Vereinbarung zur Auftragsverarbeitung
(AV)

zwischen

_____

_____

_____

Name des Datenschutzbeauftragten: _____

E-Mail-Adresse des Datenschutzbeauftragten: _____

Telefonnummer des Datenschutzbeauftragten: _____

Als Auftraggeber und Verantwortlicher

-nachfolgend der „Verantwortliche“-

und

Etix.com Event GmbH & Co. KG
Wasastraße 6
01219 Dresden

Als Auftragnehmer und Auftragsverarbeiter

-nachfolgend der „Auftragsverarbeiter“-,

zusammen nachfolgend die „Parteien“ und jeder von Ihnen als „Partei“.

Präambel

Die vorliegende Vereinbarung zur Auftragsverarbeitung regelt die Anforderung an die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Zusammenhang mit der Erbringung der im Vertrag zwischen den Parteien vereinbarten Leistungen, auf den diesbezüglich verwiesen wird.

§1
Definitionen

AV	Diese Vereinbarung zur Auftragsverarbeitung.
Arten personenbezogener Daten	Zusammenfassung personenbezogener Daten zu Gruppen von Daten mit einem ähnlichen inhärenten Verwendungszweck.
Auftragsverarbeiter	Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle - wie oben angegeben und definiert – die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 NR. 8 DS-GVO).
betroffene Person	Eine identifizierte oder identifizierbare Person; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der Physischen, Physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 4 NR.1 DS-GVO).
Dienstleistungen	Alle Dienstleistungen, die der Auftragsverarbeiter dem Verantwortlichen nach dem Vertrag zur Verfügung stellt.
Drittstaat	Staat, der weder Mitglied der Europäischen Union (EU) noch des Europäischen Wirtschaftsraum (EWR) ist.
DS-GVO	Datenschutz-Grundverordnung (Verordnung (EU) 2016/679).
Kategorien betroffener Personen	Zusammenfassung von betroffenen Personen zu einer Gruppe aufgrund deren im Wesentlichen gleichen Stellung bzw. Beziehung zum Verantwortlichen
Personenbezogene Daten	Alle Informationen, die sich auf eine betroffene Person beziehen (Art. 4 Nr.1 DS-GVO).
TOM	Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten vor unbeabsichtigter oder unrechtmäßiger Vernichtung oder unbeabsichtigter Löschung, Veränderung, unberechtigtem Zugriff oder unbeabsichtigter Offenlegung.
Verantwortlicher	Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle – wie oben angegeben und definiert – die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DS-GVO).
Verarbeitung personenbezogener Daten	Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder due Verknüpfung, die

	Einschränkung, das Löschen oder die Vernichtung (Art. 4 Nr. 2 DS-GVO).
Vertrag	Der in der Präambel bezeichnete Vertrag.
Verletzung des Schutzes personenbezogener Daten	Eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (Art. 4 Nr. 12 DS-GVO).

§ 2
Gegenstand und Laufzeit der AV

1. Diese AV legt die Rechte und Pflichten der Parteien in Bezug auf die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Namen des Verantwortlichen zum Zwecke der Erbringung der Dienstleistung fest.
2. Die Laufzeit dieser AV beginnt und endet mit der Laufzeit des Vertrages. Diese AV kann von beiden Parteien aus wichtigem Grund mit sofortiger Wirkung gekündigt werden. Die Kündigung bedarf der Schriftform.

§ 3
Zweck und Dauer der Verarbeitung / Kategorien betroffener Personen und Arten personenbezogener Daten

1. Zweck der Verarbeitung personenbezogener Daten durch den Auftragsgeber ist die Erbringung der Dienstleistungen.
2. Die Verarbeitung personenbezogener Daten beginnt und endet mit der Laufzeit dieser AV, wie in § 2 Abs. 2 beschrieben. Die Datenverarbeitung, die zur Erfüllung von Löschungs- und/oder Rückgabeverpflichtungen gemäß § 8 erforderlich ist, bleibt hiervon unberührt.
3. Die Kategorien betroffener Personen sowie die Arten personenbezogener Daten, die im Auftrag verarbeitet werden, sind in **ANLAGE 1** näher beschrieben.

