Datenschutz bei Istac

Dem Datenschutz kommt bei Istac eine große Bedeutung zu und die Mitarbeiter werden regelmäßig über die Wichtigkeit der Einhaltung der Grundsätze der Datenschutzgrundverordnung (DSGVO) informiert.
Der betriebsinterne Datenschutzbeauftragte ist im ständigen Austausch mit der Geschäftsführung und steht allen Mitarbeitern für Fragen rund um den Datenschutz zur Verfügung.

Dieses Dokument gibt einen umfangreichen Überblick über die Datenschutzmaßnahmen bei Istac:

- Unternehmenspolitik zur DSGVO & Informationssicherheit
- Ausbildung Datenschutzbeauftragter
- Verarbeitungsverzeichnis
- Maßnahmen zum Schutz von Daten
- Maßnahmen zur Erlangung der Zustimmung von Beteiligten

Unternehmenspolitik zur Einhaltung der DSGVO & Informationssicherheit

Gültig für: alle Mitarbeiter der Istac GmbH
Überprüfungszeitraum: jährlich
Verantwortlich: Geschäftsführung/Datenschutzbeauftragter

DSGVO

„Die Einhaltung der DSGVO betrifft das ganze Unternehmen und ist ein laufender Prozess."

In unserem täglichen Handeln werden die Grundsätze der DSGVO eingehalten:

1. Rechtmäßigkeit / Treu und Glauben / Transparenz

Personenbezogene Daten müssen auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden, eine Rechtsgrundlage ist daher zwingend erforderlich. Darüber hinaus müssen die betroffenen Personen über die Verarbeitung informiert werden.

2. Zweckbindung

Die personenbezogenen Daten werden für einen eindeutigen und legitimen Zweck erhoben und dürfen nicht in einer mit diesem Zweck nicht zu vereinbarenden Weise weiterverarbeitet werden.

3. Datenminimierung

Art und Umfang der verarbeiteten Daten müssen den Verarbeitungszwecken angemessen, sowie auf das für die Zwecke notwendige Maß beschränkt sein.

4. Richtigkeit

Personenbezogenen Daten müssen sachlich richtig und auf dem neuesten Stand sein. Es sind alle Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

5. Speicherbegrenzung

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies für die festgelegten Verarbeitungszwecke erforderlich ist. Nach Ablauf dieser Frist sind die Daten entweder zu löschen oder zu anonymisieren.

6. Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Durch geeignete technische und organisatorische Maßnahmen muss der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust oder unbeabsichtigter Zerstörung/Schädigung gewährleistet werden.

7. Rechenschaftsplicht

Die Maßnahmen zur Einhaltung der obig genannten Grundsätze werden nicht nur gesetzt, sondern auch Transparent dokumentiert, um die ordnungsgemäße Einhaltung jederzeit nachweisen zu können.

Wir definieren folgenden Prozess bei Datenschutzanfragen

Macht ein Kunde von einem seiner Rechte laut DSGVO gebrauch, muss folgender Prozess unbedingt eingehalten werden:

1. Ein Mitarbeiter erhält eine Anfrage des Kunden, dass dieser eine Auskunft über seine Daten / die Löschung seiner Daten / die Berichtigung seiner Daten oder die Übertragung seiner Daten möchte:

   -Wird die Anfrage per Mail gestellt, wird diese ohne Verzögerung an den Datenschutzbeauftragten jkupfer@istac.at weitergeleitet. Der Mitarbeiter teilt dem Kunden mit, dass sich der Datenschutzbeauftragte um sein Anliegen kümmert.

   -Wird die Anfrage per Telefon gestellt, wird der Kunde gebeten, eine schriftliche Anfrage an den Datenschutzbeauftragten zu stellen. Die mündliche Kontaktaufnahme wird dem Datenschutzbeauftragten ohne Verzögerung schriftlich mitgeteilt.

2. Der Datenschutzbeauftragte kümmert sich umgehend, aber zumindest innerhalb der 1-monatigen Frist um die Anfrage und klärt den Kunden über seine Rechte auf.

3. Die Anfrage und alle damit einhergehenden Schritte werden im Datenverarbeitungsverzeichnis vom Datenschutzbeauftragten dokumentiert und der dazugehörige Schriftverkehr abgelegt.

Wir definieren folgenden Prozess bei der Verletzung des Schutzes personenbezogener Daten
Im Falle einer Verletzung des Schutzes personenbezogener Daten, wird diese umgehend dem Datenschutzbeauftragten gemeldet. Selbst wenn die Verletzung zu keinem Risiko für die Betroffenen geführt hat.
Dieser informiert die Geschäftsführung, meldet den Vorfall der Datenschutzbehörde unverzüglich und möglichst binnen 72 Stunden und setzt alle Maßnahmen zur Behebung der Verletzung und gegeben Falls Maßnahmen zur Abmilderung ihrer nachteiligen Auswirkungen.

Jede Verletzung des Schutzes personenbezogener Daten wird ausnahmslos im Datenverarbeitungsverzeichnis dokumentiert, auch wenn die Verletzung zu keinem Risiko für die Betroffenen geführt hat. Die Dokumentation muss alle Fakten in Zusammenhang mit der Sicherheitsverletzung, die Auswirkungen und die ergriffenen Abhilfemaßnahmen erfassen.

Wir definieren folgenden Prozess/Fristen für die Löschung von Daten
Die Löschung der Daten erfolgt nur in Absprache mit dem Datenschutzbeauftragten. Sollte ein Kunde/Lieferant die Löschung seiner Daten wünsche. Muss der Prozess „bei Datenschutzanfragen" eingehalten werden. Auch wenn der Kunde die Löschung der Daten fordert, gibt es gesetzliche Vorgaben, wonach wir verpflichtet sind die Daten aufzubewahren. Folgende Fristen sind für unser Unternehmen unter anderem relevant:

<u>Rechnungswesen/Steuer/Zollrecht</u>

- Steuerrechtliche Aufbewahrungspflicht nach § 132 Abs 1 BAO: 7 Jahre
- Unternehmensrechtliche Aufbewahrungspflicht nach §§ 190, 212 UGB: 7 Jahre
- Umsatzsteuerrechtliche Aufbewahrungspflichten für Aufzeichnungen und Unterlagen betreffend Grundstücke nach § 18 Abs 10 UStG: 22 Jahre
- Umsatzsteuerrechtliche Aufbewahrungspflicht für Rechnungen nach § 11 Abs 2 Unterabsatz UStG: 7 Jahre
- Umsatzsteuerrechtliche Aufbewahrungspflichten für Ausfuhrbelege nach § 7 Abs 7 UStG: 7 Jahre
- Aufzeichnungen nach § 23 Abs 2Zollrechts-Durchführungsgesetz: 5 Jahre

<u>Vertragswesen</u>

- Gewährleistung nach § 933 ABGB: 2 Jahre (bewegliche Sachen)
- Kaufpreisforderung bei beweglichen Sachen nach § 1062 iVm § 1486 ABGB: 3 Jahre

<u>Arbeitsverhältnisse</u>

- Ansprüche auf Ersatz wegen diskriminierender Ablehnung einer Bewerbung nach §§ 15 Abs 1 und 29 Abs 1 GlbG sowie § 7k Abs 1 iVm Abs 2 Z 1 BEinstG: 6 Monate
- Daten betreffend Lohnsteuer- und Abgabenpflicht nach § 132 Abs 1 BAO: 7 Jahre

Diese genannten Fristen bilden die Grundlage, wonach Istac verpflichtet ist, die Daten seiner Kunden, Lieferanten und anderen Stakeholdern zu speichern. Da Istac mit allen Kunden in eine Vertragsbeziehung eintritt, müssen diese Daten 7 Jahre gespeichert werden. Nach Ablauf der Frist müssen diese dann unwiderruflich aus dem System gelöscht oder anonymisiert werden. Wird nun eine Anfrage zur Löschung der Daten an Istac übermittelt, ist vor der Löschung die Überprüfung notwendig, ob ein gesetzlicher Grund zur Speicherung vorliegt. Ist dies der Fall muss der Kunde über die gesetzliche Notwendigkeit informiert werden. Liegt kein gesetzlicher Grund vor, müssen die Daten innerhalb der gesetzlichen Frist gelöscht werden.

Der Datenschutzbeauftragte ermittelt am Jahresende die zu löschenden Daten und klärt mit der Geschäftsführung und den Kundenbetreuern ab, ob eventuell noch aufrechte Kundenbeziehungen zugrunde liegen. Ist dies der Fall, wird von den Kunden eine schriftliche Einverständniserklärung eingeholt, dass die Daten noch weiterhin gespeichert werden dürfen. Liegt keine aufrechte Geschäftsbeziehung zugrunde, werden die Daten unwiderruflich gelöscht.

Die Ausnahme bilden Daten aus Bewerbungsprozessen. Diese werden nach Ablauf der 6-monatigen Frist während des Jahres von der zuständigen Führungskraft, nach Absprache mit dem Datenschutzbeauftragten gelöscht.

Audit

Der Datenschutzbeauftragte führt jährlich Audits zur Sicherstellung der Effektivität der DSGVO-Compliance durch. Die Ergebnisse werden dokumentiert und in einem Meeting der Geschäftsführung präsentiert. Im Anschluss werden die gewonnenen Erkenntnisse diskutiert und die weiteren Schritte definiert.

Schulungen

Datenschutzbeauftragter

Der Datenschutzbeauftragte informiert sich proaktiv über die neuesten Vorschriften zum Thema Datenschutz. Nach drei Jahren werden alle nötigen Schritte zur Rezertifizierung des Datenschutzbeauftragten gesetzt.

Mitarbeiter

Der Datenschutzbeauftragte schult jährlich alle Mitarbeiter zum Thema Datenschutz und steht den Mitarbeitern jederzeit für Fragen zur Verfügung.

Sichere Entsorgung von personenbezogenen Daten

Um die sichere und unwiderrufliche Vernichtung von vertraulichen Unterlagen und Datenträger zu gewährleisten, wird der Service von Reisswolf Österreich GmbH in Anspruch genommen. Die Reisswolf Österreich GmbH stellt einen Sicherheitsbehälter zur Verfügung, in welchen alle vertraulichen Unterlagen und Datenträger gesammelt werden. Der Sicherheitsbehälter wird quartalsweise oder nach telefonischem Aviso von Reisswolf Österreich abgeholt und der Inhalt unwiderruflich vernichtet.

Jeder Mitarbeiter ist dafür verantwortlich, dass die von ihm zu vernichtenden Dokumente mit personenbezogenen Daten, täglich in den Sicherheitsbehälter der Firma Reisswolf Österreich abgelegt werden. Der Sicherheitsbehälter ist im Lagereingangsbereich aufgestellt.

