

Der vorliegende Auftragsverarbeitungsvertrag wird geschlossen zwischen:

BEW Berliner Energie und Wärme GmbH, Hildegard-Knef-Platz 2, 10829 Berlin (**Auftraggeber oder Verantwortlicher**);

und

[Name, Anschrift des Auftragsverarbeiters] (**Auftragnehmer oder Auftragsverarbeiter**),

auch gemeinsam als „**Parteien**“ und einzeln als „**Partei**“ bezeichnet.

PRÄAMBEL

Am [.....] schlossen der Auftragnehmer und der Auftraggeber einen Dienstleistungsvertrag über die Erbringung von Dienstleistungen durch den Auftragnehmer für den für die Verarbeitung Verantwortlichen (der **Dienstleistungsvertrag**).

Im Rahmen des Dienstleistungsvertrags haben der Auftraggeber und der Auftragnehmer vereinbart, dass der Auftragnehmer im Auftrag des Auftraggebers bei der Erbringung der vereinbarten Dienstleistungen personenbezogene Daten nur in Zusammenhang mit den in diesem Vertrag festgelegten Bedingungen verarbeitet.

DIE PARTEIEN VEREINBAREN FOLGENDES:

1 Vertragsbeginn und Geltungsdauer

- 1.1 Der vorliegende Auftragsverarbeitungsvertrag (**Vertrag**) tritt am selben Tag in Kraft, an dem der Dienstleistungsvertrag in Kraft tritt, und endet mit der Kündigung oder dem Auslaufen des Dienstleistungsvertrags. Sofern und solange der Auftragsverarbeiter auch nach Beendigung dieses Vertrages noch personenbezogene Daten des Verantwortlichen verarbeitet, gelten die wesentlichen Bestimmungen dieses Vertrages fort.
- 1.2 Der vorliegende Auftragsverarbeitungsvertrag ist integraler Bestandteil des Dienstleistungsvertrags. Im Falle eines Widerspruchs zwischen dem Dienstleistungsvertrag und dem Auftragsverarbeitungsvertrag geht der Auftragsverarbeitungsvertrag vor.

2 Auslegung

2.1 Die unter Ziffer 2.2 aufgeführten Begriffe finden die Bedeutung, die ihnen in der Verordnung (EU) 2016/679 (Datenschutzgrundverordnung, DSGVO) zugewiesen wird. Darüber hinaus sind die Regelungen dieses Vertrages im Lichte der Bestimmungen der Datenschutzgrundverordnung in ihrer jeweils gültigen Fassung zu verstehen und auszulegen. Die vorliegenden Bestimmungen sind nicht so auszulegen, als stünden sie den in der Datenschutzgrundverordnung vorgesehenen Rechten und Pflichten entgegen oder beeinträchtigten die Grundrechte oder -freiheiten der betroffenen Personen.

2.2 Definitionen

Verantwortlicher: Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet; werden die Zwecke und Mittel einer solchen Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten bestimmt, so können der Verantwortliche oder die konkreten Kriterien für dessen Benennung im Unionsrecht oder im Recht der Mitgliedstaaten geregelt sein;

Auftragsverarbeitungsvertrag: Der vorliegende Vertrag;

Datensicherheitsvorfall: Die Bedeutung ist in Ziffer 10 des vorliegenden Vertrages angegeben;

Betroffene Personen: Personen, auf die sich die personenbezogenen Daten beziehen;

DSGVO: Datenschutzgrundverordnung vom 27. April 2016 (Verordnung (EU) 2016/679);

Personenbezogene Daten: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

Auftragsverarbeiter: Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

Verarbeitung: Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, so z.B. das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Dienstleistungsvertrag: Der Vertrag zwischen dem Auftraggeber und dem Auftragnehmer, der die entsprechende Erbringung von Dienstleistungen durch den Auftragnehmer im Auftrag des Auftraggebers beinhaltet;

Standardvertragsklauseln: Von der Europäischen Kommission für die Übermittlung personenbezogener Daten zwischen Verantwortlichen oder dem Auftragsverarbeiter in der EU/im EWR und dem Verantwortlichen oder dem Auftragsverarbeiter außerhalb der EU/des EWR verabschiedete Standard-Datenschutzklauseln.

Datenübermittlung in Drittländer: Übermittlung von personenbezogenen Daten in ein bzw. Zugriff auf personenbezogene Daten in einem Land außerhalb der EU/des EWR, das nicht die gleichen Datenschutzstandards wie das EU-Recht garantiert. Hiervon umfasst sind auch Übermittlungen personenbezogener Daten an internationale Organisationen.

3 Einhaltung der gesetzlichen Datenschutzvorschriften

Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen zum Datenschutz in der jeweils geltenden Fassung, die von Zeit zu Zeit geändert, ergänzt oder ersetzt werden kann, in Bezug auf die von ihm im Rahmen des Dienstleistungsvertrags verarbeiteten personenbezogenen Daten einzuhalten.

4 Gegenstand, Art und Zweck

Gegenstand, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind im Einzelnen in Anhang A des vorliegenden Vertrags festgelegt. Dazu gehören auch die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen im Rahmen der Verarbeitung durch den Auftragnehmer.

