postserver

VERTRAG ZUR AUFTRAGS-VERARBEITUNG

I.S.V. ART. 28 DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Vertrag zur Auftragsverarbeitung
i.S.v. Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen dem Auftraggeber / der Auftraggeberin:

Firmenname: _____

Firmenanschrift: _____

_____

Im Folgenden auch „Auftraggeber“ genannt,

und den Auftragnehmer:

Postserver Onlinezustelldienst GmbH

Mariahilfer Straße 123, 1060 Wien, Österreich

im Folgenden auch „Postserver“ genannt.

1. Allgemeines

(1) Diese Vereinbarung wird mit Unterzeichnung integrierender Bestandteil des jeweiligen Hauptvertrages zwischen dem Kunden (Auftraggeber) und Postserver.

(2) Der Vertrag zur Auftragsdatenverarbeitung ersetzt das Service-Organisationshandbuch, welches bis 25. Mai 2018 organistorische und datenschrutzrechtliche Aspekte behandelte. Der Vertrag zur Auftragsdatenverarbeitung wird daher gemäß Zertifizierung nach Rulebbok der WKO auch organistorische Aspekte umfassen (Anlagen 2 und 3).

(3) Postserver verarbeitet personenbezogene Daten im Auftrag des Auftraggebers iSv Art 4 und Art 28 DSGVO (Datenschutzgrundverordnung – Verordnung EU Nr 2016/679). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(4) Postserver verpflichtet sich den Grundsätzen des Gender Mainstreaming. Wir legen großen Wert auf Diversität und Gleichbehandlung.

Geschlechtsspezifische Bezeichnungen werden entweder neutralisierend, in der Doppelbezeichnung (Splitting), im generischen maskulinem Plural oder abwechselnd verwendet. Auf Sichtbarmachungen

via Binnen-I, Klammer oder Schrägstrich wird im Sinne einer besseren Lesbarkeit verzichtet.

(5) Im Sinne dieser Vereinbarung bezeichnet der Ausdruck

- „Personenbezogene Daten“
  alle Informationen, die sich iSv Art 4 Nr 1 EU-DSGVO auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen und nach Punkt 4 dieser Vereinbarung verarbeitet werden;
- „Datenverarbeitung“ oder „Verarbeitung“
  iSv Art 4 Nr 2 EU-DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
- „Auftragsverarbeiter“
  Postserver Onlinezustelldienst GmbH als Auftragnehmer der Datenverarbeitung iSv Art 4 Nr 8 DSGVO;
- „Auftraggeber“
  den Kunden von Postserver Onlinezustelldienst GmbH, der als Auftraggeber der Datenverarbeitung ein Verantwortlicher iSv Art 4 Nr 7 DSGVO ist;
- „Zustellung“
  jene Daten, die im Rahmen einer E-Zustellung, E-Rechnung, E-Zahlschein oder postalischen Briefsendung an den Empfänger übermittelt werden.
- „Unterauftragsverhältnis“
  solche Dienstleistungen, die sich unmittelbar auf die Erbringung der Hauptleistung (technische Abwicklung von E-Zustellungen und digitalen Postservices) beziehen. Nicht hierzu gehören Dienstleistungen, die Postserver bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben (z.B. Telekommunikationsleistungen, Post- / Transportdienstleistungen, Verwaltungsdienstleistungen, Wartung und Benutzerservice, die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen).
- „Leistungsvereinbarung“
  Einzelheiten der Leistungen, die sich aus den Allgemeinen Geschäftsbedingungen (https://www.postserver.com/de/agb) ergeben und die bei der Registrierung für Postserver ausdrücklich vom Auftraggeber akzeptiert werden, sowie vertragliche Leistungen, die im Rahmen einer Integration festgelegt werden.

2. Gegenstand und Dauer der Auftragsdatenverarbeitung

Gegenstand der Auftragsdatenverarbeitung ist die technische Abwicklung von E-Zustellungen und digitalen Postservices für den jeweils im Hauptvertrag genannten Leistungsumfang.

Postserver verarbeitet personenbezogene Daten im Auftrag des Auftraggebers.

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung. Die Regelungen zur Kündigung der Leistungsvereinbarung gelten auch für diesen Vertrag. Eine Beendigung der Leistungsvereinbarung berechtigt beide Parteien zur Kündigung dieses Vertrages.

Darüber hinaus sind sich die Parteien darüber einig, dass frühere Verträge zur Auftragsdatenverarbeitung oder Auftragsverarbeitung mit Abschluss dieses Vertrages einvernehmlich beendet werden.

3. Konkretisierung des Auftragsinhalts (Umfang, Art und Zweck der Datenverarbeitung, Art der Daten, Kreis der Betroffenen)

Umfang, Art und Zweck der Datenverarbeitung beschränken sich auf die Nutzung von

- Adressdaten des Auftraggebers für den Empfang von E-Zustellungen,
- Adressdaten von Empfängern für den Versand von Postbriefen

E-Mail Adressen für den Versand von „Einladungen“ zu Postserver werden nicht gespeichert.

Für den Inhalt einer konkreten Zustellung ist der Auftraggeber als Verantwortlicher iSv Art 4 Nr 7 DSGVO selbst verantwortlich. Postserver bietet lediglich einen sicheren Übermittlungsweg u.a. für personenbezogene und sensible Daten iSv Art 4 Abs 2 und Art 5 Abs 1f, DSGVO.

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Österreich, 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 des Art. 7 DSGVO erfüllt sind.

Kategorien betroffener Personen:

User-Kategorie	Beschreibung
Kunde	**Postserver Kunden und Partner** der Auftraggeber
Empfänger	**Empfänger** von E-Zustellungen und digitalen Postservices

Kategorien der Personen, denen gegenüber die Daten offengelegt werden

User-Kategorie	Bearbeitungsrolle	Beschreibung
Datenschutz-beauftragte	Datenschutz	**Datenschutz-beauftragte** Zuständig für die Beauskunftung
Fachkundiger Datenschutz-Mitarbeiter	Datenschutz	**Postserver Mitarbeiter mit Personal-verantwortung** Hat Zugriff auf schützenswerte Daten. Operatives Management von 2nd Level Supportfällen und Key-Account-Management.
Administrator Dritter	(technischer Zugriff)	**Infrastruktur-administrator Tele2** Hat technischen Zugriff auf den Postserver Server. Zentraler Ansprechpartner hinsichtlich Verkehrssicherung.
Administrator Dritter	(technischer Zugriff)	**Applikations-administrator CPB** Hat technischen Zugriff auf die Webservice Datenbank am Postserver Server und betreut die Integration von Business-Lösungen.
Administrator Dritter	(technischer Zugriff)	**Applikations-administrator kbprintcom** Hat technischen Zugriff auf die Datenbank der Druckstraße und betreut die Erstellung von Druckprofilen von Business-Lösungen
Mitarbeiter Dritter	(Produktions-zugriff)	**Mitarbeiter kbprintcom** Hat Produktionszugriff auf die Zustellstücke in der Druckstraße.

Die verarbeiteten Datenarten und die Löschroutine ergeben sich aus Punkt 17 dieses Vertrages.

4. Technische und organisatorische Maßnahmen, Folgenabschätzung

Postserver ist verpflichtet, die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Erhebung, Verarbeitung, oder Nutzung der personenbezogenen Daten – unter besonderer Berücksichtigung der konkreten Auftragsdurchführung – zu dokumentieren und dem Auftraggeber diese Dokumentation auf Anfrage zur Verfügung zu stellen. Die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen sind zu dem im vorgenannten Zweck in dem als Anlage 1 beigefügten Datensicherheitskonzept aufgeführt und sind Teil dieser Vereinbarung.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung; insoweit ist es Postserver gestattet, alternative adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Postserver 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 geprüfte Wirksamkeit wird auf die vorliegende Zertifizierung durch die Wirtschaftskammer Österreich nach Rulebook der WKÖ (zugelassen mit Vertrag vom 10.03.2010) und Zertifizierung gemäß § 4 Zustelldiensteverordnung (zugelassen mit Bescheid vom 4.9.2012) verwiesen, deren Vorlage Postserver für den Nachweis geeigneter Garantien ausreicht (vgl. Anlage 1).

5. Berichtigung, Löschung und Sperrung von Daten

Postserver hat auf Weisung des Auftraggebers die personenbezogenen Daten, die im Auftrag erhoben, verarbeitet oder genutzt werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an Postserver zwecks Berichtigung, Löschung oder Sperrung seiner Daten wenden sollte, ist Postserver verpflichtet, dieses Ersuchen

unverzüglich nach Erhalt an den Auftraggeber weiterzuleiten. Etwaige dafür anfallende Kosten trägt der Auftraggeber.

6. Datenschutzkontrolle und Informationspflicht

Postserver hat nach Art. 28ff DSGVO folgende Pflichten:

- Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten. Dessen Kontaktdaten werden dem Auftraggeber auf Anforderung mitgeteilt.
- Wahrung des Datengeheimnisses entsprechend Art. 29 DSGVO. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, werden auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt.
- Unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der

Postserver Onlinezustelldienst GmbH | Mariahilfer Straße 123/3 | 1060 Vienna | Austria
UniCredit Bank Austria AG | IBAN: AT37 1200 0529 4901 3147 | BIC: BKAUATWW
Registriert beim Handelsgericht Wien unter FN 367446 m | UID-Nummer: ATU 66678268

Aufsichtsbehörde nach Art. 57 DSGVO. Dies gilt auch, soweit eine zuständige Behörde nach Art. 83 DSGVO beim Auftragnehmer ermittelt.

- Erstattung von Meldungen an den Auftraggeber in allen Fällen, in denen durch ihn oder die bei ihm beschäftigten Personen oder Unterauftragnehmer Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind. Dies gilt auch im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten und bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers.
- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

7. Unterauftragsverhältnisse

Postserver ist berechtigt, sich für die Erfüllung der Leistungsvereinbarung und/oder dieses Vertrages Unterauftragnehmer zu bedienen. Voraussetzung ist die Zustimmung des Auftraggebers. Die Zustimmung gilt als erteilt, wenn

- dem Auftraggeber die Identität des Unterauftragnehmers in Textform mitgeteilt wird (Anlage 1)
- die vertraglichen Vereinbarungen mit dem Unterauftragnehmer so gestaltet sind, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen
- bei der Unterbeauftragung dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung eingeräumt werden. Dies umfasst insbesondere das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.
- der Auftraggeber nicht binnen einer Woche ab Mitteilung schriftlich widersprochen hat.

Der Auftraggeber darf einen Widerspruch gegen die Einschaltung eines Unterauftragnehmers nur aus wichtigem Grund erheben.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die Postserver bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Postserver ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

8. Pflichten des Auftraggebers

Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenverarbeitung durch den Auftragnehmer allein

verantwortlich und somit „Verantwortlicher“ im Sinne von Art. 4 Nr. 7 DSGVO.

Die Verantwortlichkeit betrifft auch und insbesondere eine etwaige Pflicht zur Führung eines Verzeichnisses nach Art. 30 DSGVO und die Informationspflichten nach Art. 12 - 14 DSGVO.

Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt Punkt 8 Abs. 9 dieses Vertrages.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

Der Auftraggeber nennt Postserver den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

9. Weisungsbefugnis des Auftraggebers / Pflichten des Auftragnehmers

(1) Postserver darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall des Art. 28 Abs. 3 a) DSGVO vor.

Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, welches er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf Postserver nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Erteilt der Auftraggeber Einzelweisungen hinsichtlich des Umgangs mit personenbezogenen Daten, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

Postserver verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate 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.

Postserver ist verpflichtet, die zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3a DSGVO vor. Postserver informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Postserver darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde. Offensichtlich datenschutzwidrige Weisungen muss Postserver nicht ausführen.

(2) Postserver unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 - 36 DSGVO genannten Pflichten. Für die Erbringung dieser

Postserver Onlinezustelldienst GmbH | Mariahilfer Straße 123/3 | 1060 Vienna | Austria
UniCredit Bank Austria AG | IBAN: AT37 1200 0529 4901 3147 | BIC: BKAUATWW
Registriert beim Handelsgericht Wien unter FN 367446 m | UID-Nummer: ATU 66678268

Unterstützungsleistungen berechnen wir eine Vergütung von € 100,00 zzgl. 20% USt. je angefangener Arbeitsstunde.

(3) Postserver gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet Postserver, 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 Auftrags fort.

(4) Postserver unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Postserver 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.

(5) Postserver nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen:

Name und Kontakt Verantwortlicher:
Alexander Mittag-Lenkheym
Postserver Onlinezustelldienst GmbH,
Mariahilfer Straße 123, 1060 Wien, Österreich

Datenschutz-Verantwortliche
Carola Zentara, CMO

Fachkundiger Datenschutz-Mitarbeiter
Unterstützt wird die Datenschutzbeauftragte durch einen fachkundigen Mitarbeiter mit beschränkten Bearbeitungsrechten mit der Rolle „Datenschutz“.

Zentrale Kontaktmöglichkeit
Anfragen, die das Auskunftsrecht, Berichtigungsrecht und Löschungsrecht oder Einschränkung der Verarbeitung sowie Widerspruchsrecht und das Recht auf Datenübertragbarkeit betreffen, können an folgende Adresse gestellt werden:
Postserver Onlinezustelldienst GmbH,
Mariahilfer Straße 123, 1060 Wien, Österreich
E-Mail: datenschutz@posterver.com

(6) Postserver gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit d DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(7) Postserver berichtigt oder löscht die vertragsgegenständlichen 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 Postserver die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. Für die Erbringung dieser Unterstützungsleistungen berechnen wir eine Vergütung von € 100,00 zzgl. 20% USt. je angefangener Arbeitsstunde.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Eine Vergütung sowie Schutzmaßnahmen sind hierzu gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart. Für die Erbringung dieser Schutzmaßnahmen berechnen wir eine Vergütung von € 100,00 zzgl. 20% USt. je angefangener Arbeitsstunde. Die Kosten für die geschäftliche Aufbewahrung von Daten bestimmt sich nach der Größe der Daten sowie der Dauer der Aufbewahrung. Soweit die Aufbewahrung gewünscht ist, ist hierzu eine einzelvertragliche Regelung zu treffen.

(8) 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.

(9) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich Postserver den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Für die Erbringung dieser Unterstützungsleistungen berechnen wir eine Vergütung von € 100,00 zzgl. 20% USt. je angefangener Arbeitsstunde.

10. Anfragen betroffener Personen

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

11. Löschung der personenbezogenen Daten nach Beendigung des zugrundeliegenden Auftrags

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat Postserver sämtliche in seinen Besitz gelangte 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.

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.

12. Nachweismöglichkeiten

(1) Postserver weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

Postserver Onlinezustelldienst GmbH | Mariahilfer Straße 123/3 | 1060 Vienna | Austria
UniCredit Bank Austria AG | IBAN: AT37 1200 0529 4901 3147 | BIC: BKAUATWW
Registriert beim Handelsgericht Wien unter FN 367446 m | UID-Nummer: ATU 66678268

(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. Postserver 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 Aufragnehmer stehen, hat Postserver gegen dieses ein Einspruchsrecht.

Für die Unterstützung bei der Durchführung einer Inspektion verlangt Postserver eine eine Vergütung von € 100,00 zzgl. 20% USt. je angefangener Arbeitsstunde 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. Die Unterzeichnung einer Verschwiegenheits-verpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß strafbewehrt ist.

13. Subunternehmer

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(2) Ein zustimmungspflichtiges Subunternehmer-verhältnis liegt vor, wenn Postserver weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Postserver wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 1 beschriebenen Dienstleiter ausgeführt.

Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt Postserver die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

(3) Erteilt Postserver Aufträge an Subunternehmer, so obliegt es Postserver, seine datenschutzrechtlichen Pflichten aus diesem Vertrag an den Subunternehmer zu übertragen.

14. Hinweis auf rechtskonformes Verhalten

Der Auftraggeber trägt die Verantwortung für die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung.

15. 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

Postserver den Auftraggeber unverzüglich darüber zu informieren. Postserver wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber zu informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei Auftraggeber als “Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser standardisierten Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer separaten, schriftlichen Vereinbarung 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.

Eine Vereinbarung in elektronischem Format (Textform) wird von den Vertragsparteien ebenso als wirksam anerkannt.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht. Anstelle der unwirksamen Teile finde die entsprechende gesetzliche Regelung Anwendung.

(4) Es gilt österreichisches Recht. Gerichtsstand ist Wien.

16. Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 83 DSGVO getroffenen Regelung.

17. Daten

Die folgenden Arten von personenbezogenen Daten werden im Rahmen dieser Vereinbarung verarbeitet:

Verar-beitungs-Kategorie	Daten-Kategorien	Beschreibung und Datenart
Vertrags-wesen	Kundenkern-stammdaten	Datenobjekte, die erforderlich sind, um das Kundenkonto zu bilden (das aufrechterhalten werden muss, um den Aufbewahrungspflichten zukommen), werden als Kernstammdaten bezeichnet. • Person • Vertretung
	Aufzeich-nungen Zustellung	Allgemeine Aufzeichnung zur Nutzung • Login • E-Mail • Bankident
	Verbindungs-daten Zustellung	Metadaten von empfangenen und gesendeten Zustellungen • Zustellung in • Benachrichtung • Zustellung out
Zustellung	Inhaltsdaten E-Zustellung	End-2-End verschlüsselte Inhaltsdaten, nur durch den Empfänger einsehbar.
Einladung	Kontakt Einladung	Einladung eines Users zu Postserver an seinen persönlichen Kontakt • E-Mail • Name

Löschroutine:

Verar-beitungs-Kategorie	Lösch-klasse	Lösch-routine	Frist
Vertrags-wesen	Verbindungs-daten Zustellung	Aufbewah-rungspflicht nach 11.2.3 Abs. 2 Rule-book WKO	Ab Ende Vorgang 7 Jahre
	Verbindungs-daten Zustellung	Aufbewah-rungspflicht nach 11.2.4 Rule-book WKO	Ab Ende Dienst 3 Monate
	Aufzeich-nungen Zustellung	Aufbewah-rungspflicht nach 11.2.3 Abs. 2 Rulebook WKO	Ab Ende Vorgang 7 Jahre
	Kernstamm-daten Zustellung	Aufbewahr-ungspflicht nach 11.2.3 Abs. 1 Rulebook WKO	Ab Ende Beziehung 5 Jahre
Zustellung	Inhaltsdaten E-Zustellung nicht abgeholt	Aufbewahr-ungspflicht nach 11.2.3 Abs. 3 Rulebook WKO	Ab Ende Vorgang 3 Monate
	Inhaltsdaten E-Zustellung nicht abgeholt	Aufbewahr-ungspflicht nach 11.2.4 Rulebook WKO	Ab Ende Dienst 3 Monate
Einladung	Einladung	Zur Nachverfolg ung, ob eine Einladung angenom-men wurde, werden die Daten 7 Tage gespeichert.	Ab Ende Vorgang 7 Tage

Anlage 1: Datensicherheitskonzept

Anlage 2: Prozessmodell

Anlage 3: Betriebsablauf

Auftraggeber

Ort	Datum
Name	Funktion des Auftraggebers / der Auftraggeberin im Betrieb

Postserver Onlinezustelldienst GmbH

Wien	
Ort	Datum
Carola Zentara	CMO, Datenschutzbeauftragte
Name	Funktion bei Postserver

Absenden

Textform i.S.v. Art. 28 Abs. 9 DSGVO. Bei der Textform handelt es sich um eine unterschriftlose Erklärung, auf einem dauerhaften Datenträger (Download) und gegen nachträgliche Änderungen geschützt (PDF).

Anlage 1

Datensicherheitskonzept

Maßnahmen zur Datenschutzkontrolle gemäß Art. 32 DSGVO

Stand 5. Mai 2018

Bei Fragen zum Datenschutzkonzept oder zu Beauskunftungen wenden Sie sich bitte an:

Postserver Onlinezustelldienst GmbH
Mariahilferstraße 123
1020 Wien, Österreich
E-Mail: datenschutz@postserver.com

Der Auftragnehmer dokumentiert hiermit nachfolgend getroffene technischen und organisatorischen Maßnahmen zur Datensicherheit gemäß Art. 32 DSGVO.

1. Allgemeines

Datensicherheit und Datenschutz sind wichtige Grundsätze der Verarbeitung von Daten bei Wirecard. Als Payment Service Provider (PSP) ist sich Wirecard bewusst, dass sie eine große Menge personenbezogener Daten verarbeitet und diese Daten als eines ihrer wichtigsten Güter besonders schützen muss.

Neben den Vorgaben der österreichischen und unionsrechtlichen Datenschutzvorschriften unterliegt Wirecard den strengen Regelungen des PCI DSS (Payment Card Industry Data Security Standard), im Rahmen dessen jährliche Audits der Datensicherheitsmaßnahmen durchgeführt werden. Wirecard erreichte als erster österreichischer PSP eine Zertifizierung nach PCI DSS und ist seit dem Jahre 2007 durchgehend zertifiziert.

Wirecard versichert hiermit die Einhaltung aller datenschutzrechtlichen Vorgaben im Rahmen der Auftragsdatenverarbeitung, insbesondere der Datensicherheitsmaßnahmen nach § 54 DSG (Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DSG), BGBl. I Nr. 2017/120).

2. Zugang zur IT Lösung

Postserver trifft geeignete Maßnahmen bzw. hat entsprechende Methoden und Einrichtungen im Einsatz um die unbefugte Nutzung von Daten mit Hilfe von Datenübertragungseinrichtungen zu verhindern.

Sämtliche Systeme sind mit Benutzerkontrollsystemen ausgestattet. Der Zugriff auf verschiedene Dienste kann ohne Benutzerkennung nicht erfolgen.

Für den Zugriff auf das Webservice ist ein Login notwendig. Die Vertrauensstufen nach Rulebook WKO definieren die erfolgte Methode der Identitätsprüfung bei der erstmaligen Registrierung sowie Login beim Zustelldienst.

