Nutzung von IT-Systemen der easybill GmbH durch ihre Kunden

Datenschutzvereinbarung nach Art. 28 DSGVO

zwischen

easybill GmbH, Düsselstr. 21, 41564 Kaarst

– easybill –

und

, ,

– Kunde –

Präambel

Der Kunde nutzt den von easybill betriebenen internetbasierten Dienst zum Erstellen von Rechnungen. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Kunde personenbezogene Daten verarbeitet. Nach Art. 28 DSGVO ist hierfür der Abschluss eines Auftragsverarbeitungsvertrags erforderlich.

Voraussetzung für die Zulässigkeit einer solchen Auftragsverarbeitung i. S. d. Art. 28 DSGVO ist, dass der Kunde easybill den Auftrag erteilt. Dieser Vertrag enthält diesen Auftrag des Kunden an easybill und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit dieser Datenverarbeitung sowie die sich daraus ergebenden besonderen Pflichten in Bezug auf Datenschutz und Datensicherheit.

Grundsätzlich ist der Kunde für die Einhaltung der Vorschriften der DSGVO und anderer Vorschriften über den Datenschutz verantwortlich und behält insofern die Herrschaft über die zu verarbeitenden Daten. easybill wird den Kunden hierbei in geeigneter Weise unterstützen.

1. Allgemeines

a) easybill verarbeitet personenbezogene Daten im Auftrag des Kunden i. S. d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

b) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i. S. d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Diese Vereinbarung findet Anwendung auf alle Tätigkeiten, die mit dem zugrunde liegenden Auftrag in Zusammenhang stehen und bei denen Mitarbeiter von easybill oder durch easybill beauftragte Dritte mit personenbezogenen Daten des Kunden in Berührung kommen können. Der Auftrag des Kunden an easybill umfasst die in der **Anlage 1** wiedergegebenen Arbeiten und/oder Leistungen. Aus der Anlage ergibt sich zudem der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen.

3. Rechte und Pflichten des Kunden

a) Der Kunde ist Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch easybill. easybill steht nach Ziff. 4 c) das Recht zu, den Kunden darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

b) Der Kunde ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. easybill wird den Kunden unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber easybill geltend machen.

c) Der Kunde hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber easybill zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.

d) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Kunden bei easybill entstehen, bleiben unberührt.

e) Der Kunde informiert easybill unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch easybill feststellt.

f) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Kunden geltenden gesetzlichen Meldepflicht besteht, ist der Kunde für deren Einhaltung verantwortlich.

4. Pflichten von easybill

a) easybill verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Kunden erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die easybill ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt easybill dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Kunden. Eine hiervon abweichende Verarbeitung von Daten ist easybill untersagt, es sei denn, dass der Kunde dieser schriftlich zugestimmt hat.

b) easybill verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

c) easybill wird den Kunden unverzüglich darüber informieren, wenn eine vom Kunden erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. easybill ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Kunden bestätigt oder geändert wird. Sofern easybill darlegen kann, dass eine Verarbeitung nach Weisung des Kunden zu einer Haftung von easybill nach Art. 82 DSGVO führen kann, steht easybill das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

5. Meldepflichten von easybill

a) easybill ist verpflichtet, dem Kunden jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Kunden, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die easybill im Auftrag des Kunden verarbeitet.

b) Ferner wird easybill den Kunden unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber easybill tätig wird und dies auch eine Kontrolle der Verarbeitung, die easybill im Auftrag des Kunden erbringt, betreffen kann.

c) easybill ist bekannt, dass für den Kunden eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. easybill wird den Kunden bei der Umsetzung der Meldepflichten unterstützen. easybill wird dem Kunden insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen. Die Meldung von easybill an den Kunden muss insbesondere folgende Informationen beinhalten:
   a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
   b. eine Beschreibung der von easybill ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

6. Mitwirkungspflichten von easybill

a) easybill unterstützt den Kunden bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO.

b) easybill wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Kunden mit.

c) easybill unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

7. Kontrollbefugnisse

a) Der Kunde hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Kunden durch easybill im erforderlichen Umfang zu kontrollieren.

b) easybill ist dem Kunden gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i. S. d. Absatzes a) erforderlich ist.

c) Der Kunde kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Abs. a) in der Betriebsstätte von easybill zu den jeweils üblichen Geschäftszeiten vornehmen. Der Kunde wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe von easybill durch die Kontrollen nicht unverhältnismäßig zu stören. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Kunden unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Kunde easybill die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenen Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Kunden von easybill vor Durchführung der Kontrolle mitgeteilt.

d) Nach Wahl von easybill kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Kunden in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 3** zu diesem Vertrag zu überzeugen. Sollte der Kunde begründete Zweifel an der Eignung des Prüfdokuments i. S. d. Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Kunden erfolgen. Dem Kunden ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.

e) easybill ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Kunden i. S. d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Kunden zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Kunde ist über entsprechende geplante Maßnahmen von easybill zu informieren.

