Allgemeine Vertragsbedingungen

Stand: 01.07.2025

§ 1 Vertragsgegenstand

Die nPro Energy GmbH (nachfolgend „Anbieter“ genannt) ermöglicht im Wege des sogenannten Software-as-a-Service (SaaS) die zeitweise Nutzung der Softwareapplikation nPro - erreichbar unter https://www.npro.energy - per Fernzugriff durch die Verwendung eines Internet-Browsers. Der Anbieter erbringt während der Laufzeit des Vertrages folgende Leistungen:

(1) Der Anbieter stellt dem Kunden die Softwareapplikation und deren Funktionen zur zeitlich befristeten Nutzung per Fernzugriff zu eigenen Zwecken zur Verfügung.
(2) Der Anbieter stellt dem Kunden zudem die erforderlichen Serverkapazitäten zur Speicherung und weiteren Bearbeitung der vom Benutzer mit dem Softwaretool erzeugten Daten zur Verfügung.
(3) Weitergehende Rechte an der Softwareapplikation werden nicht eingeräumt. Insbesondere ist der Vertragspartner nicht berechtigt, die Softwareapplikation zu vervielfältigen, zu veräußern oder zeitlich begrenzt zu überlassen, vor allem nicht zu vermieten oder zu verleihen oder sie über die vertraglich vereinbarte Nutzung und die vorliegenden Bedingungen hinaus zu nutzen oder Dritten zugänglich zu machen.
(4) Mit der Nutzung der Software akzeptiert der Kunde die Nutzungsbedingungen einschließlich des Vertrags zur Auftragsverarbeitung (Anhang).

§ 2 Vergütung

(1) Für die Nutzung der Softwareapplikation fallen die vereinbarten Nutzungsentgelte an. Jede Benutzerlizenz ist mit genau einem Benutzerkonto verknüpft. Die Benutzerkonten sind von den Benutzern selbst in der Softwareapplikation anzulegen. Hierbei ist eine personengebundene E-Mail-Adresse (keine Funktions-E-Mail-Adresse) zu verwenden.
(2) Das Nutzungsentgelt wird im Voraus in Rechnung gestellt. Bei Überschreiten der Zahlungsfrist kann der Zugriff auf die Softwareapplikation eingeschränkt werden.

§ 3 Vertragslaufzeit und Kündigung

(1) Der Kunde hat bei Vertragsschluss die Wahl zwischen einem **Prepaid-Modell** mit begrenzter Laufzeit und einem **Abonnement** mit automatischer Lizenzverlängerung.
   a. **Prepaid-Modell**: Die Laufzeit für die Bereitstellung der Softwareapplikation wird bei Vertragsschluss individuell vereinbart. Der Vertrag endet nach Ablauf des vereinbarten Nutzungszeitraums automatisch; eine Kündigung ist nicht erforderlich. Der Kunde kann den Nutzungszeitraum jederzeit durch eine weitere Buchung um ein Jahr verlängern.
   b. **Abonnement-Modell**: Die Vertragslaufzeit verlängert sich nach Ablauf des Nutzungszeitraums automatisch um jeweils ein weiteres Jahr (12 Monate). Die Kündigung kann formlos, zum Beispiel per E-Mail, erfolgen. Sie muss spätestens 14 Tage vor Ende der aktuellen Vertragslaufzeit beim Anbieter eingehen.
(2) Nach Beendigung des Vertragsverhältnisses ist der Anbieter verpflichtet, auf Anweisung des Kunden sämtliche auf dem eigenen Server gespeicherten Kundendaten vollständig zu löschen. Die Löschung erfolgt unter Berücksichtigung etwaiger gesetzlicher Aufbewahrungspflichten sowie technischer Anforderungen an Datensicherungen (Backups).

§ 4 Verfügbarkeit der Software (Service Level Agreement)

(1) Die Vertragssoftware steht grundsätzlich an **sieben Tagen der Woche jeweils 24 Stunden** zur Verfügung. Die durchschnittliche Verfügbarkeit während der Hauptzeit beträgt **99 % im Jahresmittel**. Die Hauptzeit ist – mit Ausnahme bundeseinheitlicher Feiertage – von Montag bis Freitag in der Zeit von 7 Uhr bis 18 Uhr mitteleuropäischer Zeit. Der Anbieter ist nicht für internet-/netzbedingte

Ausfallzeiten verantwortlich, in denen die Vertragssoftware aufgrund von technischen oder sonstigen Problemen, die nicht im Einflussbereich des Anbieters liegen, nicht verfügbar ist.

