**Vereinbarung zur Auftragsverarbeitung**
i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

Stand: 25.05.2018

zwischen (bitte ausfüllen)

_____
_____
_____
_____

im Folgenden »Auftraggeber« genannt

und

**Druckhaus Blochwitz**
**Inh. Dipl.-Ing. S. Gotzmann e.Kfr.**
**Baderstraße 6**
**06712 Zeitz**

im Folgenden »Auftragnehmer« genannt

- gemeinsam »Vertragsparteien« genannt.

## Präambel

Diese Vereinbarung regelt die Verpflichtungen der Vertragsparteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die mit der Beauftragung durch den Auftraggeber im Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

## § 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Der Auftragnehmer erbringt für den Auftraggeber vertragliche Leistungen im Bereich der Herstellung und Lieferung von (personalisierten) Drucksachen und Werbeartikeln/-zubehör sowie der Erstellung/Gestaltung von Druckvorlagen. Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Dauer, Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus den jeweiligen Aufträgen. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Vertragsparteien die vorliegende Vereinbarung.

(3) Die Bestimmungen dieser Vereinbarung finden Anwendung auf alle Tätigkeiten, die mit der Bearbeitung der erteilten Aufträge im Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit

personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(4) Diese Vereinbarung läuft auf unbestimmte Zeit und ist mit einer Frist von drei Monaten zum Quartalsende ordentlich kündbar.

## § 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in den jeweiligen Aufträgen konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Vereinbarung 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).

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

## § 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des jeweiligen Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren Wirksamkeit wird auf die Verhaltensregeln nach Art. 40 DS-GVO verwiesen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem.

Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen der jeweiligen Aufträge anfallende Datenschutzfragen.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der Auftragnehmer berichtigt oder löscht auftragsgegenständliche Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

## § 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

## § 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

## § 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

## § 7 Subunternehmer (weitere Auftragsverarbeiter)

(1) Vom Auftraggeber beauftragte Leistungen werden ganz oder teilweise unter Einschaltung von Subunternehmern erbracht. Die eingesetzten Subunternehmer werden dem Auftraggeber auf Anforderung benannt. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den

Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarung mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

## § 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des jeweiligen Auftrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(4) Es gilt deutsches Recht. Ausschließlicher Gerichtsstand ist Zeitz.

## §9 Haftung und Schadensersatz

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

## §10 Verweise auf die DS-GVO

(1) Alle in dieser Vereinbarung enthaltenen Verweise auf die DS-GVO gelten für die DS-GVO in Ihrer jeweiligen aktuellen Fassung bzw. etwaige Nachfolgeregelungen.

## §11 Schlussbestimmungen

(1) Die Regelungen dieser Vereinbarung genießen Vorrang vor allen anderen Vereinbarungen der Vertragsparteien.

(2) Als Bestandteile dieser Vereinbarung gelten die folgenden Anlagen:

Anlage 1 – Beschreibung der schutzbedürftigen Daten/-kategorien und der Betroffenen.

Anlage 2 – Beschreibung der technischen und organisatorischen Maßnahmen des Auftraggebers.

| | |
|---|---|
| Ort, Datum | blochwitz DRUCK \| MEDIENDESIGN \| WERBETECHNIK Mediendesign Blochwitz Sibylle Gotzmann 06712 Zeitz, Badersstr. 6 T 03441 8047-0 |
| Unterschrift Auftraggeber | Unterschrift Auftragnehmer |

## Anlage 1 zur Vereinbarung zur Auftragsverarbeitung

Beschreibung der schutzbedürftigen Daten/-kategorien und der Betroffenen

| Arten der Verarbeitung personenbezogener Daten | Zwecke der Verarbeitungen | Arten der personenbezogenen Daten | Kategorien betroffener Personen |
|---|---|---|---|
| • Erhebung<br>• Speicherung<br>• Verwendung<br>• Übermittlung an Post-/Paketdienstleister<br>• Löschung<br>• Übermittlung an weitere Auftrags-verarbeiter, die als Subunternehmer für den Auftrags-verarbeiter tätig sind | • Vertragserfüllung (Gestaltung und Herstellung von [personalisierten] Drucksachen und Werbemitteln) | • Personen- bzw. Unternehmensstammdaten<br>• Kommunikationsdaten<br>• Vertrags- und Bestelldaten<br>• Vertragsabrechnungs- & Zahlungsdaten<br>• Planungs- & Steuerungsdaten<br>• Verbindungsdaten<br>• Bildmaterial | • Kunden<br>• Interessenten<br>• Lieferanten<br>• Handelsvertreter<br>• Ansprechpartner<br>• Externe Dienstleister |
| | Erfüllung der gesetzlichen Verpflichtungen (AO/HGB o.ä.) | • wie oben | • wie oben<br>• Rechnungsempfänger |

## Anlage 2 zur Vereinbarung zur Auftragsverarbeitung

Technische und organisatorische Maßnahmen gem. Art. 32 DS-GVO

Version 1.0

Gemäß Art. 32 DS-GVO sind geeignete technische und organisatorische Maßnahmen, 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 der Risiken für die Rechte und Freiheiten natürlicher Personen, seitens des Verantwortlichen und der Auftragsverarbeiter zu treffen.

