

**Vereinbarung zur Auftragsverarbeitung  
der subreport Verlag Schawe GmbH  
gemäß Art. 28 Abs. 3 DS-GVO  
(Stand: 08. September 2021)**

zwischen der

subreport Verlag Schawe GmbH  
Buchforststr. 1-15  
D-51101 Köln

nachfolgend „Auftragsverarbeiter“

und

dem Nutzer/der Nutzerin der online angebotenen Dienste:

[demo.subreportCAMPUS.de](https://demo.subreportCAMPUS.de), [demo.subreport-ELViS.de](https://demo.subreport-ELViS.de),  
[www.subreportCAMPUS.de](https://www.subreportCAMPUS.de), [www.subreport-ELViS.de](https://www.subreport-ELViS.de)

nachfolgend „Verantwortlicher“

## **Präambel**

Der Verantwortliche nutzt die vom Auftragsverarbeiter online angebotenen Dienste ([demo.subreportCAMPUS.de](https://demo.subreportCAMPUS.de), [www.subreportCAMPUS.de](https://www.subreportCAMPUS.de), [demo.subreport-ELViS.de](https://demo.subreport-ELViS.de) und [www.subreport-ELViS.de](https://www.subreport-ELViS.de)) zur Durchführung von Vergabeverfahren. Um das Online-Vergabeverfahren über diese angebotenen Dienste zweckmäßig durchführen zu können, werden dem Auftragsverarbeiter in diesem Zusammenhang unter anderem auch personenbezogene Daten zur Verfügung gestellt, die dieser im Auftrag des Verantwortlichen verarbeitet. Zur Gewährung eines rechtskonformen Umgangs mit den personenbezogenen Daten vereinbaren die Parteien Folgendes:

### **1. Gegenstand und Dauer der Vereinbarung**

Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Sinne von Art. 4 Nr. 2 und Art. 28 der Europäischen Datenschutzgrundverordnung 2016/679 vom 27.04.2016 (DS-GVO) nach den Regelungen dieser Vereinbarung.

Dabei handelt es sich um personenbezogene Daten, die im Zusammenhang mit der Nutzung der vom Auftragsverarbeiter online angebotenen Dienste ([www.demo.subreportCAMPUS.de](https://www.demo.subreportCAMPUS.de), [www.subreportCAMPUS.de](https://www.subreportCAMPUS.de), [www.demo.subreport-ELViS.de](https://www.demo.subreport-ELViS.de) und [www.subreport-ELViS.de](https://www.subreport-ELViS.de)) durch den Auftragsverarbeiter verarbeitet werden, konkret bei:

- der Bereitstellung von Ausschreibungsdaten,
- der Durchführung des Vergabeprozesses von Aufträgen (einschließlich der Aufbewahrung der im Vergabeprozess generierten Unterlagen/Daten),

## Vereinbarung zur Auftragsverarbeitung

---

- der Unterstützung der Kommunikation zwischen Bewerbern/Bietern und Ausschreibern.

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 Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

### **Dauer des Auftrags**

Die Vereinbarung wird auf unbestimmte Zeit geschlossen. Kündigungsfristen für Einzelverträge sind in Abschnitt A, §1 der Allgemeinen Geschäftsbedingungen der subreport Verlag Schawe GmbH enthalten.

## **2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen**

### **Zweck der Verarbeitung**

- Bereitstellung von Ausschreibungsdaten
- Durchführung des Vergabeprozesses von Aufträgen
- Datenverarbeitung zur Unterstützung der Kommunikation zwischen Bewerbern / Bietern und Ausschreibern.

### **Art der Verarbeitung**

Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne von Art. 4 Nr. 2 DS-GVO.