(2) Wird die vertraglich geschuldete Verfügbarkeit aus vom Anbieter oder ihren Erfüllungsgehilfen zu vertretenden Gründen nicht erreicht, so ist der Vertragspartner berechtigt, das Nutzungsentgelt entsprechend dem Anteil der Verfügbarkeitsunterbrechung zu mindern.

(3) Der Anbieter kann die Softwareapplikation jederzeit aktualisieren und erweitern, ohne eine vorherige Benachrichtigung oder Zustimmung des Kunden.

§ 5 Mitwirkungspflichten und Obliegenheiten des Kunden

(1) Der Vertragspartner ist für die Eingabe, Pflege und Inhalte der zur Nutzung der angebotenen Services erforderlichen Daten und Informationen selbst verantwortlich. Der Vertragspartner wird auf dem Computer, über den er die Services nutzt, dem Stand der Technik entsprechende und regelmäßig aktualisierte **Virenschutzprogramme** einsetzen und die von ihm erzeugten Daten und Informationen vor der Übermittlung auf schädliche Codes, insbesondere auf Viren prüfen.

(2) Die **Zugangsdaten** des Vertragspartners dürfen nicht an Dritte weitergegeben werden und sind vor dem Zugriff durch Dritte geschützt aufzubewahren.

§ 6 Support

(1) Der Anbieter stellt dem Kunden einen technischen Support zur Verfügung. Dieser ist im begrenzten Umfang im Lizenzpreis kostenfrei enthalten. Sollte der Bedarf an technischem Support ein übliches Maß überschreiten, kann ein separates Support-Paket hinzugebucht werden. Der technische Support wird **per E-Mail, Telefon oder Videoanruf** zur Verfügung gestellt.

(2) Der Anbieter erbringt Schulungsleistungen nach gesonderter Beauftragung und gegen gesonderte Vergütung. Programmierungsaufwand zur Herstellung von besonderen, an die Wünsche des Kunden angepassten Funktionalitäten wird individuell nach Aufwand zu gesondert zu vereinbarenden Stundensätzen berechnet.

§ 7 Mängelansprüche

(1) Der Anbieter übernimmt die Pflege der Services einschließlich der dazugehörigen Softwareapplikation.

(2) Sachmängel der angebotenen Services werden vom Anbieter innerhalb einer angemessenen Frist beseitigt. Ein Sachmangel liegt vor, wenn die Software nicht die vertraglich vereinbarte Beschaffenheit aufweist. Unerhebliche Abweichungen stellen keinen Mangel dar. Fehler der Softwareapplikation sind nur reproduzierbare Abweichungen von den vertraglich und in der Benutzerdokumentation festgelegten Spezifikationen.

(3) Ansprüche nach § 536a BGB, insbesondere die verschuldensunabhängige Garantiehaftung und das Selbstvornahmerecht betreffend, sind ausgeschlossen.

§ 8 Haftung

(1) Der Anbieter haftet für die Verletzung wesentlicher Vertragspflichten (sog. Kardinalspflichten). Soweit die Kardinalspflichten fahrlässig verletzt wurden, ist der Schadensersatzanspruch des Kunden begrenzt auf den vertragstypisch vorhersehbaren Schaden, maximal jedoch auf einen Betrag in Höhe von 10.000,-- €.

(2) Der Anbieter haftet nicht für Schäden, die auf schädlichen Code (Virusbefall), Hackerangriffe, Softwarefehler oder Datenverlust zurückzuführen sind.

(3) Die Haftung des Anbieters für Schäden, die durch höhere Gewalt, technische Störungen außerhalb des Einflussbereichs des Anbieters oder durch unzureichende Sicherheitsmaßnahmen des Kunden verursacht wurden, ist ausgeschlossen.

(4) Der Anbieter haftet nicht für mangelnden wirtschaftlichen Erfolg, entgangenen Gewinn, mittelbare Schäden, Mangelfolgeschäden und Ansprüche Dritter, die durch die Nutzung der Software entstehen. Eine Haftung für die Richtigkeit und Vollständigkeit der Berechnungsmethoden und -ergebnisse wird nicht übernommen werden.

(5) Der Anbieter haftet gemäß den gesetzlichen Bestimmungen nach den Vorschriften des Produkthaftungsgesetzes und für Schäden, die durch die Verletzung des Lebens, des Körpers oder der Gesundheit des Kunden entstanden sind.