Die Vertrauensstufen des Systems ermöglichen es allen Teilnehmern die Sicherheit der Identitätsfeststellung einzuschätzen. Zu diesem Zweck wird auf bereits vorhandene Abläufe und Regelungen zurückgegriffen und diese in Stufen vertypt.

Alle juristischen Personen benötigen eine „ID“ (Firmenbuch, Vereinsregister, etc.). Falls diese noch

nicht vorhanden ist, muss sich die juristische Person im Ergänzungsregister eintragen (lassen).

(1) Vertrauensstufe I „Niedrig“, E-Mail Authentifizierung

Die Identität des Benutzers wird in Stufe 1 nicht persönlich überprüft und ist daher für die Zustellung von rechtlich verbindlichen Erklärungen (Rechnung, Mahnung, Kündigung etc) nicht geeignet. Die Dienste und der Zustellkopf haften daher nicht für die tatsächliche Identität der handelnden Personen und sich daraus ergebende Rechtswirkungen. Die Dienste kommunizieren dies in geeigneter Weise an die Benutzer.

Die Identifizierung erfolgt per E-Mail, deren Empfang mit einem vorgegebenen Hyperlink zum Dienst durch Anklicken seitens des Benutzers bestätigt wird. Die Identifizierung kann auch mittels Übersendung einer SMS-PIN und darauffolgender Eingabe derselben beim Dienst erfolgen (hier wird die „Identität“ nur hinsichtlich Mailadresse und Handynummer geprüft).

(2) Vertrauensstufe II „Mittel“, Persönliche Authentifizierung bzw. qualifizierte digitale Signatur

Die Identitätsprüfung in dieser Vertrauensstufe wird in sinngemäßer Anwendung des § 40 BWG idF BGBl. I Nr. 145/2011 durchgeführt.
Demnach haben die Dienste die Identität eines Kunden in folgender Weise festzustellen und zu überprüfen:
„Die Identität eines Kunden ist durch persönliche Vorlage seines amtlichen Lichtbildausweises festzustellen. Als amtlicher Lichtbildausweis in diesem Sinn gelten von einer staatlichen Behörde ausgestellte Dokumente, die mit einem nicht austauschbaren erkennbaren Kopfbild der betreffenden Person versehen sind, und den Namen, das Geburtsdatum und die Unterschrift der Person sowie die ausstellende Behörde enthalten;

Die Feststellung der Identität der juristischen Person hat anhand von beweiskräftigen Urkunden zu erfolgen, die gemäß dem am Sitz der juristischen Personen landesüblichen Rechtsstandard verfügbar sind.“ (Auszug aus § 40 BWG)

Die Identitätsprüfung in der Vertrauensstufe II kann bei Inhabern von qualifizierten digitalen Signaturen/Zertifikaten gem. § 2 Abs 3a SigG idF BGBl. I Nr. 75/2010 auch durch Auslesen der Personendaten aus einem qualifizierten Zertifikat einer digitalen Signatur durchgeführt werden. Dabei ist darauf zu achten, dass im Zertifikat kein Pseudonym verwendet wird.

(3) Vertrauensstufe III „Hoch“, Bürgerkarte, „eindeutige Identität“

Die Authentisierungsprüfung in der Vertrauensstufe III setzt das Kriterium der „eindeutigen Identität“ lt. § 2 Z 2 EGovG idf BGBl. I Nr. 111/2010 voraus. Diese „eindeutige Identität“ haben die Dienste nach der Spezifikation bzw dem Stand der Technik zu prüfen und zu dokumentieren. In Österreich hat dies durch die Bürgerkartenfunktion oder gleichgestellte Funktionalitäten zu erfolgen.

(4) Vertretungsvollmacht

Juristische Personen können nur durch vertretungsbefugte natürliche Personen handeln. Soll eine juristische Person Nutzer eines Zustelldienstes sein, muss bei der erstmaligen Registrierung die Identität der natürlichen Person und die Vertretungsbefugnis nachgewiesen werden. Dies kann entweder durch eine auf der Bürgerkarte eingetragene Vertretungsmacht entsprechend § 9 der Stammzahlenregisterverordnung iVm § 5 des E-Government-Gesetzes oder durch die Vorlage eines

amtlichen Lichtbildausweises und die Vertretungsbefugnis z.B. bei im Firmenbuchregister eingetragenen Unternehmen durch Vorlage eines aktuellen Auszugs, bei Vereinen durch Vorlage eines aktuellen Vereinsregisterauszuges geschehen. In Folge wird davon ausgegangen, dass bei Entzug der Vertretungsbefugnis seitens des Vollmachtgebers die juristische Person auch für den Entzug der Identifizierungsmittel für die E-Zustellung sorgt. Die Dienste kommunizieren dies in geeigneter Weise an die Benutzer.

(5) Zertifikate Automatische Abholung

Postserver prüft jedes Zertifikat (auch selbstsignierte für eine frei gewählte End-2-End Verschlüsselung) direkt gegen den Datastore nicht nur via der PKI-Kette.

(6) Zugriff durch fachkundige Datenschutz-Mitarbeiter und 2nd Level Applikationsadministrator

Auf das Verzeichnis E-Zustellung, Postservices und behördliche Dokumente zur 2nd Line Bearbeitung von Supportfällen betreffend E-Zustellungen wird ausschließlich über einen gesicherten Tunnel zugegriffen. Der SSH-Tunnel ist ein gesicherter Kanal, der Netzwerk-Protokolle einbetten und verschlüsselt übertragen kann. eines fremden, potenziell unsicheren Netzwerks zu einem Server bzw. Netz des Vertrauens. Durch diese Form der Portweiterleitung können TCP-Protokolle durch ein fremdes Netz hindurch vertraulich genutzt bzw. überhaupt erst zugänglich gemacht werden. Der Tunnel wird durch den Infrastrukturadministrator Tele2 dezidiert auf eine IP eingestellt.

Benutzeraccounts von ausgeschiedenen Mitarbeitern werden nach dem letzten Arbeitstag (Ende des Dienstverhältnisses) deaktiviert.

Das Benutzermanagement ist durch zentrale Sicherheitssoftware gegen Schadsoftware, Störungen und unberechtigte Zugriffe abgesichert.

3. Verschlüsselung

(1) Übertragungskontrolle

Postserver verpflichten sich nach Rulebook WKO, die Sicherheit des Systems durch Verschlüsselung aller Kommunikationsschritte zwischen den Diensten untereinander und zwischen den Diensten und dem Zustellkopf zu gewährleisten.

Es kann jederzeit überprüft und festgestellt werden, welche Daten zur welcher Zeit durch wen an Einrichtungen zur Datenübertragung übermittelt wurden. Ebenso ist abschließend dokumentiert, an welchen Stellen Input- oder Outputdaten übermittelt werden (bzw. nicht übermittelt werden) und über welche Netzwerke (intern/extern) diese Übermittelung erfolgt.

Jede Datenübermittlung wird durch interne Systeme protokolliert und die Übermittlung selbst mit starker Verschlüsselung und sicherheitsgeprüften Protokollen durchgeführt, die dem Stand der Technik bzw. aktuellen Branchenstandards entsprechen. Eine Datenübermittlung darf zudem nur durchgeführt werden, wenn die Authentizität der Übermittlungsberechtigten geprüft wurde (z.B. durch Zertifikate oder Benutzerkennung).

(2) Tunnel Verzeichnis E-Zustellung, Postservices und behördliche Dokumente

Auf das Verzeichnis E-Zustellung, Postservices und behördliche Dokumente zur 2nd Line Bearbeitung von Supportfällen wird ausschließlich über einen gesicherten Tunnel zugegriffen.

Der SSH-Tunnel ist ein gesicherter Kanal, der Netzwerk-Protokolle einbetten und verschlüsselt

Postserver Onlinezustelldienst GmbH | Mariahilfer Straße 123/3 | 1060 Vienna | Austria
UniCredit Bank Austria AG | IBAN: AT37 1200 0529 4901 3147 | BIC: BKAUATWW
Registriert beim Handelsgericht Wien unter FN 367446 m | UID-Nummer: ATU 66678268

übertragen kann. Durch diese Form der Portweiterleitung können TCP-Protokolle durch ein fremdes Netz hindurch vertraulich genutzt bzw. überhaupt erst zugänglich gemacht werden.

(3) Identifizierungsmittel Nutzerinnen und Nutzer

Die Sicherheitsmaßnahmen der erstmaligen Übermittlung von Identifizierungsmittel sind nach Rulebook WKO von der jeweiligen Vertrauensstufe abhängig.

In der Vertrauensstufe I erhält der Benutzer seine Zugangsdaten auf die Art, wie er sich gegenüber seinem Dienst authentifiziert hat (E-Mail oder SMS).

In der Vertrauensstufe II muss die Übermittlung der Zugangsdaten nachweisbar erfolgen. Authentisiert sich der Benutzer erstmalig mit seiner qualifizierten digitalen Signatur, hat die Übergabe etwaiger weiterer Zugangsdaten mittels des Zustellsystems gesichert zu erfolgen.

In der Vertrauensstufe III authentisiert sich der Benutzer erstmalig mit seiner eindeutigen Identität. Die Übergabe etwaiger weiterer Zugangsdaten hat mittels des Zustellsystems gesichert zu erfolgen.

4. Kategorien der IT-Attacken und technischer Ausfall

Es wurde eine Risikoanalyse mit dem Fokus auf die folgenden drei Datentypen durchgeführt:

- sensible Daten (inkl. besonders schutzwürdige Daten)
- personenbezogene Daten (inkl. indirekt personenbezogene Daten)
- nicht personenbezogene Daten

Im Zuge der Analyse wurde festgestellt, wo diese Daten verarbeitet bzw. über welche Schnittstellen auf diese zugriffen werden kann. Basierend darauf wurde anschließend die Eintrittswahrscheinlichkeit verschiedener Bedrohungen ermittelt. Aus dem Schutzbedarf der Informationen und der Eintrittswahrscheinlichkeit der einzelnen Bedrohungen wurde anschließend das Risiko berechnet.

Die wesentlichen Risiken gehen von potentiellem Schadcode in der Software, unbefugtem Zugriff auf Daten-Backups und potentiellen Social Engineering Angriffen aus.