Informationssicherheit

Neben der Einhaltung der DSGVO zum Schutz personenbezogener Daten, ist auch die Informationssicherheit zum Schutz jeglicher Daten zu beachten. Folgende Punkte werden definiert und sind im Unternehmensalltag zu berücksichtigen:

E-Mail-Nutzung

- Öffnen sie keine E-Mails und Dateianhänge, wenn Ihnen Absender oder Betreffzeile verdächtig erscheinen
- Auch bei vermeintlich bekannten und vertrauenswürdigen Absendern ist zu prüfen:
  - Passt der Text der E-Mail zum Absender
  - Erwarten Sie die beigelegten Dateien
- Sogenannte Phishing-Mails, die zur Übermittlung von persönlichen Online-Banking-Daten oder Passwörtern auffordern, müssen gelöscht werden
- Oftmals kann in einem E-Mail ein Link angeklickt werden, um eine Webseite aufzurufen. Seien Sie dabei vorsichtig, in betrügerischen E-Mails wird diesen Links oft eine völlig andere Internet-Adresse hinterlegt, als im Mail zu sehen ist.
- Beantworten Sie keine Spam-Mails
- Benachrichtigen sie auch Ihre Kollegen über verdächtige Zusendungen!

Internetnutzung

- Die private Internetnutzung ist laut der von Ihnen unterzeichneten Geheimhaltungs-vereinbarung verboten!
- Übermitteln Sie keine persönlichen Daten, vor allem nicht, wenn die Verbindung nicht als sicher (HTTPS) markiert wird.
- Laden Sie keine Daten herunter, dies kann neben das Einschleppen einer Schadsoftware auch zu lizenz- und urheberrechtlichen Problemen führen.

istac

Verschlüsselte Kommunikation

- Bitte achten Sie auf eine verschlüsselte Kommunikation. Ihr Browser signalisiert dies mit einem Schloss. Alle übermittelten Daten sind demnach verschlüsselt.
- Eine E-Mail stellt KEINE sichere Kommunikation dar.

Social Media

- Posten Sie keine Fotos von Ihrem Arbeitsplatz
- Posten Sie keine Statusinformationen, die das Unternehmen betreffen

Clear Desk Policy

- Verschließen Sie alle vertraulichen Dokumente, die sich auf dem Arbeitsplatz befinden
- Bei Verlassen des Arbeitsplatzes:
    - alle Ausdrucke, Kopien usw. so verstauen, dass diese Dokumente nicht für Dritte zugänglich sind
    - sperren Sie Ihren Computer (z.B.: „Windows Taste + L")
- Lassen Sie keine Ausdrucke im Drucker/Kopierer liegen
- Bewahren Sie unter keinen Umständen Passwortnotizen an Ihrem Arbeitsplatz auf.
- Begleiten Sie Besucher innerhalb des Firmengebäudes, damit diese keine Zugriffe auf Daten erhalten

Persönliche Passwörter

- Verwenden Sie niemals:
    - das gleiche Passwort für unterschiedliche Zugänge
    - Namen, Vornamen, Geburtsdaten, Tel.-Durchwahlen, etc.
    - Begriffe aus einem Wörterbuch (auch nicht in einer anderen Sprache). Es gibt Programme, die Wortlisten mit mehreren tausend Begriffen sofort abrufen und so mögliche Passwörter finden.
    - Trivial-Passwörter (hallohallo, abcdefgh, 08/15, 1234 etc.)
- Geben Sie Ihr Passwort niemanden weiter
    - Bei Urlaub nutzen Sie die E-Mail-Weiterleitungs-Funktion oder die Postfach-Freigabe-Funktion
- Verwenden Sie Kennwörter, die mindestens 8 Zeichen haben. Ein Passwort muss aus einem Großbuchstaben, Kleinbuchstaben, Ziffer und einem Sonderzeichen bestehen
    - Ändern Sie Ihr Kennwort in regemäßigen Abständen (mind. alle 180 Tage)
- Sie sind für Ihr Kennwort verantwortlich! Sollten Sie den Verdacht haben, dass ein Dritter Ihr Kennwort kennt, ändern sie dieses sofort.

Umgang mit mobilen IT-Geräten

- Mobile IT-Geräte (Notebooks, Smartphones…) stellen durch ihre mobile Verwendung ein erhöhtes Sicherheitsrisiko dar
- Bitte beachten Sie folgende Punkte:
  - Lassen Sie das Gerät nicht unbeaufsichtigt
  - Überlassen Sie das Gerät nicht anderen Personen
  - Achten Sie bei Passworteingabe am Gerät auf Ihren Sichtschutz
  - Verwenden Sie Ihren privaten Cloud-Speicher nicht für Unternehmensdaten
  - Installieren Sie keine Anwendungen –setzten Sie sich mit unserem IT-Partner in Verbindung
  - Melden Sie einen Diebstahl oder Verlust sofort der Geschäftsführung und dem Datenschutzbeauftragten

Beratung & Berichterstattung für Mitarbeiter

Bei Istac wird eine offene und ehrliche Kommunikation zwischen allen Mitarbeitern geschätzt und respektiert. Engagement für die DSGVO und Informationssicherheit bedeutet, dass jeder einzelne Verantwortung trägt, potenzielle oder tatsächliche Verstöße gegen diese Politik offen anzusprechen. Um eine mögliche Verletzung dieser Risiken anonym zu melden ist eine Kontaktaufnahme mit unserem Mitarbeiteranwalt per E-Mail m.guetlbauer@guetlbauer-partner.at oder telefonisch unter 07242/47541 jederzeit möglich. Die Kontaktdaten finden Sie auch jederzeit am „Schwarzen Brett". Dieser ist verpflichtet, alle ihm gemeldeten Vorfälle mit der Geschäftsführung zu thematisieren damit diese umgehend entsprechende Korrekturmaßnahmen ergreifen kann.

Kirchberg-Thening, April 2021

Klaus Pohn
Geschäftsführer

Jürgen Prunk
Geschäftsführer

Appendix

Ziele unserer Politik hinsichtlich Einhaltung der DSGVO & Informationssicherheit

Anzahl der gemeldeten Verletzungen des Schutzes personenbezogener Daten	0
Anzahl der durchgeführten Audits pro Jahr	1
Anzahl der durchgeführten Mitarbeiterschulungen zum Thema DSGVO & Informationssicherheit pro Jahr	1
Anzahl gemeldeter Verstöße gegen die Informationssicherheit	0

Erfolgreiche Ausbildung zum Datenschutzbeauftragten

AUSTRIAN STANDARDS

ZERTIFIKAT

Nr.: P 006367

Die Austrian Standards plus GmbH (Zertifizierungsstelle gemäß ISO/IEC 17024) stellt dieses Zertifikat aus.

Zertifikatsinhaber:	Herr Jakob Kupfer, MSc 1992-09-22
Bezugsdokument(e):	AS+C Zertschema P43:2020-01-01 *Datenschutzbeauftragte/r* Dieses Zertifikat bestätigt die Kompetenz der zertifizierten Person gemäß der Anforderungen des Bezugsdokumentes.
Kompetenzprofil:	Personen, die gemäß diesem Zertifizierungsschema zertifiziert sind, sind in der Lage, die Aufgaben eines Datenschutzbeauftragten nach Art 39 DSGVO wahrzunehmen und kennen die Grundlagen der Informationssicherheit gem. Art 32 DSGVO. Sie sind in der Lage, Personen oder Organisationen hinsichtlich ihrer Pflichten nach der DSGVO und den österreichischen Datenschutzvorschriften zu beraten. Sie sind kompetent, die Einhaltung der geltenden Datenschutzvorschriften zum Schutz personenbezogener Daten zu überwachen und zu koordinieren. Weiters sind sie in der Lage, bei Datenschutz-Folgenabschätzungen gem. Art 35 DSGVO zu beraten und ihre Durchführung zu überwachen. Sie sind kompetent, mit Aufsichtsbehörden im Bereich Datenschutz zusammenzuarbeiten und als Anlaufstelle für die Aufsichtsbehörde zu fungieren sowie Beratung zu allen sonstigen Fragen in Bezug auf Datenschutz an betroffene Personen zu leisten.
Konformitätszeichen:	Dieses Zertifikat berechtigt zur Führung des Konformitätszeichens:
Ausstellungsdatum:	2020-05-14
Erstaustellungsdatum:	2020-05-14
Ablaufdatum:	2023-05-14

CERTIFIED BY AUSTRIAN STANDARDS

Dr. Peter Jonas
Director Certification

Datenverarbeitungsverzeichnis

Das Datenverarbeitungsverzeichnis wurde vom Datenschutzbeauftragten wie gesetzlich vorgeschrieben erstellt. Das Verarbeitungsverzeichnis besteht aus einem Stammdatenblatt und dem Datenverarbeitungsverzeichnis. Darüber hinaus werden noch alle Datenschutzanfragen und etwaige Verletzungen der Datensicherheit dokumentiert.
Das Datenverarbeitungsverzeichnis erfasst alle Verarbeitungsschritte von personenbezogenen Daten. Dabei werde folgende Informationen je Verarbeitungsschritt dokumentiert:

- Verarbeitung
- Verarbeitungszweck
- Kategorie personenbezogener Daten
- die Rechtsgrundlage zur Datenverarbeitung
- die Aufbewahrungsfristen
- Datenübermittlungsempfänger
- die getroffenen Sicherheitsmaßnahmen zum Schutz der personenbezogenen Daten

Das Datenverarbeitungsverzeichnis darf aus datenschutzrechtlichen Gründen in diesem Dokument nicht abgebildet werden. Nachstehend werden die einzelnen erhobenen Punkte kurz erläutert. Bei weiteren Fragen steht der Datenschutzbeauftragte Herr Kupfer(jkupfer@istac.at) jederzeit zur Verfügung.

Verarbeitung
Hier wird der Prozess, in welchem Zusammenhang die Daten verarbeitet werden definiert. Werden die Daten beispielsweise im Rahmen eines Rekrutierungsprozesses erhoben, würde in diese Rubrik Bewerbungsprozess eingetragen werden.

Verarbeitungszweck
Bei Verarbeitungszweck wird der eigentliche Grund der Verarbeitung festgehalten. Beim Beispiel des Rekrutierungsprozesses würden unter anderem die Zwecke „Kontaktaufnahmen mit Bewerber“ oder „Sichtung der eingehenden Bewerbungen“ dokumentiert werden.

Kategorie personenbezogener Daten
Unter dieser Rubrik erfolgt die abstrakte Beschreibung der einzelnen verarbeiteten Daten, wie zum Beispiel: Telefonnummer, Name, Adresse

Rechtsgrundlage zur Datenverarbeitung
Bei der Rechtsgrundlage muss genau festgehalten werden, wieso das Unternehmen, in diesem Fall Istac berechtigt ist, die Daten zu verarbeiten. Beim Bewerbungsprozess wäre das beispielsweise die Vertragsanbahnung.

Aufbewahrungsfristen
Eine der wesentlichen Rubriken im Datenverarbeitungsverzeichnis betrifft die Aufbewahrungsfristen. In dieser muss genau definiert werden, wie lange die personenbezogenen Daten im System gespeichert werden. Nach Ablauf der Frist müssen diese dann unwiderruflich aus dem System gelöscht oder anonymisiert werden. Die genauen Fristen und der Prozess der Löschung werden in der Politik zur Datenschutzgrundverordnung definiert.

