Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO für myElectricPlan

VERANTWORTLICHER
Der Kunde, der myElectricPlan nutzt

AUFTRAGSVERARBEITER
Lumiotechsolutions UG (haftungsbeschränkt)
Hangstraße 20, 74743 Seckach, Deutschland

FASSUNG
1.0, Stand Oktober 2026. Vereinbart mit der Annahme der AGB bei der Registrierung.

Präambel

Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien, die sich aus der Nutzung der Software myElectricPlan nach den Allgemeinen Geschäftsbedingungen (im Folgenden „Hauptvertrag“) ergeben, soweit der Auftragsverarbeiter dabei personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Auftragsverarbeiter: Lumiotechsolutions UG (haftungsbeschränkt), Hangstraße 20, 74743 Seckach, Deutschland, E-Mail: support@myelectricplan.com, Datenschutz-Kontakt: contact@lumiotechsolutions.com (im Folgenden „Auftragsverarbeiter“).

Verantwortlicher: der Kunde, der myElectricPlan nutzt und diesen Vertrag abschließt (im Folgenden „Verantwortlicher“).

§ 1 Gegenstand und Dauer

(1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen bei der Bereitstellung der webbasierten Software myElectricPlan als Software-as-a-Service.

(2) Nicht Gegenstand dieses Vertrags ist die Verarbeitung von Daten, für die der Auftragsverarbeiter selbst Verantwortlicher ist, insbesondere die Verwaltung des Nutzerkontos, die Vertragsabwicklung einschließlich Kündigungen, die Abrechnung, der Support sowie eigene Kommunikation und Werbung. Hierfür gilt die Datenschutzerklärung des Auftragsverarbeiters.

(3) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags einschließlich etwaiger Projektlizenzen aus Einmalkäufen. Er endet nicht vor Abschluss der Löschung nach § 7.

§ 2 Art und Zweck der Verarbeitung, Art der Daten, Kategorien betroffener Personen

(1) **Art und Zweck:** Speicherung, Anzeige, Bearbeitung, Auswertung und Export der Daten, die der Verantwortliche in myElectricPlan eingibt oder hochlädt, zur Erstellung und Verwaltung elektrischer Planungen. Dazu gehören insbesondere Installationspläne auf Grundlage hochgeladener PDF-Grundrisse, Stromlaufpläne, Schaltschrankaufbauten, Stücklisten, Stromkreislisten, KNX-Gruppenadressen und Prüfberichte sowie die Erzeugung von PDF- und Tabellenexporten und die Bearbeitungshistorie (Rückgängig machen und Wiederherstellen).

(2) **Art der Daten:**

- Stammdaten von Auftraggebern und Bauherren des Verantwortlichen (z. B. Name, Firma, Anschrift, E-Mail-Adresse), soweit im Projekt erfasst;

- Angaben zum Objekt (z. B. Anschrift des Gebäudes, Raumbezeichnungen, Grundrisse und deren Inhalte);
- Daten in Prüfberichten (z. B. Name des Prüfers, Name, Ort und Datum der Bestätigung durch den Auftraggeber, Messwerte und Prüfergebnisse);
- Angaben zum ausführenden Betrieb, soweit im Projekt erfasst (Name, Anschrift, E-Mail-Adresse), sowie hochgeladene Logos und Deckblätter;
- Freitexte und Bezeichnungen, die der Verantwortliche in Projekten eingibt;
- Protokolldaten zu Änderungen an Projekten (Zeitpunkt, ausführender Nutzer, geänderte Werte).

Der Verantwortliche verarbeitet über myElectricPlan keine besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO. Gibt er solche Daten dennoch in Freitextfelder oder Uploads ein, geschieht dies in seiner Verantwortung.

(3) **Kategorien betroffener Personen:**

- Kunden, Auftraggeber, Bauherren und Eigentümer des Verantwortlichen sowie deren Ansprechpartner;
- Bewohner und Nutzer der geplanten Objekte, soweit sie aus Grundrissen oder Raumbezeichnungen erkennbar sind;
- Beschäftigte und Beauftragte des Verantwortlichen, die in Projekten genannt sind oder Projekte bearbeiten.

§ 3 Weisungen

(1) Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen werden durch den Hauptvertrag, diesen Vertrag und die Nutzung der Funktionen der Software durch den Verantwortlichen erteilt. Weitere Weisungen erteilt der Verantwortliche in Textform an support@myelectricplan.com. Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, werden als Änderungswunsch behandelt.

(3) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, weist er den Verantwortlichen unverzüglich darauf hin. Er darf die Ausführung der Weisung aussetzen, bis der Verantwortliche sie bestätigt oder ändert.

