

# Vertrag zur Auftragsverarbeitung



**Auftraggeber (Verantwortlicher):**

Verein :

Vorstand:

---

**Auftragnehmer (Auftragsverarbeiter):**

**pro-WINNER GmbH  
Fritz-Walter-Weg 19  
70372 Stuttgart**

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

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage des Nutzungsvertrags.

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

### **Dauer des Auftrags**

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des unter Punkt 1 genannten Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

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

Siehe Nutzungs-, Service- bzw. Updatevertrag

### **Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):**

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

.....

### **Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO):**

Im Sinne dieser Regelung bezeichnet man als „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

.....

### **Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):**

Mitglieder-/Kontaktdaten (Stammdaten)

.....

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

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 Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

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

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

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

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

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

### 4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen (Vorstand) des Auftraggebers sind:

**X**

.....  
(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragnehmer sind:

Dagmar Schunke, pro-WINNER GmbH, Tel. 0711/ 28077-881

.....  
(Vorname, Name, Organisationseinheit, Telefon)

Für Weisung zu nutzende Kommunikationskanäle:

pro-WINNER GmbH, Fritz-Walter-Weg 19, 70372 Stuttgart, <mailto:info@pro-winner.de>, Tel.: 0711/28077-881

.....  
(genaue postalische Adresse/ E-Mail/ Telefonnummer)

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

## 5. Pflichten des Auftragnehmers

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

Der Auftragnehmer 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 Auftraggebers nicht erstellt.

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

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber eine entsprechende Dokumentation zu führen und diese regelmäßig zu kontrollieren.

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

.....

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

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechnigte Interessen des Auftragnehmers dem nicht entgegenstehen.

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

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. H DS-GVO).

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

Keine besonderen Vereinbarungen  
.....

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen.

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

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

Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz Herr/Frau

Hannes Stelzer, Stratego IT management GmbH, Mail: <mailto:externer-datenschutz@stratego-it.de>

(Vorname, Name, Organisationseinheit, Kontakt)

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

## **6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten**

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber 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 Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

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

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 Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber 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 Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

Prüfung und Bewertung der technisch-/organisatorischen Maßnahmen (TOM's) gem. DSGVO.  
.....

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

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

Zurzeit sind für den Auftragnehmer die in **Anlage 1** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

## **8. 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 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. Für die auftragsgemäße Verarbeitung personenbezogener Daten wird die im Datenschutz-Handbuch beschriebene Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt.

Das im **Anlage 2** beschriebene Datenschutzkonzept (TOM's der pro-WINNER GmbH) stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

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

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.



## 9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen wie folgt datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:

Die Löschung bzw. Vernichtung (entsprechend gesetzlicher Aufbewahrungspflicht) ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

## 10. Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

-----  
Ort, Datum

**Unterschriften:**

\_\_\_\_\_  
Verein

(Auftraggeber)



\_\_\_\_\_  
pro-WINNER GmbH

(Auftragnehmer)

## Anlage 1

### Subunternehmer der pro-WINNER GmbH

	<b>Subunternehmer</b>	<b>Zweck</b>
1.	WLSB Service GmbH Fritz-Walter-Weg 19 70372 Stuttgart	Bereitstellung der Server – nur für Online-Nutzer
2.	Kanzlei HSP Hagellocher Weg 1 72070 Tübingen	Finanzbuchhaltung der pro- WINNER GmbH
3.	Druckerei Aickelin GmbH Lindenstraße 1 71229 Leonberg	Druck von Anschreiben (z.B. Updateanschriften für Offline-Nutzer)

# Technische und organisatorische Maßnahmen i.S.d. Art.32 – EU-DSGVO – Sicherheit der Verarbeitung

der Firma

pro-WINNER GmbH  
Fritz-Walter-Weg 19  
70372 Stuttgart



## 1. Zutrittskontrolle

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

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Alarmanlage                               | <input type="checkbox"/> Absicherung von Gebäudeschächten                      |
| <input checked="" type="checkbox"/> Automatisches Zugangskontrollsystem       | <input checked="" type="checkbox"/> Chipkarten-/Transponder-Schließsystem      |
| <input type="checkbox"/> Schließsystem mit Codesperre                         | <input type="checkbox"/> Manuelles Schließsystem                               |
| <input type="checkbox"/> Biometrische Zugangssperren                          | <input checked="" type="checkbox"/> Videoüberwachung der Zugänge               |
| <input type="checkbox"/> Lichtschranken / Bewegungsmelder                     | <input checked="" type="checkbox"/> Sicherheitsschlösser                       |
| <input checked="" type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Personenkontrolle beim Pförtner / Empfang             |
| <input checked="" type="checkbox"/> Protokollierung der Besucher              | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input checked="" type="checkbox"/> Sorgfältige Auswahl von Wachpersonal      | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen               |