Datenübermittlungsempfänger
Hier müssen alle Empfänger genannt werden, denen die Daten übermittelt werden.

Sicherheitsmaßnahmen zum Schutz der personenbezogenen Daten
In dieser abschließenden Rubrik müssen alle Sicherheitsmaßnahmen zum Schutz der Daten benannt werden.

Datenverarbeitungsverzeichnis

nach Art 30 Abs 1 EU-Datenschutzgrundverordnung (DSGVO)

Istac Promotion GmbH

Inhalt

Klicken Sie hier, um D

Maßnahmen zum Schutz von personenbezogenen Daten

Der 6. Grundsatz der DSGVO betrifft die Integrität und Vertraulichkeit im Umgang mit personenbezogenen Daten. Die personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Durch geeignete technische und organisatorische Maßnahmen muss der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust oder unbeabsichtigter Zerstörung/Schädigung gewährleistet werden.

Um diesen Grundsatz zu erfüllen, hat Istac folgende Maßnahmen gesetzt:

- Auftrags-Verarbeiter Verträge
- DSGVO konforme Vernichtung durch Reisswolf Österreich
- Maßnahmen der Politik zur Informationssicherheit
- Nutzung des Service von Conova Communications GmbH

Auftrags-Verarbeiter Verträge

Die erhobenen Daten werden nicht nur im eigenen Unternehmen gespeichert, sondern auch an Dienstleister zur Verarbeitung weitergegeben. Um sicherzustellen, dass diese die Daten schützen und die Grundsätze der DSGVO verfolgen, hat Istac Auftrags-Verarbeiter Verträge mit den wichtigsten Dienstleistern abgeschlossen.

Mit folgenden Dienstleitern wurden Auftrags-Verarbeiter Verträge abgeschlossen:

- Post AG
- Asseco Solutions AG
- UPS
- Reisswolf Österreich GmbH
- Hobex AG
- PayPal AG
- Consens (Zeiterfassung)
- Hokify GmbH

Auftragsverarbeiter Verträge (Auswahl)

CONSENS ZEITERFASSUNG GMBH

ZEITERFASSUNG • EINFACH • FUNKTIONELL

Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:	Der Auftragsverarbeiter:
ISTAC Service GmbH	**Consens Zeiterfassung GMBH**
Industriepark 20	Ambachweg 1
4061 Pasching	A-6421 Rietz
(im Folgenden Auftraggeber)	(im Folgenden Auftragnehmer)

1. Gegenstand der Vereinbarung

(1) Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben:
Remotesupport / Fernwartung

CONSENS Zeiterfassung GmbH
A-6421 Rietz, Ambachweg 1
Tel: +43 (0) 5262 62 437
Fax: +43 (0) 5262 62 437 - 20
verkauf@consens.co.at • www.consens.a

UID-Nr. ATU 38676900 • HRB: FN 133 101M
Bankverbindung: Sparkasse Tirol BLZ 20503 Konto 00800-004723
BIC: SPIHAT22 IBAN: AT 06 20503 00800004723

Diese Vereinbarung ist als Ergänzung zum bestehenden Wartungsvertrag zu verstehen und gilt nur in Kombination mit selbigen. Mit Kündigung des Wartungsvertrages erlischt auch die Gültigkeit dieser Vereinbarung.

(2) Folgende Datenkategorien werden verarbeitet: Mitarbeiterspezifische Daten im Rahmen der Zeiterfassung des Verantwortlichen zum Zweck der Wartung und Betreuung.

(3) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: Mitarbeiter des Verantwortlichen bzw. Personen, die vom Verantwortlichen im Rahmen der Zeiterfassung verwaltet werden.

2. Dauer der Vereinbarung

Die Vereinbarung ist an einen aufrechten Wartungsvertrag gebunden und erlischt mit dessen Kündigung. Kündigungsmöglichkeit für den Wartungsvertrag sind für Auftraggeber sowie Auftragnehmer drei Monate zum jeweiligen Stichtag

3. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung

beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage ./1 zu entnehmen).

(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(6) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format

verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

(9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. Ort der Durchführung der Datenverarbeitung

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

5. Sub-Auftragsverarbeiter

Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

Der Auftragnehmer kann Sub-Auftragsverarbeiter für erweiterte Hilfestellung hinzuziehen.

Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

PASCHING, am 15.10.2020

Für den Auftraggeber:

istac service gmbh
Industriepark 20 | A-4061 Pasching
Tel. +43 (0)7221 637 60 | ATU 72670503

.....

[Name samt Funktion]

JAKOB KUPFER
DATENSCHUTZBEAUFTRAGTER

Rietz, am 15.10.2020

Für den Auftragnehmer:

.....

Andreas Neurauter, Geschäftsführer

VEREINBARUNG ÜBER EINE AUFTRAGSVERARBEITUNG nach Art 28 DSGVO

1. Gegenstand der Vereinbarung

a) Die Österreichische Post AG (Post) stellt für die Versandvorbereitung durch die Kunden (Verantwortlicher) / dessen Erfüllungsgehilfen den Post-Labelcenter (PLC) zur Verfügung.
Bei Verwendung dieses Versandsystems durch die Kunden / dessen Erfüllungsgehilfen tritt die Post als datenschutzrechtlicher Auftragsverarbeiter auf.

b) Verarbeitet werden Kategorien personenbezogener Daten und Kategorien betroffener Personen gemäß Anlage 1.

2. Pflichten des Auftragsverarbeiters

a) Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der Versandaufträge des Verantwortlichen zu verarbeiten.

b) Der Auftragsverarbeiter ist nicht befugt, personenbezogene Daten des Verantwortlichen ohne dessen schriftliche Einwilligung Dritten offenzulegen.

c) Soweit der Auftragsverarbeiter dazu aufgrund gesetzlicher Bestimmungen verpflichtet ist, hat er den Verantwortlichen unverzüglich im Vorhinein zu informieren.

d) Die Übermittlung von personenbezogenen Daten an Dritte, zu der keine gesetzliche Verpflichtung des Auftragsverarbeiters besteht, setzt einen schriftlichen (E-Mail ausreichend) Auftrag des Verantwortlichen voraus.

e) Eine Verarbeitung der personenbezogenen Daten für eigene Zwecke des Auftragsverarbeiters darf nur nach vorherigem schriftlichem (E-Mail ausreichend) Einverständnis des Verantwortlichen erfolgen.

f) Der Auftragsverarbeiter verpflichtet sich zur Wahrung des Datengeheimnisses und erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen.
Er hat alle mit der Datenverarbeitung betrauten Personen verpflichtet, personenbezogene Daten, die diesen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut oder zugänglich werden, unbeschadet sonstiger gesetzlicher Verschwiegenheitsverpflichtungen, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung/Bekanntgabe der Daten besteht.
Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht.

g) Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat.
Der Auftragsverarbeiter sichert zu, die in Anlage 2 beschriebenen und ausgewählten, dem Risiko angemessenen, technischen und organisatorischen Maßnahmen ergriffen zu haben und auch in Zukunft zu ergreifen, um die personenbezogenen Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust zu schützen, um ihre ordnungsgemäße Verarbeitung und die Nichtzugänglichkeit für unbefugte Dritte sicherzustellen. Der Auftragsverarbeiter verpflichtet sich dazu, die technischen und organisatorischen Maßnahmen in obigem Sinne auf dem Stand der Technik zu halten und nach technischem Fortschritt bzw. geänderter Bedrohungslage zu aktualisieren bzw. anzupassen.

h) Der Auftragsverarbeiter stellt sicher, dass der Verantwortliche die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch sowie automatisierte Entscheidungsfindung im Einzelfall) und unter Berücksichtigung des österreichischen Bundesgesetzes zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DSG idgF) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann, überlässt dem Verantwortlichen alle dafür notwendigen Informationen und unterstützt diesen bei der Erfüllung diesbezüglicher Pflichten nach besten Kräften.
Wird ein entsprechender Antrag, mit dem Betroffenenrechte geltend gemacht werden, an den Auftragsverarbeiter gerichtet und ist aus dem Inhalt des Antrages ersichtlich, dass der

Antragsteller den Auftragsverarbeiter irrtümlich für den Verantwortlichen der von ihm für den Verantwortlichen durchgeführten Verarbeitungstätigkeit hält, hat der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiterzuleiten und dies dem Antragsteller unter Bekanntgabe des Datums des Einlangens des Antrages mitzuteilen.

i) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation) nach besten Kräften.

j) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.
Über Ersuchen des Verantwortlichen wird diesem im Einzelfall auch die Erklärung über die Wahrung des Datengeheimnisses hinsichtlich jener Personen vorgelegt, die mit der Durchführung des Auftrags betraut sind.

k) Dem Verantwortlichen wird hinsichtlich der Verarbeitung der von ihm überlassenen personenbezogenen Daten das Recht eingeräumt, selbst durch qualifizierte und zur Geheimhaltung verpflichtete Mitarbeiter oder durch eine zur Berufsverschwiegenheit verpflichtete Person (gerichtlich zertifizierter Sachverständiger etc.) beim Auftragsverarbeiter die Ordnungsgemäßheit der Datenverarbeitung nach vorheriger Ankündigung von mindestens 30 Werktagen (ausgenommen Samstag) auf eigene Kosten zu überprüfen. Dies während der büroüblichen Zeiten und in Abstimmung mit dem Datenschutzbeauftragten des Auftragsverarbeiters oder einer sonst für den Datenschutz verantwortlichen Person.

l) Der Auftragsverarbeiter ist nach Beendigung des Auftrags verpflichtet, dem Verantwortlichen alle Verarbeitungsergebnisse und Unterlagen, die vertragsgegenständliche personenbezogene Daten enthalten, zu übergeben; davon unberührt bleibt die Speicherung der dem Auftragsverarbeiter überlassenen personenbezogenen Daten und Verarbeitungsergebnisse soweit und solange dieser für seine Leistungen Gewähr zu leisten hat.
Nach Ablauf der Gewährleistungsfrist hat der Auftragsverarbeiter sämtliche vertragsgegenständliche personenbezogene Daten zu löschen oder diese nach Aufforderung des Verantwortlichen vor Durchführung der Löschung sicher zu verwahren. Dies gilt insbesondere, soweit der Auftragsverarbeiter zu einer weiteren Aufbewahrung von personenbezogenen Daten nicht aufgrund zwingender gesetzlicher Bestimmungen verpflichtet ist.
Über Ersuchen des Verantwortlichen bestätigt der Auftragsverarbeiter die Datenlöschung schriftlich.
Wenn der Auftragsverarbeiter die personenbezogenen Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die personenbezogenen Daten nach Beendigung des Auftrags entweder in diesem Format oder nach Wunsch des Auftragsverarbeiters in dem Format, in dem er die personenbezogenen Daten vom Verantwortlichen erhalten hat oder in einem anderen gängigen Format herauszugeben.

m) Die Haftung richtet sich nach gesetzlichen Vorschriften und allfälligen datenschutzrechtlichen Haftungsbestimmungen der Hauptleistungsvereinbarung.
Sie ist mit der Höhe eines einjährigen Auftragsvolumens der Hauptleistungsvereinbarung gemäß Punkt 1a) begrenzt, sofern darin oder gesetzlich keine für den Auftragsverarbeiter günstigere Regelung besteht.