§ 4 Pflichten des Auftragsverarbeiters

(1) **Vertraulichkeit:** Der Auftragsverarbeiter setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Personen greifen auf Daten des Verantwortlichen nur zu, soweit es für die Leistungserbringung, den Betrieb, die Fehlerbehebung oder eine Supportanfrage des Verantwortlichen erforderlich ist.

(2) **Technische und organisatorische Maßnahmen:** Der Auftragsverarbeiter trifft die in Anlage 2 beschriebenen Maßnahmen nach Art. 32 DSGVO. Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf sie durch gleichwertige oder bessere Maßnahmen ersetzen; das Schutzniveau darf dabei nicht sinken. Wesentliche Änderungen werden dokumentiert. Eine aktuelle Übersicht der Maßnahmen stellt der Auftragsverarbeiter auf Anfrage zur Verfügung.

(3) **Ort der Verarbeitung:** Die Verarbeitung findet in der Europäischen Union statt. Eine Übermittlung in ein Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(4) **Unterstützung bei Betroffenenrechten:** Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte betroffener Personen nach Kapitel III DSGVO. Die Software ermöglicht dem Verantwortlichen, Daten selbst einzusehen, zu berichtigen, zu exportieren und zu löschen. Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst, soweit keine Weisung vorliegt.

(5) **Weitere Unterstützung:** Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der ihm vorliegenden Informationen bei den Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation). Für Unterstützungsleistungen, die über die Bereitstellung der vorhandenen Dokumentation hinausgehen und nicht auf einem Verstoß des Auftragsverarbeiters beruhen, kann er eine Vergütung nach tatsächlichem Aufwand zu einem angemessenen Stundensatz verlangen. Er weist den Verantwortlichen vorher auf die Vergütungspflicht hin.

(6) **Meldung von Datenschutzverletzungen:** Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten, die Daten des Verantwortlichen betrifft, ohne schuldhaftes Zögern, spätestens jedoch innerhalb von 48 Stunden, nachdem sie ihm bekannt geworden ist. Die Meldung erfolgt in Textform an die im Nutzerkonto hinterlegte E-Mail-Adresse und enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO. Fehlende Angaben werden unverzüglich nachgereicht. Der Auftragsverarbeiter ergreift unverzüglich Maßnahmen zur Eindämmung und zur Minderung möglicher nachteiliger Folgen.

(7) **Kontrolle und Information:** Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde, soweit sie die Verarbeitung nach diesem Vertrag betreffen.

(8) **Ansprechpartner für Datenschutz:** contact@lumiotechsolutions.com. Ein Datenschutzbeauftragter ist nicht benannt, da beim Auftragsverarbeiter keine Benennungspflicht nach Art. 37 DSGVO in Verbindung mit § 38 BDSG besteht.

(9) **Verzeichnis:** Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

§ 5 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 1 aufgeführt und gelten als genehmigt. Die aktuelle Übersicht ist unter https://myelectricplan.com/de/avv/ abrufbar.

(2) Der Auftragsverarbeiter teilt dem Verantwortlichen jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in der Regel mindestens 14 Tage vorab in Textform mit.

(3) Der Verantwortliche kann der Änderung aus wichtigem datenschutzrechtlichem Grund innerhalb dieser Frist in Textform widersprechen. Der Widerspruch ist zu begründen. Die Parteien bemühen sich um eine einvernehmliche Lösung. Kommt keine Lösung zustande, kann der Verantwortliche den Hauptvertrag zum Zeitpunkt des Wirksamwerdens der Änderung kündigen; bei einer Projektlizenz kann er stattdessen die Löschung des betroffenen Projekts nach § 7 verlangen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Änderung als genehmigt.

(4) Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. Er bleibt gegenüber dem Verantwortlichen für die Einhaltung dieser Pflichten durch den Unterauftragsverarbeiter verantwortlich.

(5) Keine Unterauftragsverarbeitung im Sinne dieses Vertrags sind Nebenleistungen, bei denen kein Zugriff auf Daten des Verantwortlichen besteht, etwa Telekommunikationsleistungen, Postdienste oder die reine Bereitstellung von Programmbibliotheken.

§ 6 Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO und diesem Vertrag zur Verfügung.

(2) Der Nachweis erfolgt vorrangig durch Dokumentation, insbesondere durch die Übersicht der technischen und organisatorischen Maßnahmen, Selbstauskünfte, Nachweise der Unterauftragsverarbeiter (z. B. deren Zertifikate oder Prüfberichte) und die Beantwortung schriftlicher Fragen.

