VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

zwischen

dem Nutzer von VLB-TIX

und

MVB GmbH
Braubachstr. 16
60311 Frankfurt am Main

(nachstehend Auftragnehmer genannt):

I. GEGENSTAND UND DAUER DES AUFTRAGS

1. Gegenstand des Auftrags ist der Vertrag des Auftraggebers mit dem Auftragnehmer über die Nutzung des Portals VLB-TIX.

2. Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit »der Leistungsvereinbarung VLB-TIX«.

II. 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 zu „VLB-TIX «.

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

2. ART DER DATEN

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenstammdaten (E-Mail-Adressen, ggf. Namen der Adressaten)
- Kommunikationsdaten (E-Mail)

3. KATEGORIEN DER BETROFFENEN PERSONEN

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen

- Interessenten
- Abonnenten

III. 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 in der Anlage dieser Vereinbarung

dokumentiert. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

2. Der Auftragnehmer hat die Sicherheit gem. Artt. 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 Umsetzung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme.

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. Der Auftraggeber informiert sich vor Abschluss dieser Vereinbarung und anschließend in regelmäßigen Abständen über die technischen und organisatorischen Maßnahmen. Der Auftraggeber trägt die Verantwortung dafür, dass die jeweils aktuell geltenden, vertraglich vereinbarten technischen und organisatorischen Maßnahmen für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

IV. 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 umzusetzen.

V. QUALITÄTSSICHERUNG UND SONSTGE PFLICHTEN DES AUFTRAGNEHMERS

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

1. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Dr. Adil-Dominik Al-Jubouri, MVB GmbH, Braubachstr. 16, 60311 Frankfurt am Main bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

2. Die Wahrung der Vertraulichkeit gemäß Artt. 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.

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

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

5. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige

Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

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

7. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um dafür zu sorgen, 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.

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

VI. 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.

3. 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:

- Globalways AG, Neue Brücke 8, 70173 Stuttgart
- iucon GmbH, Hüttenstraße 50, 45527 Hattingen

4. 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.

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

6. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

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

VII. 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 in der Regel rechtzeitig 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 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

Der Auftraggeber und dem Auftragnehmer sind sich einig, dass die vorgenannten Bescheinigungen eine Kontrolle der betreffenden Maßnahmen und Pflichten des Auftragnehmers durch den Auftraggeber ausschließen. Hierdurch wird ein nicht erforderlicher Prüfungsaufwand vermieden und der Umfang und die Dauer der Kontrollen auf das gebotene Minimum zu beschränkt. Satz 1 gilt nicht, wenn der Auftraggeber Tatsachen darlegt, die nahelegen, dass die Bescheinigungen unzutreffend sind.

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

5. Besteht bei Kontrollen die Möglichkeit zur Kenntnisnahme von vertraulichen Informationen, ist der Auftragnehmer berechtigt, eine Verschwiegenheitserklärung vom Auftraggeber sowie von dessen beauftragten Prüfer zu verlangen.

VIII. 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 nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

IX. WEISUNGSBEFUGNIS DES AUFTRAGSGEBERS

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

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.

X. 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. Der Auftragnehmer wird dies dem Auftraggeber auf Nachfrage bestätigen. Gleiches gilt für Test- und Ausschussmaterial.

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.

XI. PFLICHTEN DES AUFTRAGGEBERS

1. Verantwortlich für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung ist im Rahmen dieser Vereinbarung allein der Auftraggeber (als Verantwortlicher gem. Art. 4 Nr. 7 DSGVO). Dies gilt auch im Hinblick auf die in dieser Vereinbarung geregelten Zwecke und Mittel der Verarbeitung und die Beschreibung der betroffenen Daten.

2. Auf Anfrage des Auftragnehmers nennt der Auftraggeber seinen Ansprechpartner für sämtliche datenschutzrechtlich relevanten Fragen im Rahmen der vorliegenden Auftragsverarbeitung.

3. Stellt der Auftraggeber im Hinblick auf die Verarbeitung bzgl. Datenschutzrechtlicher Bestimmungen Fehler oder Unregelmäßigkeiten fest, wird er den Auftragnehmer unverzüglich und umfassend informieren.

Anlage – Technisch-organisatorische Maßnahmen

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

- Zutrittskontrolle
  - ➔ Der Empfang ist von 08:00 bis 18:00 besetzt.
  - ➔ Alle Außentüren sind grundsätzlich verschlossen. Einzig der Haupteingang zum Empfang ist geöffnet. Nach 18:00 Uhr ist er verschlossen.
  - ➔ Ein elektronisches Schließsystem regelt den Zugang zu allen Türen des Gebäudes über ein Berechtigungssystem.
  - ➔ Die den Mitarbeitern zur Verfügung gestellten elektronischen Schlüssel sind personengebunden registriert.
  - ➔ Die Schlüsselausgabe wird dokumentiert.
  - ➔ Besucher werden am Empfang abgeholt und können sich nur in Begleitung eines Mitarbeiters in den Räumlichkeiten bewegen.
  - ➔ Der Zutritt zum Rechenzentrum ist nur autorisierten Personen gestattet.
  - ➔ Die Anzahl autorisierter Personen ist auf ein Minimum beschränkt.
  - ➔ Der Zutritt zum Rechenzentrum ist durch ein durch einen elektronischen Schlüssel und eine PIN-Eingabe gesichert.
  - ➔ Im Eingangsbereich der Serverräume ist mit einer Videoüberwachung über Bewegungsmelder ausgestattet.
  - ➔ Eine Alarmanlage im Rechenzentrum ist vorhanden mit einer Anbindung an einen externen Sicherheitsdienst