3. Sub-Auftragsverarbeiter

a) Der Auftragsverarbeiter kann Sub-Auftragsverarbeiter heranziehen. Er hat den Verantwortlichen von der beabsichtigten Heranziehung so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann.
Nicht hierzu gehören Nebendienstleistungen, die der Auftragsverarbeiter z.B. als Post-/Transport-/Telekommunikationsdienstleistungen oder zur Wartung/ Servicierung von Datenträgern und Datenverarbeitungsanlagen in Anspruch nimmt.

b) Der Auftragsverarbeiter schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass

der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragsverarbeiter auf Grund dieser Vereinbarung obliegen. Die Überbindung der Verpflichtungen ist dem Verantwortlichen über Aufforderung nachzuweisen.

c) Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

d) Der Verantwortliche erteilt seine Zustimmung zur Heranziehung der in Anlage 3 genannten Sub- Auftragsverarbeiter.

4. Dauer der Vereinbarung

Die Laufzeit der Vereinbarung richtet sich nach der Nutzung des Versandsystems lt. Punkt 1). Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von drei Monaten zum Monatslende schriftlich gekündigt werden. Die Möglichkeit zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

5. Sonstige Bestimmungen

a) Sämtliche Streitigkeiten aus und im Zusammenhang mit diesem Vertrag unterliegen österreichischem Recht, unter Ausschluss des UN-Kaufrechts und kollisionsrechtlicher Bestimmungen. Für sämtliche Streitigkeiten wird das für 1030 Wien sachlich und örtlich zuständige Gericht vereinbart.

b) Verbindlich ist nur, was schriftlich vereinbart ist; es bestehen keine mündlichen Nebenabreden. Änderungen und Ergänzungen der Vereinbarung bedürfen zu ihrer Gültigkeit der Schriftform; dies gilt auch für ein Abgehen vom Formerfordernis der Schriftlichkeit.

c) Sämtliche Rechte und Pflichten aus dieser Vereinbarung gehen auf allfällige Rechtsnachfolger beider Vertragsparteien über.

d) Die Parteien vereinbaren, den Abschluss dieser Vereinbarung und deren Inhalt vertraulich zu behandeln. Dies gilt, insoweit die gegenständliche Vereinbarung keine entgegenstehenden Bestimmungen enthält und keine gesetzlichen Auskunftspflichten bestehen.

e) Der Verantwortliche verpflichtet sich, (i) dass sich seine gesetzlichen Vertreter, Mitarbeiter und eingesetzte und/oder beauftragte Subunternehmer an sämtliche geltenden gesetzlichen Bestimmungen im Zusammenhang mit Anti-Korruptionsvorschriften halten sowie (ii) geeignete Maßnahmen zu setzen, um die Einhaltung der Anti-Korruptionsvorschriften sicherzustellen. Ein Verstoß gegen Anti-Korruptionsvorschriften berechtigt den Auftragsverarbeiter – unbeschadet sonstiger Rücktritts- und Kündigungsrechte – zur fristlosen außerordentlichen Kündigung der Vereinbarung sowie zur Geltendmachung allfälliger Schadenersatzansprüche.

f) Sollten einzelne Bestimmungen der Vereinbarung ungültig oder unwirksam sein oder werden, so werden die Vertragsparteien einvernehmlich eine gültige bzw. wirksame Bestimmung festlegen, die den ungültigen bzw. unwirksamen Bestimmungen wirtschaftlich am nächsten kommt.
Die Ungültigkeit oder Unwirksamkeit einzelner Bestimmungen hat keine Auswirkung auf die Gültigkeit bzw. Wirksamkeit des gesamten Vertrages.

g) Die Anlagen 1, 2 und 3 gelten als integrierte Bestandteile des Vertrages.

Anlage 1- Kategorien personenbezogener Daten und betroffener Personen

a) Folgende Kategorien personenbezogener Daten werden verarbeitet

x Personenstammdaten (Vor- und Nachname)

x Kontaktdaten (Telefonnummer, E-Mail-Adresse, Fax)

x Adressdaten (postalische Anschrift)

b) Zu folgenden Kategorien betroffener Personen werden personenbezogene Daten verarbeitet

x Kunden

Anlage 2 - Technisch - organisatorische Maßnahmen
(Alle zu treffenden Maßnahmen sind konkret zu bestimmen, daher wurde Zutreffendes vom Auftragsverarbeiter angekreuzt)

1) VERTRAULICHKEIT

Zutrittskontrolle - Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen

☒ Alarmanlage	☒ Sicherheitspersonal
☒ Schlüsselregelung	☒ Videoüberwachung der Zugänge
☒ Sicherheitsschlösser	☒ Personenkontrolle beim Empfang
☒ Berechtigungsausweise	☒ Protokollierung Besucher

Zugangskontrolle - Schutz vor unbefugter Systembenutzung

☒ Rollenbasierte Zuordnung von Benutzerrechten	☒ Security Incident Management & Security Operation Center
☒ sichere Kennwörter/Passwortrichtlinie	☒ automatische Sperrmechanismen/Bildschirmsperre

Zugriffskontrolle - Schutz vor unbefugtem Lesen, Kopieren, Verändern od. Entfernen innerhalb des Systems

☒ Berechtigungskonzept „need to know-Basis"	☒ sichere Aufbewahrung von Datenträgern
☒ Protokollierung von Zugriffen	☒ Pseudonymisierung
☒ Verschlüsselung von Datenträgern	☒ Firewall
☒ Verwaltung der Rechte durch Systemadministratoren	☒ datenschutzkonforme Entsorgung der Datenträger und Protokollierung
☒ Klassifikationsschema für Daten	☒ Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
☒ VPN-Technologie	

2) INTEGRITÄT

Weitergabekontrolle - Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei Übermittlung

☒ verschlüsselte Datenübertragung	☒ Dokumentation der Datenempfänger
☒ sichere Transportbehältnisse	☒ Anti-Viren-Software
☒ Datenträgerverschlüsselung	☒ Übersicht über regelmäßige Abruf - und Übermittlungsvorgänge
☒ Intrusion-Detection-System	

Eingabekontrolle - Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

☒ Protokollierung	☒ Eingabevalidierung

☒ Dokumentenmanagement	

3) VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeitskontrolle - Schutz vor Zerstörung und Verlust von Daten

☒ Backup & Restore-Tests	☒ Feuer- und Rauchmeldeanlagen
☒ unterbrechungsfreie Stromversorgung	☒ Recovery-Konzept/Wiederaufbauplan
☒ Redundanzkonzepte/Notversorgungsplan	☒ Klimaanlage
☒ Löschungsfristen	☒ Meldewege und Notfallpläne

4) VERFAHREN ZUR ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

☒ Datenschutz-Management	☒ regelmäßige Mitarbeiterschulungen
☒ Sicherheitsmanagement	☒ Security Checks auf Infrastruktur- und Applikationsebene

5) SONSTIGE

☒ datenschutzfreundliche Voreinstellungen/ Techniken	☒ Weisungsrecht
☒ eindeutige Vertragsgestaltung	☒ formalisiertes Auftragsmanagement
☒ sorgfältige Auswahl von Dienstleistern	☒ Kontroll-/Auditrecht
☒ Prüfung und Dokumentation von Sicherheitsmaßnahmen	☒ physische/logische Trennung von Daten
☒ Verpflichtung auf Datengeheimnis (z. B.Mitarbeiter)	☒ Trennung von Produktiv- und Testsystem

Anlage 3 - Sub- Auftragsverarbeiter

Der Auftragsverarbeiter ist befugt, folgende Sub-Auftragsverarbeiter heranzuziehen:

Name	Adresse	Art der Tätigkeit
ondot solutions GmbH	Brown-Boveri-Straße 8/1, 2351 Wiener Neudorf	Software Entwicklung Kundensupport
SVISS GmbH | IT-Service Management Solutions	Industriestraße 24 – 2A A-7400 Oberwart	Kundensupport

Anlage 1 - Auftragsverarbeitung

Vertrag

zur Auftragsverarbeitung gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)[1]

Der AN verpflichtet sich gegenüber dem AG nach Maßgabe der folgenden Bestimmungen.

Präambel

Ab dem 25. Mai 2018 ist die DSGVO einzuhalten. Als europaweit unmittelbar anwendbares Gesetz regelt die DSGVO, im Besonderen im Artikel 28, die Pflichten des Auftragsverarbeiters. Diesbezügliche Regelungen werden auch im § 48 DSG in der Fassung des Datenschutz-Anpassungsgesetzes BGBL 120/2017 getroffen.

Teil 1 – Allgemeine Bestimmungen

1 Gegenstand und Dauer des Auftrags

Der Gegenstand und die Dauer des Auftrags ergeben sich jeweils aus den diesem Vertrag zur Auftragsverarbeitung zugrundeliegenden weiteren vertraglichen Vereinbarungen (Deckblatt Leistungsmodulvertrag samt den dort genannten Anlagen).

2 Umfang, Art und Zweck der Datenverarbeitung, die Datenarten und der Kreis der Betroffenen

Folgende Kategorien von Daten sind Gegenstand dieses Auftrags
(die maßgeblichen Kategorien von Daten sind vom AG anzukreuzen bzw. zu ergänzen):

- ☒ Adressdaten
- ☒ Bankverbindungsdaten
- ☐ Leistungsdaten
- ☒ Gesprächshistorie
- ☒ Mitarbeiterdaten
- ☐ Videoaufzeichnungen
- ☐ Nutzerkennungen
- ☐ Passwörter
- ☒ Bewerberdaten
- ☐ Gesundheitsdaten
- ☒ Telefonnummern
- ☒ Personenstammdaten
- ☒ Kontaktdaten
- ☒ Kontodaten
- ☒ Finanzdaten
- ☐ Transaktionsdaten
- ☒ Personalverwaltung
- ☐ Geburtsdaten
- ☐ Kreditkartendaten
- ☐ Reisebuchungsdaten
- ☒ Zahlungsdaten
- ☐ Hobbys
- ☐ Biometrische Daten
- ☒ Kundenstammdaten
- ☒ Vertragsdaten
- ☒ Abrechnungsdaten
- ☒ Angebotsdaten
- ☐ Auskünfte
- ☐ Qualifikationsdaten
- ☐ Arbeitszeitdaten
- ☐ Bilddaten
- ☒ E-Mails
- ☐ Personal- und Identifikationsnummern
- ☒ Mitarbeiterbewertungen
- ☐ Sozialversicherungsdaten
- ☒ Kommunikationsdaten

Sonstige:

Folgende Kreise von Betroffenen sind Gegenstand des Auftrags
(die maßgeblichen Kreise von Betroffenen sind vom AG anzukreuzen):

- ☒ Mitarbeiter
- ☒ Praktikanten
- ☐ Unterhaltsberechtigte
- ☒ Interessenten
- ☐ Makler
- ☐ Gesellschafter
- ☒ Kontaktpersonen
- ☐ Patienten
- ☐ Pensionisten
- ☒ Frühere Mitarbeiter
- ☐ Angehörige
- ☒ Lieferanten/Dienstleister
- ☐ Vermittler
- ☐ Geschädigte
- ☐ Pressevertreter
- ☐ Vertreter
- ☐ Auszubildende
- ☒ Bewerber
- ☒ Kunden
- ☐ Berater
- ☐ Mieter
- ☐ Zeugen
- ☐ Mandanten
- ☐ Besucher

Sonstige:

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

Teil 2 – Auftragsverarbeitung gemäß Art. 28 DSGVO

1 Weisungsgebundene Verarbeitung und Remonstrationspflicht

Der Auftragsverarbeiter darf personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Weisungen werden vom Verantwortlichen grundsätzlich in Textform (z.B. per E-Mail) erteilt. Soweit eine Weisung ausnahmsweise mündlich erfolgt, wird diese vom Verantwortlichen entsprechend in Textform (z.B. per E-Mail) bestätigt.

Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf hinweisen, wenn die Befolgung einer vom Verantwortlichen erteilten Weisung nach seiner Ansicht gegen die DSGVO oder eine andere Vorschrift über den Datenschutz verstößt (Remonstrationspflicht).

2 Vertraulichkeits- / Verschwiegenheitspflicht

Der Auftragsverarbeiter wird zur Durchführung des Vertrages nur Personen beschäftigen, die er zur Vertraulichkeit verpflichtet hat oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3 Sicherheit der Verarbeitung / Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Der Auftragsverarbeiter ergreift alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Artikel 32 DSGVO.

Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses Auftrags sind diese durch den Auftragsverarbeiter fortlaufend an die Anforderungen dieses Auftrags anzupassen und dem technischen Fortschritt entsprechend weiterzuentwickeln. Das Sicherheitsniveau der im Folgenden festgelegten technischen und organisatorischen Maßnahmen darf nicht unterschritten werden.

Der Auftragsverarbeiter verpflichtet sich, Änderungen der technischen und organisatorischen Maßnahmen, die einen wesentlichen Einfluss auf das gewährleistete Sicherheitsniveau haben, als Ergänzung der folgenden Maßnahmen schriftlich zu dokumentieren, was auch in einem elektronischen Format erfolgen kann, und dem Verantwortlichen zur Kenntnis zu geben.

Der Auftragsverarbeiter ergreift folgende Maßnahmen:

3.1 Pseudonymisierung

Personenbezogene Daten des Verantwortlichen können in einer Weise verarbeitet werden, sodass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die eine unbefugte Identifizierung der Betroffenen gewährleisten. Dies erfolgt wie folgt:

	Akten- und Datenträger-vernichtung	Physische Archivierung mit Funktionalität RWUM	Digitalisierung & REISSWOLF i.U.
• Verschlüsselung von Zusatzinformationen zur Identifikation	-	X	X
• Verwaltung und Dokumentation von differenzierten Berechtigungen auf die Zusatzinformationen zur Identifikation	-	X	X
• Autorisierungsprozess oder Genehmigungsroutinen für Berechtigungen zur Verarbeitung von Zusatzinformationen zur Identifikation	-	X	X
• Kopierschutz hinsichtlich Zusatzinformationen zur Identifikation	-	X	X
• Vier-Augen-Prinzip für Identifikation	-	-	X

3.2 Maßnahmen zur Verschlüsselung

	Akten- und Datenträger-vernichtung	Physische Archivierung mit Funktionalität RWAH	Digitalisierung & REISSWOLF f.i.t.
▪ Verschlüsselung von mobilen Endgeräten wie Laptops, Tablets, Smartphones	x	x	x
▪ Verschlüsselung von Dateien	x	x	x
▪ Verschlüsselung von Systemen/Anlagen	x	x	x
▪ Verschlüsselte Aufbewahrung von Passwörtern	x	x	x
▪ Gesicherte Datenweitergabe (z.B. SSL, FTPS, TLS)	x	x	x
▪ Gesichertes WLAN	x	x	x
▪ Sonstiges/Spezifizierung der o.g. Maßnahmen: **Gesicherte Datenverbindungen, VPN (intern/extern)**	x	x	x

3.3 Maßnahmen zur Sicherstellung von Vertraulichkeit

a. Zutrittskontrolle

	Akten- und Datenträger-vernichtung	Physische Archivierung mit Funktionalität RWAH	Digitalisierung & REISSWOLF f.i.t.
▪ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)	x	x	x
▪ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)	x	x	x
▪ Sicherheitstüren	x	x	x
▪ Zaunanlagen	x	x	x
▪ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe	x	x	x
▪ Alarmanlage	x	x	x
▪ Videoüberwachung	x	x	x
▪ Spezielle Schutzvorkehrungen des Serverraums	x	x	x
▪ Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern	x	x	x
▪ Nicht-reversible Vernichtung von Datenträgern	x	x	x
▪ Mitarbeiter- und Berechtigungsausweise	x	x	x
▪ Sperrbereiche	x	x	x
▪ Besucherregelung (bspw. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)	x	x	x

b. Zugangskontrolle

	Akten- und Datenträger-vernichtung	Physische Archivierung mit Funktionalität RWAH	Digitalisierung & REISSWOLF f.i.t.
▪ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk	x	x	x
▪ Autorisierungsprozess für Zugangsberechtigungen	x	x	x
▪ Begrenzung der befugten Benutzer	x	x	x
▪ Single Sign-On	x	-	-
▪ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)	x	x	x
▪ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff	x	x	x
▪ Personalisierte Chipkarten, Token, PIN-/TAN, etc.	x	x	x
▪ Protokollierung des Zugangs	x	x	x
▪ Zusätzlicher System-Log-In für bestimmte Anwendungen	x	x	x
▪ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)	x	x	x
▪ Firewall	x	x	x

c. Zugriffskontrolle

	Akten- und Datenträger-vernichtung	Physische Archivierung mit Funktionalität RWAH	Digitalisierung & REISSWOLF f.i.t.
▪ Verwaltung und Dokumentation von differenzierten Berechtigungen	x	x	x
▪ Auswertungen/Protokollierungen von Datenverarbeitungen	x	x	x
▪ Autorisierungsprozess für Berechtigungen	x	x	x
▪ Genehmigungsroutinen	x	x	x
▪ Profile/Rollen	x	x	x
▪ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops (etwa per Betriebssystem, Safe Guard Easy, PGP)	x	x	x
▪ „Mobile Device Management-System"	x	x	x
▪ Vier-Augen-Prinzip	x	x	x
▪ Funktionstrennung „Segregation of Duties"	x	x	x
▪ Fachkundige Akten- und Datenträgervernichtung gemäß ÖNORM S 2109	x	x	x
▪ Nicht-reversible Löschung von Datenträgern	x	x	x

3.4 Maßnahmen zur Sicherstellung von Integrität

	Akten- und Datenträger-vernichtung	Physische Archivierung mit Funktionalität RWAH	Digitalisierung & REISSWOLF f.i.t.
▪ Zugriffsrechte	x	x	x
▪ Systemseitige Protokollierungen	x	x	x
▪ Dokumenten Management System (DMS) mit Änderungshistorie	x	x	x
▪ Sicherheits-/Protokollierungssoftware	x	x	x
▪ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten	x	x	x
▪ Mehraugenprinzip	x	x	x
▪ Protokollierung von Datenübertragung oder Datentransport	x	x	x
▪ Protokollierung von lesenden Zugriffen	x	x	x
▪ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten	x	x	x

3.5 Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

	Akten- und Datenträger-vernichtung	Physische Archivierung mit Funktionalität RWAH	Digitalisierung & REISSWOLF f.i.t.
▪ Sicherheitskonzept für Software- und IT-Anwendungen	x	x	x
▪ Back-Up Verfahren	x	x	x
▪ Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)	x	x	x
▪ Gewährleistung der Datenspeicherung im gesicherten Netzwerk	x	x	x
▪ Bedarfsgerechtes Einspielen von Sicherheits-Updates	x	x	x
▪ Spiegeln von Festplatten	x	x	x
▪ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)	x	x	x
▪ Geeignete Archivierungsräumlichkeiten für Papierdokumente	x	x	x
▪ Brand- und/oder Löschwasserschutz des Serverraums	x	x	x
▪ Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten	x	x	x

▪ Klimatisierter Serverraum	x	x	x
▪ Virenschutz	x	x	x
▪ Firewall	x	x	x
▪ Notfallplan	x	x	-
▪ Erfolgreiche Notfallübungen (Brandschutz)	x	x	x
▪ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)	x	x	x

3.6 Maßnahmen zur Sicherstellung der Belastbarkeit

	Akten- und Datenträger-vernichtung	Physische Archivierung mit Funktionalität RWAM	Digitalisierung & REISSWOLF f.i.l.
▪ Notfallplan für Maschinenausfall	x	x	x
▪ Redundante Stromversorgung	x	x	x
▪ Ausreichende Kapazität von IT-Systemen und Anlagen	x	x	x
▪ Logistisch gesteuerter Prozess zur Verhinderung von Leistungsspitzen	x	x	x
▪ Redundante Systeme/ Anlagen	x	x	x
▪ Resilienz und Fehler-Management	x	x	x

3.7 Maßnahmen zur Gewährleistung der Wirksamkeitskontrolle

	Akten- und Datenträger-vernichtung	Physische Archivierung mit Funktionalität RWAM	Digitalisierung & REISSWOLF f.i.l.
▪ Verfahren für regelmäßige Kontrollen / Audits	x	x	x
▪ Penetrationstests	-	-	x
▪ Notfalltests (Brand)	x	x	x

3.8 „Weisungskontrolle/ Auftragskontrolle"

	Akten- und Datenträger-vernichtung	Physische Archivierung mit Funktionalität RWAM	Digitalisierung & REISSWOLF f.i.l.
▪ Vertrag zur Auftragsverarbeitung gem. Art. 28 Abs. 3 DSGVO mit Regelungen zu den Rechten und Pflichten des Auftragsverarbeiters und Verantwortlichen	x	x	x
▪ Prozess zur Erteilung und / oder Befolgung von Weisungen	x	x	x
▪ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern	x	x	x
▪ Kontrolle/ Überprüfung weisungsgebundener Auftragsdurchführung	x	x	x
▪ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer	x	x	x
▪ Verpflichtung der Mitarbeiter zur Vertraulichkeit	x	x	x
▪ Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen	x	x	x

4 Inanspruchnahme der Dienste weiterer Auftragsverarbeiter

Der Auftragsverarbeiter darf zur Vertragsdurchführung weitere Auftragsverarbeiter einsetzen. Der Verantwortliche stimmt einer etwaigen Einschaltung von weiteren Auftragsverarbeitern zu.

Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags, der schriftlich abzufassen ist, was auch in einem elektronischen Format erfolgen kann, oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in diesem Teil 2 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

5 Mitwirkungs- / Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung mit geeigneten technischen organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen (Berücksichtigung von Betroffenenrechten hinsichtlich der Gewährleistung von Transparenz; Recht auf Auskunft; Berichtigungsrecht; Recht auf Löschung („Vergessenwerden"); Recht auf Einschränkung der Verarbeitung; Mitteilungsrecht bei Berichtigung und Löschung sowie Einschränkung der Verarbeitung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; Rechte bei automatisierten Einzelfallentscheidungen).

6 Unterstützung zur Pflichterfüllung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten (Gewährleistung der Sicherheit der Verarbeitung; Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden; Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; Datenschutz-Folgenabschätzung; Vorherige Konsultation).

7 Löschung und Rückgabe personenbezogener Daten

Nach Abschluss der Erbringung der Verarbeitungsleistungen werden alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder gelöscht oder zurückgegeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

8 Pflichtennachweis und Unterstützung bei Überprüfungen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung. Er ermöglicht Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu ihrer Durchführung bei.

istac

hokify GmbH
Web: www.hokify.com
E-mail: info@hokify.com
Tel: +43 (0) 676 303 2269

hokify

Vereinbarung über eine Auftragsverarbeitung nach Art 28 DSGVO

Diese Vereinbarung zur Auftragsverarbeitung wird zwischen dem Unternehmen spezifiziert in folgender Tabelle (in Folge Verantwortlicher) und der hokify GmbH (in Folge hokify) als Auftragsverarbeiter geschlossen.

Verantwortlicher:

Firmenname	ISTAC PROMOTION GMBH
Straße	INDUSTRIEPARK 20
PLZ Ort	4061 PASCHING
Land	AUSTRIA

Auftragsverarbeiter:
hokify GmbH
Raimundgasse 3/21
1020 Wien
Austria

hokify GmbH
Web: www.hokify.com
E-mail: info@hokify.com
Tel: +43 (0) 676 303 2269

1. Anleitung

Diese Vereinbarung wurde von hokify vor-unterschrieben. Um diese Vereinbarung einzugehen müssen Sie folgende Schritte unternehmen:

a) Vereinbarung vervollständigen und unterschreiben
b) Die vollständige Vereinbarung an datenschutz@hokify.com übermitteln.

2. Gegenstand der Vereinbarung

a) Gegenstand

Der Gegenstand dieser Vereinbarung ist die Schaltung von Stelleninseraten und die Veröffentlichung von einem Unternehmensprofil auf der mobilen Job Plattform hokify.

b) Kategorien betroffener Personen:

- Mitarbeiter des Unternehmens des Verantwortlichen

b) Verarbeitete Datenkategorien:

- Email
- Passwort
- Geschlecht
- Name
- Telefonnummer
- Dienstort
- Bilder von Mitarbeitern und Unternehmen
- Videos von Mitarbeiter und Unternehmen
- Zitate von Mitarbeitern
- Positionsbeschreibungen von Mitarbeitern
- Ansprechpartner für das jeweilige Inserat inkl. Bild, Name und Position

3. Dauer der Vereinbarung

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von einem Monat zum Monatsende gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

hokify GmbH
Web: www.hokify.com
E-mail: info@hokify.com
Tel: +43 (0) 676 303 2269

4. Pflichten des Auftragsverarbeiters

a) Der Auftragsverarbeiter verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Verantwortlichen zu verarbeiten. Erhält der Auftragsverarbeiter einen behördlichen Auftrag, Daten des Verantwortlichen herauszugeben, so hat er - sofern gesetzlich zulässig - den Verantwortlichen unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragsverarbeiters eines schriftlichen Auftrages.

b) Der Auftragsverarbeiter erklärt, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht.

c) Der Auftragsverarbeiter erklärt, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (mehr unter Anlage 1).

d) Der Auftragsverarbeiter ergreift die technischen und organisatorischen Maßnahmen, damit der Verantwortliche die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Verantwortlichen alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragsverarbeiter gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Verantwortlicher der von ihm betriebenen Datenanwendung hält, hat der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiterzuleiten und dies dem Antragsteller mitzuteilen.

e) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgenabschätzung, vorherige Konsultation).
f) Der Auftragsverarbeiter wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

g) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

hokify GmbH
Web: www.hokify.com
E-mail: info@hokify.com
Tel: +43 (0) 676 303 2269

h) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Verantwortlichers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

5. Sub-Auftragsverarbeiter

Der Auftragsverarbeiter kann Sub-Auftragsverarbeiter hinzuziehen. Der Auftragsverarbeiter schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragsverarbeiter auf Grund dieser Vereinbarung obliegen.

Wien, am 23.04.2018

Für den Auftragsverarbeiter:

Karl Edlbauer
Geschäftsführer hokify GmbH

Daniel Laminger
Geschäftsführer hokify GmbH

Simon Tretter
Geschäftsführer hokify GmbH

Für den Verantwortlichen:

Vorname	JAKOB
Nachname	KUPFER
Ort	PASCHING
Datum	05.08.2020

hokify GmbH
Web: www.hokify.com
E-mail: info@hokify.com
Tel: +43 (0) 676 303 2269

Unterschrift	

Anlage 1 - Technisch-organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen wir bei hokify folgende technischen und organisatorischen Maßnahmen um ein dem Risiko angemessenes Schutzniveau für die uns anvertrauten Daten zu gewährleisten:

1. Zutrittskontrolle

Durch Zutrittskontrollen verwehren wir Unbefugten den Zutritt zu unseren Büroräumlichkeiten und damit zu unseren PCs und Laptops:

- Mit Sicherheitsschlüssel (EVVA) versperrte Außentüren
- Zur Dokumentation über die Schlüssel für diese Außentüren gibt es ein Schlüsselbuch
- Eigene Schlüssel nur für befugte und Datenschutz geschulte Mitarbeiter
- Für die Reinigung der Büroräumlichkeiten wird auf ein renommiertes Dienstleistungsunternehmen vertraut

Hinweis: In den Büroräumlichkeiten befinden sich keine Serveranlagen. Alle unsere Server werden bei Amazon in Frankfurt gehostet.

2. Zugangskontrolle und Zugriffskontrolle

Durch Zugangskontrollen verwehren wir Unbefugten Zugang zu unseren PCs/Laptops beziehungsweise zu unseren IT-Systemen:

- Zugang zu unseren IT-Systemen ist mit Benutzernamen und Passwörtern geschützt
- Zusätzlich vergibt der IT-Administrator die Benutzerrechte so, dass von den jeweiligen Benutzern nur die wirklich benötigten Daten eingesehen werden können (need to know Prinzip)
- Datenkritische Kommunikation wird über VPN Verbindung durchgeführt
- Es besteht eine Passwort-Policy und diese ist den Befugten auch bekannt. Passwörter sind in periodischen Abständen zu ändern. Es ist sichergestellt, dass alle

hokify GmbH
Web: www.hokify.com
E-mail: info@hokify.com
Tel: +43 (0) 676 303 2269

befugten Personen informiert sind, dass Passwörter sicher zu verwahren sind und nicht weitergegeben werden. Die befragten Personen sind informiert, dass einzigartige Passwörter, dh Passwörter, die vom Nutzer bei keinem anderen (insbesondere privaten) Systemen verwendet werden sollen.

- Alle Datenrelevanten Änderungen im IT-System werden protokolliert und aufgezeichnet
- Unsere IT-Systeme sind durch eine Firewall geschützt
- Wir verwenden modernste Verschlüsselungen (SSL mit 2048 Bits Verschlüsselung) für unsere IT-Systeme

3. Datenträgerkontrolle

Es soll sichergestellt werden, dass Datenträger, dh Speichermedien, Festplatten etc nur von berechtigten Personen verwendet werden können und ein Zugriff auf die Geräte von unbefugten Personen unterbleibt:

- Personenbezogene Daten werden bei Amazon auf Servern in einem Hochsicherheitsgebäude gespeichert
- Zusätzlich sind die Daten verschlüsselt
- Die PCs/Laptops selbst sind mit Benutzernamen und Passwörtern geschützt
- Unsere Daten laufen in der Cloud und sobald einem Benutzer die Berechtigung entzogen wird hat dieser keinen Zugriff mehr auf die Datencloud
- Es besteht die Weisung, dass Daten nicht auf mobilen Datenträgern gespeichert werden (USB-Sticks, Smartphones).
- Der Laptop/PC darf nur von befugten Personen verwendet und transportiert werden.

4. Speicherkontrolle

Es soll sichergestellt werden, dass nur befugte (zuständige) Personen die Möglichkeit haben, personenbezogene Daten zu verarbeiten und auf diese zuzugreifen, um diese zu manipulieren:

- Die personenbezogenen Daten sind nur von Berechtigten mit Passwort zugänglich.
- Zugriffe werden protokolliert (need to know).
- Die Daten werden überdies verschlüsselt abgelegt

5. Eingabekontrolle

Es wird - wenn mehrere Benutzer auf Systeme und personenbezogene Daten zugreifen können - mitprotokolliert, welcher Benutzer welche Daten zu welchem Zeitpunkt manipuliert hat. Diese Protokolle stehen der IT-Administration zur Verfügung und werden nur im Anlassfall (zB. bei technischen Beeinträchtigungen oder aus datenschutzrechtlichen Gründen) eingesehen. Dadurch soll die Nachvollziehbarkeit sichergestellt werden.

hokify GmbH
Web: www.hokify.com
E-mail: info@hokify.com
Tel: +43 (0) 676 303 2269

6. Übertragungskontrolle

Durch unsere Maßnahmen soll sichergestellt werden, dass Daten im Rahmen der Übertragung nur an berechtigte Empfänger übermittelt werden.

- Unser Email verschlüsselt Nachrichten und führt automatisch einen Virenscan durch

7. Wiederherstellung

Durch unsere Maßnahmen soll sichergestellt werden, dass die IT-Systeme nach einem Zwischenfall möglichst rasch – mit den personenbezogenen Daten – wiederhergestellt werden können:

- Es besteht eine Sicherung der Daten - tägliche Backups auf getrennten Servern
- IT-Administration ist in der Lage, die Sicherung zeitnahe einzuspielen; das Szenario wird in periodischen Abständen getestet

8. Zuverlässigkeit und Integrität

Durch unsere Maßnahmen wird so gut wie möglich sichergestellt, dass es durch Fehlfunktionen keine Beeinträchtigungen an den personenbezogenen Daten gibt.

- Es erfolgen die notwendigen Updates der Software und der sonstigen Programme.
- Es gibt einen ausreichend Schutz gegen Intrusion und Viren.
- Es gibt ein laufendes Monitoring des IT-Systems mit automatischen Alerts bei Fehlfunktionen
- Es gibt eine komplett getrennte Testumgebung um neue Funktionen vorab zu testen

9. Evaluierungsmaßnahmen

Es ist bei hokify min. 1 Mal halbjährlich ein explizites Meeting eingeplant um die Wirksamkeit der oben festgelegten Maßnahmen zur Gewährleistung der Datensicherheit zu überprüfen, zu bewerten und dementsprechend anzupassen. Zusätzlich werden alle Mitarbeiter regelmäßig zum Thema Datenschutz eingewiesen.

