Datenschutzhinweise

für Nutzerinnen und Nutzer des qngine ZV-Portals | Version 2026-10-19

1. Verantwortlicher

Verantwortlicher für die Verarbeitung personenbezogener Daten von Portal-Nutzern ist HFB GmbH, Thüler Str. 3, 49681 Garrel, vertreten durch die Geschäftsführer Heinz-Gerd Biemann und Frank Bauer, Amtsgericht Oldenburg, HRB 215254, USt-IdNr. DE 329109581, E-Mail: info@hfb.one.

Datenschutzkontakt: Heinz-Gerd Biemann, hgb@hfb.one. Diese Kontaktstelle ist nicht als förmlich benannter Datenschutzbeauftragter bezeichnet.

2. Geltungsbereich und Rollen

Diese Hinweise betreffen die Verarbeitung von Daten zur Einrichtung und Nutzung des qngine ZV-Portals, zur Vertragsverwaltung, Sicherheit, Kommunikation und Unterstützung. Für Fachdaten, die ein Mandant im Rahmen seiner Verwaltungsaufgaben verarbeitet, ist grundsätzlich der jeweilige Mandant Verantwortlicher und HFB Auftragsverarbeiter. Einzelheiten regelt die ADV.

3. Verarbeitete Daten

- Stammdaten wie Name, geschäftliche E-Mail-Adresse, Telefonnummer, Rolle, Mandantenzuordnung und Firmenangaben.
- Anmeldedaten wie Magic-Link-Token, Zeitpunkt der Anmeldung, Sitzungs- und Sicherheitsinformationen sowie technisch erforderliche Cookie-Daten.
- Nutzungs- und Protokolldaten wie Zeitpunkte, aufgerufene Funktionen, Fehlermeldungen, Änderungen und sicherheitsrelevante Ereignisse.
- Supportdaten wie Ticketinhalt, Kommentare, Anhänge, freigegebene Supportzugriffe und Kommunikation.
- Nachweise zu AGB, Datenschutzhinweisen und ADV mit Dokumentversion, Zeitpunkt und bestätigendem Benutzer.
- Abrechnungs-, Vertrags- und Kontaktdaten der Kundenunternehmen.

4. Zwecke und Rechtsgrundlagen

Die Verarbeitung erfolgt zur Anbahnung und Durchführung des Nutzungs- und Kundenvertrags nach Art. 6 Abs. 1 Buchstabe b DSGVO, zur Erfüllung gesetzlicher Nachweis-, Handels- und Steuerpflichten nach Art. 6 Abs. 1 Buchstabe c DSGVO sowie auf Grundlage berechtigter Interessen nach Art. 6 Abs. 1 Buchstabe f DSGVO.

Berechtigte Interessen sind insbesondere ein sicherer und stabiler Betrieb, Missbrauchsvermeidung, Fehleranalyse, Produktverbesserung, Bearbeitung von Supportfällen sowie die Dokumentation rechtsgeschäftlicher Erklärungen. Soweit ausnahmsweise eine Einwilligung erforderlich ist, wird diese gesondert eingeholt; die Kenntnisnahme dieser Datenschutzhinweise ist keine Einwilligung.

5. Anmeldung, Cookies und Sicherheit

qngine verwendet technisch erforderliche, hostgebundene und mit HttpOnly geschützte Sitzungscookies. Sie dienen ausschließlich der Authentifizierung, Portalauswahl und Sicherheit. Marketing- oder Reichweiten-Cookies werden im Portal derzeit nicht eingesetzt.

Anmeldelinks und Einmalcodes sind zeitlich begrenzt. Zur Abwehr automatisierter Angriffe können Zugriffe nach E-Mail-Adresse und IP-Adresse begrenzt sowie sicherheitsrelevante Vorgänge protokolliert werden.

6. Empfänger und Dienstleister

Zugriff erhalten nur berechtigte Beschäftigte und Dienstleister, soweit dies für Betrieb, Support, Kommunikation oder Vertragserfüllung erforderlich ist. Eingesetzt werden insbesondere Hetzner für Hosting und Sicherungen, Microsoft 365 und STRATO für E-Mail-Kommunikation, BANKSapi für angebundene Bankfunktionen sowie - abhängig von der aktivierten Funktion - OpenAI, Google/Gemini und Anthropic für KI-Verarbeitung. Eine optionale verschlüsselte Remote-Sicherung kann über Google Drive erfolgen.