8. Unterauftragsverhältnisse

a) easybill ist berechtigt, die in der **Anlage 2** zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz b) genannten Voraussetzungen zulässig.

b) easybill hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen dem Kunden und easybill getroffenen Vereinbarungen einhalten kann. easybill hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. easybill wird den Kunden im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Kunde hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information“ zu widersprechen. Der Widerspruch kann vom Kunden jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann easybill das Vertragsverhältnis mit dem Kunden mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. easybill wird bei der Kündigungsfrist die Interessen des Kunden angemessen berücksichtigen. Wenn kein Widerspruch des Kunden binnen drei Wochen nach Zugang der „Information“ erfolgt gilt dies als Zustimmung des Kunden zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers. Auf die Bedeutung seines Schweigens wird der Kunde in der „Information“ gesondert hingewiesen.

c) easybill ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat, sofern der Unterauftragnehmer zur Benennung eines Datenschutzbeauftragten gesetzlich verpflichtet ist.

d) easybill hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Kunden auch gegenüber dem Unterauftragnehmer gelten.

e) easybill hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat easybill dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Kunde und easybill festgelegt sind. Dem Kunden ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

f) easybill ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse des Kunden und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte des Kunden und der Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

g) Nicht als Unterauftragsverhältnisse i. S. d. Absätze a) bis f) sind Dienstleistungen anzusehen, die easybill bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die easybill für den Kunden erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. easybill ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i. S. d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Kunden genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Kunden verarbeitet werden.

9. Vertraulichkeitsverpflichtung

a) easybill ist bei der Verarbeitung von Daten für den Kunden zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

b) easybill hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

c) Die Verpflichtung der Beschäftigten nach Absatz b sind dem Kunden auf Anfrage nachzuweisen.

10. Wahrung von Betroffenenrechten

a) Der Kunde ist für die Wahrung der Betroffenenrechte allein verantwortlich. easybill ist verpflichtet, den Kunden bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. easybill hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Kunden erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

b) Soweit eine Mitwirkung von easybill für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Kunden erforderlich ist, wird easybill die jeweils erforderlichen Maßnahmen nach Weisung des Kunden treffen. easybill wird den Kunden nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

c) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Kunden bei easybill entstehen, bleiben unberührt.

11. Vergütung

Die Vergütung von easybill wird gesondert vereinbart.

12. Technische und organisatorische Maßnahmen zur Datensicherheit

a) easybill verpflichtet sich gegenüber dem Kunden zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

b) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird easybill im Voraus mit dem Kunden abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können easybill ohne Abstimmung mit dem Kunden umgesetzt werden. Der Kunde kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der von easybill getroffenen technischen und organisatorischen Maßnahmen anfordern.

13. Dauer des Auftrags

a) Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über Nutzung der Dienstleistungen von easybill durch den Kunden.

b) Der Kunde kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß von easybill gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, easybill eine Weisung des Kunden nicht ausführen kann oder will oder easybill den Zutritt des Kunden oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

14. Beendigung

Nach Beendigung des Vertrages hat easybill sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Kunden an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

15. Schlussbestimmungen

a) Diese Vereinbarung unterliegt deutschem Recht.

b) Für Nebenabreden ist die Schriftform erforderlich.

c) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Kaarst, den ...

Andreas Seifert
Geschäftsführer easybill GmbH

Der Kunde hat seine Willenserklärung zum Abschluss des Vertrages elektronisch am ... über die IP-Adresse ... abgegeben.

Anlage 1

Leistungen von easybill

Umfang, Art und Zweck: Erstellung von Rechnungen, Angeboten, Lieferscheinen und ähnlichen Dokumenten über eine internetbasierte Software

Arten von Daten: Jegliche durch den Kunden im Dienst gespeicherte Daten, insbesondere von seinen Endkunden, Lieferanten oder Mitarbeitern, nämlich Name, Anschrift, E-Mail-Adresse, ggf. Rufnummer sowie Details zu getätigten Bestellungen und Zahlungen

Betroffene: Endkunden, Lieferanten, Mitarbeiter

Anlage 2

easybill setzt derzeit folgende Unterauftragnehmer ein:

Webhosting: Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen

Rechnungsdruck: DocuSystem GmbH, Rudolf-Diesel-Str. 4, 63322 Rödermark

Faxversand: GTC TeleCommunication GmbH, Zimmermannstr. 15, 70128 Stuttgart

Datensicherung: Amazon.com Inc., 2012 Seventh Ave., Seattle, Washington 98121, USA
(Serverstandort Deutschland, AES-256 verschlüsselt)

Automatische Belegerfassung (OCR): natif.ai GmbH, Campus Starterzentrum Gebäude A1 1, 66123 Saarbrücken

Anlage 3

Technische und organisatorische Maßnahmen von easybill

easybill trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i. S. d. Art. 32 DSGVO.