### **Art der personenbezogenen Daten**

Es handelt sich um alle Arten personenbezogener Daten, die der Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet. Konkret sind dies:

- Kontaktdaten (insbesondere Anrede, Titel, Vor- und Zuname, Anschrift und Position der betroffenen Person beim Verantwortlichen/bei Dritten)
- Angaben über berufliche Qualifikationen/Lebensläufe/Referenzen der Bewerber/Bieter/Interessenten und deren Mitarbeiter

### **Kategorien betroffener Personen**

- Beschäftigte, Beauftragte oder Vertreter des Verantwortlichen
- Bewerber/Bieter/Interessenten in/an Vergabeverfahren und deren Mitarbeiter
- Referenzpartner der Bewerber/Bieter/Interessenten und deren Mitarbeiter

## Vereinbarung zur Auftragsverarbeitung

---

### 3. Rechte und Pflichten sowie Weisungsbefugnisse des Verantwortlichen

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Verantwortliche verantwortlich.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Verantwortlichem und Auftragsverarbeiter abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Verantwortliche 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 durch den Verantwortlichen zu bestätigen.

Der Verantwortliche ist berechtigt, sich wie unter Ziffer 4 festgelegt, vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Unregelmäßigkeiten bei einer solchen Prüfung feststellt.

Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters streng vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen.

### 4. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen, 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 mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Verantwortlichen nicht erstellt.

## Vereinbarung zur Auftragsverarbeitung

---

Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Verantwortlichen verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Verantwortlichen, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Verantwortlichen hat der Auftragsverarbeiter im notwendigen Umfang mitzuwirken und den Verantwortlichen soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils an den Verantwortlichen auf Anfrage weiterzuleiten. Etwaige Kosten für solche Unterstützungsleistungen können vom Auftragsverarbeiter an den Verantwortlichen in angemessener Höhe berechnet werden.

Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine vom Verantwortlichen erteilte Weisung gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen so weit geändert wird, dass sie nicht mehr gegen gesetzliche Vorschriften verstößt.

Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Verantwortliche dies mittels einer Weisung verlangt und berechnete Interessen des Auftragsverarbeiters dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Verantwortlichen erteilen.

Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche - 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 Verantwortlichen 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 DS-GVO). Kontrollen beim Auftragsverarbeiter sind mindestens 10 Werktagen vorher beim Auftragsverarbeiter anzumelden.

Der Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Der Auftragsverarbeiter hat das Recht, Aufwände, die dem Auftragsverarbeiter durch etwaige Kontrollen entstehen, in angemessener Höhe zu berechnen.

## Vereinbarung zur Auftragsverarbeitung

---

Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Verantwortlichen die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung der Vereinbarung fort.

Der Auftragsverarbeiter 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 Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragsverarbeiter ist der Beauftragte für den Datenschutz unter folgenden Kontaktdaten zu erreichen:

subreport Verlag Schawe GmbH  
An den Datenschutzbeauftragten  
Buchforststraße 1-15  
51103 Köln  
Telefon: 0221/98578-85  
E-Mail: [datenschutz@subreport.de](mailto:datenschutz@subreport.de)

### **5. Mitteilungspflichten des Auftragsverarbeiters bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten**

Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich mit, falls ein Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten des Verantwortlichen besteht. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Verantwortlichen nach Art. 33 und Art. 34 DS-GVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. Ziff. 3 dieser Vereinbarung durchführen.

### **6. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)**

Die Beauftragung von Subunternehmern zur Verarbeitung von personenbezogenen Daten des Verantwortlichen ist dem Auftragsverarbeiter nur mit Genehmigung des Verantwortlichen gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 3) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragsverarbeiter dem Verantwortlichen Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragsverarbeiter dafür Sorge tragen, dass er den Subunterneh-

## Vereinbarung zur Auftragsverarbeitung

---

mer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Verantwortlichen auf Anfrage zur Verfügung zu stellen.

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

Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Verantwortlichem und Auftragsverarbeiter auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragsverarbeiters und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Verantwortliche berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

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

Der Auftragsverarbeiter hat die Einhaltung der Pflichten des/der Subunternehmer(s) zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Verantwortlichen auf Verlangen zugänglich zu machen.

Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichem dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragsverarbeiter im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Die für den Auftragsverarbeiter tätigen Subunternehmer sind im Anhang „Subunternehmer-Verzeichnis der subreport Verlag Schawe GmbH gemäß Art. 28 Abs. 2 DS-GVO“ mit Namen, Anschrift und Auftragsinhalt über die Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang aufgeführt. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer. Der Verantwortliche hat das Recht, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO), indem er die Vereinbarung zur Auftragsverarbeitung sowie der zugrunde liegenden Vereinbarung mit einer Frist von zwei Wochen ab Zugang der Information über die beabsichtigte Änderung kündigt. Mit der Kündigung der Vereinbarung zur Auftragsverarbeitung erfolgt gleichsam auch eine Kündigung des Hauptvertra-

## Vereinbarung zur Auftragsverarbeitung

---

ges mit den online angebotenen Diensten [www.demo.subreportCAMPUS.de](http://www.demo.subreportCAMPUS.de), [www.demo.subreport-ELViS.de](http://www.demo.subreport-ELViS.de), [www.subreportCAMPUS.de](http://www.subreportCAMPUS.de) und [www.subreport-ELViS.de](http://www.subreport-ELViS.de). Weitergehende Ansprüche des Verantwortlichen bestehen in diesem Fall nicht.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Post- und Transportdienstleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern sowie Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragsverarbeiter wird jedoch zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen treffen sowie Kontrollmaßnahmen ergreifen.

### **7. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)**

Es wird für die konkrete Auftragsverarbeitung durch den Auftragsverarbeiter ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Der Auftragsverarbeiter hat regelmäßig 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 DS-GVO).

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Verantwortlichen auf Verlangen anzuzeigen.

Die vom Auftragsverarbeiter realisierten Maßnahmen sind in der Anlage „Technische und organisatorische Maßnahmen (TOM) zur Daten- und IT-Sicherheit der subreport Verlag Schawe GmbH gemäß Art. 32 DS-GVO“ dokumentiert und sind Bestandteil dieser Vereinbarung.



## Vereinbarung zur Auftragsverarbeitung

---

### **8. Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO**

Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitung- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu löschen bzw. zu vernichten / vernichten zu lassen.

Die Löschung bzw. Vernichtung ist dem Verantwortlichen mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

### **9. Haftung**

Auf Art. 82 DS-GVO wird verwiesen. Im Falle einer gemeinsamen Haftung des Auftragsverarbeiters und des Verantwortlichen gegenüber Dritten gemäß Art. 82 DSGVO erstattet der Verantwortliche dem Auftragsverarbeiter über die Rückforderung im Innenverhältnis gemäß § 82 Abs. 4 DS-GVO hinaus entsprechend seinem Anteil an der Verantwortung alle weiteren Schäden im Zusammenhang mit der betreffenden Verarbeitung, einschließlich etwaiger Bußgelder, und stellt ihn von den Kosten der Verteidigung gegen alle Ansprüche frei.

Im Übrigen gelten die Regelungen aus Abschnitt A, §5 der Allgemeinen Geschäftsbedingungen der subreport Verlag Schawe GmbH.

### **10. Sonstiges**

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.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Verantwortlichen verarbeiteten personenbezogenen Daten und der zugehörigen Datenträger ausgeschlossen.



## Vereinbarung zur Auftragsverarbeitung

---

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Datum: 08.09.2021

**Subunternehmer-Verzeichnis  
der subreport Verlag Schawe GmbH  
gemäß Art. 28 Abs. 2 DS-GVO  
(Stand: 08.09.2021)**

Dieses Verzeichnis führt die Auftragsverarbeiter, die derzeit im Zusammenhang mit der „Ver- einbarung zur Auftragsdatenverarbeitung der subreport Verlag Schawe GmbH gemäß Art. 28 Abs. 3 DS-GVO“ im Auftrag für subreport Verlag Schawe personenbezogene Daten verarbei- ten, auf. Eine Datenübermittlung von personenbezogenen Daten in Drittländer wird nicht vor- genommen.