Verkehrssicherungs-Kategorien (Supporting Assets)	Vertraulichkeit			Integrität			Verfügbarkeit		
	EWSK [1]	BIA [2]	Risiko	EWSK	BIA	Risiko	EWSK	BIA	Risiko
Räumlichkeiten									
Rechenzentrum Tele2	1	8	8	1	4	4	2	2	4
Büro CPB	2	8	16	1	4	4	1	2	4
Serverraum kbprintcom	2	8	16	1	4	4	1	2	2
Produktion kbprintcom	4	8	32	1	4	4	1	2	2
Büro Postserver	2	8	16	1	4	4	2	2	4
Büro Datenschutzbeauftragte Postserver	2	8	16	2	4	8	2	2	4
Homeoffice Postserver	4	8	32	2	4	8	2	2	4
Hardware									
Firewall Tele 2	4	8	32	2	4	8	2	2	4
Server Tele 2	2	8	32	2	4	8	2	2	4
Bandlaufwerke Tele2	4	8	32	4	4	16	2	2	4
Laptop CPB	4	8	32	2	4	8	1	2	2
Server kbprintcom	4	8	32	2	4	8	2	2	4
Desktop Geräte kbprintcom	2	8	16	2	4	8	2	2	4
Drucker kbprintcom	2	8	16	2	4	8	2	2	4
Backups kbprintcom	4	8	32	2	4	8	2	2	4
Firewall kbprintcom	2	8	16	2	4	8	2	2	4
Desktop Geräte Postserver	2	8	16	2	4	8	2	2	4
Laptop Postserver	4	8	32	2	4	8	1	2	2
Software Anwendungen									

[1] EWSK steht für Eintrittswahrscheinlichkeit

[2] BIA für Business Impact Analyse / Schutzbedarf

Eintrittswahrscheinlichkeit 1 = gering; einmal in 5 Jahren oder seltener
Eintrittswahrscheinlichkeit 2 = mittel; einmal in 2 Jahren bis einmal in 5 Jahren
Eintrittswahrscheinlichkeit 4 = hoch; einmal im Jahr bis einmal in 2 Jahren
Eintrittswahrscheinlichkeit 8 = hoch; mehrmals im Jahr

Schutzbedarf 1 = geringfügige Konsequenzen; Verstöße gegen Verträge und Gesetze mit geringfügigen Konsequenzen, geringfügige Vertragsverletzungen mit geringer Konventionalstrafe
Schutzbedarf 2 = nennenswerte Konsequenzen; Verstöße gegen Verträge und Gesetze mit nennenswerten Konsequenzen, Vertragsverletzungen mit Konventionalstrafen
Schutzbedarf 4 = beträchtliche Konsequenzen; Verstöße gegen Verträge und Gesetze mit beträchtlichen Konsequenzen Vertragsverletzungen mit sehr hohen Konventionalstrafen
Schutzbedarf 8 = existenzbedrohende Konsequenzen, Existenzbedrohender Verstoß gegen Verträge und Gesetze, Vertragsverletzungen, deren Haftungsschäden ruinös sind

Postserver Onlinezustelldienst GmbH | Mariahilfer Straße 123/3 | 1060 Vienna | Austria
UniCredit Bank Austria AG | IBAN: AT37 1200 0529 4901 3147 | BIC: BKAUATWW
Registriert beim Handelsgericht Wien unter FN 367446 m | UID-Nummer: ATU 66678268

Linux Betriebssystem Tele2	4	8	32	4	4	16	2	2	4
Webserver Tomcat Tele2	4	8	32	2	4	8	2	2	4
MYSQL DB Tele2	4	8	32	2	4	8	2	2	4
SFTP Tele2	2	1	2	2	2	4	2	2	4
Virtualisierung Tele2	2	8	16	2	4	8	2	2	4
Internet Anschluss Tele2	1	8	8	1	4	4	2	2	4
Internes Netzwerk Tele2	4	8	32	2	4	8	2	2	4
Versandmodul CPB	8	8	64	8	4	32	4	2	8
Monitoring Administration Modul CPB	8	8	64	8	4	32	4	2	8
Windows OS Laptop CPB	4	8	32	2	4	8	2	2	4
Windows OS kbprintcom	2	8	16	2	4	8	2	2	4
Windows OS Desktop kbprintcom	2	8	16	2	4	8	2	2	4
MAC OS Desktop kbprintcom	2	8	16	2	4	8	2	2	4
SFTP kbprintcom	2	8	16	2	4	8	4	2	8
Virtualisierung kbprintcom	2	8	16	2	4	8	2	2	4
Internet Anschluss kbprintcom	2	8	16	1	4	4	1	2	2
Internes Netzwerk kbprintcom	4	8	32	2	4	8	2	2	4
Windows OS Desktop Postserver	2	8	16	2	4	8	2	2	4
Windows OS Laptop Postserver	4	8	32	2	4	8	2	2	4
Internet Anschluss Postserver	2	8	16	1	4	4	1	2	2
Internet Anschluss Datenschutzbeauftragte Postserver	2	8	16	1	4	4	1	2	2
Internet Anschluss Homeoffice Postserver	2	8	16	1	4	4	1	2	2
Internet Anschluss Smartphone Postserver	2	8	16	1	4	4	1	2	2
Personen									
Infrastrukturadministrator Tele2	4	8	32	2	4	8	4	2	8
Applikationsadministrator CPB	4	8	32	2	4	8	2	2	4
Administratoren kbprintcom	2	8	16	2	4	8	2	2	4
Mitarbeiter kbprintcom	2	8	16	2	4	8	2	2	4
Fachkundiger Datenschutz-Mitarbeiter Postserver	4	1	4	2	2	4	2	2	4
Fachkundiger Datenschutzbeauftragte Postserver	4	1	4	2	2	4	2	2	4

Postserver Onlinezustelldienst GmbH | Mariahilfer Straße 123/3 | 1060 Vienna | Austria
UniCredit Bank Austria AG | IBAN: AT37 1200 0529 4901 3147 | BIC: BKAUATWW
Registriert beim Handelsgericht Wien unter FN 367446 m | UID-Nummer: ATU 66678268

5. Verzeichnis IT-Attacken und technischer Ausfall

(1) Verzeichnis Verkehrssicherung Webseite

Im Postserver Backend ist das Verzeichnis der IT-Attacken und technischen Ausfälle aufrufbar. Dieses Verzeichnis wird zu Dokumentationszwecken geführt. Ab Ende Vorgang

Zur Einsichtnahme wird eine Verzeichnis-Übersicht geführt. Diese enthält Datum, Datenvorfall, Risikoprognose**,** Maßnahmen zur Beseitigung, eine Liste der Zugriffsberechtigungen auf Verarbeitungstätigkeit und Meldepflichten.

Um eine Auskunft für Strafverfolgungsbehörden, Datenschutzbehörde nach NIS-Richtlinie und Betroffene zu ermöglichen, kann jeder Datensatz gedruckt bzw. als PDF exportiert werden. Der Datensatz-Auszug aus dem Verzeichnis Verkehrssicherung Webseite enthält folgende Informationen:

- Verkehrssicherungs-Kategorie des Datenvorfalls
- eine Beschreibung des Vorfalls
- Risikoprognose
- eventuell Uptime
- Anzahl der betroffenen Personen und der betroffenen User-Kategorien
- ungefähren Anzahl der betroffenen personenbezogenen Datensätze
- Name und Kontaktdaten des Verantwortlichen, der Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- User-Kategorien der Zugriffsberechtigungen auf Verarbeitungstätigkeit
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten
  inkl. durchgeführte Hotfixe von Tele2 mit Datum und grober Hotfixbeschreibung
- gegebenenfalls Empfehlungen zur Abmilderung der möglichen nachteiligen Auswirkungen gegenüber der betroffenen Person
- Begründung, falls die Meldung länger als 72 Stunden nachdem der Vorfall dem Verantwortlichen bekannt wurde, erfolgte

Der Zugang zum Verzeichnis Verkehrssicherung Webseite ist mittels Login und Beschränkung auf die Bearbeitungsrollen „Datenschutzbeauftragte“ (in Personalunion mit Webadministratorin Postserver) und „fachkundiger Datenschutz-Mitarbeiter“ beschränkt.

(2) Verzeichnis Verkehrssicherung auf Systemebene

Durch die datenverarbeitungsbeauftragte Tele2 wird auf Systemebene ein Verzeichnis geführt. Dieses Verzeichnis dokumentiert in Echtzeit technische Vorfälle und IT-Attacken.

Im Falle eines Vorfalls erfolgt eine Meldung durch den Infrastrukturadministrator Tele2 an die Webadministratorin Postserver. Entsprechend der internen und externen Kompetenzen werden entsprechende Maßnahmen veranlasst.

Prinzipiell werden folgende Berichte durch den Infrastrukturadministrator Tele 2 an die Webadministratorin Postserver übermittelt:

- Eventuell durchgeführte Hotfixe mit Datum und grober Hotfixbeschreibung
- Uptime

Eine Dokumentation des Vorfalls erfolgt durch die Webadministratorin Postserver im Verzeichnis Backend.

Um eine Auskunft für Strafverfolgungsbehörden, Datenschutzbehörde nach NIS-Richtlinie und Betroffene zu ermöglichen, kann jeder Datensatz exportiert werden.

Der Zugang zum Verzeichnis Verkehrssicherung auf Systemebene ist auf den Infrastrukturadministrator Tele2 beschränkt.

(3) Löschroutine Verzeichnis Verkehrssicherung Webseite

Risiko-wert	Lösch-klasse	Lösch-routine	Frist
1, 2, 4, 8, 16, 32	Verkehrs-sicherung	Datensatz wird im Verzeichnis gelöscht sobald der Datenvorfall positiv bearbeitet wurde: Rückmeldung via E-Mail durch Tele2.	Ab Ende Vorgang 1 Jahr
1, 2, 4, 8, 16, 32	Verkehrs-sicherung Geschäfts-fall	Falls eine Meldung an die Datenschutz-behörde erfolgte, ist der Datensatz selbst aufgrund der Aufbewahrungspflicht nach §§ 190, 212 UGB 7 Jahre gesondert zu archivieren.	Ab Ende Vorgang 7 Jahre

6. Präventive Maßnahmen

Prinzipiell ist festzuhalten, dass die Daten in zwei mehr als vier Kilometer voneinander entfernten Rechenzentren vorgehalten und in Echtzeit gespiegelt werden. Selbstverständlich verfügt jeder einzelne Standort über eine entsprechende unterbrechungsfreie, redundante Stromversorgung (getrennte Steigleitungen und E-Verteiler etc.) inkl. UVS, redundante Klimaschränke und Kältemaschinen, Brandmelder, Brandfrühesterkennung, automatische Löschanlagen, Brandschutz- und Notfallkonzept, Alarmanlage und Videoüberwachung, Alarmpläne und Wiederanlaufpläne. Der Zutritt zu den Rechenzentren ist sowohl organisatorisch (personell überwachte Eingangsanlagen) als auch technisch (Vereinzelungsanlagen, Zutritt nur mit Chipkarten mit personalisiertem PIN) geregelt.

Als Hardwareplattform für Tele2 Dedicated Server Systeme kommen ausschließlich Geräte der HP DL Serverreihe zum Einsatz. Diese zeichnen sich durch hohe Ausfallsicherheit und Stabilität aus. Durch das ständige Vorhandensein von cold-standby-Hardware gewährleistet Tele2 den kurzfristigen Austausch defekter Komponenten.

Die Server sind mit 100 MBit/s Full Duplex an das Internet angebunden. Grundsätzlich bekommt jedes Tele2 Dedicated Server Produkt eine statische IP-Adresse zugewiesen. Durch die redundante GBit-Anbindung an den High-Speed Backbone von Tele2 ist eine hohe Verfügbarkeit der Internetanbindung garantiert.