5 Verarbeitung auf Weisung

5.1 Der Auftragnehmer darf:

- a. personenbezogene Daten nur in der Weise und zu den Zwecken zu verarbeiten, die in Anhang A aufgeführt sind;
- b. personenbezogene Daten ausschließlich auf schriftliche Weisung des Auftraggebers – auch in Bezug auf eine Datenübermittlung in Drittländer – hin verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedsstaaten, der der Auftragnehmer unterliegt, hierzu verpflichtet ist;
- c. personenbezogene Daten nicht länger als für die angewiesene Verarbeitung erforderlich speichern und darüber hinaus personenbezogene Daten nur unter strikter Einhaltung des geltenden Rechts und der als Anhang D beigefügten allgemeinen Informationssicherheitsanforderungen speichern; und
- d. keine im Auftrag und auf Weisung des Auftraggebers verarbeiteten personenbezogenen Daten für eigene Zwecke verarbeiten, es sei denn, dies ist im vorliegenden Vertrag abweichend geregelt;

5.2 Die Parteien werden Anhang A während der Laufzeit des vorliegenden Vertrags erforderlichenfalls aktualisieren.

5.3 Der Auftragnehmer hat den Auftraggeber unverzüglich darüber zu unterrichten, wenn eine Weisung seiner Ansicht nach gegen Datenschutzvorschriften verstößt.

5.4 Im Falle einer Verarbeitung aufgrund einer gesetzlichen Verpflichtung nach Ziffer 5.1(b) dieses Vertrages teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.5 Die Weisungen in Bezug auf die Verarbeitungen im Rahmen dieses Vertrages sind durch den Auftragnehmer zu dokumentieren.

6 Vertraulichkeit der personenbezogenen Daten

6.1 Sofern nicht der Auftraggeber schriftlich etwas anderes verlangt, verpflichtet sich der Auftragnehmer und gewährleistet, dass er personenbezogene Daten nicht an andere Personen weitergibt als:

- a. an diejenigen seiner Beschäftigten, Unterauftragsverarbeiter (und Beschäftigte solcher Unterauftragsverarbeiter), denen gegenüber eine solche Offenlegung für die Erbringung der Leistungen unbedingt erforderlich ist, vorausgesetzt:

- i. jede Offenlegung gemäß Ziffer 6.1(a) unterliegt strengen Vertraulichkeits- und Datenschutzverpflichtungen, die nicht weniger streng sind als die, die dem Auftragnehmer im Rahmen des Dienstleistungsvertrags und vorliegenden Vertrags auferlegt werden, und die mit den vom Auftraggeber ggf. konkret festgelegten Verfahren übereinstimmen; die in Ziffer 6.1(a) genannten Personen haben sich zur Einhaltung der oben genannten Einhaltung der Vertraulichkeit verpflichtet bzw. unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht;
 - ii. die Personen, an die personenbezogene Daten gemäß Ziffer 6.1(a) weitergegeben werden können, haben eine geeignete Schulung in Bezug auf die Datenschutzverpflichtungen erhalten, zu deren Einhaltung der Auftragnehmer gemäß den geltenden gesetzlichen Vorschriften zum Datenschutz und gemäß dem vorliegenden Vertrag verpflichtet ist;
 - iii. der Auftragnehmer ergreift Maßnahmen, um sicherzustellen, dass alle Personen, an die die personenbezogenen Daten gemäß Ziffer 6.1(a) weitergegeben werden können, die personenbezogenen Daten nur auf Weisung des Auftraggebers verarbeiten; und
- b. soweit dies nach geltendem Recht, von einer Aufsichtsbehörde, einem Gericht oder einer anderen zuständigen Behörde verlangt wird:

Der Auftragnehmer ist verpflichtet,

- i. den Auftraggeber schriftlich von jeglicher Offenlegung personenbezogener Daten zu informieren, die der Auftragnehmer gemäß Ziffer 6.1(b) vornehmen muss, sobald er davon Kenntnis erlangt; und
- ii. mit dem Auftraggeber hinsichtlich der Terminierung und des Inhalts einer solchen Offenlegung und etwaiger Maßnahmen, die der Auftraggeber möglicherweise ergreifen möchte, um die Gültigkeit der Anforderung anzufechten, zusammenzuarbeiten.

7 Unterstützung des Auftraggebers

- 7.1 Der Auftragnehmer verpflichtet sich bei der Bearbeitung von Anfragen betroffener Personen, die ihre Rechte gemäß den auf den Auftraggeber anwendbaren Datenschutzvorschriften (z. B. Artikel 15 bis 22 DSGVO) wahrnehmen, zur uneingeschränkten Zusammenarbeit mit dem Auftraggeber und dazu, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei seiner Pflicht zur Beantwortung von Betroffenenanfragen zu unterstützen.
- 7.2 Sofern sich eine betroffene Person bezüglich ihrer Rechte direkt an den Auftragnehmer wendet, wird der Auftragnehmer den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiterleiten.
- 7.3 Der Auftragnehmer darf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, nicht eigenmächtig, sondern nur auf dokumentierte Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken.
- 7.4 Der Auftragnehmer ist verpflichtet, dafür zu sorgen, dass die personenbezogenen Daten richtig und auf dem neuesten Stand sind. Darüber hinaus hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind.
- 7.5 Der Auftragnehmer arbeitet bei der Durchführung von Datenschutz-Folgenabschätzungen im Zusammenhang mit der Erbringung der Dienstleistungen auf eigene Kosten und Aufwendungen uneingeschränkt mit dem Auftraggeber zusammen. Im Falle einer vorherigen Konsultation der Aufsichtsbehörde gemäß Art. 36 Abs. 1 DSGVO unterstützt der Auftragnehmer den Auftraggeber, wenn aus der Datenschutz-Folgenabschätzung gemäß

Artikel 35 DSGVO hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Auftraggeber keine Maßnahmen zur Eindämmung des Risikos trifft.

- 7.6 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Artikel 32 bis 36 DSGVO genannten Pflichten.