Reisswolf Österreich

Um die personenbezogenen Daten zu schützen welche in ausgedruckter Form vorliegen, wurde mit Reisswolf Österreich GmbH ein Servicevertrag abgeschlossen. Die Firma Reisswolf Österreich GmbH stellt einen Sicherheitsbehälter mit 240 Liter Fassungsvermögen bei, welcher per telefonischem Aviso abgeholt und der Inhalt DSGVO konform vernichtet wird. Nach erfolgreicher Vernichtung übermittelt die Reisswolf Österreich GmbH ein Datenträgervernichtungszertifikat laut ÖNORM S-2109.

Daten. Leben.

REISSWOLF

Deckblatt Leistungsmodulvertrag

Vertragsnummer: 10236_2020.2

Vertragsparteien	**Auftragnehmer (AN): REISSWOLF**	**Auftraggeber (AG):** Abweichende Rechnungsanschrift und ggf. weitere Leistungsstandorte in Anlage 4
	REISSWOLF Österreich GmbH Reisswolf Straße 1 2100 Leobendorf FN 105021 v	ISTAC Promotion GmbH Titanstraße 3 4062 Kirchberg-Thening FN 254427 h
		weitere Ansprechpartner ggf. in Anlage 4
Ansprechpartner	Wolfgang Niedermayr	Klaus Pohn
Funktion	Gebietsverkaufsleiter	Geschäftsführer
Telefon	+43 7221 72 700 33	+43 676 6842662
E-Mail	wolfgang.niedermayr@reisswolf.at	kpohn@istac.at

☒ **Akten- & Datenträgervernichtung**

- Gestellung von Sicherheitsbehältern
- Abholung und Transport der vom AG befüllten Sicherheitsbehälter
- Vernichtung

Bereitstellung:
☒ Dauer ☐ Archiv

Abholung:
☒ auf Abruf ☐ Intervall

☐ **Physische Archivierung & RWAM**

- Übernahme von Akten und Datenträgern
- Erfassung
- Archivierung (Akteneinlagerung)
- Bereitstellung RWAM
- Recherche
- Archivzugriffe & Transporte
- Vernichtung / Löschung

☐ **Digitalisierung**

☐ **REISSWOLF f.i.t.**

- Übernahme von Akten und Datenträgern
- Erfassung und Digitalisierung
- Digitale Archivierung
- Bereitstellung REISSWOLF f.i.t.
- Transportleistungen
- Vernichtung / Löschung

Konditionen in Anlage 2	
Datum Vertrags- & Leistungsbeginn	15.09.2020
Laufzeit des Vertrages & Kündigungsfrist	2 Jahre, automatische Verlängerung um jeweils 1 Jahr, Kündigungsfrist: 3 Monate vor Laufzeitende
Zahlungsweise & -frist	Elektronische Rechnung, sofort netto

Daten. Leben.

REISSWOLF

Deckblatt Leistungsmodulvertrag

Vertragsnummer: 10236_2020.2

Vertragsparteien	**Auftragnehmer (AN): REISSWOLF**	**Auftraggeber (AG):** Abweichende Rechnungsanschrift und ggf. weitere Leistungsstandorte in Anlage 4
	REISSWOLF Österreich GmbH Reisswolf Straße 1 2100 Leobendorf FN 105021 v	ISTAC Promotion GmbH Titanstraße 3 4062 Kirchberg-Thening FN 254427 h
		weitere Ansprechpartner ggf. in Anlage 4
Ansprechpartner	Wolfgang Niedermayr	Klaus Pohn
Funktion	Gebietsverkaufsleiter	Geschäftsführer
Telefon	+43 7221 72 700 33	+43 676 6842662
E-Mail	wolfgang.niedermayr@reisswolf.at	kpohn@istac.at

☒ **Akten- & Datenträgervernichtung**

- Gestellung von Sicherheitsbehältern
- Abholung und Transport der vom AG befüllten Sicherheitsbehälter
- Vernichtung

Bereitstellung:
☒ Dauer ☐ Archiv

Abholung:
☒ auf Abruf ☐ Intervall

☐ **Physische Archivierung & RWAM**

- Übernahme von Akten und Datenträgern
- Erfassung
- Archivierung (Akteneinlagerung)
- Bereitstellung RWAM
- Recherche
- Archivzugriffe & Transporte
- Vernichtung / Löschung

☐ **Digitalisierung**

☐ **REISSWOLF f.i.t.**

- Übernahme von Akten und Datenträgern
- Erfassung und Digitalisierung
- Digitale Archivierung
- Bereitstellung REISSWOLF f.i.t.
- Transportleistungen
- Vernichtung / Löschung

Konditionen in Anlage 2	
Datum Vertrags- & Leistungsbeginn	15.09.2020
Laufzeit des Vertrages & Kündigungsfrist	2 Jahre, automatische Verlängerung um jeweils 1 Jahr, Kündigungsfrist: 3 Monate vor Laufzeitende
Zahlungsweise & -frist	Elektronische Rechnung, sofort netto

Maßnahmen der Politik zur Informationssicherheit

Ein weiterer wichtiger Aspekt im Zuge des Schutzes personenbezogener Daten, ist der tägliche Umgang mit diesen. Um die Mitarbeiter dahingehend zu sensibilisieren, wurde die Politik zur Informationssicherheit definiert und den Mitarbeitern im Zuge der DSGVO Schulung nähergebracht.

Die Politik der Informationssicherheit umfasst folgende Punkte:

- E-Mail-Nutzung
- Internetnutzung
- Verschlüsselte Kommunikation
- Social Media
- Clear Desk Policy
- Persönliche Passwörter
- Umgang mit mobilen Endgeräten

Auszug aus der Politik DSGVO und Informationssicherheit:

Informationssicherheit

Neben der Einhaltung der DSGVO zum Schutz personenbezogener Daten, ist auch die Informationssicherheit zum Schutz jeglicher Daten zu beachten. Folgende Punkte werden definiert und sind im Unternehmensalltag zu berücksichtigen:

E-Mail-Nutzung

- Öffnen sie keine E-Mails und Dateianhänge, wenn Ihnen Absender oder Betreffzeile verdächtig erscheinen
- Auch bei vermeintlich bekannten und vertrauenswürdigen Absendern ist zu prüfen:
  - Passt der Text der E-Mail zum Absender
  - Erwarten Sie die beigelegten Dateien
- Sogenannte Phishing-Mails, die zur Übermittlung von persönlichen Online-Banking-Daten oder Passwörtern auffordern, müssen gelöscht werden
- Oftmals kann in einem E-Mail ein Link angeklickt werden, um eine Webseite aufzurufen. Seien Sie dabei vorsichtig, in betrügerischen E-Mails wird diesen Links oft eine völlig andere Internet-Adresse hinterlegt, als im Mail zu sehen ist.
- Beantworten Sie keine Spam-Mails
- Benachrichtigen sie auch Ihre Kollegen über verdächtige Zusendungen!

Internetnutzung

- Die private Internetnutzung ist laut der von Ihnen unterzeichneten Geheimhaltungs-vereinbarung verboten!
- Übermitteln Sie keine persönlichen Daten, vor allem nicht, wenn die Verbindung nicht als sicher (HTTPS) markiert wird.
- Laden Sie keine Daten herunter, dies kann neben das Einschleppen einer Schadsoftware auch zu lizenz- und urheberrechtlichen Problemen führen.

Verschlüsselte Kommunikation

- Bitte achten Sie auf eine verschlüsselte Kommunikation. Ihr Browser signalisiert dies mit einem Schloss. Alle übermittelten Daten sind demnach verschlüsselt.
- Eine E-Mail stellt KEINE sichere Kommunikation dar.

Social Media

- Posten Sie keine Fotos von Ihrem Arbeitsplatz
- Posten Sie keine Statusinformationen, die das Unternehmen betreffen

Clear Desk Policy

- Verschließen Sie alle vertraulichen Dokumente, die sich auf dem Arbeitsplatz befinden
- Bei Verlassen des Arbeitsplatzes:
  - alle Ausdrucke, Kopien usw. so verstauen, dass diese Dokumente nicht für Dritte zugänglich sind
  - sperren Sie Ihren Computer (z.B.: „Windows Taste + L")
- Lassen Sie keine Ausdrucke im Drucker/Kopierer liegen
- Bewahren Sie unter keinen Umständen Passwortnotizen an Ihrem Arbeitsplatz auf.
- Begleiten Sie Besucher innerhalb des Firmengebäudes, damit diese keine Zugriffe auf Daten erhalten

Persönliche Passwörter

- Verwenden Sie niemals:
  - das gleiche Passwort für unterschiedliche Zugänge
  - Namen, Vornamen, Geburtsdaten, Tel.-Durchwahlen, etc.
  - Begriffe aus einem Wörterbuch (auch nicht in einer anderen Sprache). Es gibt Programme, die Wortlisten mit mehreren tausend Begriffen sofort abrufen und so mögliche Passwörter finden.
  - Trivial-Passwörter (hallohallo, abcdefgh, 08/15, 1234 etc.)
- Geben Sie Ihr Passwort niemanden weiter
  - Bei Urlaub nutzen Sie die E-Mail-Weiterleitungs-Funktion oder die Postfach-Freigabe-Funktion
- Verwenden Sie Kennwörter, die mindestens 8 Zeichen haben. Ein Passwort muss aus einem Großbuchstaben, Kleinbuchstaben, Ziffer und einem Sonderzeichen bestehen
  - Ändern Sie Ihr Kennwort in regemäßigen Abständen (mind. alle 180 Tage)
- Sie sind für Ihr Kennwort verantwortlich! Sollten Sie den Verdacht haben, dass ein Dritter Ihr Kennwort kennt, ändern sie dieses sofort.

Umgang mit mobilen IT-Geräten

- Mobile IT-Geräte (Notebooks, Smartphones…) stellen durch ihre mobile Verwendung ein erhöhtes Sicherheitsrisiko dar
- Bitte beachten Sie folgende Punkte:
  - Lassen Sie das Gerät nicht unbeaufsichtigt
  - Überlassen Sie das Gerät nicht anderen Personen
  - Achten Sie bei Passworteingabe am Gerät auf Ihren Sichtschutz
  - Verwenden Sie Ihren privaten Cloud-Speicher nicht für Unternehmensdaten
  - Installieren Sie keine Anwendungen –setzten Sie sich mit unserem IT-Partner in Verbindung
  - Melden Sie einen Diebstahl oder Verlust sofort der Geschäftsführung und dem Datenschutzbeauftragten

Nutzung des Service von Conova Communications GmbH
Um die personenbezogenen Daten zu schützen, hat sich Istac entschieden das Service von Conova in Anspruch zu nehmen. Conova Communications GmbH ist ein strategischer Partner für den hochverfügbaren und sicheren Betrieb von maßgeschneiderten IT Services. Das Unternehmen betreibt derzeit sieben Rechenzentren in Österreich und bietet darin höchste Sicherheit. Das Unternehmen ist seit 2013 mit der international führenden Qualitätsnorm für Informationssicherheit – der ISO 27001 zertifiziert.