Tele2 sorgt für Korrekturen und Erweiterungen des Betriebssystems und der Dienstprogramme, die einer Leistungssteigerung und/oder der Erweiterung der Betriebssicherheit dienen.

Tele2 übernimmt die Verantwortung für den ordnungsgemäßen Betrieb der Software-Applikationen. Dazu zählt insbesondere die Installation aktueller Sicherheits-Updates.

Die Webadministratorin Postserver erhält keinen Root-Zugriff. Die Webadministratorin Postserver erhält Zugriff über FTP/sFTP/ssh.

Das 24x7 Monitoring der Dienste inkludiert:

Hardware:

- Host up/down Ping-Check
- Status von Soft- oder Hardware-RAID

Performance:

- CPU-Auslastung

- Speicher/Swap Auslastung
- Systemlast
- Uptime
- Disk io, space und mount-options
- Netzwerk interfaces

Security:

- OS Version
- Security updates

Externe aktive Checks:

- SSH, FTP
- HTTP, HTTPS
- MySQL, postgres
- SMTP(S), IMAP(S), POP(S)

Proaktives Störungsmanagement:

Aufgrund von Monitoring Alarmen wird, sofern möglich, durch das Infrastrukturadministrator Tele2 Team eine aktive Störungsbeseitigung durchgeführt. Tele2 behält sich das Recht vor, bei häufig auftretenden Alarmen, nach vorheriger Kundeninfo, einzelne Checks so lange zu deaktivieren, bis eine dauerhafte Lösung gefunden wird (z.B. Diskspace Alarm - da Kundendaten nicht vom Tele2 Administrator gelöscht werden dürfen).

Die Wartung und Betreuung folgender Software-Applikationen ist inkludiert:

- Linux-Betriebssystem: Debian, CentOS
- Datenbank: MySQL, Postgres
- WebServer: Apache, nginx

Das Daten Backup bietet professionelle Datensicherung für alle Tele2 Dedicated Server Produkte. Im Falle eines Datenverlustes können einzelne Dateien oder auch der ganze Server (abhängig von der Backupstrategie) wiederhergestellt werden.

Dabei kommt "Bacula" als Backuplösung zum Einsatz. Aus Sicherheits- und Performancegründen wird das Backup, wenn möglich, über eine eigene Netzwerkkarte und ein eigenes Backup-LAN geführt. Um eine vollständige Datensicherung zu gewährleisten, werden täglich alle Veränderungen (inkrementell) und wöchentlich alle zum Backup vorgesehenen Daten auf Bandlaufwerken gesichert (Full Backup). Die Backup-Bänder werden sicher archiviert (Off-Site). Bei Bedarf sind zudem auch individuelle Backup-Strategien gegen Aufpreis möglich. Auf Kundenwunsch werden einzelne Files innerhalb von 24 Stunden wiederhergestellt, oder ein Full-Restore (Dauer abhängig von der Datenmenge) durchgeführt. Spezifikationen:

- Täglich inkrementelles Backup
- Wöchentliches Full-Backup
- Off-Site Archivierung
- Restore einzelner Files innerhalb von 24 Stunden
- Restore einzelner Files in verschiedenen Versionen
- Getrenntes Accounting des Backuptraffics
- Monitoring des Backups 24/7
- Optional individuelle Backup-Strategien
- Optional längere Speicherzeiten

Die Hochverfügbarkeit, Katastrophensicherheit und Datensicherheit wird über den Einsatz der DRBD (Distributed Replicated Block Device) Technologie gewährleistet. Diese spiegelt einen produktiven physischen Server (Primary) in Echtzeit auf einen anderen Server (Secondary), welcher auf einem anderen Standort (Offsite) betrieben wird. Somit kann, gemäß dem unwahrscheinlichen Fall, dass ein Standort nicht mehr erreichbar ist o. ä., ohne Datenverlust auf den Standort (des „gespiegelten" Servers) geswitched werden. Dies garantiert die Erreichbarkeit und Hochverfügbarkeit der Applikation.

7. Verfügbarkeit

(1) Software

Für Testzwecke bzw. um neue Funktionalitäten bzw. Softwareversionen testen zu können bzw. diese vom Auftraggeber abnehmen zu lassen, wird eine zweite Instanz der angebotenen Lösung auf einer eigenen virtuellen Maschine zur Verfügung gestellt. Diese kann auf weniger Systemressourcen zugreifen, um das Produktivsystem nicht zu beeinträchtigen. Der für die Druckstraße generierte Output wird nur im Dateisystem abgelegt und nicht direkt an diese übertragen. Somit können von der Anlieferung über die Verarbeitung und Anreicherung der Daten bis zur Auslieferung bzw. Anlieferung an die Druckstraße alle Verarbeitungsschritte getestet werden.

(2) Hardware

Der ISP garantiert eine einwandfreie Funktionalität der eingesetzten Hardware, die dem Auftraggeber auf Basis eines gültigen Mietvertrages zur Verfügung gestellt wird. Sollte es zu Hardwaredefekten kommen, erfolgt ein Hardwaretausch innerhalb von 4 Stunden. Die Ausfallzeit beginnt ab dem Zeitpunkt der ordentlichen Meldung durch den Auftraggeber in Form einer telefonischen Störungsmeldung und der Eröffnung eines Tickets durch den Support - Mitarbeiter. Die Störungsmeldung wird damit im Ticketsystem dokumentiert. Nach Störungsbeseitigung wird der Auftraggeber durch das Support - Team informiert. Zeitgleich wird das Ticket geschlossen. Der Zeitpunkt dieser Aktion definiert die Wiederherstellung der Hardwareverfügbarkeit.

(3) Backbone

Garantierte Verfügbarkeit	99,80%
max. nicht verfügbare Zeit	17,52 h/Jahr
Core Latency	20ms
Core Packet Loss	< 3 %
Monitoring	24x7
Störungsannahme	24x7
Verfügbarkeit Servicetechniker	24x7
Reaktionszeiten (8-20 Uhr, werktags)	max. 30 min
Reaktionszeiten (20-8 Uhr, werktags; Sam-, Sonn- und Feiertagen)	max. 4 Stunden

8. Qualitätskontrolle Druck

(1) Bei kbprintcom ist seit Jahren gelebter Standard, dass die Druckqualität online – d.h. in Echtzeit – auf Vorder- und Rückseite mittels hochauflösender Bahnbetrachtungsgeräte (Kamerasystem) überprüft wird.

Eine Closed-Loop-Verarbeitung der gegenständlichen Aufträge ist selbstverständlich.

Bereits bei der Datenübertragung wird die Vollständigkeit der Datenübermittlung überprüft. Die Daten werden für den Druck aufbereitet und die fertig aufbereitete Menge wird auf Seiten-/Blatt-Sendungsebene mit den vom Auftraggeber übermittelten Daten abgeglichen. Im Zuge der Datenaufbereitung erhält jedes Dokument eine eindeutige einmalige Kennung. Diese Kennung enthält u.a. Auftraggeber, Jobnummer,

Dokumentennummer, Blattanzahl, fortlaufende Nummer, etc.

Diese Kennung wird in einer Datenbank gespeichert und als Datamatrix auf den Dokumenten aufgedruckt. Bei dem in der Prozesskette letzten Schritt - dem Kuvertieren - wird die Datamatrix gelesen (Eingangslesung) um

- die Zusammengehörigkeit der Blätter sicherzustellen und
- durch die Stationsverfolgung innerhalb der Kuvertiermaschine die einwandfreie Kuvertierung des Dokuments - bzw. aller Dokumente und derer Teile (Beilagen wie Rückantwortkuverts, SEPA-Zahlungsanweisung, ...) sicherzustellen.

Nach Erhalt der Daten entsteht ein ausführliches Datenprotokoll - der erste Zeitstempel in der Datenbank wird vergeben, wenn das Dokument auch IT-mäßig (d.h. nach Aufbereitung der vom Auftraggeber zur Verfügung gestellten Daten) vorhanden ist. Beim Personalisieren der Daten wird der jeweilige Datamatrix-Code auf die einzelnen Blätter der Dokumente aufgebracht. Dieser wird im Rahmen der Kuvertierung gelesen. Zeitpunkt und Ort (in der Kuvertiermaschine bei Fehlern) wird in der Datenbank festgeschrieben. Gleichzeitig zum Zeitstempel wird auch der Status des einzelnen Dokumentes vermerkt. Nach Abschluss der Kuvertierung wird das Dokument in der Datenbank mit Zeitstempel versehen. Datenbankeinträge ohne „OK“ und Zeitstempel werden nach Beendigung der Kuvertierung automatisch als Nachproduktion dargestellt.

Eine Produktion gilt erst als abgeschlossen, wenn alle Dokumente dieses Jobs in der Datenbank mit Zeitstempel als OK gemeldet sind.

Um die Vollständigkeit und Richtigkeit (Reihenfolge der Blätter im Kuvert, Lesbarkeit der Folgeblätter, ...) einzelner Sendungen sicherzustellen, gehen wir wie folgt vor:

- Lesung am Eingang der Kuvertiermaschine (vor dem Schneider)
- Übergabe der ausgelesenen Codes an die jeweils nächste Maschinenkomponente in elektronischer Form (bis zur Sammelstation)
- In der Sammelstation wird das in der Zeitabfolge richtige Einlaufen der Dokumente (Reihenfolge bleibt gewahrt und wird elektronisch überwacht) geprüft.
- Bei der Weitergabe des Dokumentes - nun schon als komplettes Package - in den Kuvertierkopf wird die Datamatrix der ersten Seite des jeweiligen Packages (Brief) vollautomatisch, elektronisch geprüft.

Somit ist nicht nur sichergestellt, dass das erste Blatt im Dokument ist, sondern auch die jeweils folgenden Blätter eines Dokumentes in der richtigen Anzahl und richtigen Reihenfolge im Dokument enthalten sind, wenn das Kuvert verschlossen maschinell wird.

(2) Als wöchentlicher Jour fixe werden unter Beteiligung aller Abteilungsleiter der betreffenden Schnittstellen regelmäßig die Kundenprojekte besprochen, organisiert und mögliche Herausforderungen der einzelnen Projekte proaktiv erarbeitet.

(3) Nach Beendigung der Einlaufphase eines neuen Kundenprojektes ein dokumentiertes „Lessons Learned"-Meeting abgehalten.

(4) Intern hat kbprintcom den KVP-Prozess (Kontinuierlicher Verbesserungsprozess) initiiert, dadurch haben ALLE Mitarbeiterinnen und Mitarbeiter die Möglichkeit,

Postserver Onlinezustelldienst GmbH | Mariahilfer Straße 123/3 | 1060 Vienna | Austria
UniCredit Bank Austria AG | IBAN: AT37 1200 0529 4901 3147 | BIC: BKAUATWW
Registriert beim Handelsgericht Wien unter FN 367446 m | UID-Nummer: ATU 66678268

Verbesserungsvorschläge einzubringen.

9. Technische Maßnahmen im Falle einer IT-Attacke

(1) Server

Aufgrund von Monitoring Alarmen wird, sofern möglich, durch das Infrastrukturadministrator Tele2 Team eine aktive Störungsbeseitigung durchgeführt.