8 Sicherheit der Verarbeitung

- 8.1 Der Auftragnehmer hat die Sicherheit der Verarbeitung personenbezogener Daten gemäß Artikel 28 Abs. 3 lit. c und Artikel 32 DSGVO in Verbindung mit Artikel 5 Abs. 1, 2 DSGVO sicherzustellen. Unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sind durch den Auftragnehmer technische, physische und organisatorische Maßnahmen zu ergreifen und aufrechtzuerhalten, um eines dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies ist gemäß den Allgemeinen Anforderungen an die Informationssicherheit (Anhang D) oder mit einer vom Auftragnehmer dokumentierten Übersicht der technischen und organisatorischen Maßnahmen mit dem Ziel:
- a. die Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit, und
 - b. die Verhinderung einer unbefugten oder unrechtmäßigen Offenlegung von, bzw. ebensolchen Zugriffs auf, personenbezogene(n) Daten bzw. deren Verarbeitung sowie des versehentlichen oder unrechtmäßigen Verlusts, der Zerstörung, Veränderung oder Beschädigung personenbezogener Daten sicherzustellen.
- 8.2 Der Auftragnehmer hat vor Beginn der Verarbeitung personenbezogener Daten die Umsetzung der im Vorfeld des Auftrags festgelegten technischen, physischen und organisatorischen Maßnahmen unter Angabe des tatsächlich einzuhaltenden Ablaufs zu dokumentieren und dem Auftraggeber zur Prüfung vorzulegen. Die implementierten Maßnahmen sind nach Abnahme durch den Auftraggeber Grundlage des Auftrags und daher als Anlage zu diesem Vertrag zu dokumentieren. Ergibt sich bei dieser Prüfung oder bei einem Audit durch den Auftraggeber Änderungsbedarf, so werden diese Änderungen einvernehmlich umgesetzt.
- 8.3 Die technischen, physischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung, und insofern kann der Auftragnehmer adäquate alternative Maßnahmen umsetzen. Diese dürfen jedoch nicht das durch die konkret festgelegten Maßnahmen gewährleistete Sicherheitsniveau unterschreiten. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber mitzuteilen. Ist der Auftragnehmer hinsichtlich seiner Einhaltung der Datenschutzgrundverordnung zertifiziert, sind eine Kopie der Zertifikate sowie weitere Unterlagen zu den technischen und organisatorischen Maßnahmen diesem Vertrag als Anlage beizufügen.

9 Überprüfung der Einhaltung der Datenschutzverpflichtungen

- 9.1 Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten bereit.
- 9.2 Der Auftraggeber ist berechtigt, Audits durchzuführen oder durch einen im Einzelfall zu bestimmenden Auditor durchführen zu lassen. Der Auftraggeber ist berechtigt, sich von der Einhaltung des vorliegenden Vertrags durch den Auftragnehmer in dessen Geschäftsbetrieb durch stichprobenartige Kontrollen zu überzeugen, die im Regelfall rechtzeitig anzukündigen sind.
- 9.3 Der Auftragnehmer gewährt dem Auftraggeber, durch diesen beauftragten Prüfern sowie zuständigen Aufsichtsbehörden – im Regelfall während der üblichen Geschäftszeiten – zwecks Prüfung auf Einhaltung der Verpflichtungen des Auftragnehmers gemäß dem vorliegenden Vertrag und den geltenden Datenschutzvorschriften und insbesondere auf

Umsetzung der technischen, physischen und organisatorischen Maßnahmen Zugang zum Personal und zu den Systemen des Auftragnehmers, zu den Aufzeichnungen über die Leistungen und zu allen anderen Informationen im Zusammenhang mit den Leistungen, zu dem Dienstleistungsvertrag oder dem vorliegenden Vertrag.

- 9.4 Der Nachweis der technischen, physischen und organisatorischen Maßnahmen kann – unbeschadet des Kontrollrechts nach Ziffer 9.3 – erbracht werden durch:
- a. Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 DSGVO;
 - b. Zertifizierung nach einem anerkannten Zertifizierungsverfahren gemäß Artikel 42 DSGVO;
 - c. aktuell gültige Testate bzw. Prüfbescheinigungen, Berichte oder Auszüge aus Berichten unabhängiger Stellen (z.B. Wirtschaftsprüfer, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor, Qualitätsauditor)
 - d. geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzauditierung (z.B. gemäß BSI-Grundschutz oder ISO/IEC 27001).
- 9.5 Der Auftragnehmer ist verpflichtet, auf eigene Kosten und Ausgaben jede vertretbare Unterstützung bei der Durchführung solcher Prüfungen zu leisten.
- 9.6 Ergibt die Prüfung, dass der Auftragnehmer seinen Verpflichtungen aus vorliegendem Vertrag nicht in vollem Umfang nachkommt, hat der Auftragnehmer die bei der Prüfung festgestellten Mängel unverzüglich und auf eigene Kosten zu beseitigen oder zu beheben. In diesem Fall trägt der Auftragnehmer auch die Kosten des Audits, unbeschadet des Rechts des Auftraggebers, vom Auftragnehmer sonstigen Schadenersatz zu verlangen.

10 Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten

- 10.1 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, in jedem Fall jedoch innerhalb von 24 Stunden nach Bekanntwerden eines tatsächlichen oder potenziellen Verstoßes schriftlich von
- a. einer Verletzung der Sicherheit, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Offenlegung von oder zum Zugriff auf personenbezogene(n) Daten im Besitz des Auftragnehmers führt (oder führen kann);
 - b. der unbefugten Verarbeitung personenbezogener Daten im Besitz des Auftragnehmers;
 - c. Verstößen des Auftragnehmers gegen seine Datenschutzverpflichtungen aus vorliegendem Vertrag oder aus geltendem Datenschutzrecht; oder
 - d. einem Vollstreckungsverfahren, einer Klage, einem Gerichtsverfahren oder anhängigen bzw. angedrohten Vollstreckungsverfahren, Klagen oder Gerichtsverfahren, das/die gegen den Auftragnehmer eingeleitet oder angedroht wurde und sich in irgendeiner Weise auf personenbezogene Daten bezieht (jeweils ein **Datensicherheitsvorfall**).
- 10.2 Der Auftragnehmer sendet stets unverzüglich eine Kopie der schriftlichen Mitteilung über die Datenschutzverletzung an den jeweiligen Vertragsverantwortlichen und an die Datenschutzorganisation des Auftraggebers über mailto:datenschutz@bew.berlin.
- 10.3 Die schriftliche Mitteilung nach Ziffer 10.1 muss mindestens die folgenden Angaben enthalten:
- a. eine hinreichend detaillierte Beschreibung der Art des Datensicherheitsvorfalls, darunter u.a.:

- b. die Kategorien und Anzahl (einschließlich der Mindest- und Höchstzahl) betroffener Personen;
 - c. die Kategorien und Anzahl (einschließlich der Mindest- und Höchstzahl) der fraglichen betroffenen Datensätze;
 - d. Namen und Kontaktangaben des Datenschutzbeauftragten oder eines anderen Vertreters des Auftragnehmers, der dem Auftraggeber zusätzliche Informationen über den Datensicherheitsvorfall zur Verfügung stellen kann;
 - e. wann der Datensicherheitsvorfall stattgefunden hat (Datum oder Zeitraum);
 - f. die Art der personenbezogenen Daten, die von dem Datensicherheitsvorfall betroffen sind;
 - g. ob die betroffenen personenbezogenen Daten verschlüsselt, gehasht oder auf andere Weise für Unbefugte weder verständlich noch zugänglich waren und wie dies erfolgt ist;
 - h. die (vermutete) Ursache des Datensicherheitsvorfalls;
 - i. Zusammenhang mit etwaigen früheren Datensicherheitsvorfällen;
 - j. die wahrscheinlichen Folgen des Datensicherheitsvorfalls;
 - k. die Maßnahmen, die der Auftragnehmer gemäß Ziffer 10.7 ergriffen hat oder zu ergreifen beabsichtigt; und
 - l. vom Auftraggeber ggf. angeforderte weitere Informationen.
- 10.4 Unmittelbar nach der Meldung eines Datensicherheitsvorfalls durch den Auftragnehmer an den Auftraggeber stimmen sich die Parteien zur Untersuchung des Datensicherheitsvorfalls ab. Der Auftragnehmer kooperiert bei der Bearbeitung des Datensicherheitsvorfalls auf eigene Kosten und Aufwendungen in vollem Umfang mit dem Auftraggeber, unter anderem durch:
- a. Mitwirkung bei Ermittlungen (einschließlich Ermittlungen, die von oder im Namen einer zuständigen Behörde durchgeführt werden);
 - b. Gewährung des Zutritts des Auftraggebers zu den betroffenen Einrichtungen und Betrieben (einschließlich der vom Auftragnehmer betriebenen);
 - c. Vermittlung von Gesprächen mit Mitarbeitern des Auftragnehmers und anderen an der Angelegenheit Beteiligten; und
 - d. Bereitstellung sämtlicher Aufzeichnungen, Protokolle, Dateien, Berichte und anderer Materialien zu den Leistungen, die für die Untersuchung des Datensicherheitsvorfalls nützlich sein können oder es dem Auftraggeber ermöglichen, den Datensicherheitsvorfall einer zuständigen Behörde oder den betroffenen Personen zu melden.
- 10.5 Der Auftragnehmer wird jeden Datensicherheitsvorfall ordnungsgemäß dokumentieren. Eine solche Dokumentation muss mindestens die in den Ziffern 10.3.a bis 10.3.k genannten Angaben sowie die Ergebnisse der in Ziffer 10.4.a genannten Untersuchung enthalten.
- 10.6 Der Auftragnehmer darf ohne vorherige schriftliche Zustimmung des Auftraggebers keine Einreichung, Mitteilung, Bekanntmachung, Pressemitteilungen oder Berichte über Datensicherheitsvorfälle freigeben oder veröffentlichen, es sei denn, der Auftragnehmer ist nach geltendem Recht dazu verpflichtet. Im letzteren Fall hat der Auftragnehmer den Auftraggeber mit angemessener Frist schriftlich hiervon zu benachrichtigen, sofern eine Offenlegung dem Auftragnehmer nach geltendem Recht nicht untersagt wurde, um dem Auftraggeber die Möglichkeit zu geben, einer solchen Offenlegung zu widersprechen.

- 10.7 Der Auftragnehmer ergreift auf eigene Kosten die in vertretbarem Umfang erforderlichen Maßnahmen
- a. zur Behebung von Datensicherheitsvorfällen;
 - b. zur Verhinderung eines erneuten Auftretens des Datensicherheitsvorfalls oder weiterer Datensicherheitsvorfälle;
 - c. zur Minderung der Auswirkungen des Datensicherheitsvorfalls auf die Privatsphäre der betroffenen Personen;
 - d. zur Minderung nachteiliger Auswirkungen des Datensicherheitsvorfalls auf den Auftraggeber.

11 Nichteinhaltung der Bestimmungen und Vertragsbeendigung

- 11.1 Unbeschadet der Bestimmungen der DSGVO kann der Auftraggeber im Falle eines Verstoßes des Auftragnehmers gegen seine Verpflichtungen aus den vorliegenden Bestimmungen den Auftragnehmer anweisen, die Verarbeitung personenbezogener Daten so lange auszusetzen, bis der Auftragnehmer diese Bestimmungen einhält oder der Vertrag beendet wird. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er diese Bestimmungen, gleich aus welchen Gründen, nicht einhalten kann.
- 11.2 Der Auftraggeber ist berechtigt, den Vertrag, insoweit er die Verarbeitung personenbezogener Daten gemäß diesen Bestimmungen betrifft, zu kündigen, wenn
- a. die Verarbeitung personenbezogener Daten durch den Auftragnehmer von dem Auftraggeber gemäß Ziffer 11.1 ausgesetzt wurde und die Einhaltung dieser Bestimmungen nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach Aussetzung wiederhergestellt wird;
 - b. der Auftragnehmer in erheblichem oder anhaltendem Maße gegen diese Bestimmungen oder seine Verpflichtungen gemäß der DSGVO verstößt;
 - c. der Auftragnehmer einer verbindlichen Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde in Bezug auf seine Verpflichtungen gemäß den vorliegenden Bestimmungen oder der DSGVO nicht nachkommt.
- 11.3 Bei Beendigung, Auflösung oder Kündigung des vorliegenden Vertrags, gleich aus welchem Grund oder auf welche Weise, hat der Auftragnehmer auf eigene Kosten und unaufgefordert alle in seinem Besitz befindlichen personenbezogenen Daten (einschließlich etwaig vorhandener Kopien) zu vernichten oder diese personenbezogenen Daten an den Auftraggeber zu übertragen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten eine Verpflichtung zur weiteren Speicherung besteht. In diesem Falle wird der Auftragnehmer den Auftraggeber hierüber und über die zugrundeliegende Verpflichtung informieren.

Der Auftragnehmer ist verpflichtet, nach Wahl des Auftraggebers

- a. alle personenbezogenen Daten, die sich im Besitz oder in der Verfügungsgewalt des Auftragnehmers befinden, an den Auftraggeber in einem zu diesem Zeitpunkt üblichen elektronischen Format zurückgeben, oder
 - b. seine Computersysteme und Dateien mit personenbezogenen Daten, die sich im Besitz oder in der Verfügungsgewalt des Auftragnehmers befinden, zu vernichten oder zu löschen.
- 11.4 Der Auftragnehmer übermittelt dem Auftraggeber eine schriftliche Mitteilung, (i) in der er bestätigt, dass die Rückgabe, Vernichtung und Löschung gemäß Ziffer 11.3 erfolgt ist, und (ii) aus der in angemessener Detailtiefe die personenbezogenen Daten hervorgehen, die der Auftragnehmer nach geltendem Recht nach Beendigung, Auflösung oder Kündigung des vorliegenden Vertrages aufbewahren muss.

12 Einsatz von Unterauftragsverarbeitern

- 12.1 Durch den Auftragnehmer sind die in Artikel 28 Absätze 2 und 4 DSGVO genannten Anforderungen zu erfüllen, wenn er einen weiteren Auftragsverarbeiter (Unterauftragsverarbeiter) beauftragen will. Der Auftragnehmer darf daher nur dann einen Unterauftragsverarbeiter zur Erfüllung des vorliegenden Vertrags beauftragen, wenn:

der Auftraggeber seine konkrete vorherige schriftliche Zustimmung erteilt hat

Der Auftragnehmer hat durch sorgfältige Auswahl des Unterauftragsverarbeiters und insbesondere durch Umsetzung geeigneter technischer und organisatorischer Maßnahmen sicherzustellen, dass die Verarbeitung personenbezogener Daten den Anforderungen der Bestimmung unter Ziffer 8 genügt; ferner hat der Auftragnehmer mit dem Unterauftragsverarbeiter eine schriftliche Vereinbarung abzuschließen, welche dem Unterauftragsverarbeiter mindestens dieselben Datenschutzpflichten auferlegt wie der vorliegende Vertrag vorsieht, einschließlich direkten Kontrollrechten des Auftraggebers bei dem einzusetzenden Unterauftragsverarbeiter.

Der Auftragnehmer darf keinen Unterauftragsverarbeiter ohne vorherige konkrete Genehmigung durch den Auftraggeber beauftragen. Den Antrag auf Erteilung einer konkreten Genehmigung stellt der Auftragnehmer mindestens vier Wochen vor Beauftragung des betreffenden Unterauftragsverarbeiters in Verbindung mit den Angaben, die für die Entscheidung des Auftraggebers über die Genehmigung erforderlich sind. Der Auftraggeber kann seine Zustimmung jederzeit widerrufen, wenn der Unterauftragsverarbeiter den Datenschutzverpflichtungen nicht nachkommt oder der Auftraggeber vernünftigerweise zum Schluss gelangt, dass der Unterauftragsverarbeiter den Datenschutzverpflichtungen nicht nachkommen wird; der Auftragnehmer hat seine Vereinbarung mit dem Unterauftragsverarbeiter unverzüglich zu kündigen.

- 12.2 Möchte der Auftragnehmer im Rahmen dieses Vertrages durchgeführte Tätigkeiten zur Verarbeitung personenbezogener Daten an Unterauftragsverarbeiter vergeben, so hat er dem Auftraggeber zuvor schriftlich seine Absicht, einen Unterauftragsverarbeiter zu beauftragen, mitzuteilen und hierbei zumindest die folgenden Angaben in ausreichender Detailtiefe zu machen:

- a. Name und Anschrift des vorgeschlagenen Unterauftragsverarbeiters;
- b. Gegenstand des vorgeschlagenen Untervertrags einschließlich einer Beschreibung der durch den vorgeschlagenen Unterauftragsverarbeiter zu erbringenden Dienstleistungen sowie seiner geplanten Beteiligung an der Verarbeitung personenbezogener Daten;
- c. Land oder Länder, in denen der vorgeschlagene Unterauftragsverarbeiter beabsichtigt, personenbezogene Daten zu verarbeiten;
- d. eine schriftliche Bestätigung, dass der Unterauftragsverarbeiter damit einverstanden ist, an einen schriftlichen Auftragsverarbeitungsvertrag gebunden zu sein, in der die gleichen (oder strengere) Verpflichtungen wie im vorliegenden Vertrag festgelegt sind, insbesondere die Bestätigung, dass der vorgeschlagene Unterauftragsverarbeiter geeignete technische, physische und organisatorische Maßnahmen zum Schutz der Sicherheit, Vertraulichkeit und Integrität personenbezogener Daten so ergriffen hat, dass die Verarbeitung die Anforderungen dieser Bestimmung und der DSGVO erfüllt. Der Auftragsverarbeiter ist daher dafür verantwortlich, zu verlangen, dass der Unterauftragsverarbeiter zumindest die Verpflichtungen einhält, denen der Auftragnehmer gemäß den Bestimmungen und der DSGVO unterliegt;
- e. etwaige zusätzliche Angaben, die der Auftraggeber nach vernünftigem Ermessen verlangen kann.

Die Übermittlung personenbezogener Daten von dem Auftraggeber an den Auftragnehmer und der Beginn der Datenverarbeitung durch den Unterauftragsverarbeiter dürfen erst dann erfolgen, wenn alle Anforderungen erfüllt sind, darunter unter anderem die in Ziffer 13 genannten Anforderungen, und nachdem der Auftraggeber seine Zustimmung oder Genehmigung gemäß Ziffer 12.2 erteilt hat.

- 12.3 Die Liste der vom Auftraggeber bereits zugelassenen Unterauftragsverarbeiter ist dem Anhang C zu entnehmen. Der Auftragnehmer wird die Liste auf dem neuesten Stand halten.
- 12.4 Eine Kopie des Auftragsverarbeitungsvertrags und aller späteren Änderungen sowie Weisungen zwischen dem Auftragnehmer und dem jeweiligen Unterauftragsverarbeiter ist dem Auftraggeber auf dessen Verlangen vorzulegen.
- 12.5 Der Auftragnehmer vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigungsklausel, nach der – für den Fall, dass der Auftragnehmer sachlich nicht weiterbesteht, rechtlich nicht mehr existiert oder insolvent geworden ist – der Auftraggeber ein Drittbegünstigter der Vereinbarung mit dem Unterauftragsverarbeiter ist und das Recht hat, die Vereinbarung gegenüber dem vom Auftragnehmer beauftragten Unterauftragsverarbeiter durchzusetzen, so dass der Auftraggeber z. B. den Unterauftragsverarbeiter anweisen kann, die personenbezogenen Daten zu löschen oder zurückzugeben und den Vertrag mit dem Unterauftragsverarbeiter zu beenden.
- 12.6 Kommt der Unterauftragsverarbeiter seinen Datenschutzverpflichtungen nicht nach, bleibt der Auftragnehmer gegenüber dem Auftraggeber in vollem Umfang für die Erfüllung der Verpflichtungen des Unterauftragsverarbeiters haftbar. Dies berührt nicht die Rechte der betroffenen Personen gemäß DSGVO - insbesondere die in den Artikeln 79 und 82 DSGVO vorgesehenen - gegenüber dem Auftraggeber und dem Auftragnehmer einschließlich des Unterauftragsverarbeiters. Der Auftragnehmer unterrichtet den Auftraggeber, soweit der Unterauftragsverarbeiter seinen Verpflichtungen aus jenem Vertrag nicht nachkommt.
- 12.7 Der Auftragnehmer ist darüber hinaus verpflichtet, mit weiteren von ihm eingesetzten Dienstleistern geeignete und rechtsverbindliche vertragliche Maßnahmen zu vereinbaren und angemessene Kontrollrechte wahrzunehmen, um den Datenschutz und die Datensicherheit der personenbezogenen Daten des Auftraggebers zu gewährleisten, auch wenn es sich hierbei um ausgelagerte Nebenleistungen handelt, die keine (Unter-)Auftragsverarbeitung darstellen.

13 Grenzüberschreitende Übermittlung personenbezogener Daten in ein Drittland

- 13.1 Die Durchführung der vertraglich vereinbarten Verarbeitung personenbezogener Daten erfolgt ausschließlich in einem Mitgliedsstaat der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR).
- 13.2 Jegliche Übermittlung von Daten in ein Drittland durch den Auftragnehmer darf nur auf der Grundlage dokumentierter Weisungen des Auftraggebers erfolgen und muss im Einklang mit Kapitel V der DSGVO stehen.

Der Auftraggeber erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragnehmer gemäß Ziffer 12 einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Auftraggebers) beauftragt und diese Verarbeitungstätigkeiten eine Datenübermittlung in Drittländer beinhalten, der Auftragnehmer und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der DSGVO durch die Verwendung von Standardvertragsklauseln sicherstellen können, die von der EU-Kommission gemäß Artikel 46 Absatz 2 der DSGVO verabschiedet wurden, vorausgesetzt, die Bedingungen für die Verwendung dieser Standardvertragsklauseln sind erfüllt.