(6) Die Haftungsbeschränkungen gemäß vorstehender Ziffern gelten ebenso für Erfüllungsgehilfen vom Anbieter.

§ 9 Geheimhaltung und Datenschutz

(1) Der Anbieter verarbeitet personenbezogene Daten ausschließlich als Auftragsverarbeiter gemäß Art. 28 DSGVO. Die Rechte und Pflichten der Parteien zur Auftragsverarbeitung sind im **Vertrag zur Auftragsverarbeitung** geregelt, der Bestandteil dieser Nutzungsbedingungen ist. Durch die Nutzung der Software erklärt sich der Kunde mit diesen Regelungen einverstanden.

(2) Die Parteien sind verpflichtet, alle ihnen im Zusammenhang mit diesem Vertrag bekannt gewordenen vertraulichen Informationen über die jeweils andere Partei dauerhaft geheim zu halten, nicht an Dritte weiterzugeben, aufzuzeichnen oder in anderer Weise zu verwerten, sofern die jeweils andere Partei der Offenlegung oder Verwendung nicht ausdrücklich und schriftlich zugestimmt hat. Diese Verpflichtungen sind auch auf den Zeitraum nach Beendigung des Vertragsverhältnisses anzuwenden.

(3) **Projektbezogene Daten**, die vom Benutzer in der Software eingegeben werden, **werden streng vertraulich behandelt** und keinem Dritten zugänglich gemacht. Die Vertraulichkeit gilt insbesondere für sämtliche projektbezogene Daten und andere sensible Informationen. Diese Verpflichtung zur Vertraulichkeit bleibt auch über die Beendigung des Vertragsverhältnisses hinaus bestehen.

(4) Mit dem Abschluss des Vertrages gewährt der Kunde dem Anbieter das Recht, ihn medienübergreifend, insbesondere auf seiner Internetseite, gegenüber Dritten als Referenzunternehmen öffentlich für Werbezwecke zu benennen und hierfür das Logo des Kunden verwenden zu dürfen. Der Kunde kann diese Genehmigung jederzeit schriftlich widerrufen.

§ 10 Änderungen der Vertragsbedingungen, Leistungsbeschreibungen und Preise

(1) Die Leistungsbeschreibungen können geändert werden, wenn dies aus triftigem Grund erforderlich ist, der Vertragspartner hierdurch gegenüber der bei Vertragsschluss einbezogenen Leistungsbeschreibung objektiv nicht schlechter gestellt wird (z. B. Beibehaltung oder Verbesserung von Funktionalitäten) und von dieser nicht deutlich abgewichen wird.

(2) Die vereinbarten Preise können zum Ausgleich von gestiegenen Kosten erhöht werden. Dies ist z. B. der Fall, wenn Dritte, von denen der Anbieter zur Erbringung der nach diesem Vertrag geschuldeten Leistungen notwendige Vorleistungen bezieht, ihre Preise erhöhen. Ferner sind Preiserhöhungen in dem Maß möglich, in dem es durch eine Erhöhung der Umsatzsteuer veranlasst ist.

(3) Bei Änderungen der Vertragsbedingungen, der Leistungsbeschreibungen sowie Preiserhöhungen steht dem Vertragspartner zum Zeitpunkt des Wirksamwerdens der Änderungen ein Sonderkündigungsrecht zu.

§ 11 Schlussbestimmungen

(1) Vertragsänderungen und Nebenabreden bedürfen zu ihrer Gültigkeit der Schrift-, Text- oder elektronischen Form.

(2) Widersprechende Allgemeine Geschäftsbedingungen des Kunden gelten nur, wenn und soweit der Anbieter ihnen ausdrücklich schriftlich zugestimmt hat.

(3) Der Kunde kann die Rechte und Pflichten aus diesem Vertrag nur nach vorheriger schriftlicher Zustimmung des Anbieters auf einen Dritten übertragen.

(4) Diese Vertragsbedingungen gelten ausschließlich. Anderweitigen Geschäftsbedingungen des Anbieters, des Kunden oder Dritter wird hier hiermit ausdrücklich widersprochen.

(5) Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam sein oder nach Vertragsschluss unwirksam werden, so wird die Wirksamkeit der übrigen Bestimmungen hierdurch nicht berührt. Die Vertragsparteien sind in diesem Fall verpflichtet, über eine wirksame und zumutbare Ersatzregelung zu verhandeln, die dem mit der unwirksamen Bestimmung verfolgten Sinn und Zweck möglichst nahe kommt. Dies gilt auch im Falle einer Vertragslücke.

