Datenschutzinformation

BrandSicher - interne Anwendung und Kundenportal

Fassung 2026-10-26-v69 | Informationen nach Artikeln 13 und 14 DSGVO

1. Verantwortlicher und Datenschutzkontakt

Verantwortlich für die in diesen Hinweisen beschriebene Verarbeitung ist die StaBe GmbH, Neuer Weg 14, 51647 Gummersbach. Vertreten durch die Geschäftsführer Daniel Stahl und Michael Bergmann. Telefon: 02261 9259720. E-Mail für Datenschutzanfragen: arbeitsschutz@stabe.info.

Datenschutz-Ansprechpartner ist Daniel Stahl, Geschäftsführer. Ein Datenschutzbeauftragter im Sinne der Artikel 37 bis 39 DSGVO ist nicht bestellt. Diese Hinweise betreffen BrandSicher einschließlich interner Anwendung und Kundenportal. Eine gegebenenfalls ausschließlich nach Weisung eines Auftraggebers ausgeführte Auftragsverarbeitung richtet sich ergänzend nach der vereinbarten Aufgabenverteilung; für die eigenen Verarbeitungszwecke des Auftraggebers gelten dessen Datenschutzinformationen.

2. Datenarten und Herkunft

Verarbeitet werden Kundenstammdaten, zugehörige Gebäude und Anschriften, Gebäudearten, zentrale und örtliche Ansprechpartner mit dienstlichen Kontaktangaben sowie Angaben zur fachlichen Betreuung. Dazu gehören Begehungen, Beratungen, ASA-Sitzungen, Übungen, Berechnungen, Prüfkriterien und Bewertungen, Mängel, Maßnahmen, Zuständigkeiten, Fristen, Anlagen- und Gerätedaten, Fotos, Anhänge, Unterlagen und Protokolle einschließlich gespeicherter Bearbeitungsstände.

Für Benutzerkonten werden Name, E-Mail-Adresse, Rolle, Konto- und Berechtigungsstatus, Passwortprüfwert sowie Einladungs- und Aktivierungsinformationen verarbeitet. Bei Anmeldung, Änderungen und sicherheitsrelevanten Vorgängen können Zeitpunkt, Benutzerkennung oder E-Mail-Adresse, IP-Adresse und Ereignisdetails anfallen. Beim Abruf der Anwendung werden die für die technische Verbindung erforderlichen Verbindungs- und Abrufdaten verarbeitet.

Daten stammen von betroffenen Personen selbst, Auftraggebern und deren Ansprechpartnern oder Beschäftigten, berechtigten Benutzern, Prüfern und sonstigen beteiligten Dienstleistern sowie aus eigenen fachlichen Feststellungen. Fotos und Freitexte können Angaben zu anwesenden Personen enthalten. Es sollen nur erforderliche Informationen eingetragen werden. Gesundheitsdaten und andere besondere Kategorien personenbezogener Daten sind für die reguläre Nutzung nicht vorgesehen und sollen nicht hochgeladen werden.

3. Zwecke und Rechtsgrundlagen

Die Verarbeitung dient der Organisation, Durchführung und Dokumentation von Brandschutz- und Arbeitsschutzleistungen, der Kunden- und Objektbetreuung, der Bereitstellung von Nachweisen und Unterlagen sowie der Kommunikation mit den Beteiligten. Artikel 6 Absatz 1 Buchstabe b DSGVO gilt, soweit die Verarbeitung für einen Vertrag mit der betroffenen Person oder vorvertragliche Maßnahmen auf deren Anfrage erforderlich ist.

Dienstliche Ansprechpartner bei Unternehmen, fachliche Nachvollziehbarkeit, Qualitätssicherung, Sicherung und Wiederherstellung der Anwendung, Zugriffsverwaltung, Missbrauchsabwehr und Rechtsverteidigung werden, soweit einschlägig, auf Artikel 6 Absatz 1 Buchstabe f DSGVO gestützt. Berechtigte Interessen sind eine verlässliche Leistungserbringung, geschützte Kundendokumentation, ein sicherer Betrieb und die Durchsetzung oder Abwehr von Ansprüchen.