Die sichere Entsorgung bzw. Zerstörung von Datenträgern werden durch interne Vorschriften bei Tele2 geregelt. Damit kann das Risiko eines Datendiebstahls reduziert werden.

Bedrohung	Risiko-wert	Maßnahme
Diebstahl von Daten oder Dokumenten	32	• Dedicated Server Systeme • Sicherer Entsorgungsprozess
Wiederherstellung gelöschter Daten	32	• Backup Strategie • Sicherer Entsorgungsprozess

(2) Firewall

Die Tele2 Firewall beinhaltet das sogenannte Unified Threat Management (UTM), das alle erdenklichen Gefahrenquellen für Computer sichert. UTM beinhaltet Stateful Inspection, Antivirus, Antispam, Content Filtering und Grayware Handling. Mögliche Angriffe, welche sich auf IP/ICMP (Netzwerk-Layer) oder TCP/UDP (Transport-Layer) beziehen, werden innerhalb der Firewall erkannt und abgewehrt.

Updates werden, wenn dies aus Sicherheitsgründen oder zum Bereitstellen neuer Funktionen nötig ist, zeitnah eingespielt, sobald der Hersteller der eingesetzten Komponenten solche zur Verfügung stellt. Tele2 verwendet die vom Hersteller offiziell zur Verfügung gestellten Signaturen und stellt die Firewall auf ein automatisches Update ein. Darüber hinaus existieren eine ausgefeilte Backupstrategie und ein Notfallkonzept, um den sicheren Betrieb der Infrastruktur zu gewährleisten. Als zusätzliche Maßnahme zur Reduktion von Anwendungsfehlern erfolgen Änderungen nach einem definierten Schema und mit entsprechender Protokollierung.

Bedrohung	Risiko-wert	Maßnahme
Eindringen in das interne System Fehler bei der Verwendung	32	• United Threat Management • Automatische Updates der Firewall Software und Signaturen • Sicherung der aktuellen Firewall Konfiguration • Protokollierung
Malicious Code	32	
Spyware	32	

(3) Bandlaufwerke

Um die Verfügbarkeit der verarbeiteten Daten zu sichern, wird von Seiten der Tele2 ein regelmäßiges Backup durchgeführt und in einem zweiten Rechenzentrum verwahrt. Aus Sicherheits- und Performancegründen wird das Backup über eine eigene Netzwerkkarte und ein eigenes Backup-LAN geführt. Um eine vollständige Datensicherung zu gewährleisten, werden täglich alle Veränderungen (inkrementell) und wöchentlich alle zum Backup vorgesehenen Daten auf Bandlaufwerken gesichert (Full Backup). Die Backup-Bänder werden sicher archiviert (Off-Site) und aufbewahrt. Sie dürfen nur von autorisierten Personen verwendet werden. Jeder Zugriff wird protokolliert.

Bedrohung	Risiko-wert	Maßnahme
Diebstahl von Daten oder Dokumenten	32	• Off-Site Archivierung • Täglich inkrementelles Backup
Wiederherstellung gelöschter Daten	32	

Postserver Onlinezustelldienst GmbH | Mariahilfer Straße 123/3 | 1060 Vienna | Austria
UniCredit Bank Austria AG | IBAN: AT37 1200 0529 4901 3147 | BIC: BKAUATWW
Registriert beim Handelsgericht Wien unter FN 367446 m | UID-Nummer: ATU 66678268

		• Wöchentliche Full Backups • Getrenntes Accounting des Backuptraffics • Monitoring des Backups 24/7 • Sicherer Entsorgungs-prozess

(4) Backups

Backups werden regelmäßig erstellt und verschlüsselt gespeichert. Gelagert werden diese durch den IT-Leiter der Firma kbprintcom. Dadurch können Daten, welche auf den Server der kbprintcom liegen oder bereits gelöscht wurden, durch einen Administrator wiederhergestellt werden.

Bedrohung	Risiko-wert	Maßnahme
Diebstahl von Daten oder Dokumenten	32	• Verwahrung von Backups in sicherer Umgebung • Verschlüsselung der Backups • Vier-Augen-Prinzip für Backup Wiederherstellung
Diebstahl von Ausrüstung (Einbruch)	32	
Wiederherstellung gelöschter Daten	32	

(5) Laptops

Sollte eines der mobilen Geräte der Organisation gestohlen werden, so muss ausgeschlossen werden, dass ein Angreifer Zugriff auf sensible Daten erlangt. Daher muss mit organisatorischen und technischen Maßnahmen sichergestellt werden, dass ein Angreifer im Falle eines Diebstahls keinen Zugriff auf die Webservice Datenbanken erhält.

Bedrohung	Risiko-wert	Maßnahme
Diebstahl von Daten oder Dokumenten	32	• Sicherer Umgang mit Sourcecode
Wiederherstellung gelöschter Daten	32	• Leitfaden zur Verwendung von Daten • Sicherer Entsorgungsprozess • Zugang nur über Tunnel

(6) Versandmodul, Webservice, Remote Versand, Automatische Abholung

Da das Versandmodul eine zentrale Komponente im Versandprozess von Postserver darstellt, hängt die Sicherheit der verarbeiteten Daten auch sehr stark vom Sicherheitsniveau der Applikation selbst ab.

Das Sicherheitsniveau der Applikation wurde umfangreichen Tests unterzogen. Diese werden auch vor der Abnahme größerer Updates durchgeführt. Das Versandmodul und die Datenbank kommunizieren verschlüsselt.

Unmittelbar auf das Versandmodul aufbauend ist das Webservice für den Einzelversand und stellt im Wesentlichen ein grafisches Interface (GUI) dar.

Für die Integration können der Remote Versand und die Automatische Abholung genutzt werden (sh. Prozessmodell Anlage 2). Die jeweiligen Schnittstellen wurden nach Zustellgesetzt durch das EGIZ zertifiziert.

Auf das Sourcecode Repository darf nur von befugten Personen zugegriffen werden. Jeder Zugriff wird protokolliert.

Bedrohung	Risiko-wert	Maßnahme
Spionage, Ausspähen von Daten (Remote)	32	• Sicherer Umgang mit Sourcecode • Absichern der Kommunikation • Sicherheitsüberprüfung • Secure Coding Guideline
Malicious Code	64	
Sabotage (Hardware Software Infos)	64	
Verfälschung der	32	

Hardware / Software		

(7) Linux Betriebssytem, Webserver Tomcat, MySQL Datenbank

Die Verwendung von Antiviren Software ist selbstverständlich, zusätzlich verwendet Tele2 interne Mechanismen zum Erkennen von schadhaftem Code innerhalb der Systeme.

Bedrohung	**Risiko-wert**	**Maßnahme**
Wiederherstellung von gelöschten Daten	32	• Off-Site Archivierung • Täglich inkrementelles Backup • Wöchentliche Full Backups • Getrenntes Accounting des Backuptraffics • Monitoring des Backups 24/7
Malicious Code	32	• Schutz vor Schadsoftware

(8) Internes Netzwerk kbprintcom

Die Firma kbprintcom verwendet bereits verschiedene VLANs zur Segmentierung und Abschottung des internen Netzwerks. Im Netzwerk erfolgt die Kommunikation jedoch unverschlüsselt. Es wird evaluiert werden, wie weit sich die interne Datenübertragung vom SFTP-Server bis zur Druckerstraße verschlüsseln lässt.

Bedrohung	**Risiko-wert**	**Maßnahme**
Spionage, Ausspähen, Diebstahl von Daten (Remote)	32	• Absichern der Kommunikation

(9) Personen

Prinzipiell ist festzuhalten, dass alle Mitarbeiter der beteiligten Unternehmen vertraglich zur Geheimhaltung der Daten verpflichtet sind. Periodische Awareness Schulungen, regelmäßige Informationen über neu auftretende Gefahren und Bedrohungen sind selbstverständlich. Ein regelmäßiger Jour Fixe der Datenschutzbeauftragten ist eingerichtet. Awareness Schulungen und unternehmensinterne Kampagnen ergänzen diese Maßnahmen.

Bedrohung	**Risiko-wert**	**Maßnahme**
Social Engineering	32	• Schulungen • Awareness Kampagnen
Diebstahl von Daten oder Dokumenten	32	

(10) Entsorgung gedruckter Daten

Der Zutritt zum Produktionsbereich der Firma kbprintcom ist bereits durch zahlreiche Sicherheitsmaßnahmen wie Chipkartenschlösser, Zutrittslog oder Besucherregelungen gesichert. Auch während des Drucks erfolgt eine Überprüfung von gedruckten und an die Post übergebenen Stückzahlen. Müssen Ausdrucke entsorgt werden, so stehen spezielle Container zur Entsorgung zur Verfügung. Die Entsorgung dieser Container erfolgt nach dokumentierten Verfahren und wird vom jeweiligen Dienstleister bestätigt.

(11) Druckstraße

Der Einsatz von Leiharbeitern / Zeitarbeitern ist ausschließlich nach vorgängiger Absprache mit dem Auftraggeber erlaubt. Die Leiharbeiter müssen namentlich dem Auftraggeber gemeldet werden. In begründeten Fällen hat der Auftraggeber das Recht, den Einsatz von Leiharbeitern auszuschließen.

Leiharbeiter / Zeitarbeiter müssen die entsprechenden Geheimhaltungs- und Verschwiegenheitsvereinbarungen der kbprintcom nachweislich vor Antritt der Tätigkeit und Prüfung des Auftraggebers unterschrieben haben.

Leiharbeiter / Zeitarbeiter werden vor Antritt der Tätigkeit in die Sicherheitsmaßnahmen der kbprintcom unterwiesen.

Personalmutationen von Schlüsselpersonal (insbesondere Geschäftsführung, Betriebsleiter, IT-Leiter sowie Datenschutzbeauftragter), müssen vorgängig dem Auftraggeber angezeigt werden. Der Auftraggeber verpflichtet sich diesbezüglich zu Verschwiegenheit.

Sicherheitsvorfälle, die den Auftraggeber betreffen, werden dem CISO des Auftraggebers unverzüglich bei Bekanntwerden gemeldet.

Änderungen an der betrieblichen Stätte der Leistungserfüllung insbesondere der Datenspeicherung, Erzeugung des Outputs (z.B. Verlagerung an einen anderen Standort), usw. werden dem Auftraggeber vorgängig rechtzeitig angezeigt.

Dem CISO des Auftraggebers wird die jeweils gültige Version der Sicherheitsdokumente proaktiv übermittelt. Änderungen des Sicherheitsniveaus, die den Auftraggeber betreffen, werden vorgängig mit dem CISO des Auftraggebers abgeklärt.

Die Daten des Auftraggebers werden unverzüglich nach Erstellung des physischen Outputs unwiederbringlich gelöscht.

Die Daten des Auftraggebers dürfen an keinem anderen Standort, als den Standort der Outputerzeugung und nur für den absolut notwendigen Zeitraum gespeichert werden und müssen unverzüglich nach Erstellung nicht wiederherstellbar gelöscht werden.