(6) Dieser Vertrag unterliegt ausschließlich dem Recht der Bundesrepublik Deutschland.

(7) Gerichtsstand für Streitigkeiten über die Wirksamkeit und Durchführung dieses Vertrages ist Düsseldorf.

Anhang

Vertrag zur Auftragsverarbeitung

Präambel: Zweck und Notwendigkeit dieses Vertrags

Datenschutz ist ein zentrales Anliegen, insbesondere wenn personenbezogene Daten verarbeitet werden. ***Nach der Datenschutz-Grundverordnung (DSGVO) ist ein Vertrag zur Auftragsverarbeitung (AV-Vertrag) verpflichtend, sobald ein Unternehmen personenbezogene Daten durch einen externen Dienstleister verarbeiten lässt.***
Dieser Vertrag stellt sicher, dass alle datenschutzrechtlichen Anforderungen eingehalten werden und bietet beiden Vertragsparteien Rechtssicherheit. Der Auftragnehmer verarbeitet die Daten ausschließlich im Rahmen der vereinbarten Leistungen und trifft dabei alle notwendigen Maßnahmen zum Schutz der Daten.

§ 1 Gegenstand und Dauer der Vereinbarung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO im Rahmen des in der Bestellung beschriebenen Auftragsgegenstandes. Diese Regelung konkretisiert die Verpflichtungen zum Datenschutz der Vertragsparteien und findet Anwendung bei allen Tätigkeiten von Beschäftigten oder Beauftragten des Auftragnehmers bei der Verarbeitung personenbezogener Daten im Zusammenhang mit diesem Auftragsgegenstand.

(2) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(3) Die Dauer des Vertragsverhältnisses richtet sich nach den Angaben der zugrundeliegenden Bestellung bzw. den Allgemeinen Nutzungsbedingungen.

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

(1) Die Beschreibung der Leistung in Bezug auf Inhalt und Zielsetzung sowie der Art der personenbezogenen Daten und den Kategorien der Betroffenen oder Personengruppen ist der Bestellung bzw. den Allgemeinen Nutzungsbedingungen zu entnehmen.

§ 3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet die Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

(3) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(4) Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen

technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(6) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

§ 4 Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

(1) Weisungsberechtigte Personen des Auftraggebers sind die im Kundenkonto hinterlegte und als Ansprechpartner für Datenschutzfragen benannte Person oder eine hierzu bevollmächtigte Person des Auftraggebers. Änderungen oder längerfristige Verhinderungen dieser Ansprechpartner sind dem Auftragnehmer unverzüglich und grundsätzlich schriftlich oder elektronisch mitzuteilen.

(2) Kontaktperson für den Empfang von Weisungen beim Auftragnehmer ist *Dr. Marco Wirtz* (Geschäftsführer). Der Auftragnehmer ist gesetzlich nicht verpflichtet, einen Datenschutzbeauftragten zu bestellen.

(3) Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

(2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu.

(4) Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber geeignete Kontrollen in seinem Bereich durchzuführen.

(5) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO).

(6) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

(7) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

(8) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die

Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).

(9) Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf Weiteres folgendes vereinbart:

(10) Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist der Zugang zu den personenbezogenen Daten für Kontrollzwecke des Auftraggebers in geeigneter Weise sicher zu stellen. Die Maßnahmen nach Art. 32 DSGVO sind durch den Auftragnehmer sicherzustellen.

(11) Eine systematische Pseudonymisierung personenbezogener Daten wird derzeit nicht eingesetzt, da die Verarbeitung im Rahmen der vertraglich vereinbarten Leistungen auf Grundlage anderer geeigneter Schutzmaßnahmen erfolgt (z. B. Zugriffsbeschränkungen, Verschlüsselung, Protokollierung, Rechtekonzepte). Die Möglichkeit zur Pseudonymisierung wird regelmäßig geprüft und kann in besonderen Verarbeitungsszenarien in Abstimmung mit dem Auftraggeber ergänzt werden.

(12) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung relevanten datenschutzrechtlichen Vorschriften der DSGVO, des Bundesdatenschutzgesetzes sowie weitere für die Erbringung der Leistungen relevanten Datenschutznormen bekannt sind.