§ 4
Rechte und Pflichten des Verantwortlichen

1. Der Verantwortliche bleibt gegenüber den betroffenen Personen für die Einhaltung des Datenschutzes verantwortlich und stellt sicher, dass die Datenverarbeitung in Übereinstimmung mit den einschlägigen Bestimmungen des anwendbaren Datenschutzes erfolgt. Der Verantwortliche (und Auftraggeber) ist somit auch Verantwortlicher im Sinne der anwendbaren Datenschutzgesetze.
2. Zusätzlich zu den in dieser AV enthaltenen Anforderungen an Verarbeitung personenbezogener Daten kann der Verantwortliche den Auftragsverarbeiter Einzelweisungen über Art, Umfang und Ablauf der Datenverarbeitung, insbesondere über Berichtigung, Sperrung und Löschung erteilen. Diese Einzelweisungen sind schriftlich oder per E-Mail zu erteilen.
3. Der Verantwortliche hat das Recht, die Einhaltung der Verpflichtungen aus dieser AV sowie etwaiger Einzelweisungen, insbesondere die Umsetzung der beschriebenen TOM des Auftragsverarbeiters auf Anfrage und mit angemessener schriftlicher Vorankündigung zu überprüfen. Zu diesem Zweck wird der Auftragsverarbeiter dem Verantwortlichen, seinen Mitarbeitern oder bevollmächtigten Prüfern / Beratern, die

durch eine seitens des Auftragsverarbeiters gestellte Verschwiegenheitsvereinbarung verpflichtet sind, nach zeitlich angemessener vorheriger schriftlicher Mitteilung durch den Verantwortlichen einen angemessenen Zugang zu den für den Verantwortlichen verarbeiteten Daten sowie den verwendeten Datenverarbeitungssystemen, Datenverarbeitungsprogrammen und relevanten Räumlichkeiten während der normalen Geschäftszeiten gewähren. Alle internen und externen Kosten, die durch Auftragsverarbeiter durch eine solche Prüfung entstehen, gehen zu Lasten des Verantwortlichen.

§ 5
Pflichten des Auftragsverarbeiters

1. Allgemeines

Der Auftragsverarbeiter darf personenbezogene Daten ausschließlich im Namen des Verantwortlichen gemäß den Anforderungen dieser AV und gemäß etwaiger Einzelweisungen der verantwortlichen Stelle und ausschließlich zu den in dieser AV genannten Zwecken verarbeiten, es sei denn, der Auftragsverarbeiter ist zu einer hiervon abweichenden Verarbeitung personenbezogener Daten nach anwendbarem Recht verpflichtet. Im letzteren Fall wird der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung personenbezogener Daten zu diesem abweichenden Zweck über diese gesetzliche Verpflichtung informieren, es sei denn, dass das Gesetz eine solche Information aus wichtigen Gründen des öffentlichen Interesses verbietet.

2. Übermittlung ins Drittland

Die Datenverarbeitung erfolgt in einem Mitgliedstaat der Europäischen Union (EU) oder in einem Mitgliedstaat des Europäischen Wirtschaftsraums (EWR). Jede Übermittlung personenbezogener Daten in ein Drittland, einschließlich der Gewährung des Zugangs aus einem Drittland zu den in der EU/EWR gespeicherten personenbezogenen Daten, ist nur zulässig, wenn die Anforderungen der Artikel 44ff. DS-GVO erfüllt sind, bevor personenbezogene Daten übertragen bzw. zugänglich gemacht werden und der Verantwortliche einer solchen Übermittlung vorher zustimmt. Die zum Zeitpunkt des Abschlusses dieser Vereinbarung vorhandenen Empfänger in einem Drittland, an die personenbezogene Daten übermittelt werden bzw. die Zugriff auf in der EU/EWR gespeicherte personenbezogene Daten haben, werden zusammen mit den jeweils getroffenen Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus im betreffenden Drittland in **ANLAGE 2** aufgeführt.