Artikel 6 Absatz 1 Buchstabe c DSGVO gilt, soweit StaBe eigene gesetzliche Pflichten erfüllen muss, insbesondere einschlägige handels- und steuerrechtliche Aufbewahrungspflichten nach § 257 HGB und § 147 AO. Für Daten eigener Beschäftigter kommt § 26 Absatz 1 BDSG in Verbindung mit Artikel 88 DSGVO hinzu, soweit die Verarbeitung für das Beschäftigungsverhältnis erforderlich ist. Wird für einen gesonderten Zweck eine Einwilligung eingeholt, gilt Artikel 6 Absatz 1 Buchstabe a DSGVO. Die Kenntnisnahme dieser Hinweise ist keine Einwilligung.

4. Benutzerrollen und Objektberechtigungen

Administratoren verwalten Konten und Zugriffszuweisungen. Intern einem Kunden zugewiesene Mitarbeiter können dessen Stammdaten sowie bestehende und künftig angelegte Objekte im Rahmen ihrer Mitarbeiterrolle bearbeiten und neue Objekte anlegen. Gegebenenfalls noch vorhandene einzelne Objektfreigaben werden bei der zentralen Berechtigungsverwaltung berücksichtigt. Der Zugriff ist auf den jeweiligen Berechtigungsumfang begrenzt.

Kundenkonten erhalten entweder Zugang zu ausgewählten Objekten oder zu allen bestehenden und künftigen Objekten eines ausdrücklich zugeordneten Kundenstamms. Kundenkonten erhalten keinen Zugang zur internen Mitarbeiterverwaltung. Ein Kundenkonto sieht im Portal die zugänglichen Objekte, deren Anlagenübersicht und die ausdrücklich für das Portal freigegebenen archivierten Protokolle. Die Objektfreigabe allein gibt noch keine Protokolle frei.

5. Uploads, Prüfung und Zurückziehen von Unterlagen

Kunden können PDF-, JPG- oder PNG-Unterlagen bis 25 MB gezielt für ein zugängliches Objekt einreichen. Die Unterlagen werden als eingereicht gespeichert und durch eine zuständige Person geprüft, übernommen oder mit Begründung abgelehnt. Im Portal werden dem Kundenkonto seine selbst eingereichten Unterlagen angezeigt.

Ein Kundenkonto kann ausschließlich eigene Unterlagen im Status eingereicht oder abgelehnt zurückziehen und löschen, solange der Objektzugriff besteht. Bereits übernommene Unterlagen sowie fremde Dateien, Objekte und Protokolle können durch das Kundenkonto nicht gelöscht werden. Gesetzliche Löschungsansprüche können unabhängig von diesen Bedienrechten an den Datenschutzkontakt gerichtet werden.

Beim Zurückziehen wird die aktive Datei einschließlich einer vorhandenen HiDrive-Spiegelkopie entfernt, sofern die Löschung erfolgreich ausgeführt werden kann. Der Vorgang bleibt ohne Dateiinhalt im Ereignisprotokoll dokumentiert; dabei können insbesondere Zeitpunkt, handelndes Konto, Dateibezeichnung und Bearbeitungsstatus erhalten bleiben. Bereits vorhandene Sicherungsstände werden durch die Dateilöschung nicht nachträglich umgeschrieben.

6. Empfänger, Hosting und Speicherorte

Zugriff erhalten berechtigte Personen bei StaBe und die ausdrücklich zugelassenen Kundenkonten. Soweit für den jeweiligen Auftrag oder eine rechtliche Pflicht erforderlich, kommen als weitere Empfänger benannte Ansprechpartner des Auftraggebers, beteiligte Prüf- und Fachdienstleister, Behörden, Gerichte und rechtliche Berater in Betracht. Eine allgemeine Veröffentlichung der Anwendungsinhalte ist nicht vorgesehen.