Soweit dies zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen einschließlich personenbezogener Daten erforderlich ist, kann der Auftragnehmer den Wortlaut des Vertrags vor Weitergabe einer Kopie unkenntlich machen.

- 13.3 Der Auftragnehmer ist verpflichtet, eine dokumentierte Risikobewertung des Datentransfers durchzuführen, um ein angemessenes Datenschutzniveau gemäß Kapitel V der Datenschutz-Grundverordnung zu gewährleisten, wobei insbesondere die folgenden Elemente zu berücksichtigen sind:
- a. die konkreten Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übermittlungskanäle; beabsichtigte Weiterübermittlungen; die Art des Empfängers; der Zweck der Verarbeitung; die Kategorien und das Format der übermittelten personenbezogenen Daten; der Wirtschaftssektor, in dem die Übermittlung erfolgt; der Speicherort der übermittelten Daten;
 - b. die Gesetze und Praktiken des Bestimmungsdrittlandes - einschließlich derjenigen, die die Offenlegung von Daten an Behörden vorschreiben oder den Zugang solcher Behörden gestatten -, die angesichts der konkreten Umstände der Übermittlung sowie der geltenden Beschränkungen und Garantien einschlägig sind,
 - c. alle einschlägigen vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß den vorliegenden Bestimmungen eingeführt wurden, einschließlich der Maßnahmen, die während der Übermittlung und auf die Verarbeitung der personenbezogenen Daten im Bestimmungsland angewendet werden.
- 13.4 Der Auftragnehmer sichert zu, sich bei der Durchführung dieser Risikobewertung nach besten Kräften zu bemühen, dem Auftraggeber alle erforderlichen Informationen zur Verfügung zu stellen.

14 Haftung

Der Auftragnehmer haftet für alle Schäden, Verluste und Forderungen (einschließlich Bußgelder oder Strafen), die sich aus (i) einem Verstoß gegen eine Bestimmung des vorliegenden Vertrags oder (ii) einem Verstoß gegen geltende Datenschutzvorschriften ergeben, der auf die Verarbeitung personenbezogener Daten durch den Auftragnehmer oder in seinem Namen im Rahmen des vorliegenden Vertrags zurückzuführen ist. Eine etwa im Dienstleistungsvertrag vereinbarte Haftungsbeschränkung gilt nicht für die Haftung des Auftragnehmers aus vorliegendem Vertrag. Der Auftragnehmer hält den Auftraggeber in vollem Umfang schadlos in Bezug auf sämtliche Bußgelder, Strafen oder Entschädigungen an Dritte (einschließlich Aufsichtsbehörden), für die der Auftraggeber aufgrund von Verstößen des Auftragnehmers gegen seine Verpflichtungen aus vorliegendem Vertrag haftet.

15 Geltendes Recht und Streitbeilegung

Das für diesen Vertrag geltende Recht und die hierfür geltenden Regeln zur Beilegung von Streitigkeiten sind identisch mit den diesbezüglichen Bestimmungen des Dienstleistungsvertrags, sofern die Parteien nicht ausdrücklich etwas anderes vereinbart haben.

16 Sonstiges

Jede Änderung oder Ergänzung des vorliegenden Vertrags, einschließlich dieser Bestimmung, ist nur gültig, wenn sie in Schriftform erfolgt und von beiden Parteien unterzeichnet wird.

Anhang A: Spezifikationen für die Datenverarbeitung (Art der Daten, Kategorien betroffener Personen)

Anhang B: Übermittlung personenbezogener Daten in Drittländer

Anhang C: Liste der zugelassenen Unterauftragsverarbeiter

Anhang D: Allgemeine Informationssicherheitsanforderungen für Lieferanten

Datum:

[Gesellschaft]

Unterschrift

Name in Druckbuchstaben

Datum:

[Gesellschaft]

Unterschrift

Name in Druckbuchstaben

ANHANG A: SPEZIFIKATIONEN FÜR DIE DATENVERARBEITUNG

***Vor Unterzeichnung des vorliegenden Vertrags legen die Parteien in diesem Anhang Folgendes fest:

1. **Gegenstand** der Datenverarbeitung:
.....
.....
2. **Art** und den **Zweck** der Verarbeitung:
.....
.....
3. **Arten** der verarbeiteten **personenbezogenen Daten**: bitte ankreuzen [x]

Kontakt- bzw. Identifizierungsangaben

- ☐ Name, Anschrift, Ort
- ☐ Telefonnummer, E-Mail-Adresse
- ☐ Geburtsdatum
- ☐ Geschlecht

HR-Daten/Stammdaten der Mitarbeiter

- ☐ Personalnummer
- ☐ Bereich (OKZ)
- ☐ Nachweis der Arbeitsleistung
- ☐ Sozialversicherungsnummer
- ☐ Personalakten einschließlich vertraulicher Berichte
- ☐ Besondere Datenkategorien (Gesundheit, Rasse oder ethnische Abstammung, sexuelle Ausrichtung, Religionszugehörigkeit, politische Haltung, Gewerkschaftszugehörigkeit)
- ☐ Entgeltabrechnungsdaten
- ☐ Bewerbungsdaten (wie Lebenslauf, Qualifikationen)
- ☐ Steuerdaten der Mitarbeiter

Kundendaten / Vertragsinformationen

- ☐ Abrechnungsdaten
- ☐ Bankverbindung
- ☐ Verbrauchsdaten
- ☐ Vertragsdaten
- ☐ Zähl-/Messdaten

Kundenhistorie

- ☐ Mengeninformationen/Verbrauchshistorie (einschließlich Smart-Meter-Daten)

Finanzdaten

- ☐ Bankkontonummer
- ☐ Kreditkartennummer
- ☐ Zahlungsausfälle
- ☐ Kaufhistorie
- ☐ Abgeleitete finanzielle Angaben (Einkommenskategorie, Wohneigentum, Autobesitz)
- ☐ Bonitätsinformationen zum Zahlungsverhalten (Kreditwürdigkeitsprüfung)

Lebenswandel

- ☐ Familienzusammensetzung, Lebenssituation, Interessen, demografische Merkmale usw.