3. Verarbeitungsverzeichnis

Der Auftragsverarbeiter ist verpflichtet, ein schriftliches oder elektronisches Verzeichnis aller Verarbeitungstätigkeiten bezogen auf die personenbezogenen Daten entsprechend den gesetzlichen Vorgaben zu führen, es auf dem aktuellen Stand zu halten und dem Verantwortlichen auf dessen Verlangen zu übermitteln.

4. TOM (Technische und organisatorische Maßnahmen)

Der Auftragsverarbeiter wird angemessene TOM treffen. Dabei sind der Stand der Technik, die Durchführungskosten, die Art, der Umfang und die Zwecke der Verarbeitung personenbezogener Daten sowie die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Die derzeit vom Auftragsverarbeiter getroffenen TOM werden in **ANLAGE 3** beschrieben. Die TOM unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insofern ist es zulässig, dass der Auftragsverarbeiter die beschriebenen TOM ändert, solange das

bestehende Sicherheitsniveau der definierten Maßnahmen dabei insgesamt nicht reduziert wird. Ungeachtet dessen sind Änderungen zu dokumentieren und dem Verantwortlichen mitzuteilen, z.B. durch die regelmäßige Bereitstellung einer aktualisierten Liste von TOM. Wesentliche Änderungen der TOM bedürfen der schriftlichen Vereinbarung.

5. **Vertraulichkeit**

Der Auftragsverarbeiter ist zur Vertraulichkeit verpflichtet und stellt sicher, dass alle Personen, die zur Verarbeitung personenbezogener Daten des Verantwortlichen im Sinne dieser AV befugt sind, sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen. Insbesondere ist eine Offenlegung personenbezogener Daten untersagt.

6. **Überwachung**

Während der gesamten Vertragslaufzeit überwacht der Auftragsverarbeiter die Einhaltung der Bestimmungen dieser AV und ggf. der Einzelweisungen, die der Verantwortliche gemäß § 4 Abs. 2 erteilt.

7. **Kommunikation**

Sämtliche Kommunikation zwischen dem Verantwortlich und dem Auftragsverarbeiter hat, falls erforderlich, unter zusätzlichen Sicherheitsmaßnahmen zu erfolgen (z.B. Verschlüsselung der elektronischen Kommunikation).

8. **Unterstützung des Verantwortlichen**

Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter den Verantwortlichen so weit wie möglich bei der Erfüllung seiner datenschutzrechtlichen Pflichten (z.B. Meldung von Datenschutzverletzungen an die Datenschutzbehörden und die betroffenen Personen gem. §6, Durchführung von Datenschutzverträglichkeitsprüfungen sowie Beantwortung von Anfragen zur Ausübung der Rechte der betroffenen Personen). Wendet sich eine betroffene Person mit einem Antrag zur Wahrnehmung datenschutzrechtlicher Betroffenenrechte (z.B. Berichtigung, Löschung oder Einschränkung der Verarbeitung ihrer personenbezogenen Daten) direkt an den Auftragsverarbeiter, leitet dieser den Antrag unverzüglich an die Verantwortlichen weiter.

9. **Verstoß gegen das Datenschutzrecht**

Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich informieren, wenn seiner Meinung nach eine Weisung des Verantwortlichen gegen geltendes Datenschutzrecht verstößt. Der Auftragsverarbeiter ist dann berechtigt, die Ausführung der betreffenden Weisung solange auszusetzen, bis der Verantwortliche sie bestätigt oder ändert.

10. **Der Datenschutzbeauftragte**

Der Auftragsverarbeiter wird einen Datenschutzbeauftragten entsprechend den geltenden gesetzlichen Regelungen bestellen und dem Verantwortlichen unverzüglich und unaufgefordert die Kontaktdaten des Datenschutzbeauftragten mitteilen.

§ 6
Meldung einer Verletzung des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten benachrichtigt der Auftragsverarbeiter den Verantwortlichen unverzüglich (in der Regel per E-Mail oder

telefonisch den Datenschutzbeauftragten des Verantwortlichen), nachdem er Kenntnis von einer Verletzung des Schutzes personenbezogener Datenerlangt hat.