(3) Reicht dies im Einzelfall nicht aus, kann der Verantwortliche nach rechtzeitiger Anmeldung, in der Regel mit einer Frist von mindestens 30 Tagen, eine Prüfung vor Ort zu den üblichen Geschäftszeiten durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen, der kein Wettbewerber des Auftragsverarbeiters ist. Die Prüfung darf den Betrieb nicht unverhältnismäßig stören und die Daten anderer Kunden nicht offenlegen. Vor-Ort-Prüfungen sind auf eine pro Kalenderjahr beschränkt, es sei denn, es liegt ein konkreter Anlass vor, etwa eine Datenschutzverletzung. Die Kosten der Prüfung trägt der Verantwortliche; der Aufwand des Auftragsverarbeiters wird nach tatsächlichem Aufwand zu einem angemessenen Stundensatz vergütet, es sei denn, die Prüfung deckt einen Verstoß des Auftragsverarbeiters auf. Rechte der Aufsichtsbehörden bleiben unberührt.

§ 7 Löschung und Rückgabe

(1) Der Verantwortliche kann seine Daten während der Vertragslaufzeit jederzeit mit den Funktionen der Software exportieren (insbesondere PDF-Exporte der Planungen und Prüfberichte sowie Tabellenexporte) und einzelne Projekte selbst löschen; ausgenommen sind Projekte, denen ein Einmalkauf zugeordnet ist, diese werden mit dem Konto gelöscht. Eine Rückgabe darüber hinaus erfolgt über diese Exportfunktionen; ein individueller Export ist nach AGB § 8 gesondert zu beauftragen.

(2) Projektdaten und hochgeladene Dateien werden gespeichert, solange das Nutzerkonto besteht und der Verantwortliche sie nicht selbst löscht. Das Ende eines Abonnements führt nicht zur Löschung (AGB § 8). Löscht der Verantwortliche ein Projekt, werden die Projektdaten sofort gelöscht. Hochgeladene Dateien, auf die danach kein Datensatz mehr verweist, entfernt ein täglicher automatischer Bereinigungslauf, spätestens am Folgetag. Dateien, die für das Rückgängigmachen von Änderungen in noch bestehenden Projekten benötigt werden oder von anderen Projekten des Verantwortlichen weiter genutzt werden, bleiben bis zum Wegfall dieses Bedarfs erhalten.

(3) Beantragt der Verantwortliche die Löschung seines Kontos über die Kontoeinstellungen der Software oder in Textform, wird das Konto zunächst deaktiviert und kann während einer Karenzzeit von 30 Tagen über den Wiederherstellungslink in der Bestätigungs-E-Mail oder über den Support wiederhergestellt werden. Nach Ablauf der Karenzzeit löscht der Auftragsverarbeiter das Konto und alle Daten des Verantwortlichen; die hochgeladenen Dateien entfernt der tägliche Bereinigungslauf nach Abs. 2 spätestens am Folgetag. Datensicherungen werden täglich erstellt und 30 Tage aufbewahrt; Kopien der gelöschten Daten in Datensicherungen sind damit spätestens 30 Tage nach der endgültigen Löschung beseitigt. Wird eine Datensicherung in diesem Zeitraum wiederhergestellt, werden bereits gelöschte Daten erneut gelöscht.

(4) Gesetzliche Aufbewahrungspflichten des Auftragsverarbeiters bleiben unberührt; sie betreffen keine Projektdaten. Der Auftragsverarbeiter bestätigt die Löschung auf Anfrage in Textform.

§ 8 Haftung

Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregeln des Hauptvertrags (AGB § 11) auch für diesen Vertrag, soweit gesetzlich zulässig.

§ 9 Schlussbestimmungen

(1) **Vertragsschluss:** Dieser Vertrag ist Bestandteil der Allgemeinen Geschäftsbedingungen. Er wird mit der Annahme der AGB bei der Registrierung vereinbart. Für Kunden, die sich vor Aufnahme dieses Vertrags in die AGB registriert haben, wird er nach dem Verfahren für Änderungen der AGB (AGB § 14) Vertragsbestandteil. Der Auftragsverarbeiter speichert Zeitpunkt und Fassung der Annahme. Der Vertragstext ist unter https://myelectricplan.com/de/avv/ abrufbar und kann in den Einstellungen der Software als PDF gespeichert werden. Die elektronische Form genügt den Anforderungen des Art. 28 Abs. 9 DSGVO.

(2) **Vorrang:** Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen in Fragen des Datenschutzes die Regelungen dieses Vertrags vor.

