.

Die Umsetzung dieser Zugriffskontrollmaßnahmen gewährleistet die Vertraulichkeit und Integrität der personenbezogenen Daten und trägt dazu bei, das Vertrauen der betroffenen Personen in den Datenschutz zu stärken.

4.2 Verschlüsselung und Übertragung

Personenbezogene Daten werden während der Übertragung zwischen Benutzern und Systemen verschlüsselt, um die Vertraulichkeit und Integrität der Daten zu gewährleisten. Wir verwenden sichere Übertragungsprotokolle um sicherzustellen, dass Daten vor unbefugtem Zugriff während der Übermittlung geschützt sind.

4.3 Datensicherung und Wiederherstellung

Regelmäßige Backups werden durchgeführt, um sicherzustellen, dass personenbezogene Daten im Falle von Datenverlust, -beschädigung oder -zerstörung wiederhergestellt werden können. Wiederherstellungspläne werden regelmäßig überprüft und aktualisiert, um eine schnelle und effiziente Wiederherstellung im Bedarfsfall zu gewährleisten. Alle Daten sind ausschließlich auf verschlüsselte Datensicherungssystem (symmetrische Verschlüsselung unter Verwendung von AES-256) abgelegt und vor physikalischen Zugriff in einem nach ISO 27001 zertifizierten Rechenzentrum geschützt.

4.4 Überwachung und Auditierung

Wir führen kontinuierliche Überwachungen und regelmäßige Audits unserer Systeme durch, um potenzielle Sicherheitsbedrohungen zu erkennen und zu beheben. Unbefugte Zugriffe oder verdächtige Aktivitäten werden umgehend untersucht, und angemessene Maßnahmen werden ergriffen, um Sicherheitsvorfälle zu bewältigen.

4.5 Mitarbeitersensibilisierung

Unsere Mitarbeiter sind sich der Bedeutung der Datensicherheit bewusst und werden regelmäßig geschult, um sicherzustellen, dass sie bewährte Sicherheitspraktiken verstehen und anwenden. Dies umfasst auch die Sensibilisierung für Phishing-Angriffe und andere potenzielle Sicherheitsrisiken.

4.6 Datenschutz-Folgenabschätzung (DSFA)

Vor der Einführung neuer Verarbeitungstätigkeiten, insbesondere solcher, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellen, führen wir Datenschutz-Folgenabschätzungen (DSFA) durch, um potenzielle Risiken zu bewerten und angemessene Schutzmaßnahmen zu implementieren. Eine Datenschutz-Folgenabschätzung wird durchgeführt, wenn neue Verarbeitungstätigkeiten eingeführt werden, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellen.

Die DSFA umfasst eine systematische Bewertung der potenziellen Auswirkungen der Verarbeitungstätigkeiten auf die Privatsphäre und die Datenschutzrechte der betroffenen Personen. Diese berücksichtigt Faktoren wie Art, Umfang, Kontext und Zwecke der Verarbeitung, sowie die Art der betroffenen Daten und die potenziellen Risiken für die betroffenen Personen. Anhand der Ergebnisse der DSFA werden geeignete Schutzmaßnahmen identifiziert und implementiert, um die Risiken zu minimieren und die Einhaltung der Datenschutzgesetze.