7 §
Kontrolle

Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in dieser AV festgelegten Verpflichtungen des Auftragsverarbeiters, insbesondere die Implementierung angemessener TOM, nachzuweisen. Zu diesem Zweck gestattet der Auftragsverarbeiter auch Überprüfungen-, einschließlich Inspektionen unter den in § 4 Abs. 3 genannten Bedingungen.

§ 8
Beendigung und Löschung

Der Auftragsverarbeiter wird alle unter dieser AV verarbeiteten personenbezogenen Daten und alle Kopien davon nach 30 Tagen nach Beendigung dieser AV löschen, es sei denn, das anwendbare Recht verlangt eine weitere Speicherung der personenbezogenen Daten (z.B. Aufbewahrungspflichtigen). Im letzteren Fall hat der Auftragsverarbeiter dafür Sorge zu tragen, dass die Datenverarbeitung auf diesen Zweck beschränkt bleibt. Auf eine schriftliche oder per E-Mail getätigte Aufforderung der Verantwortlichen innerhalb von 30 Tagen nach Beendigung dieser AV wird der Auftragsverarbeiter alle unter dieser AV verarbeiteten personenbezogenen Daten und alle Kopien davon an den Verantwortlichen gegen Vergütung der damit verbundenen Aufwände zurückzugeben.

§ 9
Unterauftragnehmer

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die erbringen oder Hauptleistung beziehen. Nicht hierzu gehören neben Leistungen, die der Auftragnehmer zum Beispiel als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice oder deren Sohn von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard – und Software von Datenverarbeitungsanlagen in Anspruch nehmen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftragsgebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarung sowie Kontrollmaßnahmen zu ergreifen.
2. Der Verantwortliche erteilt hiermit seine Zustimmung zur Beauftragung der in ANLAGE 4 aufgeführten Unterauftragnehmer. Jede Beauftragung von Unterauftragnehmern, die nicht in ANLAGE 4 enthalten sind, bedarf der vorherigen Zustimmung des Verantwortlichen, die nicht ohne triftigen Grund verweigert werden darf. Die vorherige Zustimmung des Verantwortlichen gilt als erteilt, wenn a) der Auftragsverarbeiter die geplante Inbetriebnahme eines neuen Unterauftragnehmers dem Verantwortlichen schriftlich oder in Textform mitgeteilt hat, b) der Verantwortliche nicht binnen sieben Werktagen nach Erhalt der Mitteilung schriftlich oder in Textform widersprochen hat und c) der Auftragsverarbeiter mit dem jeweiligen Unterauftragnehmer eine Vereinbarung zur Auftragsverarbeitung nach Maßgabe des § 9 Abs. 3 abgeschlossen hat.

3. Der Auftragsverarbeiter hat mit den Unterauftragnehmern Vereinbarungen zur Auftragsverarbeitung abzuschließen, die so ausgestaltet sind, dass sie dem Datenschutzniveau dieser AV entsprechen. Der Verantwortliche hat das Recht, auf schriftliche Anfrage vom Verarbeiter Informationen über die Umsetzung der Datenschutzverpflichtungen im Rahmen des Untervertragsverhältnisses zu erhalten, gegebenenfalls durch Einsichtnahme in die entsprechende Vereinbarung zur Auftragsverarbeitung.
4. Wenn ein Unterauftragnehmer eine Verarbeitung personenbezogener Daten in oder aus einem Drittland erbringen soll, muss der Auftragsverarbeiter die Rechtmäßigkeit der Übermittlung personenbezogener Daten in das Drittland gemäß Art. 44 ff. DS-GVO sicherstellen. Der (die) betreffende(n) Unterauftragnehmer und die entsprechende Garantie zur Sicherstellung eines angemessenen Datenschutzniveaus sind in **ANLAGE 2** aufzunehmen.
5. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten dieses Unterauftragnehmers.