Soziale Medien

- ☐ Daten aus Profilen in sozialen Medien (Facebook, Twitter-Konto usw.)

Sonstiges

- ☐
- ☐

Besondere Kategorien verarbeiteter personenbezogener Daten (soweit zutreffend)

.....
.....

4. Die **Kategorien der betroffenen Personen**, deren Daten vom Auftragnehmer verarbeitet werden. Zur Gruppe der von der Verarbeitung ihrer personenbezogenen Daten betroffenen Personen gehören:

- ☐ Kunden einschl. ehemaliger Kunden
- ☐ Interessenten oder potenzielle Kunden
- ☐ Mitarbeiter
- ☐ Nutzer der IT-Infrastruktur der BEW Wärme Berlin GmbH
- ☐ Lieferanten
- ☐ Abonnenten
- ☐ andere, namentlich

5. Name des **Datenschutzbeauftragten/Ansprechpartners**.....

6. Der **Zeitraum**, für den die personenbezogenen Daten aufbewahrt werden, oder, falls dies nicht möglich ist, die Kriterien, nach denen dieser Zeitraum festgelegt wird

.....

ANHANG B - ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER

- a) ☐ Es erfolgt keine Übermittlung personenbezogener Daten in ein Drittland - keine weiteren Maßnahmen erforderlich
- b) ☐ Die Übermittlung personenbezogener Daten in ein Drittland ist beabsichtigt:

Jede Übermittlung von Daten in einen Staat, der nicht Mitgliedstaat der EU oder des EWR ist, darf nur erfolgen, wenn die konkreten Bedingungen der Artikel 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau in (z.B. Land, Territorium oder bestimmte Sektoren innerhalb eines Landes)

- ☐ ergibt sich aus den Standard-Datenschutzklauseln (Artikel 46 Absatz 2 Buchstaben c und d DSGVO);
- ☐ wurde von der Europäischen Kommission beschlossen (Artikel 45 Absatz 3 DSGVO);

soweit von europäischen Aufsichtsbehörden genehmigt:

- ☐ ergibt sich aus verbindlichen internen Datenschutzvorschriften (Artikel 46 Absatz 2 Buchstabe b in Verbindung mit Artikel 47 DSGVO);
- ☐ ergibt sich aus genehmigten Verhaltensregeln (Artikel 46 Absatz 2 Buchstabe e in Verbindung mit Artikel 40 DSGVO);
- ☐ ergibt sich aus einem genehmigten Zertifizierungsmechanismus (Artikel 46 Absatz 2 Buchstabe f in Verbindung mit Artikel 42);
- ☐ wurde auf andere Weise ermittelt:..... (Artikel 46 Absatz 2 Buchstabe a, Absatz 3 Buchstaben a und b)

ANHANG C: LISTE DER ZUGELASSENEN UNTERAUFTRAGSVERARBEITER SOWIE DER STANDORTE AUSSERHALB DER EU (DRITTLÄNDER)

Der Einsatz von Unterauftragsverarbeitern ist durch den Auftraggeber zu genehmigen. Der Auftragnehmer ist nicht berechtigt, ohne ausdrückliche schriftliche Zustimmung des Auftraggebers einen Unterauftragsverarbeiter für eine andere als die vereinbarte Verarbeitung zu beauftragen oder die beschriebene Verarbeitung durch einen anderen Unterauftragsverarbeiter durchführen zu lassen.

Um die Bewertung und die Entscheidung über die Genehmigung von Unteraufträgen zu ermöglichen, übermittelt der Auftragnehmer dem Auftraggeber alle erforderlichen Informationen zu dem vorgesehenen Unterauftragsverarbeiter, darunter zu dessen Standorten, zu den durch denselben durchzuführenden Verarbeitungstätigkeiten sowie zu umzusetzenden Garantien und Maßnahmen.

- a) ☐ Die Vergabe von Unteraufträgen ist nicht zulässig.
- b) ☐ Der Auftraggeber stimmt der Beauftragung der folgenden Unterauftragsverarbeiter unter der Voraussetzung einer vertraglichen Vereinbarung gemäß Artikel 28 Absätze 2-4 DSGVO zu:

Name des Unternehmens des Unterauftragsverarbeiters	Anschrift/Land	Dienstleistung/Beschreibung der Verarbeitung	Lieferstandorte/ (Ort der Datenverarbeitung)	Land der

- c) Der Auftraggeber erklärt sich mit den folgenden „Lieferstandorten in Drittländern“ gemäß Anhang B einverstanden:

Name des Unternehmens des Unterauftragsverarbeiters	Anschrift/Land	Dienstleistung/Beschreibung der Verarbeitung	Liefer-standorte/ Land (Ort der Datenverarbeitung)	Geeignete Garantien

ANHANG D: INFORMATIONSSICHERHEITSANFORDERUNGEN FÜR EXTERNE DATENVERARBEITUNG

Die als Anhang D beigefügten Informationssicherheitsanforderungen für externe Datenverarbeitung sind vom Auftragnehmer auszufüllen sofern relevant.