Für Hosting und Sicherung wird IONOS als Hosting- und HiDrive-Anbieter eingesetzt; technisch eingebundene Unterauftragnehmer können im Rahmen der jeweiligen Leistung beteiligt sein. Der Produktivserver befindet sich in Spanien; die HiDrive-Speicherung erfolgt in Berlin. Die genannten Speicherorte liegen in der Europäischen Union. Die Anbieter erhalten die für Betrieb und Sicherung erforderlichen Daten.

Für etwaige Übermittlungen an Empfänger außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums gelten zusätzlich die Voraussetzungen der Artikel 44 ff. DSGVO.

Eine Änderung der vorgesehenen Verarbeitung mit solchen Übermittlungen ist in den Datenschutzinformationen einschließlich einschlägiger Garantien abzubilden. Die Standorte der Hauptspeicherung allein sind keine Zusicherung über sämtliche möglichen Support- oder Unterauftragnehmerzugriffe.

7. Anmeldung, Cookies und lokale Entwürfe

Zur Anmeldung und Absicherung von Anfragen nutzt BrandSicher technisch erforderliche Sitzungs- und Sicherheitsinformationen. Das Sitzungscookie stabe_session dient der Zuordnung des angemeldeten Kontos. Die reguläre Sitzungsdauer beträgt acht Stunden; bei fortgesetzter Nutzung kann sie erneuert werden. Die Speicherung oder der Zugriff ist nach § 25 Absatz 2 Nummer 2 TDDDG zulässig, soweit dies für den ausdrücklich gewünschten Dienst unbedingt erforderlich ist. Die anschließende Verarbeitung personenbezogener Daten richtet sich nach den in Abschnitt 3 genannten Rechtsgrundlagen.

Scheitert bei internen Benutzern die zentrale Speicherung eines Objektstands, versucht die Anwendung, einen kontobezogenen Entwurf im lokalen Browserspeicher abzulegen. Dieser kann Objekt- und Kontaktdaten, Prüfinhalte, Notizen und zugehörige Dateiangaben enthalten. Nach erfolgreichem zentralem Speichern wird der entsprechende Entwurf entfernt. Andernfalls bleibt er bis zur Entfernung durch die Anwendung oder zum Löschen der Websitedaten im Browser bestehen. Das Abmelden entfernt solche Entwürfe nicht automatisch. Auf gemeinsam genutzten Geräten sind deshalb geschützte Benutzerprofile und die Bereinigung lokaler Websitedaten zu beachten.

Im geprüften Anwendungsstand sind keine Werbe- oder Analyse-Tracker eingebunden. Verlinkte externe Fach- und Rechtsquellen werden beim Öffnen als eigenständige Angebote aufgerufen; dort gelten die Hinweise der jeweiligen Anbieter.

8. Speicherdauer und Löschkriterien

Kunden-, Objekt- und fachliche Dokumentationsdaten werden gespeichert, solange sie für die Betreuung, laufende Vorgänge, erforderliche Nachweise oder berechtigte Ansprüche benötigt werden. Nach Abschluss eines Vorgangs oder Ende der Betreuung sind weitere Nachweisbedürfnisse, einschlägige Verjährungsfristen, gesetzliche Aufbewahrungspflichten und mögliche Streitfälle maßgeblich. Eine pauschale Aufbewahrungsfrist für sämtliche Brandschutzunterlagen besteht deshalb nicht. Entfallen die Zwecke und Aufbewahrungsgründe, sind personenbezogene Daten zu löschen oder zu anonymisieren.

Soweit Unterlagen den jeweiligen gesetzlichen Kategorien unterfallen, gelten insbesondere zehn Jahre für Handelsbücher und Jahresabschlüsse, acht Jahre für Buchungsbelege und sechs Jahre für Handels- oder Geschäftsbriefe nach den einschlägigen handels- und steuerrechtlichen Vorschriften. Beginn, Ausnahmen und gegebenenfalls Verlängerungen richten sich nach der jeweiligen Vorschrift. Diese Fristen gelten nicht automatisch für jede Begehung, jedes Foto oder jedes Protokoll.

