

# **Datenschutz-Vereinbarung zur Verarbeitung von Daten im Auftrag gem. Art. 28 EU-DSGVO**

Zwischen

- nachstehend Auftraggeber genannt -

Stadtwerke Herne AG, Grenzweg 18, 44623 Herne

- nachstehend Auftragnehmer genannt –

.....

## **1. Gegenstand und Dauer des Auftrags**

### **1.1 Der Gegenstand des Auftrags:**

Turnuswechsel von Gaszählern / Stromzählern  
Verlustgasmessung beim Turnuswechsel  
Kundenanschriften zur Terminvereinbarung für den Turnuswechsel

### **1.2 Die Laufzeit des Auftrags geht bis zum .....**

## **2. Konkretisierung des Auftragsinhalts**

2.1 Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret im Hauptvertrag beschrieben.

2.2 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 und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind.

2.3 Die Arten der verwendeten personenbezogenen Daten sind folgende: Name, Nachname, Kundenanschrift, Zählerstandort und ggf. Kundentelefonnummer.

2.4 Die Kategorien der durch die Verarbeitung betroffenen Personen sind:

Die Mitarbeiter der ..... über das Programm Lovion ( PC und iPhone durch Auftraggeber gestellt )

## **3. Technische und organisatorische Maßnahmen**

3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten 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 bzw. ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.2 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 Buchst. c, Art. 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 Sinn von Art. 32 Abs. 1 DSGVO zu berücksichtigen (vgl. Anlage).

3.3 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.

#### **4. Berichtigung, Einschränkung und Löschung von Daten**

4.1 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.

4.2 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 der Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

5.1. Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und Art. 39 DSGVO ausübt.

5.2. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 Buchst. b, Art. 29, Art. 32 Abs. 4 DSGVO. 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.

5.3. Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 28 Abs. 3 S. 2 Buchst. c, Art. 32 DSGVO (vgl. Anlage).

5.4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5.5. 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.

5.6. 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.

- 5.7. Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Nr. 7 dieser Vereinbarung.

## **6. Unterauftragsverhältnisse**

- 6.1 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 sowie Kontrollmaßnahmen zu ergreifen.
- 6.2 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

- ☒ X Eine Unterbeauftragung erfolgt derzeit nicht.
- ☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind nur zulässig, soweit:

- a) der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
  - b) der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
  - c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO sowie der Vorgaben dieser Vereinbarung zugrunde gelegt werden.
- 6.3 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- 6.4 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.
- 6.5 Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## **7. Kontrollrechte des Auftraggebers**

- 7.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem 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.
- 7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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.

- 7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
  - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
  - 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).
- 7.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

## **8. Mitteilung bei Verstößen des Auftragnehmers**

- 8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
- a) 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
  - b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
  - c) 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
  - d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgeabschätzung
  - e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
- 8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

## **9. Weisungsbefugnis des Auftraggebers**

- 9.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens in Textform).
- 9.2 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. 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**

- 10.1 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.
- 10.2 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.

10.3 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.

Für den Auftragnehmer:

Ort, Datum      Herne,.....

Name:            Chris Böhm

Funktion        Meister

Unterschrift

Für den Auftraggeber:

Ort, Datum      Herne, .....

Name

Funktion

Unterschrift

# Anlage: Technische und organisatorische Maßnahmen des Auftragnehmers

nach Art. 32 DSGVO  
(zu Nr. 3 der Datenschutz-Vereinbarung)

**[Praxishinweis:** Im Folgenden muss der Auftragnehmer angeben, mit welchen konkreten Maßnahmen er die einzelnen Schutzziele erreicht. Für jedes der acht gesetzlich geforderten Schutzziele sind unten Beispiele aufgelistet. Diese müssen individuell angepasst, das heißt gelöscht werden, wenn sie nicht zutreffen bzw. um weitere Maßnahmen ergänzt werden, soweit diese vorliegen.

*Wichtig: Es kommt hier nicht auf möglichst viele Maßnahmen an. Auch wenige Maßnahmen können geeignet sein, einen qualitativ ausreichenden Schutz der personenbezogenen Daten des Auftraggebers zu gewährleisten.*

**Zum Vorgehen:** Der Auftragnehmer überarbeitet die nachfolgende Liste (alternativ kann der Auftragnehmer auch ein anderes Dokument vorlegen, das die erforderlichen Inhalte enthält). Anschließend überprüft der Auftraggeber die Angaben (ggf. mit Hilfe seines Datenschutzbeauftragten). Wenn er der Meinung ist, dass die Liste einen ausreichenden Schutz gewährleistet, kann der Vertrag endgültig unterzeichnet werden.]

## **1. Vertraulichkeit (Art. 32 Abs. 1 Buchst. b DSGVO)**

### **1.1 Zutrittskontrolle**

*Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.*

**Beispiele (bitte ggf. ändern/ergänzen):**

- Zutrittskontrollsystem: Ausweisleser, Magnetkarte, Chipkarte
- dokumentierte Schlüsselvergabe
- Schlüsselvergabe/Zutrittsberechtigung nur für berechtigte Personen
- Türsicherung (Sicherheitsschlösser, elektrische Türöffner usw.)
- Abschließen von Räumen nach Arbeitsschluss
- Protokollierung von Besuchern
- Gäste werden innerhalb des Betriebsgeländes stets begleitet
- Tragepflicht von Berechtigungsausweisen
- Zutrittskontrolle durch Werkschutz, Pförtner
- Videoüberwachung
- Alarmanlage
- Bewegungsmelder
- Server in abschließbaren Serverschränken

### **1.2 Zugangskontrolle**

*Das Eindringen Unbefugter in die IT-Systeme ist zu verhindern.*

**Beispiele (bitte ggf. ändern/ergänzen):**

- Server sind nur nach einem individuellen Login nutzbar
- Clients sind nur nach einem individuellen Login nutzbar
- Login mit Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Automatische Sperrung bei Pausen und Fehlanmeldungen (z.B. Kennwort oder Pausenschaltung)
- Einrichtung eines Benutzerstammsatzes pro User
- automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware
- Verschlüsselung von Datenträgern
- Sperren von externen Schnittstellen (USB etc.)