Der Auftragnehmer als Auftragsverarbeiter wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien, geeignet sind.

Zur Erfüllung der gesetzlichen Anforderungen sind in Art. 32 DS-GVO verschiedene Anforderungen/Kontrollen definiert. Der Auftragnehmer setzt die Anforderungen in seinem Einflussbereich in Bezug auf diese Vereinbarung wie folgt um:

### 1. Zutrittskontrolle

1.1. Mit dem Begriff „Zutritt" ist der physische Zugang von Personen zu Gebäuden und Räumlichkeiten gemeint, in denen IT-Systeme betrieben und genutzt werden. Dies können z. B. Rechenzentren sein, in denen Web-Server, Applikationsserver, Datenbanken, Mainframes, Speichersysteme betrieben werden und Arbeitsräume, in denen Mitarbeiter Arbeitsplatzrechner nutzen. Auch die Räumlichkeiten, in denen sich Netzkomponenten und Netzverkabelungen befinden und verlegt sind, gehören hierzu. Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden (können), zu verwehren. Der Auftragnehmer muss deshalb dafür Sorge tragen, dass Unbefugte Räume, in denen Daten vom Auftraggeber verarbeitet oder gespeichert werden, nicht betreten können und keinen Einblick oder Zugriff auf Datenverarbeitungsgeräte (Monitore, Drucker, etc.) erlangen können, auf denen diese Daten verarbeitet oder ausgegeben werden.

1.2. Umsetzung der Zutrittskontrolle:

Der Auftragnehmer hat die folgenden Maßnahmen zur Zutrittskontrolle umgesetzt:

- ☑ Die Gebäude sind mit einer Alarmanlage gesichert
- ☐ Die Gebäude werden von einem Wachdienst gesichert

Die Eingangstüren des Gebäudes sind mit folgender Schließanlage versehen:

- ☑ Manuelle Schließanlage
- ☐ Chipkarten Schließanlage

- ☐ Die Nutzung der Schließanlage wird dokumentiert
- ☐ Der Zutritt von Besuchern zum Gebäude wird dokumentiert
- ☑ Der Zutritt und Aufenthalt von Besuchern erfolgt nur in Begleitung von Firmenpersonal
- ☐ Der Zutritt von Reinigungs- und Wartungspersonal zum Gebäude wird dokumentiert.
- ☐ Der Entzug von Gebäudezutrittsberechtigungen ist geregelt und dokumentiert
- ☐ Es besteht ein gesondertes Zutrittskonzept für Serverräume

## 2. Zugangskontrolle

2.1. Ergänzend zur Zutrittskontrolle ist es Ziel der Zugangskontrolle zu verhindern, dass DV-Anlagen von Unbefugten benutzt werden, mit denen personenbezogene Daten gespeichert, verarbeitet oder genutzt werden. Unbefugte dürfen keinen Zugang zu den Datenverarbeitungssystemen des Auftragnehmers erlangen können. Daher muss der Auftragnehmer die mit der Erfüllung der Leistungen des Auftrags beauftragten Personen mit einer sicheren Benutzeridentifikation versehen.

2.2. Umsetzung der Zugangskontrolle:

2.2.1. Der Auftragnehmer hat die folgenden Maßnahmen zur Zugangskontrolle umgesetzt:

- ☑ Das Firmennetzwerk ist durch eine Firewall geschützt
  Aktualisierungsverfahren und -häufigkeit: bei Bedarf

- ☑ Die Daten des Auftraggebers werden innerhalb des Firmennetzwerkes separiert - durch folgende Maßnahmen: Rechtevergabe

2.2.2. Die Mitarbeiter des Auftragnehmers müssen folgende Passwortvorgaben erfüllen:

- ☐ Individuelle Passwörter für verschiedene Systeme (keine Sammelpasswörter)
- ☑ Die Passwörter haben eine Mindestlänge/Komplexität
  Anzahl der Zeichen: 6 Zeichen
- ☑ Die Passwörter müssen regelmäßig gewechselt werden
  Intervall: alle 12 Monate
- ☑ Der Zugang zum System wird gesperrt bei der fehlerhaften Eingabe des Passwortes
  Anzahl der Fehlversuche: 10
  Dauer der Sperrung: 60min
- ☐ Automatische Verriegelung des Bildschirms nach Zeitintervall:

2.2.3. An den folgenden Übergängen zum Firmennetzwerk werden Virenscanner eingesetzt:

- ☑ E-Mail Account
- ☐ FTP

☑ Web

2.2.4. Es werden regelmäßig Penetrationstests aller zum Internet geöffneten IP-Adressen durchgeführt:

☐ ja ☑ nein

2.2.5. Einsatz eines Virenscanners auf allen Servern:

☑ ja ☐ nein
Aktualisierungsverfahren und -häufigkeit: wöchentlich

2.2.6. Einsatz eines Virenscanners auf allen Einzelarbeitsplatzcomputern:

☑ ja ☐ nein
Aktualisierungsverfahren und -häufigkeit: wöchentlich

2.2.7. Sicherheitsrelevante Softwareupdates werden regelmäßig in die vorhandene Software eingespielt:

☑ ja ☐ nein
Betriebssysteme: automatisch
Anwendungen: nach Bereitstellung

2.2.8. Mitarbeiter haben lokale Administrationsrechte:

☐ ja ☐ nein ☑ teilweise

2.2.9. Mitarbeiter haben Internetzugangsberechtigung mit restriktiver Browserkonfiguration:

☑ ja ☐ nein

Restriktive, von Mitarbeitern nicht änderbare Browserkonfiguration sind eingerichtet:

☐ ja ☑ nein

## 3. Zugriffskontrolle

3.1. Die Anforderungen der Zugriffskontrolle sind darauf ausgerichtet, dass nur durch Berechtigte auf die Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht und dass die Daten nicht durch Unbefugte manipuliert oder gelesen werden können. Es dafür zu sorgen, 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.

3.2. Umsetzung der Zugriffskontrolle:

Der Auftragnehmer hat die folgenden Maßnahmen zur Zugriffskontrolle umgesetzt:

- ☑ Ein Berechtigungskonzept ist vorhanden
- ☑ Die vergebenen Berechtigungen werden dokumentiert.
- ☐ Die Organisation der Berechtigungsvergabe wird namensscharf dokumentiert (insb. wer darf welche Rechte vergeben).
- ☐ Die vergebenen Berechtigungen werden namensscharf dokumentiert.

Anzahl der Administratoren mit der Berechtigung, Datenbestände des AG ganz oder in großen Mengen zu kopieren/extrahieren: 2

Anzahl der Mitarbeiter mit der Berechtigung, Datenbestände des Auftraggebers ganz oder in großen Mengen zu kopieren/extrahieren: alle

Folgende Komponenten der Arbeitsplatzcomputer wurden verriegelt/deaktiviert, damit keine Datenexporte extern gespeichert werden können:

- ☐ USB-Ports
- ☐ CD-/DVD-Brenner
- ☐ Speicherkartenslots
- ☐ andere mobile Datenträger, wenn zutreffend welche:

Fernwartungs-/Fernzugriffszugänge sind vorhanden für:

- ☐ weitere Dienstleister
- ☑ Mitarbeiter
- ☑ Administratoren

Art der Authentifizierung: RDP
Verwendete Protokolle: RDP

## 4. Weitergabekontrolle

4.1. Der Auftragnehmer muss verhindern, dass personenbezogene Daten vom Auftraggeber 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 welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

4.2. Umsetzung der Weitergabekontrolle:

Der Auftragnehmer hat die folgenden Maßnahmen zur Weitergabekontrolle umgesetzt:

Eingesetzte Verschlüsselungsart für Datenaustausch zwischen AG und AN:

- ☐ SFTP
- ☐ S/Mime
- ☑ SSL

Die per Datenträger versendeten Daten werden verschlüsselt:

☐ ja ☑ nein

Daten des Auftraggebers werden zusätzlich verschlüsselt gespeichert:

☐ ja ☑ nein

Werden Backups durchgeführt:

☑ ja, verschlüsselt ☐ ja, unverschlüsselt ☐ nein

Gesicherte Aufbewahrung der Backupmedien:

☑ ja ☐ nein

## 5. Eingabekontrolle

5.1. Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Es müssen daher für derartige Maßnahmen entsprechende Protokollierungssysteme vorhanden sein.

5.2. Umsetzung der Eingabekontrolle:

Der Auftragnehmer hat die folgenden Maßnahmen zur Eingabekontrolle umgesetzt:

- ☐ Es werden Log-Files für die Nachvollziehbarkeit der Löschung/Änderung von Daten des Auftraggebers erstellt.
- ☐ Es besteht ein restriktives Zugriffskonzept für vorgenannte Log-Files.

## 6. Auftragskontrolle

6.1. Der Auftragnehmer muss gewährleisten, dass personenbezogene Daten vom Auftraggeber nur gemäß deren Weisungen verarbeitet werden. Beschäftigt der Auftragnehmer einen Unterauftragnehmer, so muss er diesen in gleicher Weise zur Erfüllung der Weisungen und zur Einhaltung des Datenschutzes verpflichten.

