



## Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

### Vereinbarung

zwischen

- Verantwortlicher - nachstehend Auftraggeber genannt -  
und der

CDS Peter Griese GmbH

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

### Präambel

(1) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 Datenschutz-Grundverordnung (DS-GVO) als Dienstleister ausgewählt. Voraussetzung für die Zulässigkeit einer Auftragsverarbeitung ist, dass der Auftraggeber dem Auftragnehmer den Auftrag schriftlich erteilt. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung i.S.d. Art. 28 DS-GVO und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird damit allgemein die Verwendung von personenbezogenen Daten verstanden. Eine Verwendung personenbezogener Daten umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung sowie das Anonymisieren, Pseudonymisieren, Verschlüsseln oder die sonstige Nutzung von Daten.

### 1. Gegenstand und Dauer des Auftrags

#### (1) Gegenstand

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

- Der Auftragnehmer kann personenbezogene Daten im Auftrag des Kunden verarbeiten. (Auftragsverarbeitung).

Dies erfolgt auf Grund individueller, vom Auftraggeber an den Auftragnehmer, erteilter Aufträge und umfasst insbesondere die Verarbeitung personenbezogener Daten, während der vom Auftragnehmer durchgeführten Wartungsarbeiten/Softwareeinrichtungen an den IT Systemen des Auftraggebers oder deren Mandanten.

#### (2) Dauer

- Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.
- Der Auftrag wird zur einmaligen Ausführung erteilt.
- Der Auftrag beginnt am ..... und endet am .....
- Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum .....
- Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von ..... zum ..... gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

- Die Dauer dieses Auftrags läuft bis zum Widerruf



## 2. Konkretisierung des Auftragsinhalts

### (1) Art und Zweck der vorgesehenen Verarbeitung von Daten

- Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom .....
- Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: Siehe Leistungsbeschreibung wie in Punkt 1. (1).

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff DS-GVO erfüllt sind.

### (2) Art der Daten

- Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)
  - Stammdaten
  - Kommunikationsdaten (z.B. Telefon, E-Mail)
  - Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
  - Kundenhistorie
  - Vertragsabrechnungs- und Zahlungsdaten
  - Planungs- und Steuerungsdaten
  - Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
  - .....
  - .....
  - .....

### (3) Kategorien betroffener Personen

- Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: .....
- Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen (Aufzählung/Beschreibung der betroffenen Personenkategorien):
  - Mitarbeiter des Auftraggebers
  - Kunden des Auftraggebers
  - Kunden und Mitarbeiter von Kunden des Auftraggebers
  - Handelsvertreter
  - Ansprechpartner
  - Stammdaten der Mandanten und Grunddaten Rechnungswesen
  - Abonnenten
  - Lieferanten des Auftraggebers
  - Interessenten
  - .....
  - .....



### **3. Technisch-organisatorische Maßnahmen**

- (1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- (2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].
- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

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

- (1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- (2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.



## 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

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

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer

Mario Arndt, DEUDAT GmbH, [kontakt@deudat.de](mailto:kontakt@deudat.de), Tel: +49 611 950008-32

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

- b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

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

- e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

- f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

- g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

- h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.



## 6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Eine Unterbeauftragung ist unzulässig.

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

<b>Firma Unterauftragnehmer</b>	<b>Anschrift/Land</b>	<b>Leistung</b>
Günther Feucht IT Service	Bartholomäusweg 39, 63762 Großostheim	DATEV Updates und Helpdesk
SolarWinds MSP UK Ltd.	Vision Building, Greenmarket, Dundee, DD1 4QB, United Kingdom	System-Monitoring der CDSasp-Umgebung, CDS Managed Antivirus
TeamDrive Systems GmbH	Max-Brauer-Allee 50, 22765 Hamburg	Helpdesk und Lizenzreporting für die eigene Cloudlösung CDS TeamDrive
TeamViewer GmbH	Jahnstr. 30, 73037 Göppingen	Fernwerkzeug
Sophos Limited	The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, United Kingdom	CDS Managed Antivirus, CDSasp Firewallsystem
Wortmann AG	Bredenhop 20, 32609 Hüllhorst	Datensicherung
Octopus Cloud AG	Baarerstrasse 145, CH-6300 Zug, Schweiz	Microsoft SPLA Lizenzreporting-Tool
DATEV	Paumgartnerstraße 6 – 14, 90429 Nürnberg	Hosting, Rechenzentrum Zertifizierung nach ISO 27001