§ 10
Abschließende Regelungen

1. Die nachfolgenden Anlagen sind integraler Bestandteil dieser AV:
   ANLAGE 1: Kategorien betroffener Personen und Arten personenbezogener Daten
   ANLAGE 2: Übermittlung von personenbezogenen Daten in Drittländer
   ANLAGE 3: TOM
   ANLAGE 4: Liste mit genehmigten Unterauftragnehmern
2. Änderungen oder Ergänzungen dieser AV bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für Änderungen dieses Schriftformerfordernisses.
3. Alle Streitigkeiten oder Ansprüche, die sich aus oder im Zusammenhang mit dieser AV ergeben, unterliegen deutschem Recht und werden gemäß diesem Recht ausgelegt.
4. Für den Fall, dass eine oder mehrere Bestimmungen dieser AV ganz oder teilweise unwirksam sein sollten oder werden, wird die Gültigkeit und Durchsetzbarkeit der übrigen Bestimmungen dieser AV dadurch nicht berührt. Gleiches gilt für den Fall, dass der Vertrag Lücken enthalt. Eine unwirksame bzw. fehlende Bestimmung ist durch eine solche zu ersetzen, die, soweit rechtlich zulässig, dem tatsachlichen oder mutmaßlichen Willen der Parteien am nächsten kommt, sofern sie diese berücksichtigt hatten.

Dresden, den 28.06.2021

etix.com event GmbH & Co. KG
Wasastr. 6
01219 Dresden
Telefon 0351 / 30 70 80 00

Unterschrift und Stempel Auftraggeber

Unterschrift und Stempel Auftragsverarbeiter

ANLAGE 1

Kategorien betroffener Personen und Arten personenbezogener Daten

Die Verarbeitung personenbezogener Daten im Rahmen dieser AV betrifft die folgenden Kategorien betroffener Personen und die folgenden Arten personenbezogener Daten:

Kategorien betroffener Personen	**Arten personenbezogener Daten**
Interessenten und Käufer für Produkte, Dienstleistungen und Eintrittskarten für Veranstaltungen des Verantwortlichen Mitarbeiter des Verantwortlichen und des Auftragsverarbeiters	Bei den nachstehenden Daten kann es sich aufgrund der Konfigurationsmöglichkeit des Systems um optimale oder freiwillige Angaben seitens der Kunden des Auftraggebers handeln: Kennzeichen, Privatperson/Firmenkunde, Merkmale/Attribute und Merkmalsgruppen, Anrede, Titel, Branche, Namen, Adresse(n), Hausnummer, Zusatz zur Hausnummer, Land, Postleitzahl, Ort, Ortsteil, E-Mail, Telefonnummer(n), Anredetext, Geburtstag, Geschlecht, Sprache, USt.-ID, Notizen, Aliasname(n), Zahlungsmodus, Zahlungsart, Bankverbindung, Standardzustellweg, Mitglied im Fanclub, Eintritts- und Austrittsdatum,, Mandatsreferenz, SEPA-Gläubiger-ID, Newsletter-Anmeldungen, IP-Adresse, Tracking-Informationen

ANLAGE 2

Übermittlung von personenbezogenen Daten in Drittländern

Die folgende Liste enthalt Empfänger von personenbezogenen Daten in Drittländern, die direkt oder indirekt an der Verarbeitung personenbezogener Daten, die unter diese AV fallen, beteiligt sind sowie die jeweils zur Anwendung kommenden Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus gemaf1 Art. 44 ff. DS-GVO.

Name und Adresse des Empfängers im Drittland	**Rechtfertigung der Datenübermittlung / Geeignete Garantien**
Etix, Inc. 909 Aviation Parkway, Suite 900 Morrisville, NC 27560	*Etix.com entspricht den EU-Standardvertragsklauseln (SCCs)* In Übereinstimmung mit den EU-Standardvertragsklauseln verpflichtet sich Etix.com, Nachfragen oder Beschwerden über die Erhebungen oder die Nutzung Ihrer persönlichen Daten zu beantworten oder zu lösen.