(3) **Änderungen:** Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Änderungen der Anlage 1 richten sich nach § 5, Änderungen der Anlage 2 nach § 4 Abs. 2.

(4) **Anwendbares Recht und Gerichtsstand:** Es gilt deutsches Recht. Für den Gerichtsstand gilt AGB § 17.

(5) **Salvatorische Klausel:** Sollte eine Bestimmung dieses Vertrags unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine Regelung, die den Anforderungen des Art. 28 DSGVO entspricht.

Fassung 1.0, Stand Oktober 2026

Anlage 1: Unterauftragsverarbeiter

Teil A: Unterauftragsverarbeiter mit Zugriff auf Daten des Verantwortlichen

Name	Anschrift	Zweck	Ort der Verarbeitung	Grundlage der Übermittlung
netcup GmbH	Daimlerstraße 25, 76185 Karlsruhe, Deutschland	Hosting der Anwendung, der Datenbank und der hochgeladenen Dateien; Erzeugung der PDF-Exporte auf dem eigenen Server; Datensicherung (Backups); E-Mail-Postfach für Supportanfragen	Deutschland	Keine Drittlandübermittlung; AVV nach Art. 28 DSGVO

Teil B: Hinweise zu weiteren Diensten

Die folgenden Dienste erhalten nach dem Stand der Prüfung keine Projektdaten. Sie werden hier zur Transparenz genannt.

- **Resend** (Plus Five Five, Inc., San Francisco, USA): Versand von System-E-Mails (Bestätigung der E-Mail-Adresse, Passwort zurücksetzen, Abonnement- und Kontomitteilungen, Rechnungen, Kündigungsbestätigungen, Marketing-E-Mails). Die E-Mails enthalten keine Projektinhalte und keine

Exporte. Übermittelt werden Daten der Nutzer selbst, für die der Auftragsverarbeiter Verantwortlicher ist. Übermittlung in die USA auf Grundlage der Standardvertragsklauseln (Datenschutzerklärung § 6).

- **Stripe** (Stripe Payments Europe Ltd., Dublin, Irland): Zahlungsabwicklung und Ausführung von Kündigungen. Stripe handelt als eigener Verantwortlicher und erhält keine Projektdaten.
- **Lexware** (Haufe-Lexware GmbH & Co. KG): Rechnungserstellung für den Auftragsverarbeiter. Erhält nur Rechnungsdaten des Kunden, keine Projektdaten.
- **Brevo** (Sendinblue GmbH): Pflege der Kontaktdaten der Nutzer für eigene Kommunikation (E-Mail-Adresse, Vor- und Nachname, Sprache, Abostatus, Marketing-Einwilligung, Registrierungsdatum). Keine Projektdaten.
- **Google** (Anmeldung mit Google-Konto) sowie **Google Ads** und **Meta-Pixel** (nur mit Einwilligung): eigene Verarbeitung des Auftragsverarbeiters bzw. gemeinsame Verantwortlichkeit nach Datenschutzerklärung § 7; keine Projektdaten.

Anlage 2: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Der Auftragsverarbeiter betreibt myElectricPlan auf einem angemieteten Server bei netcup in Deutschland. Eigene Büroräume mit Serverbetrieb bestehen nicht; physische Maßnahmen am Rechenzentrum erbringt netcup.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

- Physischer Schutz des Rechenzentrums durch netcup nach deren TOMs.

Zugangskontrolle

- Anmeldung an der Anwendung mit E-Mail-Adresse und Passwort oder mit Google-Konto; die E-Mail-Adresse wird vor der Nutzung bestätigt.
- Passwörter werden ausschließlich als bcrypt-Hash (12 Runden) gespeichert.
- Kurzlebige, mit RS256 signierte Zugriffstoken (15 Minuten) und rotierende Aktualisierungstoken (7 Tage) in HttpOnly-Cookies mit Secure- und SameSite-Attribut. Die Wiederverwendung eines bereits rotierten Tokens wird als Diebstahl erkannt und beendet die Sitzungsfamilie; abgelaufene Token werden regelmäßig gelöscht.
- Nutzer können alle anderen Sitzungen beenden; bei Kontolöschung werden alle Sitzungen widerrufen.
- Begrenzung der Anfragerate an Anmeldung, Registrierung, Passwort-Zurücksetzen, Token-Erneuerung und öffentlichen Formularen.
- Server- und Datenbankzugang haben höchstens drei namentlich bestimmte Personen.
- Eine Firewall lässt nur die für den Betrieb nötigen Ports zu; die Datenbank ist nicht aus dem Internet erreichbar, sondern nur im internen Netz der Anwendung.
- Das Kundenkonto beim Hoster ist mit Zwei-Faktor-Authentifizierung geschützt.
- Eine Zwei-Faktor-Authentifizierung für Nutzer der Anwendung besteht derzeit nicht.