10. Technische Maßnahmen im Falle eines technischen Ausfalls

Folgende Fehlerklassen unterschieden, abgeleitet von der Leistungsbeschreibung werden folgende Reaktionszeit und Wiederherstellungszeiten garantiert:

Fehler-klasse	Reaktionszeit	Wiederherstellungszeit
1	1 Stunde	1 Tag
2	2 Stunden	2 Tage
3, 4	2 Wochen	innerhalb von 6 Monaten

(1) Incident-Annahme

Für eine detaillierte Analyse eines Incidents sind folgende Informationen vorauszusetzen:

- Einmeldung via Ticketing-System bzw. Information an Webadministratorin Postserver bei Tele2 Alarm
- Der Zeitpunkt der Störung (so genau wie möglich)
- Eventuell Informationen über den Einmelder bzw. die Einmalderin, zwecks Kontaktaufnahme

Im Rahmen der Analyse und Priorisierung erbringt der Auftragnehmer folgende Leistungen:

- Annahme der eingehenden Incidents
- Beurteilung des Einflusses des Incidents auf die Geschäftsprozessabwicklung des Auftraggebers und entsprechende Vergabe von Prioritäten/Fehlerklassen;
- Durchführung der Problem- oder Fehlerdiagnose
- Qualifizierte Unterstützung durch die Webadministratorin Postserver

Postserver Onlinezustelldienst GmbH | Mariahilfer Straße 123/3 | 1060 Vienna | Austria
UniCredit Bank Austria AG | IBAN: AT37 1200 0529 4901 3147 | BIC: BKAUATWW
Registriert beim Handelsgericht Wien unter FN 367446 m | UID-Nummer: ATU 66678268

(2) Incident-Lösung

Im Rahmen der Incident - Lösung erbringt Tele2 folgende Leistungen:

- Bearbeitung und Lösung von Incidents und gegebenenfalls Weiterleitung an die nachgelagerten Services
- Qualifizierte Beratung zur Anwendung per E-Mail und gegebenenfalls per Telefon innerhalb der vereinbarten Servicezeiten
- Lösung der Incidents

(3) Incident-Verwaltung

Im Rahmen der Incident-Verwaltung erbringt Tele2 folgende Leistungen:

- Verwalten der noch nicht abgeschlossenen Incidents
- Einleiten von Eskalationen und Nachverfolgung derselben
- Statusinformationen bzw. Rückmeldung der Lösung an die die Webadministratorin Postserver

11. Technische Maßnahme im Falle des Ausfalls der Druckstraße

kbprintcom verfügt über einen redundanten Maschinenpark, d.h. bei Stillstand einer Produktionsmaschine kann auf eine Ersatz-Maschine am gleichen Standort zurückgegriffen werden. Sofern der eigene Standort gänzlich ausfallen sollte, ist auch dann eine Produktion und damit die Auftragserfüllung sichergestellt.

Das von kbprintcom eingeführte Backup gliedert sich in die einzelnen Produktions-Abschnitte:

- Datenaufbereitung
- Personalisierung
- Kuvertierung

Diese Backup Lösung stellt sicher, dass je nach Anforderung ein betroffener Prozessschritt, bzw. zwei Prozessschritte oder der gesamte Produktionsprozess ausgelagert werden kann.

Auslagern bedeutet in diesem Zusammenhang, dass der betroffene Prozessschritt (bzw. die Prozessschritte) vom Standort Wien verlegt wird. Die Verlegung erfolgt in das Schwesterunternehmen, kb-endlos Kroiss & Bichler GmbH, Gutenbergstraße 2, 4840 Vöcklabruck.

Die Unternehmen kbprintcom und kb-endlos sind zu jeweils 100% in einer Holding vereint und haben daher einen gemeinsamen Eigentümer.

Es wird in jedem Fall sowohl die Produktionsplanung Wien als auch die Produktionsplanung Vöcklabruck informiert. Die Produktionsleitung besitzt für beide Standorte Verantwortung und damit auch Kompetenz (Anordnung von zusätzlichen Schichten, Weisungsrecht, usw.). Damit liegen Koordination und Verantwortung konzentriert an einer Position in der Organisation.

12. Zertifizierungen

(1) Zertifizierung der PCI-Konformität

PCI DSS – Postserver
Die Postserver Zertifizierung der PCI-Konformität gemäß Payment Card Industry Data Security Standard erfolgte am 18. Mai 2017 und ist bis 17. Mai 2018 gültig.

PCI DSS – Wirecard
Die Wirecard Zertifizierung der PCI-Konformität gemäß Payment Card Industry Data Security Standard erfolgte am 10. April 2017 und ist bis 9. April 2018 gültig.

(2) Zertifizierung Druckstraße

ISO Zertifizierung
kbprintcom ist seit 1994 ISO 9001 zertifiziert und erfüllt alle diesbezüglichen externen und internen Kriterien.

(3) Zertifizierung Postserver

Zertifizierung nach Zustellgesetz
Die Zulassung als behördlicher Zustelldienst beruht auf dem Zustellgesetz (ZustG), Zustelldiensteverordnung (ZustDV), Zustellformularverordnung (ZustFormV), Deregulierungsgesetz 2017 – Teil BKA, Datenschutzgesetz (DSG), EU-Datenschutzgrundverordnung (DSGVO), EU-Verordnung zur elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS).
Das Bundesministerium für Digitales und Wirtschaftsstandort hat das EGIZ eGovernment Innovation Center damit beauftragt die Zertifizierung nach der durch das EGIZ entwickelten einheitlichen dualen Zustellspezifikation vorzunehmen.
Postserver wurde mit Bescheid vom 4. September 2012 als behördlicher Zustelldienst zugelassen.

Zertifizierung nach Rulebook der WKO
Die Zulassung als privatwirtschaftlicher Zustelldienst beruht auf dem Rulebook der WKO „System private E-Zustellung Österreich“.
Die Wirtschaftskammer Österreich hat den österreichische IT-Standardisierungs-Verein AUSTRIAPRO damit beauftragt, einen technischen Standard für die elektronische Zustellung eingeschriebener Briefe und Dokumente in Österreich zu entwickeln, der – im Gegensatz zur behördlichen E-Zustellung – sowohl von Unternehmen als auch Privatpersonen einfach und sicher untereinander genutzt werden kann.
Postserver wurde mit Vertrag vom 19. März 2010 als privatwirtschaftlicher Zustelldienst zugelassen.

13. Benennung Unterbeauftragte

(1) Die durch Tele 2 erbrachte Teilleistung ist das Hosting der Server an Standorten innerhalb Österreichs.

Tele2 i.A.v. Hutchison Drei Austria GmbH
Brünner Straße 52
1210 Wien, Österreich

FN: 140132b
Firmenbuchgericht: HG Wien
Firmensitz: Wien
UID-Nr.: ATU 41029105

(2) Die durch Servotel erbrachte Teilleistung ist die Führung des 1st Level Supports mit Standort innerhalb Österreichs.

Servotel CallCenter Dienstleistungen GmbH
Hondastraße 1
2351 Wiener Neudorf, Österreich

FN: 19721v
Firmenbuchgericht: Landesgericht Wiener Neustadt
Firmensitz: Wiener Neustadt
UID-Nr.: ATU 50798800

(3) Die Unternehmen CPB und kbprintcom sind kein Auftragsverarbeiter nach Art. 28 DSGVO, dies ergibt sich bereits aus den Definitionen "Verantwortlicher" bzw. "Auftragsverarbeiter" gemäß Art. 4 DSGVO:

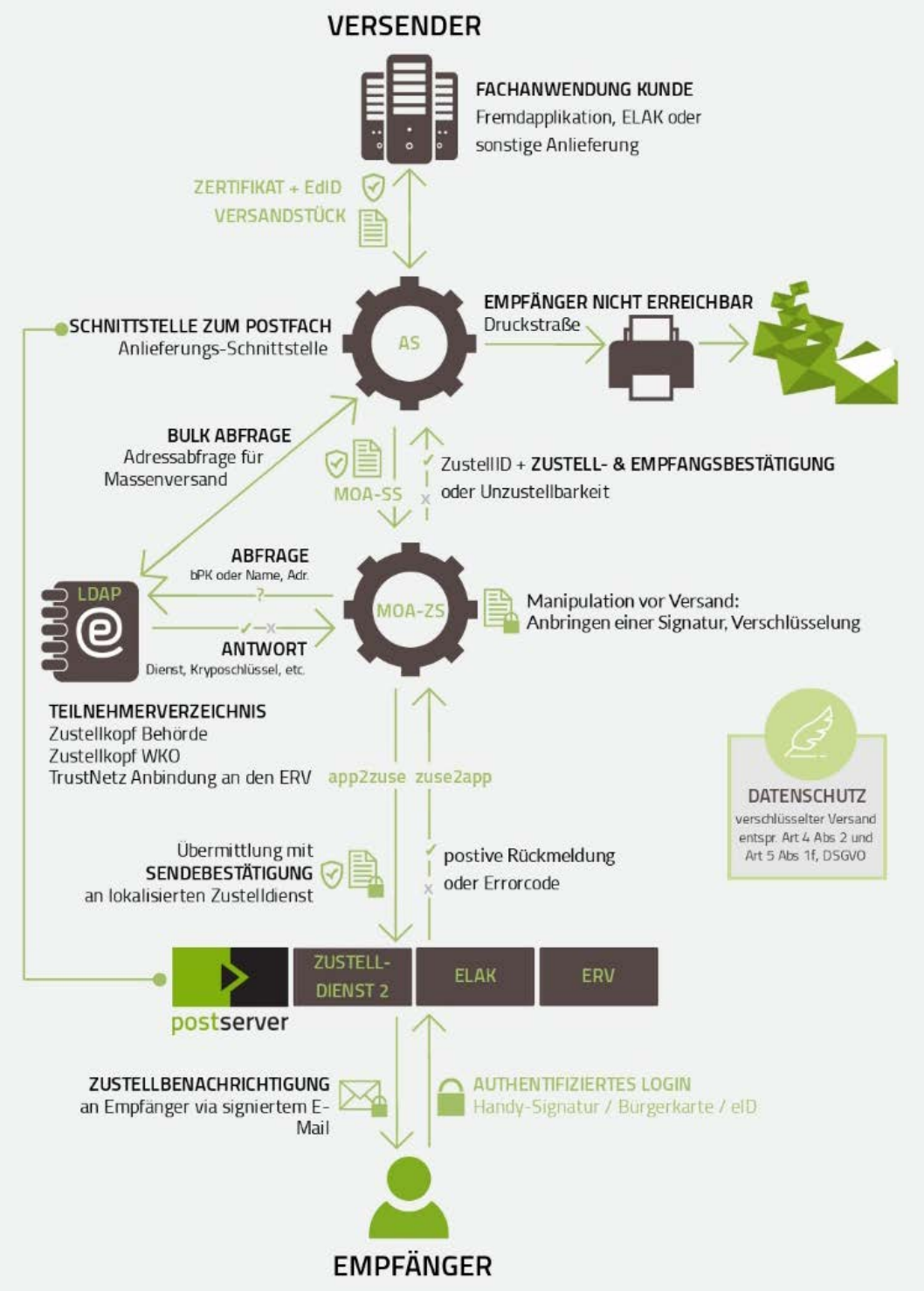
Wesentliches Merkmal des Verantwortlichen ist, dass er über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Demgegenüber handelt ein

Auftragsverarbeiter stets nur im Auftrag sowie nur auf dokumentierte Weisung des Verantwortlichen. In der Praxis kommt es daher insbesondere darauf an, ob ein Verantwortlicher in der Lage ist, fachliche Weisungen an einen Dritten zu erteilen. Nur wenn dies der Fall ist, handelt es sich bei einem Dritten um einen Auftragsverarbeiter.