ANLAGE 3

TOM (Technische und organisatorische Maßnahmen)

Die nachfolgenden Maßnahmen gelten nur im Falle des Systembetriebs durch den Auftragnehmer in dessen Rechenzentrum (sag. ASP-Lösung).

*Sofern der Systembetrieb durch den Auftraggeber selbst erfolgt (sag. Onsite-Lösung) gelten im Rahmen dieser Vereinbarung nur die mit * gekennzeichneten Maßnahmen. Alle anderen erforderlichen Maßnahmen sind in diesem Fall vom Auftraggeber selbst durchzuführen.*

1. Maßnahmen zur Sicherstellung der Vertraulichkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DS-GVO)

a) Zutrittskontrolle

Vorgabe / Anforderung:

Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Vom Auftraggeber konkret getroffene Maßnahmen:

- Ausweiskontrolle sowie Tragepflicht von Berechtigungsausweisen
- Beschränkung der Vergabe von Ausweisen, Schlüsselkarten etc.
- Dokumentation der Vergabe und Rückgabe von Schlüsselkarten etc.
- Pförtner, z. B. Personenkontrolle
- Schlüsselregelung
- Sicherheitsschlösser
- Manuelles Schließsystem
- System für Zutrittsberechtigungen für Mitarbeiter und Dritte
- Videoüberwachung der Eingänge
- Protokollierung der Besucher
- Sorgfältige Auswahl von Hilfspersonal, z.B. Reinigungskräften, Wachpersonal
- Schutz durch Sicherheitsfirmen außerhalb der Geschäftszeiten

b) Zugangskontrolle

Vorgabe / Anforderung:

Eine Nutzung der Datenverarbeitungssysteme durch Unbefugte ist zu verhindern.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Erstellung und Verwendung von Benutzerprofilen auf Personenebene
- Zuordnung der Benutzerrechte
- Passwortrichtlinie inkl. Mindestlänge, Mindestanforderung an Passwörter:
  - Müssen mindestens acht Zeichen lang sein
  - Müssen mindestens je ein Zeichen aus den Kategorien Großbuchstaben A-Z, Kleinbuchstaben von a-z, Ziffern der Basis 10 (0-9) sowie Sonderzeichen (z.B. !, $, #, %) enthalten
- Authentifikation mit persönlicher Benutzerkennung und Passwort
- Einsatz von VPN-Technologie

- Einsatz einer dem Stand der Technik entsprechenden Software-Firewall
- Einsatz einer dem Stand der Technik entsprechende Anti-Viren-Software
- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von Smartphone-Inhalten
- Automatische Bildschirmsperre
- Session Timeout für inaktive Sessions nach einem festgelegten Zeitraum

c) Zugriffskontrolle

Vorgabe / Anforderung:

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.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Erstellung eines differenzierten Berechtigungskonzepts, Freigabe der Daten nur für Befugte (Need-to-know- und Least-Privilege-Prinzip)
- Verwaltung der Zugriffsrechte durch Administrator
- Anzahl der Personen mit ‚Administrator-Status" minimiert
- Authentifizierung durch Benutzername und Passwort
- Protokollierung der Zugriffe
- Zeitnahe Sperrung der Konten ausgeschiedener Mitarbeiter
- Einsatz von Aktenvernichtern und Protokollierung der Vernichtung
- Sichere Aufbewahrung von Datenträgern
- Löschung von Datenträgern nach Verwendung
- Regelmäßige Anwendung von Sicherheits-Patches
- Trennung von Produktion und Entwicklung

d) Trennungskontrolle

Vorgabe / Anforderung:

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Trennung von Produktiv- und Testsystem, Sandboxing, physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Erstellung eines Berechtigungskonzepts
- Nachweislich logische Trennung der Daten der jeweiligen Kunden des (Unter-) Auftragnehmers, d. h. Daten verschiedener verantwortlicher Stellen und/oder (Unter-) Auftragnehmers sind getrennt zu verarbeiten und gegenseitiger Zugriff ist auszuschließen

2. Maßnahmen zur Sicherstellung der Integrität der Systeme und Dienste (Art. 32 Abs. 1 lit. b DS-GVO)

a) Weitergabekontrolle

Vorgabe / Anforderung:

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 welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- *Verschlüsselte Datenübertragung
- * Der Zugriff auf extern bereitgestellte Services erfolgt über verschlüsselte Protokolle (https, sftp etc.)
- Virtual Private Networks (VPN)
- Verschlüsselung von Datenträgern vor Versand
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Sollte eine Verschlüsselung nachweislich nicht möglich sein, muss ein sicheres Alternativverfahren durchgeführt werden (z. B. verschließbare Transportbehälter)
- * Weitergabe von Daten an Dritte ist lediglich mit schriftlicher Zustimmung des Verantwortlichen getattet
- Sorgfältige Auswahl von Transportpersonal und -fahrzeugen beim physischen Transport von Daten

b) Eingabekontrolle

Vorgabe / Anforderung:

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Richtlinien zu Eingabe und Erfassung von Daten
- 4-Augen-Prinzip
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf der Basis eines detaillierten Berechtigungskonzepts
- Protokollierung der Eingabe

3. Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit b und c DS-GVO)

a) Verfügbarkeitskontrolle

Vorgabe / Anforderung:

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Erstellung eines Backup- und Recovery-Konzepts
- Monitoring und Überwachung des Systemzustands und Meldung von Fehlfunktionen
- Test der Datenwiederherstellung aus Backup
- Unterbrechungsfreie Stromversorgung (USV)
- Aufbewahrung der Datensicherung an einem sicheren Ort
- Einsatz einer dem Stand der Technik entsprechender Anti-Viren-Software
- Einsatz einer dem Stand der Technik entsprechender Software-Firewall
- Einsatz einer dem Stand der Technik entsprechender Hardware-Firewall
- Sicherheitskonzept für Serverraume einschließlich Notfallpläne
- Überwachung der Temperatur und Feuchtigkeit in Serverräumen
- Alarmsystem, Feuer- und Rauchmelder für Serverräume
- Feuerlöschgeräte in Serverräumen
- Keine Serverraume unter sanitären Anlagen
- Physische Redundanz der Datenverarbeitungssysteme

b) Rasche Wiederherstellung

Vorgabe / Anforderung:

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Redundante Datenspeicherung
- Cloud-Services
- Doppelte lnfrastruktur

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

a) Auftragskontrolle

Vorgabe / Anforderung:

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Incident-Response-Management
- * Vertragliche Regelung der Zusammenarbeit zwischen Auftraggeber und (Unter-) Auftragnehmer
- * Sorgfältige Auswahl von Auftragnehmern
- * Kontrolle der technischen und organisatorischen Maßnahmen beim (Unter-) Auftragnehmer
- Vereinbarung von Stichprobenkontrollen (z. B. bei Änderungen, turnusmäßig)
- Vereinbarung von Vertragsstrafen bei Verstößen
- * Sicherstellung von Datenrückgabe/-löschung
- * Regelmäßige Schulungen der Mitarbeiter zum Datenschutz (Schulungspflicht)

b) Sonstige Überprüfungsmaßnahmen

- Regelmäßige Self-Assessments als Bestandteil eines PDCA-Zyklus (Pian-Do-Check-Act-Zyklus)
- Entwicklung eines Sicherheitskonzepts
- Regelmäßige Auditierung, Prüfungen (auch durch Externe)
- Fortlaufende Zertifizierungen

ANLAGE 4

Liste mit genehmigten Unterauftragnehmern

Unterauftragnehmer

Etix, Inc.
909 Aviation Parkway, Suite 900
Morrisville, NC 27560

Weitere Unterauftragnehmer:

secupay AG
Goethestr. 6
01896 Pulsnitz

paydirekt GmbH
Hamburger Allee 26-28
60486 Frankfurt am Main
Deutschland

GIROPAY GmbH
An der Welle 4
60322 Frankfurt/Main
Deutschland

PayPal (Europe)
S.à r.l. et Cie, S.C.A.
22-24 Boulevard Royal
L-2449 Luxembourg