<b>Lfd. Nr.</b>	<b>Name / Anschrift</b>	<b>Auftragsinhalt</b>
<b>01</b>	<b>centron GmbH Heganger 29 96103 Hallstadt</b>	Bereitstellung von IT-Systemen und Support-Leistungen im Rahmen des vereinbarten Umfangs.

**Technische und organisatorische Maßnahmen (TOM)  
zur Daten- und IT-Sicherheit  
der subreport Verlag Schawe GmbH  
gemäß Art. 32 DS-GVO**

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen realisiert subreport Verlag Schawe die nachfolgenden technische und organisatorische Maßnahmen (TOM).

Die Auswahl der Maßnahmen umfasst die vier Schutzziele des Art. 32 Abs.1b) DS-GVO, namentlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. Eine rasche Wiederherstellung nach einem physischen oder technischen Zwischenfall ist gewährleistet.

Alle nachfolgenden technischen und organisatorischen Maßnahmen werden regelmäßig, gem. Art. 32 Abs 1 d) DS-GVO, auf Ihre Wirksamkeit hin geprüft.

## **Inhaltsverzeichnis**

1. Vertraulichkeit der IT-Systeme und Datenverarbeitung (Art. 32 Abs. 1 lit. DS-GVO) .....	2
2. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) .....	4
3. Integrität der IT-Systeme und Datenverarbeitung (Art. 32 Abs. 1 lit. b DS-GVO).....	5
4. Verfügbarkeit und Belastbarkeit und rasche Wiederherstellbarkeit der IT-Systeme und Datenverarbeitung (Art. 32 Abs. 1 lit. b) und lit. c) DS-GVO).....	6
5. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO).....	7
6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)	

## 1. Vertraulichkeit der IT-Systeme und Datenverarbeitung (Art. 32 Abs. 1 lit. DS-GVO)

Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.

### 1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	Organisatorische Maßnahmen
Alarmanlage	Schlüsselregelung / Liste
Automatisches Zugangskontrollsystem	Empfang / Rezeption / Pförtner
Biometrische Zugangssperren	Besucherbuch / Protokoll der Besucher
Chipkarten / Transpondersysteme	Mitarbeiter- / Besucherausweise
Manuelles Schließsystem	Besucher in Begleitung durch Mitarbeiter
Sicherheitsschlösser	Sorgfalt bei Auswahl des Wachpersonals
Schließsystem mit Codesperre	Sorgfalt bei Auswahl Reinigungsdienste
Absicherung der Gebäudeschächte	
Türen mit Knauf Außenseite	
Klingelanlage mit Kamera	
Videoüberwachung der Eingänge	

### 1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen
Anti-Viren-Software Server	Erstellen von Benutzerprofilen
Anti-Virus-Software Clients	Zentrale Passwortvergabe

<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
Anti-Virus-Software mobile Geräte	Richtlinie „Sicheres Passwort“
Firewall	Richtlinie „Löschen / Vernichten“
Intrusion Detection Systeme	Richtlinie „Clean desk“
Mobile Device Management	Allg. Richtlinie Datenschutz und / oder Sicherheit
Einsatz VPN bei Remote-Zugriffen	Mobile Device Policy
Verschlüsselung von Datenträgern	Anleitung „Manuelle Desktopsperre“
Gehäuseverriegelung	
BIOS Schutz (separates Passwort)	
Sperre externer Schnittstellen (USB)	
Automatische Desktopsperre	
Verschlüsselung von Notebooks / Tablet	
Identity-Management-System zur Administration der Berechtigungen für die Systeme	

### 1.3. Zugriffskontrolle

Maßnahmen, die geeignet sind zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
Aktenschredder (mind. Stufe 3, cross cut)	Einsatz Berechtigungskonzepte