6.2. Umsetzung der Auftragskontrolle:

Der Auftragnehmer hat die folgenden Maßnahmen zur Auftragskontrolle umgesetzt:

☑ Die Mitarbeiter werden schriftlich auf das Datengeheimnis gem. Art. 28 Abs. 3 b) DS-GVO verpflichtet.
☑ Die Mitarbeiter werden schriftlich auf das Fernmeldegeheimnis gem. § 88 TKG verpflichtet.
☑ Die Mitarbeiter erhalten regelmäßig Schulungen zum Datenschutz.
☐ Der Auftragnehmer hat die folgenden Zertifikate, die mit dieser Checkliste eingereicht werden:

Folgende schriftliche Zusatzerklärungen (im Zusammenhang mit Datenschutz und Datensicherheit) holt der Auftragnehmer von seinen Mitarbeitern ein:

Es werden/wurden Subauftragnehmer beauftragt, denen auftragsrelevante Daten des Auftraggebers zur Verarbeitung übermittelt werden:

☑ ja ☐ nein

Mit Subauftragnehmern, denen Daten des Auftraggebers zur Verarbeitung übermittelt werden, bestehen Verträge gem. Art 28 DS-GVO:

☑ ja ☐ nein

Es gibt Subauftragnehmer außerhalb der EU, die Zugriff auf Daten des Auftraggebers haben:

☐ ja ☑ nein

Subauftragnehmer, denen Daten des Auftraggebers zur Verarbeitung übermittelt werden, halten die in dieser Checkliste vereinbarten technischen und organisatorischen Maßnahmen genauso wie der Auftragnehmer selbst ein und haben deren Einhaltung vertraglich zugesichert:

☑ ja ☐ nein

## 7. Verfügbarkeitskontrolle

7.1. Der Auftragnehmer muss dafür sorgen, dass personenbezogene Daten vom Auftraggeber gegen zufällige Zerstörung oder Verlust geschützt sind.

7.2. Umsetzung der Verfügbarkeitskontrolle:

Der Auftragnehmer hat die folgenden Maßnahmen zur Verfügbarkeitskontrolle umgesetzt:

Häufigkeit der Datensicherungsmaßnahmen:

☐ täglich ☑ monatlich ☐ jährlich

Aufbewahrungsort von Sicherungsdatenträgern:

☑ Safe

☑ externe Auslagerung

☐ Es bestehen Verträge für die Wartung von IT-Systemen durch externe Unternehmen

## 8. Trennungsgebot

8.1. Es ist dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden. Die Trennung der Daten muss so gestaltet sein, dass eine „Vermischung" mit Daten anderer Vertragspartner/Auftraggeber des Auftragnehmers und auch unbefugte Zugriffe Dritter (auch versehentlich) unmöglich sind. Sollten Daten anderer Vertragspartner/Auftraggeber des Auftragnehmers von behördlichen Zugriffen bzw. Beschlagnahme betroffen sein, muss gewährleistet sein, dass die Daten vom Auftraggeber davon unberührt bleiben. Die Daten dürfen nicht zu Testzwecken herangezogen werden, welche nicht Bestandteil der Leistungen des Hauptvertrages sind.

8.2. Umsetzung des Trennungsgebotes:

Der Auftragnehmer hat die folgenden Maßnahmen zum Trennungsgebot umgesetzt:

☐ Produktivdaten des Auftraggebers werden in einem eigenen Mandanten vorgehalten
☐ Es besteht ein Berechtigungskonzept für den vorgenannten Mandanten, dass den Datenzugriff von Mitarbeitern ausschließt, die nicht für den Auftraggeber tätig sind
☐ Mitarbeiter, die Daten des Auftraggebers verarbeiten sitzen räumlich getrennt von Mitarbeitern, die für andere Auftraggeber arbeiten
☑ Mitarbeiter werden schriftlich dazu verpflichtet, Informationen aus Datenbeständen des Auftraggebers nicht in andere Projekte mit einzubringen

Der Auftragnehmer versichert, dass die hier getätigten Angaben dem aktuellen Stand der bei ihm umgesetzten technischen und organisatorischen Maßnahmen zum Datenschutzniveau und zur Datensicherheit entsprechen. Abweichungen der hier getätigten Angaben sind unmittelbar dem Auftraggeber zu melden.

| Version | Datum: | Kapitel: | Inhalt der Änderung: | geändert durch: |
|---|---|---|---|---|
| 1.0 | 24.05.2018 | alle | Initiale Erstellung | Michel Blumenstein |

Zeitz, 25.05.2018

blochwitz
DRUCK | MEDIENDESIGN | WERBETECHNIK
Mediendesign Blochwitz
Dipl.-Ing. Sybille Gotzmann
06712 Zeitz · Baderstr. 6 · 03441-8047-0

Sybille Gotzmann, Inhaberin