(4) Näheres zu den organisatorischen Ansprechpartnern sind im Anlage 3 aufgeführt.

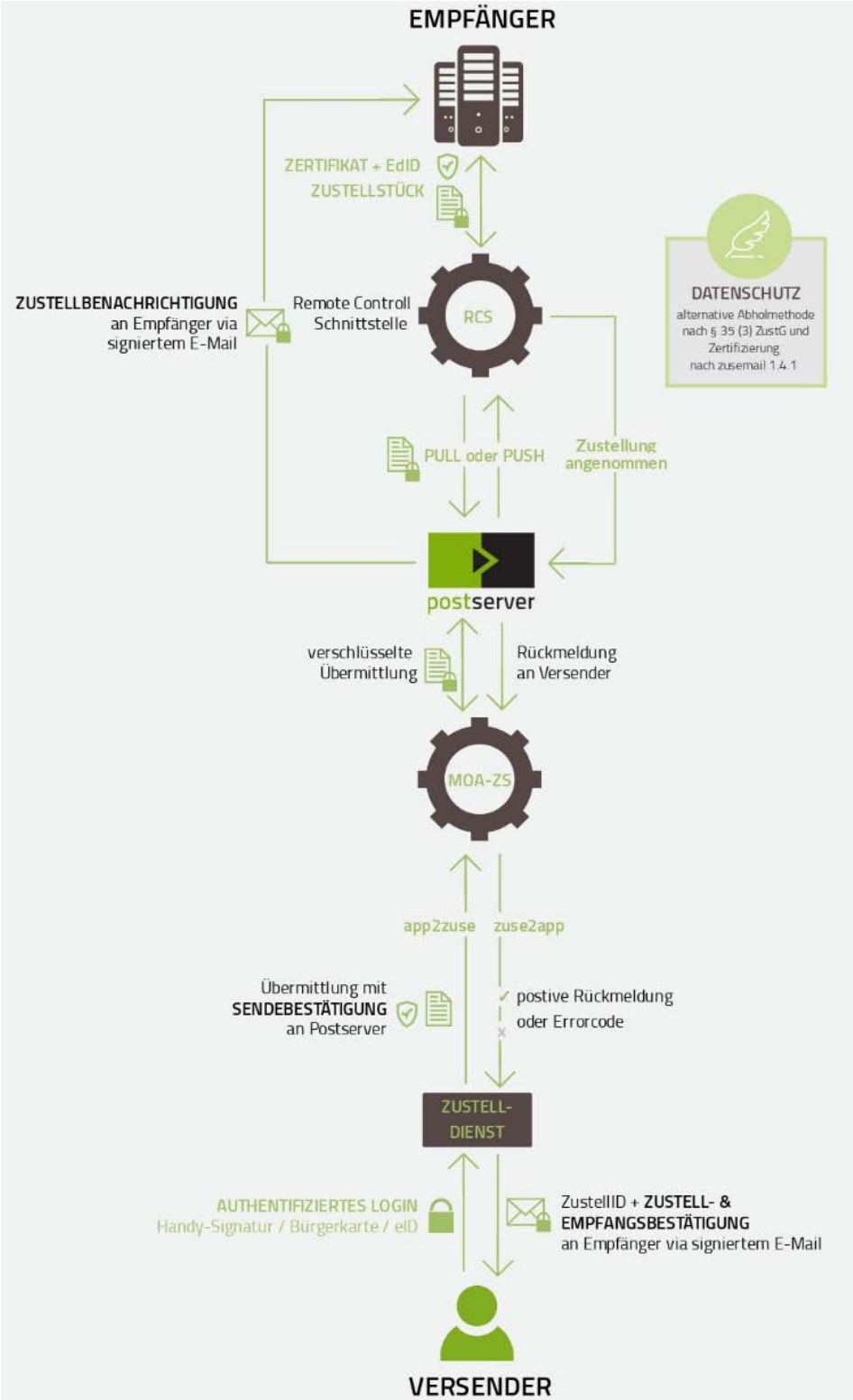
Anlage 2

Prozessmodell Duale Zustellung (Integration): Remote Versand



Postserver Onlinezustelldienst GmbH | Mariahilfer Straße 123/3 | 1060 Vienna | Austria
UniCredit Bank Austria AG | IBAN: AT37 1200 0529 4901 3147 | BIC: BKAUATWW
Registriert beim Handelsgericht Wien unter FN 367446 m | UID-Nummer: ATU 66678268

Prozessmodell Duale Zustellung (Integration): Automatische Abholung



Postserver Onlinezustelldienst GmbH | Mariahilfer Straße 123/3 | 1060 Vienna | Austria
UniCredit Bank Austria AG | IBAN: AT37 1200 0529 4901 3147 | BIC: BKAUATWW
Registriert beim Handelsgericht Wien unter FN 367446 m | UID-Nummer: ATU 66678268

Anlage 3

Betriebsablauf

1. Organisatorische Schnittstellen E-Zustellung / Druck

Im Regelbetrieb wird die Kommunikation zwischen Rechenzentrum bzw. Middleware und Druck über eine Fileshare-Schnittstelle stattfinden. Die zu druckenden Dokumente werden übergeben. Wenn der Druck erfolgreich war, erfolgt eine Rückmeldung an die Middleware u.a. mit dem Druckdatum und dem voraussichtlichen Versanddatum. Das Versandmodul prüft, ob alle übergebenen Druckaufträge auch fristgerecht gedruckt wurden.

Wenn die automatisierte Verarbeitung nicht funktioniert, muss auf die organisatorische Schnittstelle zurückgegriffen werden, d.h. diese Fälle werden auf einem Fehlerprotokoll ausgegeben. Dieses Fehlerprotokoll wird vom Betrieb kontrolliert und, falls es sich um einen Fehler handelt, werden folgende Prozessschritte durchlaufen:

(1) In einem ersten Schritt muss lokalisiert werden, wo das Problem bei der Verarbeitung liegt. Es könnte sich z. B. um ein Problem bei der Anlieferung handeln. In diesem Fall könnte das Problem im Bereich des Rechenzentrums selbst liegt. Falls das Problem im Rechenzentrum liegt, ist der Frage nachzugehen, ob das Problem in mangelnden Ressourcen liegt oder es sich um ein sonstiges Betriebsthema handelt, wie z. B. Netzwerkprobleme. In diesem Fall werden die internen Abteilungen von Tele2 kontaktiert und diese werden dann den Störfall beheben.

(2) Falls es sich um ein Problem beim Druck handelt, wird dieses durch die Firma kbprintcom gelöst.

(3) Falls das Problem in der Zuständigkeit der Middleware-Software liegt, wird der Support der Firma CPB kontaktiert. Falls es sich tatsächlich um einen Software Fehler handelt, muss ein entsprechender Change an der Software durchgeführt werden.

2. Ansprechpartner und Erreichbarkeit

(1) Support-Hotline (1st Level) für fachliche und Anwendungsthemen:

Support-Hotline

Tel.: +43 (810) 400401
E-Mail: support@postserver.com

Erreichbarkeit: 7 bis 22 Uhr, 7 Tage die Woche

(2) Sofern keine Beantwortung bzw. Fehleranalyse von den oben genannten Hotlines möglich ist, werden durch den 1st Level Support die Ansprechpartner des 2nd Level Support kontaktiert.

Das gesamte Support- und Service-Management erfolgt zentral durch Postserver. Der Auftraggeber muss keinen gesonderten Kontakt aufnehmen.

2nd Level – CPB (Softwarepartner)

CPB Software (Austria) GmbH
Franz Josefs Kai 33
1010 Wien, Österreich

FN: 153156f
Firmenbuchgericht: Handelsgericht Wien
Firmensitz: Wien
UID-Nr.: ATU 42323008

Tel.: +43 (1) 5330807
E-Mail: bbgdualesupport@cpb.at

Erreichbarkeit: 8 bis 17 Uhr, werktags

2nd Level – kbprintcom (Druckpartner)

kbprintcom.at Druck + Kommunikation GmbH
Gutenbergstraße 2
4840 Vöcklabruck, Österreich

FN: 56458b
Firmenbuchgericht: Landesgericht Wels
Firmensitz: Vöcklabruck, Wien
UID-Nr.: ATU 24826703

Tel.: +43 (1) 74051 - 1651
E-Mail: service@kbprintcom.at

Erreichbarkeit: 8 bis 17 Uhr, werktags

3. Wartungsfenster

Das Standard-Wartungsfenster ist:
Donnerstag 22 bis Freitag 6 Uhr

Ausnahmen werden im Vorhinein vom Auftraggeber an die entsprechenden Support-Mailverteiler angekündigt.

Wartungsarbeiten, die außerhalb des definierten Zeitraumes durchgeführt werden und zu Ausfällen im Minutenbereich führen z.B. das Ausrollen eines Hotfix, können kurzfristig nach Ankündigung durchgeführt werden.

4. Reporting

(1) Prinzipiell werden folgende Berichte dem Auftraggeber übermittelt:

- Auflistung der in einem definierten Zeitraum verarbeiteten Anlieferungen
  - pro Versender
  - pro Kanal (elektronische / postalisch)
  - pro Qualität
- Eventuell durchgeführte Hotfixe mit Datum und grober Hotfixbeschreibung
- Uptime des ISP (Tele2)

(2) Reporting Druck

Im Bereich Druck sind folgende Dokumente bei kbprintcom gelebter Standard:

- SLA-Vereinbarungen inkl. Change- und Eskalationsmanagement-Regelungen
- Betriebshandbücher für den jeweiligen Auftraggeber
- Regelmäßige Qualitätszirkel
- Im Fehlerfall: Erfassung mittels Reklamationsdatenbank bzw. 4-D-Bericht

Für die Druckabwicklung sind folgende Dokumentationen Usus:

- Aufstellung Materialbedarf
- Aufstellung Produktionswege
- Datenprotokolle (Datenerhalt, Datenlöschung)
- Postlieferscheine
- Lagerbestandslisten

Selbstverständlich werden alle in der gegenständlichen Ausschreibung benötigten täglichen, wöchentlichen, monatlichen und anlassbezogenen Auswertungen sowie

Übergabenachweise von Rückscheinsendungen („Einschreiberliste“) beigestellt.

Sofern darüber hinaus im Auftragsfall erkannt wird, dass zusätzliche Auswertungen benötigt werden, ersuchen wir um Benachrichtigung, damit diese kurzfristig in das regelmäßige Reporting integriert werden.