Bei KI-Funktionen werden nur die für den jeweiligen Auftrag erforderlichen Inhalte übermittelt. KI-Ergebnisse sind Vorschläge und werden nicht ohne Nutzerentscheidung als fachliche Entscheidung übernommen.

Personenbezogene Daten und sonstige Inhalte aus qngine werden weder von HFB noch von den eingesetzten KI-Anbietern zur Entwicklung, zum Training oder zur Verbesserung von KI- oder ML-Modellen verwendet. HFB nutzt KI-Anbieter ausschließlich über geschäftliche API-Zugänge, deren Bedingungen ein Training mit übermittelten Inhalten ausschließen, und gibt keine Daten zur eigenen Nutzung durch die Anbieter frei.

7. Angebundene E-Mail-Postfächer

Mandanten können geschäftliche E-Mail-Postfächer an qngine anbinden. qngine ruft E-Mails samt Anhängen ab, übernimmt sie in die Verfahrensakte und versendet E-Mails aus qngine. Die Verbindung erfolgt je nach Anbieter per IMAP und SMTP mit den hinterlegten Zugangsdaten oder über die Anmeldung beim Anbieter (Microsoft). Zugangsdaten werden verschlüsselt gespeichert. qngine verschiebt und löscht keine Nachrichten im Postfach; je nach Einstellung markiert qngine abgerufene Nachrichten als gelesen und legt versendete Nachrichten im Gesendet-Ordner ab. Der Abruf endet mit dem Trennen des Postfachs in qngine.

Bei Google-Postfächern (Gmail, Google Workspace) verbindet sich qngine wie ein E-Mail-Programm per IMAP und SMTP mit einem vom Nutzer erstellten App-Passwort. Google-Programmierschnittstellen werden dafür nicht genutzt. Das App-Passwort kann jederzeit in den Einstellungen des Google-Kontos widerrufen werden.

Inhalte angebundener Postfächer werden nicht verkauft, nicht für Werbung genutzt und weder roh noch abgeleitet oder aggregiert zur Entwicklung, zum Training oder zur Verbesserung von KI- oder ML-Modellen verwendet.

8. Drittlandübermittlungen

Einzelne Anbieter oder deren Unterauftragnehmer können Daten außerhalb des Europäischen Wirtschaftsraums verarbeiten. Übermittlungen erfolgen nur auf Grundlage eines Angemessenheitsbeschlusses der Europäischen Kommission oder geeigneter Garantien, insbesondere der EU-Standardvertragsklauseln, gegebenenfalls ergänzt um zusätzliche Schutzmaßnahmen.

9. Speicherdauer

Benutzer- und Vertragsdaten werden für die Dauer des Vertrags und anschließend nur so lange gespeichert, wie dies für Abwicklung, Nachweise oder gesetzliche Aufbewahrungspflichten erforderlich ist. Authentifizierungs-Token werden nach Ablauf nicht mehr zur Anmeldung verwendet. Support- und Protokolldaten werden nach Zweckfortfall und Ablauf erforderlicher Nachweisfristen gelöscht oder eingeschränkt.

Bestätigungsnachweise zu Rechtstexten werden für die Dauer des Vertragsverhältnisses und bis zum Ablauf möglicher zivilrechtlicher Nachweisfristen aufbewahrt. Gelöschte produktive Daten können bis zum planmäßigen Ablauf verschlüsselter Sicherungen noch enthalten sein; die derzeitige Sicherungsaufbewahrung umfasst bis zu zwölf monatliche Stände.

10. Rechte betroffener Personen

Betroffene Personen haben nach den gesetzlichen Voraussetzungen Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch. Eine erteilte Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden. Anfragen können an hgb@hfb.one gerichtet werden.

Es besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde. Für HFB ist insbesondere die Landesbeauftragte für den Datenschutz Niedersachsen, Prinzenstraße 5, 30159 Hannover, poststelle@lfd.niedersachsen.de, erreichbar.

11. Pflicht zur Bereitstellung und automatisierte Entscheidungen

Die für Benutzerkonto, Authentifizierung und Vertragserfüllung erforderlichen Daten müssen bereitgestellt werden; ohne sie ist eine Nutzung nicht möglich. HFB trifft gegenüber Portal-Nutzern keine ausschließlich automatisierten Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung im Sinne von Art. 22 DSGVO.

12. Änderungen

HFB aktualisiert diese Hinweise bei Änderungen der Verarbeitung oder Rechtslage. Eine neue Fassung wird im Portal bereitgestellt. Wenn eine erneute Kenntnisnahme erforderlich ist, wird sie beim nächsten Login dokumentiert.