(13) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

(14) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS- GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

(15) Der Auftragnehmer hat Namen und Kontaktdaten des Datenschutzbeauftragten aufzuführen bzw. anzugeben, wenn er gesetzlich nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet ist.

§ 6 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen hiernach bestehenden Pflichten zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

§ 7 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

(1) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur gestattet, wenn dies rechtzeitig (in der Regel ein Monat) auf einem der o. g. Kommunikationswege (Ziff. 4) schriftlich oder in einem dokumentierten elektronischen Format angezeigt wurde. Die Zustimmung wird erteilt, wenn der Auftragnehmer dem Auftraggeber Name und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt und der Auftraggeber keine erheblichen Gründe und Interessen geltend macht, die gegen eine Beauftragung sprechen. Außerdem hat der Auftragnehmer dafür Sorge zu tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von Subunternehmer getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.

(2) Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(3) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern.

(4) Der Vertrag mit dem Subunternehmer muss schriftlich oder in einem dokumentierten elektronischen Format (Art. 28 Abs. 4 und Abs. 9 DSGVO) vorliegen.

(5) Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

(6) Die zum aktuellen Zeitpunkt für den Auftragnehmer tätigen Subunternehmen, die mit der Verarbeitung von personenbezogenen Daten beauftragt sind:
Akamai Technologies International AG
Grafenauweg 8, 6300 Zug, Schweiz
Leistung: Hosting der Software-Infrastruktur sowie Bereitstellung von Cloud- und Content-Delivery-Netzwerk (CDN)-Diensten. Alle Daten des Auftraggebers werden ausschließlich auf Servern von Akamai gespeichert und verarbeitet. Dabei werden ausschließlich Server mit physischem Standort in Deutschland genutzt.
Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

(7) Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

§ 8 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

(1) Der Auftragnehmer gewährleistet ein, dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen, angemessenes Schutzniveau. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen angemessen berücksichtigt.

(2) Die konkret umgesetzten technischen und organisatorischen Maßnahmen sind in der beigefügten **Datensicherheits- und Datenschutzkonzeption (Anlage A)** detailliert beschrieben. Diese Maßnahmen werden regelmäßig überprüft und können bei Bedarf an den aktuellen Stand der Technik angepasst werden, wobei die vereinbarten Sicherheitsstandards nicht unterschritten werden dürfen.

(3) Der Auftragnehmer wird eine dokumentierte Datenschutz- und Datensicherheitskonzeption mit den festgelegten technischen und organisatorischen Maßnahmen, passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik, detailliert und unter besonderer Berücksichtigung der eingesetzten IT- Systeme und Verarbeitungsprozesse über die Laufzeit dieses Vertrages umsetzen.

(4) Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

(5) Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO). Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

(6) Alternativ kann die Auswahl der geeigneten technischen und organisatorischen Maßnahmen des Auftragnehmers und deren Einhaltung durch den Nachweis einer Auditierung oder Zertifizierung durch eine unabhängige externe Stelle nachgewiesen werden. Die Prüfunterlagen und Auditberichte können vom Auftraggeber jederzeit eingesehen werden.

(7) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen. Wesentliche Änderungen sind zwischen Auftragnehmer und Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abzustimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

§ 9 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags (Art. 28 Abs. 3 Satz 2 lit. g DSGVO)

(1) Sobald das Beenden des Auftragsverhältnisses erklärt wird oder es sich um eine konkrete abgeschlossene Leistungen handelt, sind Vereinbarungen zu treffen, wie der Auftragnehmer mit den in seinen Besitz befindlichen sowie an Subunternehmen weitergegebene Daten, Unterlagen und Verarbeitungs- oder Nutzungsergebnissen aus diesem Auftrag zu verfahren hat. Soweit eine Löschung oder Vernichtung vereinbart wird, ist dies dem Auftraggeber mit Zeitpunktangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

§ 10 Vergütung

(1) Die Vergütung ergibt sich aus der dieser Vereinbarung zugrundeliegenden Bestellung bzw. des zugrundeliegenden Vertragsverhältnisses.