## 2. Zugangskontrolle

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

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Zuordnung von Benutzerrechten                | <input checked="" type="checkbox"/> Erstellen von Benutzerprofilen   |
| <input checked="" type="checkbox"/> Passwortvergabe                              | <input type="checkbox"/> Authentifikation mit biometrischen Verfahren  |
| <input checked="" type="checkbox"/> Authentifikation mit Benutzername / Passwort | <input type="checkbox"/> Zuordnung von Benutzerprofilen zu IT-Systemen   |
| <input type="checkbox"/> Gehäuseverriegelungen                                   | <input checked="" type="checkbox"/> Einsatz von VPN-Technologie  |
| <input type="checkbox"/> Sperren von externen Schnittstellen (USB etc.)          | <input type="checkbox"/> Personenkontrolle beim Pförtner / Empfang   |
| <input type="checkbox"/> Protokollierung der Besucher                            | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal   |
| <input checked="" type="checkbox"/> Sorgfältige Auswahl von Wachpersonal         | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen   |
| <input type="checkbox"/> Einsatz von Intrusion-Detection-Systemen                | <input type="checkbox"/> Verschlüsselung von mobilen Datenträgern  |
| <input type="checkbox"/> Verschlüsselung von Smartphone-Inhalten                 | <input type="checkbox"/> Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) |

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> Einsatz von Anti-Viren-Software | <input checked="" type="checkbox"/> Verschlüsselung von Datenträgern in Laptops / Notebooks |
| <input checked="" type="checkbox"/> Einsatz einer Hardware-Firewall | <input checked="" type="checkbox"/> Einsatz einer Software-Firewall                         |

### 3. Zugriffskontrolle

*Maßnahmen, die 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.*

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Erstellen eines Berechtigungskonzepts  | <input checked="" type="checkbox"/> Verwaltung der Rechte durch Systemadministrator         |
| <input checked="" type="checkbox"/> Anzahl der Administratoren auf das „Notwendigste“ reduziert                                    | <input type="checkbox"/> Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel            |
| <input checked="" type="checkbox"/> Protokollierung von Änderung und Löschung von Daten  | <input checked="" type="checkbox"/> Sichere Aufbewahrung von Datenträgern                   |
| <input type="checkbox"/> physische Löschung von Datenträgern vor Wiederverwendung  | <input checked="" type="checkbox"/> ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) |
| <input checked="" type="checkbox"/> Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) | <input type="checkbox"/> Protokollierung der Vernichtung                                    |
| <input checked="" type="checkbox"/> Verschlüsselung von Datenträgern   |   |

### 4. Weitergabekontrolle

*Maßnahmen, die 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.*

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> Einrichtungen von Standleitungen bzw. VPN-Tunneln   | <input type="checkbox"/> Weitergabe von Daten in anonymisierter oder pseudonymisierter Form           |
| <input checked="" type="checkbox"/> Personenbezogene Daten werden immer verschlüsselt weitergegeben   | <input type="checkbox"/> Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen |
| <input type="checkbox"/> Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen | <input type="checkbox"/> Beim physischen Transport: sichere Transportbehälter/-verpackungen           |
| <input type="checkbox"/> Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen                               |   |

## 5. Eingabekontrolle

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

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Protokollierung der Eingabe, Änderung und Löschung von Daten  | <input type="checkbox"/> Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. |
| <input checked="" type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) | <input type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind                                    |
| <input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts                    |  |

## 6. Auftragskontrolle

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

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)              | <input checked="" type="checkbox"/> vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen |
| <input checked="" type="checkbox"/> schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG | <input checked="" type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)              |
| <input checked="" type="checkbox"/> Auftragnehmer hat Datenschutzbeauftragten bestellt   | <input checked="" type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags                           |
| <input checked="" type="checkbox"/> Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart   | <input checked="" type="checkbox"/> laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten                                  |
| <input checked="" type="checkbox"/> Vertragsstrafen bei Verstößen  |   |

## 7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV)                              | <input checked="" type="checkbox"/> Klimaanlage in Serverräumen                |
| <input checked="" type="checkbox"/> Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | <input checked="" type="checkbox"/> Schutzsteckdosenleisten in Serverräumen    |
| <input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen   | <input checked="" type="checkbox"/> Feuerlöschgeräte in Serverräumen           |
| <input type="checkbox"/> Alarmmeldung bei unberechtigten Zutritten zu Serverräumen                         | <input checked="" type="checkbox"/> Erstellen eines Backup- & Recoverykonzepts |
| <input checked="" type="checkbox"/> Testen von Datenwiederherstellung                                      | <input checked="" type="checkbox"/> Erstellen eines Notfallplans               |
| <input checked="" type="checkbox"/> Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort   | <input checked="" type="checkbox"/> Serverräume nicht unter sanitären Anlagen  |
| <input type="checkbox"/> In Hochwassergebieten: Serverräume über der Wassergrenze                          |  |

## 8. Trennungsgebot

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

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern | <input checked="" type="checkbox"/> Logische Mandantentrennung (softwareseitig)   |
| <input checked="" type="checkbox"/> Erstellung eines Berechtigungskonzepts  | <input type="checkbox"/> Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden   |
| <input type="checkbox"/> Versehen der Datensätze mit Zweckattributen/Datenfeldern                                 | <input type="checkbox"/> Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System |
| <input checked="" type="checkbox"/> Festlegung von Datenbankrechten   | <input checked="" type="checkbox"/> Trennung von Produktiv- und Testsystem  |

Stuttgart, 04.05.2018

Ort, Datum

Bastian Mörbe

Verantwortlicher für die Erstellung (in Druckbuchstaben)



Unterschrift des Verantwortlichen