- mobile IT-Systeme sind verschlüsselt
- mobile Datenträger sind verschlüsselt
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum Löschen von Daten aus der Ferne)

### 1.3 Zugriffskontrolle

*Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.*

Beispiele (bitte ggf. ändern/ergänzen):

- es besteht ein Berechtigungskonzept mit differenzierten Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Verfahren zur Vergabe und periodischen Überprüfung der Berechtigungen ist definiert
- Anzahl der Administratoren weitgehend reduziert
- Zugriffe auf Anwendungen und/oder Daten werden protokolliert und können ausgewertet werden
- nicht mehr verwendete Datenträger werden sicher gelöscht / vernichtet
- Papierunterlagen mit personenbezogenen Daten werden sicher vernichtet
- Daten-Löschungen/-Vernichtungen werden protokolliert

### 1.4 Trennungskontrolle

*Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.*

Beispiele (bitte ggf. ändern/ergänzen):

- Interne Mandantenfähigkeit (z.B.: Daten von unterschiedlichen Kunden von logisch/physikalisch voneinander getrennt)
- Funktionstrennung (Produktion/Test)
- Zuständigkeiten und Verantwortlichkeiten sind eindeutig festgelegt

### 1.5 Pseudonymisierung (Art. 32 Abs. 1 Buchst. a DSGVO; Art. 25 Abs. 1 DSGVO)

*Ein Personenbezug ist nur möglich, wenn zusätzliche Informationen hinzugezogen werden können.*

Beispiele (bitte ggf. ändern/ergänzen):

- personenbezogene Daten werden, soweit möglich, nur unter einem Pseudonym gespeichert
- die zusätzlichen Informationen, die einen Personenbezug herstellen können, werden unter Verschluss aufbewahrt

## 2. Integrität (Art. 32 Abs. 1 Buchst. b DSGVO)

### 2.1. Weitergabekontrolle

*Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle, ...*

Beispiele (bitte ggf. ändern/ergänzen):

- Verschlüsselte Leitungen
- Zugriff von extern nur über verschlüsselte VPN-Tunnelverbindung
- Elektronische Signatur
- Protokollierung
- Transportsicherung
- Versand von passwortgeschützten Dateien per E-Mail
- E-Mail-Verschlüsselung

### 2.2. Eingabekontrolle

*Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.*

Beispiele (bitte ggf. ändern/ergänzen):

- Protokollierungs- und Protokollauswertungssysteme (wer hat was eingegeben, geändert, gelöscht?)
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Kontrolldaten werden aufbewahrt
- Zugriff auf die Protokolle ist nur Berechtigten möglich

### **3. Verfügbarkeit und Belastbarkeit** (Art. 32 Abs. 1 Buchst. b DSGVO)

#### **3.1. Verfügbarkeitskontrolle**

*Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.*

Beispiele (bitte ggf. ändern/ergänzen):

- Backup- und Recovery-Verfahren
- getrennte / katastrophensichere Aufbewahrung der Backups
- Spiegeln von Festplatten, z.B. RAID-Verfahren
- Einsatz von Unterbrechungsfreier Stromversorgung (USV)
- Serverraum ist klimatisiert
- Einsatz von Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, Spam-Filter)
- Feuer- und Rauchmeldeanlagen sind vorhanden
- Notfallplan liegt vor

### **4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** (Art. 32 Abs. 1 Buchst. d DSGVO; Art. 25 Abs. 1 DSGVO)

#### **4.1 Datenschutz-Management**

*Ist beim Auftragnehmer ein Verfahren im Einsatz, das die Beachtung des Datenschutzes sicherstellt? Wenn ja, beschreiben Sie es.*

- ein Datenschutz-Management-System (DSMS) ist implementiert
- Handbuch / Richtlinie zum Datenschutz ist für die Mitarbeiter vorhanden
- Datenschutzbeauftragter ist benannt
- regelmäßige Kontrolle durch den Datenschutzbeauftragten
- Beschäftigte werden im Datenschutz geschult
- Beschäftigten sind zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet
- Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 DSGVO wird geführt

#### **4.2 Incident-Response-Management**

*Ist beim Auftragnehmer ein Verfahren im Einsatz, das den Umgang mit datenschutzrechtlichen Vorfällen beschreibt? Wenn ja, beschreiben Sie es.*

- Vorgaben vorhanden, was als Datenpanne anzusehen ist
- Vorgaben vorhanden, wie mit Datenpannen umzugehen ist
- Notfallplan vorhanden

#### **4.3 Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DS-GVO)

*Ist beim Auftragnehmer ein Verfahren im Einsatz, mit dem datenschutzrechtliche Voreinstellungen gewährleistet werden? Wenn ja, beschreiben Sie es.*

- Rechte- und Rollenkonzept nach dem „Need to know“-Prinzip
- Vermeidung externer Ressourcen



#### **4.4 Auftragskontrolle**

*Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.*

Beispiele (bitte ggf. ändern/ergänzen):

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung (Auftragsformular)
- Kriterien zur Auswahl des Auftragnehmers
- Kontrolle der Vertragsausführung
- Subunternehmer werden schriftlich beauftragt