§ 11 Haftung

(1) Der Auftragnehmer haftet für Schäden, die durch eine schuldhafte Verletzung seiner Pflichten aus diesem Vertrag oder den anwendbaren Datenschutzgesetzen entstehen.
(2) Die Haftung des Auftragnehmers ist – außer im Fall von Vorsatz oder grober Fahrlässigkeit – auf die Höhe der jährlichen Vergütung des Auftraggebers für die Nutzung der Software, maximal jedoch auf 10.000 €, beschränkt.
(3) Eine Haftung für mittelbare Schäden, Mangelfolgeschäden oder entgangenen Gewinn ist ausgeschlossen, sofern nicht zwingende gesetzliche Vorschriften entgegenstehen.
(4) Die Haftung des Auftragnehmers bleibt unberührt für: Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, Schäden, die durch vorsätzliches oder grob fahrlässiges Verhalten verursacht wurden, gesetzliche Ansprüche nach Art. 82 DSGVO (Verantwortlichkeit und Haftung des Auftragsverarbeiters).

§ 12 Sonstiges

(1) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
(2) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
(3) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
(4) Sollte eine Bestimmung dieser Vereinbarung oder ihrer Bestandteile unwirksam sein oder werden, lässt dies die Wirksamkeit der übrigen Regelungen unberührt. Die Parteien sind im Rahmen des Zumutbaren nach Treu und Glauben verpflichtet, eine unwirksame Regelung durch eine im Erfolg gleichkommende wirksame Regelung zu ersetzen. Das gleiche gilt, falls ein regelungsbedürftiger Sachverhalt nicht ausdrücklich geregelt ist.

A. **Technische und organisatorische Maßnahmen** (nach Art. 32 Abs. 1 lit. b DS-GVO)

Zur Sicherstellung eines angemessenen Schutzniveaus personenbezogener Daten setzen wir bei nPro Energy die folgenden technischen und organisatorischen Maßnahmen (TOM) um:

Zutrittskontrolle
Der physische Zugang zu Räumlichkeiten, in denen personenbezogene Daten verarbeitet oder gespeichert werden, ist durch ein mehrstufiges Sicherheitssystem geschützt:

- Zutrittsregelungen für autorisierte Mitarbeitende
- Schlösser / elektronische Schließsysteme
- Begleitung von Besuchern durch interne Mitarbeitende

Zugangskontrolle
Zur Verhinderung des unbefugten Zugangs zu unseren IT-Systemen kommen verschiedene Maßnahmen zum Einsatz:

- Passwortschutz mit Anforderungen an die Komplexität
- Vermeidung von Standard- oder trivialen Passwörtern
- Zwei-Faktor-Authentifizierung bei administrativen Zugängen sowie im Produktivsystem
  Firewall-Systeme und Netzwerksicherheitslösungen zur Abschirmung sensibler Bereiche

Zugriffskontrolle
Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen durch:

- Ein differenziertes Rollen- und Rechtekonzept, basierend auf dem Need-to-Know-Prinzip
- Regelmäßige Überprüfung und Anpassung der vergebenen Berechtigungen
- Protokollierung sensibler Zugriffe

Trennungskontrolle:
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden durch:

- Mandantenfähige Systemarchitektur
- Getrennte Datenbanken bzw. Datenbank-Schemata für unterschiedliche Kundenzwecke
- Technische Maßnahmen zur logischen Trennung innerhalb von Anwendungen

Weitergabekontrolle
Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei Übertragung oder Transport durch:

- Datenübertragungen erfolgen ausschließlich verschlüsselt, z. B. via TLS oder VPN
- Schnittstellen sind abgesichert und nur auf autorisierte Empfänger beschränkt

Eingabekontrolle
Protokollierung der Eingabe, Veränderung und Löschung personenbezogene Daten, durch:

- Es besteht ein Protokollsystem zur Nachvollziehbarkeit von Datenänderungen
- Dokumentenmanagementsysteme unterstützen die Nachverfolgbarkeit

Verfügbarkeitskontrolle
Zur Sicherstellung der Datenverfügbarkeit und zur Minimierung des Datenverlusts wurden folgende Maßnahmen implementiert:

- Regelmäßige, automatisierte Backups mit Prüfprotokollen
- Notfallkonzepte zur schnellen Wiederherstellung (Disaster Recovery Plan)
- Einsatz aktueller Virenschutzlösungen und Firewalls
- Regelmäßige Durchführung von Penetrationstests

Auftragskontrolle
Die Verarbeitung personenbezogener Daten durch Dritte erfolgt ausschließlich im Rahmen von Auftragsverarbeitungsverträgen gemäß Art. 28 DSGVO:

- Dienstleister werden sorgfältig ausgewählt und regelmäßig überprüft
- Verträge enthalten datenschutzrechtliche Mindestanforderungen