Technische Maßnahmen	Organisatorische Maßnahmen
Externer Aktenvernichter (DIN 66399)	Minimale Anzahl an Administratoren <ul style="list-style-type: none"> <li>• Ein (1) System- und Netzwerkadministrator</li> </ul>
Physische Löschung von Datenträgern (Überspielung mit Leerdaten)	Datenschutztresor
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	Verwaltung Benutzerrechte durch Administratoren

#### 1.4. Trennungskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung von Produktiv- und Testumgebung	Steuerung über Berechtigungskonzept
Physikalische Trennung (Systeme / Datenbanken / Datenträger)	Festlegung von Datenbankrechten
Mandantenfähigkeit der Anwendungen	

## 2. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Maßnahmen, die geeignet sind zu gewährleisten, dass die personenbezogenen Daten in einer Weise verarbeitet werden, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt)	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

### 3. Integrität der IT-Systeme und Datenverarbeitung (Art. 32 Abs. 1 lit. b DS-GVO)

#### 3.1. Weitergabekontrolle

Maßnahmen, die geeignet sind zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
E-Mail-Verschlüsselung	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
Einsatz von VPN	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
Protokollierung der Zugriffe und Abrufe	Weitergabe in anonymisierter oder pseudonymisierter Form
Sichere Transportbehälter	Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen
Bereitstellung über verschlüsselte Verbindungen wie sftp, https	Persönliche Übergabe mit Protokoll
Nutzung von Signaturverfahren	

#### 3.2. Eingabekontrolle

Maßnahmen, die geeignet sind zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können



<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
Manuelle oder automatisierte Kontrolle der Protokolle	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	Klare Zuständigkeiten für Löschungen

#### **4. Verfügbarkeit und Belastbarkeit und rasche Wiederherstellbarkeit der IT-Systeme und Datenverarbeitung (Art. 32 Abs. 1 lit. b) und lit. c) DS-GVO)**

Maßnahmen, die geeignet sind zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, dass IT-Systeme belastbar sind und dass IT-Systeme und personenbezogene Daten bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
Feuer- und Rauchmeldeanlagen	Backup & Recovery-Konzept (ausformuliert)
Feuerlöscher Serverraum	Kontrolle des Sicherungsvorgangs
Serverraumüberwachung Temperatur und Feuchtigkeit	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
Serverraum klimatisiert	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
USV	Keine sanitären Anschlüsse im oder oberhalb des Serverraums
Schutzsteckdosenleisten Serverraum	Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)

<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quell- dichtung etc.)	Getrennte Partitionen für Betriebssysteme und Daten
RAID System / Festplattenspiegelung	
Videoüberwachung Serverraum	
Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

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

Maßnahmen, die geeignet sind sicherzustellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Dies gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	

### 6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Verfahren und Maßnahmen, die geeignet sind zu gewährleisten, dass die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Sicherstellung der Daten- und IT-Sicherheit regelmäßig überprüft, bewertet und evaluiert werden.

**6.1. Datenschutz-Management**

<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
Software-Lösungen für Datenschutz-Management im Einsatz	Datenschutzbeauftragter
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	Regelmäßige Sensibilisierung der Mitarbeiter, Mindestens jährlich
Anderweitiges dokumentiertes Sicherheitskonzept	Interner / externer Informationssicherheitsbeauftragter Name / Firma Kontakt
Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

**6.2. Incident-Response-Management**

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
Einsatz von Firewall und regelmäßige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
Einsatz von Spamfilter und regelmäßige Aktualisierung	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Virens Scanner und regelmäßige Aktualisierung	Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
Intrusion Detection System (IDS)	Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
Intrusion Prevention System (IPS)	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

### 6.3. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
	Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	Abschluss eines Auftragsvertrags nach Art. 28 Abs. 3 DS-GVO
	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
	Schriftliche Weisungen an den Auftragnehmer
	Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht

<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
	Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	Regelung zum Einsatz weiterer Subunternehmer
	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus