Vertrag über
die Auftragsverarbeitung personenbezogener Daten mit NU

1. Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Datengeber und -verarbeiter (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Dieser Vertrag gilt erst wenn beiden Parteien ihn wirksam im Hauptvertrag unterzeichnet haben.

(3) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Datenverarbeiters personenbezogene Daten des Datengebers verarbeiten.

(4) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Datenverarbeiter übernimmt folgende Verarbeitungen: Es werden personenbezogene Daten, die vom Datengeber in beliebiger Form (digital, analog) auf Anforderung des Datenverarbeiters bereitgestellt werden, verarbeitet. Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Vertrages zu dem dort bezeichneten Projekt (im Folgenden „Hauptvertrag“).

2.2 Dauer

Die Verarbeitung beginnt und endet mit den Fristen des Hauptvertrages und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei oder mit Ablauf der gesetzlich vorgeschriebenen Fristen nach Abschluss des dem Hauptauftrages zu Grunde liegenden Projektes.

3. Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

3.1 Art und Zweck der Verarbeitung

Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten.

Die Verarbeitung dient folgendem Zweck: Die Verarbeitung der personenbezogenen Daten erfolgt aufgrund des berechtigten Interesses des Datenverarbeiters dieses Vertrages zur Erfüllung seiner vertraglich vereinbarten Leistungen und gesetzlichen Verpflichtungen.

3.2 Art der Daten

Es werden folgende Daten verarbeitet:
Vorname, Name, Geburtsdatum, Staatsangehörigkeit, Passbild, Kommunikationsdaten (z.B. Emailadresse, Telefon, Anschrift), Sozialversicherungsausweis-/ersatzausweisnummer, Sozial-, Krankenversicherungsnummer, Aufenthaltserlaubnis-Nr. inkl. Gültigkeit und Ausweisdokumenten-Nummer.

3.3 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind Mitarbeiter des Datengebers dieses Vertrages. Der Datenverarbeiter verarbeitet personenbezogene Daten ausschließlich im sachlichen und zeitlichen Rahmen des Hauptvertrages sowie nach Weisung des Projekt-Auftraggebers. Der Datenverarbeiter verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Die Verarbeitung der Daten findet ausschließlich im Geltungsgebiet der EU-DSGVO statt.

4. Technische und organisatorische Maßnahmen des Datenverarbeiters

(1) Der Datenverarbeiter wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Datengebers treffen, die den gesetzlichen Anforderungen genügen. Hierbei sind die Vertraulichkeit, Integrität,

Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

(2) Der Datenverarbeiter gewährleistet ein Verfahren zur Überprüfung der technischen und organisatorischen Maßnahmen. Er ist verpflichtet, die technischen und organisatorischen Maßnahmen an den Stand der Technik anzupassen, soweit dies erforderlich und wirtschaftlich zumutbar ist. Der Datengeber ist über wesentliche Änderungen vorab zu informieren. Die Änderungen sind schriftlich niederzulegen und werden Vertragsbestandteil. Vorschläge des Datengebers für Änderungen hat der Datenverarbeiter zu prüfen. Der Datengeber ist über das Ergebnis zu informieren.

(3) Beauftragt der Datenverarbeiter zur Erfüllung seiner vertraglichen Pflichten einen Unterdatenverarbeiter, stellt er sicher, dass die erforderlichen technischen und organisatorischen Maßnahmen vom Unterdatenverarbeiter getroffen werden und dem Stand der Technik entsprechen.

4.1 Organisatorische Maßnahmen

Der betriebliche Datenschutzbeauftragte ist unter Pkt. 5 genannt.

☒ Mitarbeiter wurden nachweislich über Datenschutzrecht und Datensicherheit geschult.
☒ Alle Mitarbeiter sind nachweislich auf das Datengeheimnis, ggf. auf das Fernmeldegeheimnis, verpflichtet.
☒ Ein Datensicherheitskonzept/ Informationssicherheitsmanagement ist vorhanden.
☒ Verhaltensregeln nach Art. 40 DSGVO sind vorhanden.

4.2 Vertraulichkeit

a) Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle
Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden.

☒ Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)
☒ Manuelles Schließsystem
☒ Empfang mit Anmeldung
☒ Sorgfältige Auswahl von Reinigungspersonal
☒ Feuerfeste Türen

b) Zugangs- und Benutzerkontrolle
Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

☒ Passwortvergabe
Länge des Passworts: min. 6 Zeichen
Wechselfristen: 120 Tage
Anzahl der Fehleingaben: keine Beschränkung
☒ Authentifikation mit Benutzername/Passwort
☒ Einsatz von VPN-Technologie

c) Zugriffskontrolle
Maßnahmen, die gewährleisten, dass Personen nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

☒ Schriftliches Berechtigungskonzept vorhanden
☒ Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen
☒ Verwaltung der Rechte durch System-Administrator
☒ Anzahl der Administratoren auf das "Notwendigste" reduziert
☒ Einsatz von Akten-/Datenträgervernichtern bzw. Dienstleistern unter Beachtung von DIN 66399
☒ Sichere Aufbewahrung von Datenträgern
☒ Ordnungsgemäße Vernichtung von Datenträgern
☒ Protokollierung der Vernichtung

d) Transport- und Übertragungskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
☒ Firewall: Die nach dem Stand der Technik erforderlichen Firewall-Technologien sind implementiert und werden auf dem aktuellen Stand gehalten
☒ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
☒ Protokollierung von Übermittlungen
☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen

e) Auftragskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragnehmers verarbeitet werden können.

☒ Vorhandene Vereinbarungen zur Auftragsverarbeitung
☒ Kontrolle der Vertragsausführung
☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☒ Regelung zu Wartungen (speziell Fernwartung)

4.3 Integrität

a) Eingabekontrolle/Verarbeitungskontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

b) Dokumentationskontrolle
Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

☒ Führung eines Verarbeitungsverzeichnisses
☒ Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration

4.4 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und im Störfall wieder hergestellt werden können.

☒ Unterbrechungsfreie Stromversorgung (USV)
☒ Testen von Datenwiederherstellung
☒ Klimaanlage in Serverräumen
☒ Schutzsteckdosenleisten in Serverräumen
☒ Feuerlöschgeräte in Serverräumen
☒ Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort)
☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
☒ Virenschutzsystem
☒ Spiegelung von Festplatten (z. B. RAID-Verfahren)

4.5 Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

☒ Physikalisch getrennte Speicherung

☒ Logische Mandantentrennung (softwareseitig)
☒ Trennung von Produktiv- und Testsystem
☒ Festlegung Technologie von Datenbankrechten
☒ Trennung von Daten verschiedener Auftraggeber

Für die Vernichtung gem. DIN 66399 gilt Schutzklasse 1.

5. Kontrollen und sonstige Pflichten des Datenverarbeiters

(1) Der Datenverarbeiter ist verpflichtet, das Datengeheimnis sowie etwaige berufliche Verschwiegenheitsverpflichtungen zu wahren. Er hat bei der Verarbeitung ausschließlich Beschäftigte einzusetzen, die entsprechend verpflichtet und geschult sind. Er hat insbesondere sicherzustellen, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung dieses Vertrages betraut sind, sorgfältig ausgewählt werden, die gesetzlichen Datenschutzbestimmungen beachten und die vom Datengeber erlangten Informationen nicht unbefugt an Dritte weitergeben oder anderweitig verwerten.

Der Datenverarbeiter nennt dem Datengeber den Ansprechpartner für sämtliche vertragsrelevanten Angelegenheiten des Datenschutzes. Der Datenverarbeiter hat einen betrieblichen Datenschutzbeauftragten bestellt.

	Verantwortlicher	Datenschutzbeauftragter
Name	BAUER Elektroanlagen Holding GmbH	zu kontaktieren unter: datenschutz@bauer-netz.de
Adresse	Kaspar-Graf-Str. 2	
PLZ / Ort	84428 Buchbach	
Telefon	08086/9300-0	
E-Mail:	info@bauer-netz.de	

(2) Der Datenverarbeiter ist verpflichtet, ein Verarbeitungsverzeichnis gemäß Art. 30 Abs. 2 DSGVO zu führen. Der Datenverarbeiter gewährt dem zuständigen Landesdatenschutzbeauftragten Zugang zu den Arbeitsräumen und unterwirft sich der Kontrolle nach Maßgabe des Landesdatenschutzgesetzes in seiner jeweiligen Fassung. Der Datenverarbeiter informiert den Datengeber unverzüglich über Kontroll- und Ermittlungshandlungen der Aufsichtsbehörde.

6. Regelungen zur Berichtigung, Sperrung und Löschung von Daten, Auskunft über Daten

(1) Der Datenverarbeiter hat die Daten nach Weisung des Datengebers zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Datenverarbeiter zwecks Berichtigung, Sperrung oder Löschung seiner Daten wendet, leitet der Datenverarbeiter dieses Ersuchen unverzüglich an den Datengeber weiter. Das gleiche gilt für Auskunftsersuche.

7. Unterauftragsverhältnisse (z. B. Projekt-AG, Planer, Sicherheitsdienst)

(1) Der Datengeber genehmigt die im Hauptvertrag benannten Unterauftragsverhältnisse, die der Datenverarbeiter vor Abschluss dieser Vereinbarung begründet hat. Über Änderungen hat der Datenverarbeiter den Datengeber unverzüglich zu informieren. Der Abschluss neuer Unterauftragsverhältnisse bedarf der vorherigen Zustimmung des Datengebers.

(2) Der Datenverarbeiter hat dem Unterdatenverarbeiter dieselben Pflichten aufzuerlegen, die er selbst gegenüber dem Datengeber zu erfüllen hat. Der Unterdatenverarbeiter ist sorgfältig auszuwählen. Der Datenverarbeiter haftet gegenüber dem Datengeber vollumfänglich für Datenverstöße seiner Unterdatenverarbeiter.

8. Kontrollrechte des Datengebers

(1) Der Datengeber hat das Recht, vor Beginn und während der Datenverarbeitung die Einhaltung der vom Datenverarbeiter sowie von den Unterdatenverarbeitern getroffenen technischen und organisatorischen Maßnahmen zu kontrollieren oder von zu benennenden Prüfern kontrollieren zu lassen. Das Ergebnis ist zu dokumentieren.

(2) Der Datenverarbeiter gewährleistet die Möglichkeit zur Kontrolle. Hierzu weist er dem Datengeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO nach. Der Nachweis kann durch Vorlage aktueller Testate oder durch Berichte unabhängiger Prüfer (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Datenschutzauditoren, Qualitätsauditoren) erbracht werden.

(3) Haben sich der Datenverarbeiter und die von ihm beauftragten Unterdatenverarbeiter Verhaltensregeln unterworfen oder ein Zertifizierungsverfahren erfolgreich durchlaufen, sind sie verpflichtet, dem Datengeber dies nachzuweisen. Zertifikate sind zu aktualisieren.

(4) Der Datengeber ist berechtigt, einmal in 12 Monaten eine Stichprobenkontrolle durchzuführen. Dies ist den Ansprechpartnern des Datenverarbeiters anzukündigen.

9. Mitteilungspflichten

(1) Der Datengeber meldet dem Datenverarbeiter unverzüglich sämtliche Verstöße gegen Pflichten aus diesem Vertrag. Dies gilt insbesondere bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten. Der Datenverarbeiter hat im Benehmen mit dem Datengeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung bzw. zum Ausschluss möglicher nachteiliger Folgen für die Betroffenen zu ergreifen.

10. Weisungen

(1) Der Datengeber ist berechtigt, dem Datenverarbeiter jederzeit Weisungen zu erteilen, insbesondere hinsichtlich der Art, des Umfangs und des Zeitpunkts der Verarbeitung von Daten. Die Weisungen des Datengebers erfolgen in Textform.

(2) Erachtet der Datenverarbeiter eine Weisung des Datengebers als rechtswidrig, hat er den Datengeber unverzüglich darauf hinzuweisen. Er ist berechtigt, die Durchführung der Weisung auszusetzen, bis sie durch den Datengeber bestätigt oder geändert wird.

(3) Erteilt der Datengeber Einzelweisungen bzgl. des Umgangs mit personenbezogenen Daten, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, z.B. Änderungen der technischen und organisatorischen Maßnahmen, werden sie als Antrag auf Leistungsänderung behandelt.

(4) Zur Erteilung und Annahme von Weisungen sind ausschließlich die im Hauptvertrag genannten Personen und der Verantwortliche befugt.

11. Beendigung des Auftrags

(1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Datengebers hat der Datenverarbeiter die im Auftrag verarbeiteten Daten nach Wahl des Datengebers entweder zu vernichten oder an den Datengeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt mindestens Schutzklasse 1.

(2) Der Datenverarbeiter ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Unterdatenverarbeitern unter Pkt. 7 herbeizuführen.

(3) Der Datenverarbeiter hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Datengeber unverzüglich vorzulegen.

(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Datenverarbeiter den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Datengeber bei Vertragsende übergeben.

12. Vergütung

Die Vergütung des Datengebers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

13. Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Datenverarbeiter und Datengeber als Gesamtschuldner.

(2) Der Datenverarbeiter trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Datenverarbeiter dem Datengeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Datengeber erhoben werden. Unter diesen Voraussetzungen ersetzt der Datenverarbeiter dem Datengeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

(3) Der Datenverarbeiter haftet dem Datengeber für Schäden, die der Datenverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Unterdatenverarbeiter im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

(4) Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Datengeber erteilten Weisung entstanden ist.