Benutzerkonten und Berechtigungsdaten werden für die autorisierte Nutzung benötigt. Sicherheits- und Änderungsnachweise werden nach dem Erfordernis der Missbrauchsaufklärung, Nachvollziehbarkeit und Rechtsverteidigung aufbewahrt. Für eingereichte oder abgelehnte Unterlagen sind die laufende Prüfung, eine notwendige Rückfrage und gegebenenfalls deren Dokumentation maßgeblich.

Sicherungskopien dienen der Wiederherstellung und dürfen nur so lange vorgehalten werden, wie dies für diesen Zweck erforderlich ist. Maßgeblich sind die für den Wiederanlauf benötigten Sicherungsstände, deren Aktualität und die erforderliche Absicherung gegen Datenverlust. Bei einer Wiederherstellung sind bereits umgesetzte Löschungen und Einschränkungen erneut zu

berücksichtigen. Für lokal gespeicherte Entwürfe gelten zusätzlich die in Abschnitt 7 genannten Löschkriterien.

9. Rechte betroffener Personen und Widerspruch

Nach Maßgabe der gesetzlichen Voraussetzungen bestehen die Rechte auf Auskunft nach Artikel 15 DSGVO, Berichtigung nach Artikel 16, Löschung nach Artikel 17, Einschränkung der Verarbeitung nach Artikel 18 und Datenübertragbarkeit nach Artikel 20. Für die Bearbeitung kann eine angemessene Prüfung Ihrer Identität erforderlich sein.

Widerspruch: Soweit die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f DSGVO beruht, können Sie aus Gründen Ihrer besonderen Situation nach Artikel 21 DSGVO widersprechen. Die Verarbeitung wird dann eingestellt, sofern keine nachgewiesenen zwingenden schutzwürdigen Gründe überwiegen und sie nicht der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Eine gegebenenfalls erteilte Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden; die Rechtmäßigkeit der vorherigen Verarbeitung bleibt unberührt.

Für diese Anliegen wenden Sie sich bitte an arbeitsschutz@stabe.info oder die in Abschnitt 1 genannte Anschrift. Die Ausübung Ihrer Datenschutzrechte setzt kein aktives Benutzerkonto voraus.

10. Beschwerderecht

Sie können sich nach Artikel 77 DSGVO bei einer Datenschutzaufsichtsbehörde beschweren, insbesondere am Ort Ihres gewöhnlichen Aufenthalts, Ihres Arbeitsplatzes oder des vermuteten Verstoßes. Für StaBe kommt insbesondere die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen in Betracht: Postfach 20 04 44, 40102 Düsseldorf; Telefon 0211 38424-0; E-Mail poststelle@ldi.nrw.de; Internet https://www.ldi.nrw.de.

11. Erforderliche Angaben und automatisierte Entscheidungen

Die für ein Benutzerkonto, die konkrete Auftragserfüllung oder gesetzlich erforderliche Nachweise notwendigen Angaben müssen für die jeweilige Nutzung bereitgestellt werden. Ohne sie kann ein Zugang gegebenenfalls nicht eingerichtet oder eine Leistung nicht vollständig erbracht werden. Zusätzliche, nicht erforderliche Freitext- oder Fotoangaben sind freiwillig und sollen auf das notwendige Maß beschränkt bleiben.

Die Anwendung unterstützt Berechnungen, Bewertungen und Terminübersichten. Diese ersetzen keine fachliche Prüfung. Eine ausschließlich automatisierte Entscheidung mit rechtlicher oder vergleichbar erheblicher Wirkung einschließlich Profiling im Sinne des Artikels 22 DSGVO findet im beschriebenen Anwendungsstand nicht statt.

12. Fassung und dokumentierte Kenntnisnahme

Diese Information beschreibt den Anwendungsstand mit zentraler Mitarbeiter-/Kundenzuweisung und objektbezogenem Kundenportal. Die aktuelle Fassung ist im Programm unter Datenschutz und als PDF abrufbar. Beim erstmaligen Zugang und nach Änderung der Informationsfassung wird die Kenntnisnahme mit Konto, Zeitpunkt und Versionskennung dokumentiert. Diese Bestätigung ist keine Einwilligung und beschränkt keine Datenschutzrechte.