Die Auslagerung auf Unterauftragnehmer

oder

der Wechsel des bestehenden Unterauftragnehmers

sind zulässig, soweit:

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

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

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

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Information und Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(6) Der Auftragsverarbeiter führt regelmäßige Kontrollen der Unterauftragsverarbeiter durch. Diese Kontrollen sind zu dokumentieren und nach Anfrage dem Auftraggeber zur Verfügung zu stellen.



## 7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig, mindestens 14 Tage vorher, anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

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

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

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

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

## 8. Mitteilung bei Verstößen des Auftragnehmers

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

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

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

## 9. Weisungsbefugnis des Auftraggebers

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

Der Auftragnehmer hat dem Auftraggeber die Person(en) zu benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind.

Weisungsempfangsberechtigte Personen des Auftragnehmers sind:

Thorsten Lucas, Geschäftsleitung, 0611 90 90 0, [tlucas@cds-systeme.de](mailto:tlucas@cds-systeme.de)

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der

entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## 10. Löschung und Rückgabe von personenbezogenen Daten

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

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

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

## 11. Sonstiges

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung oder Beschlagnahme oder durch sonstige Ereignisse gefährdet sein, hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Der Auftragnehmer weist die Dritten darauf hin, dass die Verantwortlichkeit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

(2) Änderungen und Ergänzungen dieser Zusatzvereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung.

(3) Sollte eine oder mehrere Klauseln aus diesem Vertrag unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

---

Ort, Datum

Wiesbaden, 06.06.2018

---

Ort, Datum



---

Auftraggeber

---

Auftragnehmer CDS Peter Griese GmbH



**CDS** · we make **IT** easy



## Anlage 1 – Technisch-organisatorische Maßnahmen

### 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  - Schlüsselausgabe nur an Angestellte der Firma und den Vermieter.
  - Elektronische Schlüssel können deaktiviert werden.
  - Schlüsselausgabe wird schriftlich dokumentiert.
  - Unterbringung der Server in einem Rechenzentrum in Kürze, daher keine Einrichtung von Sicherheitsbereichen.
- Zugangskontrolle
  - Zugang zu den Datenverarbeitungsanlagen haben nur Angestellte.
  - Kunden werden in den Besprechungsraum/Schulungsraum begleitet.
  - Externe Dienstleister werden beaufsichtigt.
  - Einige Notebooks sind verschlüsselt.
- Zugriffskontrolle
  - Über die Active Directory ist geregelt welcher User Zugriff auf welches Laufwerk hat.
  - Die Benutzer müssen sich zur Einwahl ins System mit Name und Kennwort authentifizieren.
- Trennungskontrolle
  - Ein externer Datenschutzbeauftragter ist bestellt.
  - Eine Verfahrensdokumentation ist vorhanden
  - IT-Richtlinien und Arbeitsanweisungen sind in Arbeit
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  - Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

### 2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

#### Beispiele für Maßnahmen zur Sicherstellung der **Integrität**.

- Weitergabekontrolle
  - Nicht mehr benötigte, sensible Papierdokumente werden geschreddert.
  - Ausgediente Festplatten werden von einem externen Dienstleister vernichtet.
- Eingabekontrolle
  - Erstanlage und Änderungen von Datensätzen in der Warenwirtschaft und in den DATEV Produkten werden protokolliert.

### 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Beispiele für Maßnahmen zur Sicherstellung der **Verfügbarkeit und Belastbarkeit**.

- Verfügbarkeitskontrolle
  - Eine inkrementelle Datensicherung der letzten 28 Tage wird durchgeführt.
  - USV und Überspannungsschutz ist eingerichtet.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

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

Maßnahmen zur Sicherstellung der **regelmäßigen Überprüfung, Bewertung und Evaluierung**.

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

#### Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.