**Weisungen zur Auftragsverarbeitung**

gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO)

zwischen der

Stromnetz Berlin GmbH, Eichenstr. 3a, 12435 Berlin

– Verantwortliches Unternehmen - nachstehend Auftraggeber genannt –

und dem/der

[Name, Anschrift des Auftragsverarbeiters für HA-Begehung]

– Auftragsverarbeiter - nachstehend Auftragnehmer genannt –

## 1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrages zur Verarbeitung personenbezogener Daten sind Begehungen von Hausanschlüssen (HA) und ergibt sich aus der Leistungsvereinbarung Vertragsnummer [SAP Nummer oder andere Registrierungsnummer] vom [Unterzeichnungsdatum].

(2) Dauer

Die Dauer dieses Auftrags entspricht der Laufzeit der Leistungsvereinbarung.

## 2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

Die Daten werden durch den Auftragnehmer ausschließlich in Systemen des Auftragnehmers gespeichert. Der Datenaustausch zwischen Auftraggeber und Auftragnehmer erfolgt über das Dienstleister Portal des AG, welche die Daten verschlüsselt überträgt.

(2) Art der Daten und Kategorien betroffener Personen

Die Art der verwendeten personenbezogenen Daten und die Kategorien betroffener Personen sind in dem Annex A zu diesen Weisungen beschrieben.

(3) Übermittlung personenbezogener Daten in Drittländer

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers.

Wenn Übermittlungen in Drittländer geplant werden und der Auftraggeber zugestimmt hat, ist der Annex B hinzuzufügen und auszufüllen.

## 3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen, siehe „Checkliste Auftragnehmer-Kontrolle“.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber mitzuteilen.

Sollte der Auftragnehmer bezüglich der Einhaltung der Datenschutzregelungen zertifiziert sein, so sind die Zertifikate in Kopie sowie ergänzende Unterlagen zu den technischen und organisatorischen Maßnahmen diesen Weisungen als Anlage beizufügen.

## 4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt

1. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
2. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO.
3. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
4. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
5. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
6. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
7. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.
8. Meldung von Datenschutzvorfällen und unverzügliche Aufklärung seitens des Auftragnehmers

## 6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Die genehmigten Unterauftragnehmer sind im Annex C aufgeführt.

Der Wechsel von bestehenden Unterauftragnehmern ist zulässig, soweit:

* der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
* der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
* eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## 7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

* die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
* die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
* aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
* eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

## 8. Mitteilung bei Verstößen des Auftragnehmers und Unterstützung beim Nachweis eines den Risiken angemessenen Schutzniveaus

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

1. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
2. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
3. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
4. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
5. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

## 9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften oder andere Gesetze. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## 10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .   
Ort, Datum Ort, Datum

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .   
Auftraggeber (OLC, Unterschrift) Auftragnehmer (Stempel, Unterschrift)

# Annex A - Art der personenbezogenen Daten und die Kategorien betroffener Personen

Art der personenbezogenen Daten

Gegenstand der Verarbeitung der personenbezogenen Daten sind folgende Datenarten / -kategorien:

* Personaldaten/Personalstammdaten

[ ] Personalnummer

[ ] Organisation

[ ] Arbeits-/stundennachweise

[ ] Sozialversicherungsnummer

[ ] Personalakten incl. Beurteilungen

[ ] Besondere Kategorien personenbezogener Daten z.B. Gesundheitsdaten, Religion, Gewerkschaftszugehörigkeit

[ ] Lohnkonten

[ ] Lohnsteuerdaten

* Kommunikationsdaten

[ X ] Name, Anschriften

[ X ] Telefonnummern, E-Mail-Adresse

[ X ] Fax-Nummer

[ X ] Firmenname, Arbeitsort/Büroanschrift

* Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

[ ] Umsatz

[ ] Vertragsbeginn

[ ] Vertragsende

[ ] Konditionen

* Kundenhistorie

[ ] Verbrauchshistorie

* Vertragsabrechnungs- und Zahlungsdaten

[ ] Bankkonto Informationen

[ ] Zahlungsausfälle

* Planungs- und Steuerungsdaten

[ ] Arbeitspläne für Instandhaltung

[ ] Arbeitsorte für Instandhaltung

[ ] personenbezogene Daten zu kritischen Infrastrukturen

* Rating Daten

[ ] Wahrscheinlichkeitswerte für Zahlungsausfälle

[ ] Kreditwürdigkeit

* Lieferantenstammdaten

[ ] Kontaktpersonen

[ ] Adressen

[ ] Lokationen

* Andere Kategorien Personbezogener Daten (Bitte ausfüllen)

[ X ] Zugehöriges Grundstück bzw. Haus

Betroffene Personen

Der Kreis der Betroffenen, deren personenbezogene Daten im Rahmen dieses Auftrags verarbeitet werden, umfasst:

[ X ] Kunden incl. ehemalige Kunden

[ ] Interessenten oder potentielle Kunden

[ X ] Beschäftigte der Stromnetz Berlin

[ ] Benutzer der IT Infrastruktur der Vattenfall Group

[ ] Lieferanten

[ ] Abonnenten (z.B. Newsletter)

[ X ] Ansprechpartner z.B. von Hausverwaltung

[ X ] Grundstückseigentümer, Hauseigentümer

[ ] … (weitere Personengruppe, bitte festlegen)

# Annex B - 3rd country transfer of personal data

1. 3rd country transfer of personal data is not relevant – no further actions relevant to Annex B necessary
2. 3rd country transfer of personal data is relevant – the following test is agreed:

Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled. The adequate level of protection in …………. (e.g. country, territory or specific sectors within a country)

* is the result of Standard Data Protection Clauses (Article 46 Paragraph 2 Points c and d GDPR);
* has been decided by the European Commission (Article 45 Paragraph 3 GDPR);

In future also applicable if approved by European supervisory authorities:

* is the result of binding corporate rules (Article 46 Paragraph 2 Point b in conjunction with Article 47 GDPR);
* is the result of approved Codes of Conduct (Article 46 Paragraph 2 Point e in conjunction with Article 40 GDPR);
* is the result of an approved Certification Mechanism. (Article 46 Paragraph 2 Point f in conjunction with Article 42 GDPR).
* is established by other means:………. (Article 46 Paragraph 2 Point a, Paragraph 3 Points a and b GDPR)

**Please Note**

* Third Countries are all countries except
  + European Economic Area (EEA) includes
    - All member states of the European Union
    - Norway
    - Iceland
    - Liechtenstein and
    - Switzerland
* A 3rd country transfer includes access from outside EU to personal data for IT support and maintenance.
* A 3rd country transfer requires a data protection impact assessment in advance, that documents appropriate and sufficient measures envisaged to address the risks.
* Follow WP 176 issued by ARTICLE 29 DATA PROTECTION WORKING PARTY to apply Standard Data Protection Clauses and establish a lawful contract chain.
* All delivery locations in 3rd countries must be listed, see Annex C.
* For the purposes of preventive or occupational medicine and for the assessment of the working capacity of the employee processing (includes transfer) of health data is prohibited outside EU. (Art. 9 (3) GDPR)
* Generally a 3rd country transfer of special categories of personal data is prohibited by German law until May 2018.
* Generally the data subject must be informed in advance about the intention of 3rd country transfers and how the specific Conditions of Article 44 et seq. GDPR have been fulfilled.

# Annex C – Liste der genehmigten Unterauftragnehmer

1. Eine Unterbeauftragung findet nicht statt.
2. Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO:

|  |  |  |  |
| --- | --- | --- | --- |
| Firma / Unterauftragnehmer | Adresse/Land | Leistung | Standort der Leistungserbringung |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Annex D – Nationale Besonderheiten

|  |
| --- |
| **Beschreibung** |
| - |
| **Verfasser/Datum**  - |