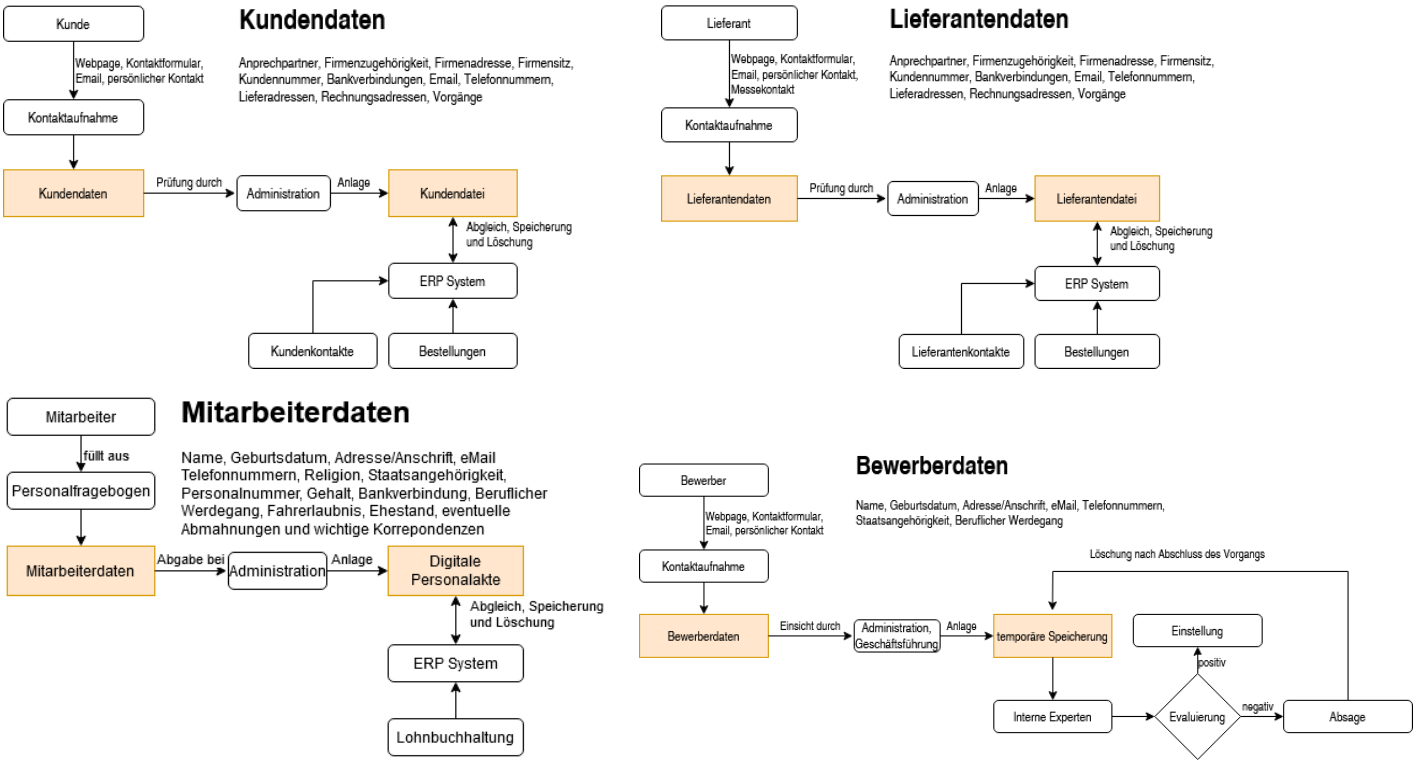
Eine DSFA wird unter der Leitung des CIO durchgeführt, protokolliert, der Geschäftsführung vorgestellt und durch diese freigegeben.

Die Umsetzung dieser Maßnahmen unterstreicht unser Engagement für die Sicherheit personenbezogener Daten und gewährleistet die Einhaltung der DSGVO und anderer relevanter Datenschutzgesetze.

5 Weitergabe von personenbezogenen Daten

Personenbezogene Daten können an Dritte weitergegeben werden, wenn dies zur Erfüllung rechtlicher Verpflichtungen, zur Vertragserfüllung oder auf Grundlage des berechtigten Interesses des Unternehmens erforderlich ist. Das Unternehmen stellt sicher, dass Dritte ebenfalls angemessene Datenschutzstandards einhalten.

6 Datenfluss Diagramme



7 Betroffenenrechte

Betroffene Personen haben das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten. Um diese Rechte auszuüben, kann sich die betroffene Person an die unter Abschnitt 2 genannte Verantwortliche Stelle wenden.

8 Datenschutzbeauftragter

Das Unternehmen hat einen Datenschutzbeauftragten ernannt, der über die Kontaktdaten

Bastian E. Rapp, Chief Information (CIO) Glassomer GmbH, In den Kirchenmatten 54, cio@glassomer.com.

erreichbar ist.

9 Änderungen der Datenschutzrichtlinie

Diese Datenschutzrichtlinie kann bei Bedarf aktualisiert werden. Alle wesentlichen Änderungen werden den betroffenen Personen mitgeteilt.

10 Kontaktdaten

Für Fragen oder Anliegen zur Datenschutzrichtlinie kann man sich an cio@glassomer.com wenden.