Zugriffskontrolle

- Jeder Zugriff auf ein Projekt und seine Inhalte wird serverseitig gegen das Nutzerkonto geprüft; Abfragen sind auf die Projekte des angemeldeten Nutzers beschränkt.
- Downloads von Exporten werden über die Berechtigung am zugehörigen Projekt geprüft.
- Interne Administrationsoberfläche als getrennte Anwendung, nur für Konten mit Administratorrecht.
- Dateizugriffe auf Symbolgrafiken laufen über eine zentrale Pfadprüfung, die Zugriffe außerhalb der Bibliothek verhindert; hochgeladene SVG-Dateien werden mit einem gehärteten XML-Parser verarbeitet.
- Mitarbeiter greifen auf Projektdaten nur für Betrieb, Fehlerbehebung oder auf Supportanfrage des Verantwortlichen zu.
- Daten aus dem Produktivbetrieb werden in Entwicklungsumgebungen nur anonymisiert verwendet.

Trennungskontrolle

- Mandantentrennung auf Anwendungsebene über Nutzerkonto, Arbeitsbereich und Projekt.
- Getrennte Umgebungen für Entwicklung und Produktion; in der Produktion sind die Schnittstellendokumentation und die OpenAPI-Beschreibung abgeschaltet.
- Getrennte Zugangsdaten für Test- und Live-Betrieb der Zahlungsabwicklung.

Pseudonymisierung und Verschlüsselung

- Hochgeladene Dateien und Exporte werden unter zufälligen Dateinamen (UUID) gespeichert, nicht unter dem ursprünglichen Dateinamen.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

- Übertragung zwischen Browser und Server ausschließlich verschlüsselt über HTTPS/TLS; HSTS mit einer Gültigkeit von einem Jahr.
- Sicherheitsheader gegen Einbettung in fremde Seiten und MIME-Sniffing (X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy).
- Cross-Origin-Anfragen nur von festgelegten eigenen Domains.
- Webhooks des Zahlungsdienstleisters werden über Signaturprüfung verifiziert.
- PDF-Exporte werden auf dem eigenen Server erzeugt; Projektdaten werden dafür nicht an Dritte übermittelt.

Eingabekontrolle

- Jede Änderung an Projektdaten wird in einer Änderungshistorie je Anfrage mit Zeitpunkt und ausführendem Nutzer protokolliert und kann rückgängig gemacht werden.
- Anfragebezogene Protokollierung mit Anfrage-ID und Nutzerkennung. Server-Logfiles werden maximal 7 Tage aufbewahrt.
- Eingaben werden serverseitig validiert; fehlerhafte Verweise auf Dateien werden abgewiesen, bevor sie gespeichert werden.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Tägliche Datensicherung von Datenbank und Dateien bei netcup mit einem Ziel von höchstens 24 Stunden Datenverlust (RPO, AGB § 4); Aufbewahrung 30 Tage, danach werden die Sicherungen überschrieben.
- Wiederherstellung aus Backups ist durch ein Skript geregelt und wird praktisch genutzt.
- Betrieb in Containern; Bereitstellung neuer Versionen über automatisch gebaute Images, Datenbankmigrationen werden beim Start versioniert angewendet.
- Begrenzung der Anfragerate und paralleler PDF-Erzeugung zum Schutz vor Überlastung.
- Rechenzentrum mit redundanter Strom- und Netzversorgung durch netcup.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Codeänderungen werden über Pull Requests mit automatischer Prüfung (Tests, Linting, Typprüfung) eingespielt.
- Automatisierte Backend-, Frontend- und End-to-End-Tests bei jedem Pull Request, unter anderem für die vollständige Erfassung von Änderungen in der Änderungshistorie.
- Regelmäßige Sicherheitsupdates von Betriebssystem, Laufzeitumgebung und Abhängigkeiten.
- Prozess für Datenschutzvorfälle mit Meldung an den Verantwortlichen nach § 4 Abs. 6.
- Verpflichtung der eingesetzten Personen auf Vertraulichkeit und regelmäßige Datenschutzschulung.
- Datenschutzfreundliche Voreinstellungen: Marketing-Cookies und Tracking in der Anwendung nur nach Einwilligung; Projektdaten werden nicht für eigene Zwecke des Auftragsverarbeiters ausgewertet.
- Überprüfung dieser Anlage mindestens einmal jährlich.