1. Vertraulichkeit

a) Zutrittskontrolle
Unbefugten ist der Zutritt zu Daten-verarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

Speicherung der Daten in einem Rechenzentrum, dort:

• elektronisches Zutrittskontrollsystem mit Protokollierung
• dokumentierte Schlüsselvergabe an Mitarbeiter
• Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
• 24/7 personelle Besetzung der Rechenzentren
• Videoüberwachung an den Ein- und Ausgängen

b) Zugangskontrolle
Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

• Umsetzung durch Benutzerkontensteuerung, Zugriff auf EDV-Systeme nur mit Benutzername/ Passwort möglich.
• Auftraggeber vergeben selbst Passwörter, die nach erstmaliger Inbetriebnahme erneut geändert werden können und die dem Auftragnehmer nicht bekannt sind

c) Zugriffskontrolle
Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

• Einrichtung eines Berechtigungskonzepts, bei dem einzelnen Auftraggebern ausschließlich der Zugriff auf eigene Bereiche und Daten zugewiesen wird;
• Protokollierung des Zugriffs in Logfiles;
• Für die Geheimhaltung der Zugangsdaten und ggf. deren Weitergabe an Mitarbeiter ist der Auftraggeber selbst verantwortlich.

d) Trennungskontrolle
Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

• Daten der Auftraggeber werden physikalisch oder logisch von anderen Daten ge-trennt gespeichert.
• Datensicherung erfolgt ebenfalls physikalisch oder logisch.

2. Integrität

a) Eingabekontrolle
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:

• Die Daten werden vom Auftraggeber selbst eingegeben und verarbeitet,
• der Zugriff durch den Auftraggeber wird protokolliert.

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

• Mitarbeiter sind auf das Datengeheimnis nach Art. 28 Abs. 3 Satz 2 lit.b DSGVO und § 203 StGB verpflichtet,
• die Übertragung der Daten von und zu den Kundenbereichen erfolgt nur SSL-verschlüsselt,
• für die Einrichtung von Übertragungswegen auf externe Systeme (Datenexport) ist der Auftraggeber selbst verantwortlich.

3. Verfügbarkeit und Belastbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Daten des Auftraggebers werden regelmäßigen Datensicherungen unterzogen,
- Einsatz redundanter Systeme,
- Einsatz unterbrechungsfreier Stromversorgung.

4. Auftragskontrolle

Es muss sichergestellt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, gemäß den Weisungen des Auftraggebers verarbeitet werden:

- AV-Vertrag enthält eindeutige Festlegung der Weisungsbefugnisse,
- Kontrollrechte, inkl. Vor-Ort Kontrollen, sind vertraglich festgelegt,
- AV-Vertrag folgt den gesetzlichen Vorgaben und lässt Verarbeitung nur im Auftrag zu,
- AV-Vertrag sieht vor, dass Subunternehmer gleichen Pflichten unterliegen müssen.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die Mitarbeiter von easybill werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag., auch im Hinblick auf das Weisungsrecht des Auftraggebers.

Jeder Mitarbeiter wird spätestens am ersten Tag zu Beginn seiner Tätigkeit schriftlich zur Einhaltung der datenschutzrechtlichen Anforderungen nach der DSGVO verpflichtet. Ohne Vorliegen dieser Erklärung erhält der Mitarbeiter keinen Zugriff auf personenbezogene Daten.

In unserer Anwendung easybill werden dem Nutzer alle Möglichkeiten angeboten, die notwendig sind, um Daten in einer DSGVO-konformen Art und Weise zu verarbeiten. easybill gestaltet seine Technik und Anwendung dergestalt, dass datenschutzfreundliche Voreinstellungen grundsätzlich vorausgewählt sind.

Es existiert ein Verarbeitungsverzeichnis i. S. d. Art. 30 Abs. 1, 2 DSGVO und ein Prozess zur Folgeabschätzung (DSFA), der regelmäßig durchgeführt wird und dauerhafter Bestandteil der Evaluierung und Implementierung von neuen Funktionen innerhalb der easybill Anwendung ist.