- Zugangskontrolle
  - ➔ Die Anzahl der Administratoren ist auf ein Minimum beschränkt.
  - ➔ Passwortrichtlinie über Länge und Komplexität zu wählender Passwörter.
  - ➔ Mitarbeiter arbeiten ausschließlich mit den personalisiert angelegten Benutzerprofilen.
  - ➔ Automatisches Sperren des Arbeitsplatzgeräts bei fehlender Nutzeraktivität.
  - ➔ Verpflichtung zum manuellen Sperren bei Verlassen des Arbeitsplatzgeräts über eine IT-Richtlinie.
  - ➔ Alle technischen Systeme werden durch eine Firewall geschützt.
  - ➔ Der vorhandene Virenschutz (Anti-Virensoftware) wird regelmäßig gepflegt und aktualisiert.
  - ➔ Zugriffe von außerhalb sind nur über VPN möglich.
  - ➔ Eine Festplattenverschlüsselung der mobilen Arbeitsplatzgeräte besteht.

- Zugriffskontrolle
  - ➔ Benutzerprofile mit differenzierten Berechtigungen nach Rollenprinzip.
  - ➔ Vergabe von Laufwerksrechten auf Verzeichnis- und Einzeluserebene.
  - ➔ Ein Schutz gegen unberechtigte interne und externe Zugriffe durch Verschlüsselung und Firewalls besteht.
  - ➔ Sichere Aufbewahrung von Datenträgern.
  - ➔ Ordnungsgemäße Vernichtung von Datenträgern.
  - ➔ Einsatz von Aktenvernichtern bzw. geprüften Dienstleistern zur Aktenvernichtung.
  - ➔ Protokollierung der Vernichtung.

- Trennungskontrolle
  - ➔ Funktionstrennung von Test- und Produktivsystemen.
  - ➔ Getrennte Verarbeitung von zweckgebundenen Daten.

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  - ➔ Die Übermittlung personenbezogener Daten erfolgt verschlüsselt.

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

- Weitergabekontrolle
  - ➔ Eine Weitergabe von Daten erfolgt an berechtigte Personen und nur aufgrund einer rechtlichen Grundlage
  - ➔ Einrichtung von Standleitungen zur Datenkommunikation.
  - ➔ Einsatz von VPN-Technologie (SSL/TLS) zur Datenkommunikation.

- Eingabekontrolle
  - ➔ Die Zugriffsrechte orientieren sich (sowohl für Anwender, wie auch für Administratoren) an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen.

3. VERFÜGBARKEIT UND BELASTBARKEIT (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
  - ➔ Getrennte Stromkreise im Rechenzentrum
  - ➔ Redundant ausgelegte unterbrechungsfreie Stromversorgung (USV)
  - ➔ Redundante Firewall
  - ➔ Redundante Klimaanlage im Rechenzentrum.
  - ➔ Monitoring-System der Server rund um die Uhr (24/7). Meldungen werden dabei per push-Messages sowie per SMS-Technologie übermittelt.
  - ➔ Anti-Viren-Software
  - ➔ Überwachung von Temperatur und Feuchtigkeit in Serverräumen
  - ➔ Feuer- und Rauchmeldeanlage sowie Feuerlöscher in den Serverräumen
  - ➔ Eine Feuerlöschanlage mit Spezialgas ist in den in den Serverräumen installiert

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);
  - ➔ Sicherungen erfolgen in fest definierten in Datensicherungszyklen.
  - ➔ Alle Backups werden in einem feuerfesten Datensicherungs-Schrank aufbewahrt.
  - ➔ Die Aufbewahrung von Datensicherungen erfolgt an einem ausgelagerten Ort.
  - ➔ Eine schnellere Wiederherstellbarkeit kann durch die Virtualisierung der Systeme erfolgen
  - ➔ Festplattenspiegelungen

4. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- ➔ Erarbeitung eines Datenschutz-Managements;
- ➔ Erstellung von internen Datenschutz- und Sicherheitsrichtlinien (Policies) sowie Arbeitsanweisungen.
- ➔ Bestellung eines internen Datenschutzbeauftragten.
- ➔ Regelmäßige Kontrolle durch den Datenschutzbeauftragten.
- ➔ Regelmäßige Datenschutz-Schulungen der Beschäftigten
- ➔ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- ➔ Auftragskontrolle (Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen)
- ➔ Gelegentliche unangekündigte interne Kontrollen der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen.