Vertragsverlängerung:

CONOVA

ISTAC promotion GmbH
Herr Klaus Pohn
Industriepark 20
4061 Pasching
Austria

Angebot Nr.: 90210059

Kundennr.: 408585 **Datum:** 25.01.2021 **Ihr Betreuer:** Daniel Gold
Referenz: Vertragsverlängerung +43 662/2200 357

Sehr geehrter Herr Pohn,
wie besprochen erlauben wir uns, Ihnen das folgende Angebot zu übermitteln:

conova ist Ihr langfristiger strategischer Partner für den hochverfügbaren und sicheren Betrieb von maßgeschneiderten IT Services. Diese liefern wir aus den eigenen Rechenzentren sowie in Kombination mit hybriden Cloud Lösungen: Housing, Hosting, Full-Outsourcing sowie Cloud- und Managed Services zählen zu unseren Kernkompetenzen und sind beliebig skalierbar, ganz nach Ihren individuellen Bedürfnissen.

Als Unternehmen sind wir ISO 27001 zertifiziert, entsprechend der international führenden Qualitätsnorm für Informationssicherheit. Zusätzlich sind unsere zwei neuen conova Rechenzentren 6 & 7 EN 50600 zertifiziert und erfüllen somit die Europäische Norm für den Neubau und den Betrieb von Rechenzentren.

Mit über 80 hoch qualifizierten Mitarbeitern und Standorten in Salzburg und Wien/Schwechat betreuen wir namhafte Großkunden wie die Porsche Informatik, bellaflora Gartencenter GmbH, Salzburg AG, XXXLutz KG und die Salzburger Nachrichten sowie mittelständische und kleine Unternehmen in ganz Österreich sowie in unseren Nachbarländern.

Möchten Sie mehr über unsere Kundenprojekte erfahren? Eine Übersicht finden Sie auf unserer Website unter www.conova.com/referenzen oder kontaktieren Sie Ihren Ansprechpartner direkt.

Freundliche Grüße
Ihr conova Sales Team

Positionen zu Angebot Nr. 90210059

Menge Einheit	Beschreibung	Produkt-ID	Einmalig Gesamt	Monatlich Gesamt
	Position 1.0 - Verlängerung TopFirewall small			
1,00 Stk.	C-TXT-VV Dieser Auftrag ersetzt den Auftrag Nr. 20180500			
1,00 Stk.	C-TFW-SMA-G-V6 TopFirewall small physikalisch V6	istacfw001		
1,00 Stk.	C-TFW-SMA-HOU-M-V6 TopFirewall small V6 - Housing im conova Rack			
	Position 1.0 - Verlängerung TopFirewall small			**70,69**
	Position 2.0 - Verlängerung TopCloud medium			
1,00 Stk.	C-TXT-VV Dieser Auftrag ersetzt den Auftrag Nr. 20180500			
1,00 Stk.	C-TCL-MED-G-V9 TopCloud medium V9 (8 GHz, 16 GB RAM, 100 GB PS, 150 GB BS)	istac_vDC004		
11,00 Stk.	C-RES-PP2 Performance Pack 2 (8 GB RAM, 2 GHz)			
16,00 Stk.	C-RES-PS100-M Primärstorage 100 GB			
5,00 Stk.	C-RES-PS10-M Primärstorage 10 GB			
4,00 Stk.	C-RES-SS100-M Sekundärstorage 100 GB			
8,00 Stk.	C-TCL-BCK-M-V9 TopCloud Backup-Service V9 - monatliche Betriebsführung			
1,00 TB	C-RES-BSP1TB-M Backupspace 1 TB			
10,00 Stk.	C-SON-WIN-M Windows Server Standard Lizenz			
5,00 Stk.	C-SON-MIC-RDP-LIC Microsoft Windows Remote Desktop CAL (User/Device)			
2,00 Stk.	C-SON-MIC-SQL-LIC Microsoft SQL Server Standard 2-Core MVL SPLA Lizenz			
	Position 2.0 - Verlängerung TopCloud medium			**2.129,40**

Auszeichnungen von Conova:

CONOVA

News & Tech Info Lösungen Rechenzentren Karriere Unternehmen Service & Support Kontakt

AUSGEZEICHNET

1-A QUALITÄT

2013 erhielt conova erstmals die Auszeichnung der international führenden Qualitätsnorm für Informationssicherheit. 2016 und 2019 wurden wir rezertifiziert – und bestanden erfolgreich. Das Besondere: Bei uns sind nicht nur die Rechenzentren ISO 27001 zertifiziert. Auch die dahinterliegenden Prozesse wurden unter die Qualitätslupe genommen.

Seit 2020 sind unsere Rechenzentren DC 6 & 7 zusätzlich EN 50600 zertifiziert und entsprechen somit der Europäischen Norm für den Neubau und Betrieb von Rechenzentren.

1. SAP-PARTNER IM BEREICH INFRASTRUCTURE OPERATIONS SERVICES IN ÖSTERREICH

conova ist seit 2015 der erste zertifizierte Anbieter von Infrastruktur für SAP-Lösungen in Österreich. Dies ist ein wichtiges Qualitätssiegel für alle Kunden, die auf SAP-Lösungen setzen. Die Zertifizierung von SAP SE bestätigt das hohe Niveau der conova Dienstleistungen im Bereich Infrastructure Operations Services. Alle zwei Jahre findet eine Rezertifizierung statt.

Ö-CLOUD INITIATIVE

conova ist Teil der Ö-Cloud Initiative des BMDW, die den notwendigen standardisierten Rahmen schafft, damit der Datenschatz der österreichischen Unternehmen bestmöglich gesichert ist. Cloud-Anbieter, die diese Prinzipien unterstützen und einen hohen Qualitätsanspruch an sich stellen, werden mit dem Ö-Cloud Gütesiegel ausgezeichnet. conova hat diese Auszeichnung für die TopCloud erhalten.

CONOVA

News & Tech Info Lösungen Rechenzentren Karriere Unternehmen Service & Support Kontakt

ROT-WEISS-ROTE CLOUD

conova wurde mit dem Gütesiegel „Austrian Cloud" ausgezeichnet. Dieses Qualitätssiegel holt explizit jene Cloud-Anbieter vor den Vorhang, die eine Datenspeicherung innerhalb von Österreich garantieren. Neben dem Speicherort werden auch Faktoren wie Datenschutz, Sicherheit, rechtliche Konformität und technische Infrastruktur überprüft. Wir erhielten diese Auszeichnung für das Produkt „TopCloud".

1. KLIMANEUTRALES RECHENZENTRUM ÖSTERREICHS

conova arbeitet als erstes Rechenzentrum in Österreich CO_2-neutral. Wir nutzen die Abwärme der Server und beheizen damit unser Gebäude. Gleichzeitig wird Regenwasser als Nutzwasser verwendet – etwa in den Sanitäranlagen. Den Rest kompensieren wir durch den Kauf von Klimaschutzzertifikaten.

Maßnahmen zur Erlangung der Zustimmung von Beteiligten

Grundsatz 1 der DSGVO besagt, dass personenbezogene Daten auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden müssen, eine Rechtsgrundlage ist daher zwingend erforderlich. Darüber hinaus sind die betroffenen Personen über die Verarbeitung zu informieren.

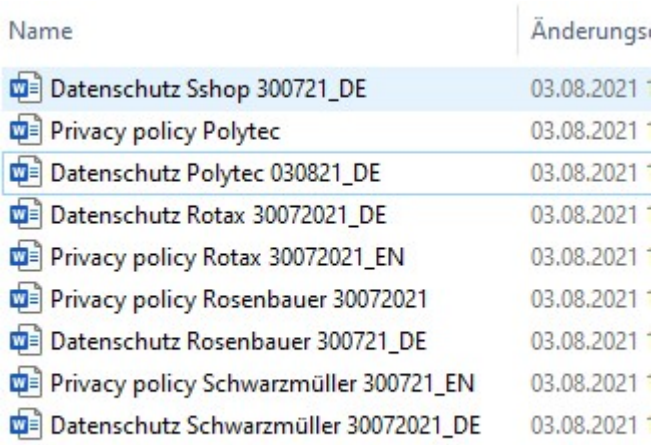
Den Großteil der personenbezogenen Daten wird über die Online-Shops, welche Istac für seine Kunden betreibt, erhoben. Als Beispiel kann hier der Rosenbauer Fanshop angeführt werden. Alle nachfolgenden Informationen können hier https://fanshop.rosenbauer.com/fanshop/start/ überprüft werden.

Cookie Einstellungen

Gelangt ein User auf einen unserer Online-Shops, muss er zuerst die Cookie Einstellungen speichern. Hier hat er die Möglichkeit nur die notwendigen Cookies zu speichern, oder „Alle Cookies“ auszuwählen. Die Entscheidung kann er jederzeit in der Datenschutzerklärung im Shop rückgängig machen.

Um die Online-Shop User ausführlich über die Verarbeitung der personenbezogenen Daten zu informieren, befindet sich eine deutsche sowie eine englische Version der Datenschutzerklärung in den Online-Shops. Bei den Cookie Einstellungen wird der User direkt auf die Datenschutzerklärung verlinkt.

Die Datenschutzerklärung wurde in ausnahmslos allen Onlineshops eingefügt.



Datenschutzerklärung

Datenschutz / Cookies

Die ISTAC GmbH (im Folgenden: ISTAC) nimmt den Schutz personenbezogener Daten sehr ernst. Mit dieser Datenschutzerklärung werden Nutzer darüber aufgeklärt, welche personenbezogenen Daten erhoben, gespeichert und verarbeitet werden und welche Rechte sie nach dem Datenschutzgesetz (DSGVO) haben.

Soweit im Text geschlechterspezifische Ausdrücke verwendet werden, gelten diese für beide Geschlechter gleich.

Der Rosenbauer Merchandising Shop wird von ISTAC GmbH, A-4062 Kirchberg-Thening, Titanstraße 3 („wir“ bzw. „uns“) bereitgestellt. Diese Mitteilung beschreibt wie wir, als datenschutzrechtlich Verantwortlicher, Ihre personenbezogenen Daten im Zusammenhang mit dieser Website verarbeiten.

Alle Informationen, Daten und Materialien, die Sie im Rahmen der Nutzung des Webshops mitteilen, sowie alle sonstigen Informationen, Daten und Materialien, die sie gegebenenfalls überlassen, unterliegen auch der Datenschutzrichtlinie der Rosenbauer International AG, welche unter https://www.rosenbauer.com/de/at/group/meta-navigation/datenschutz abrufbar ist. Die jeweils aktuelle Version ist Bestandteil der Nutzungsbedingungen.

1. Welche Daten wir über Sie verarbeiten

Im Zuge Ihres Besuches dieser Website werden wir folgende Informationen erheben: Das Datum und die Uhrzeit des Aufrufs einer Seite auf unserer Website, Ihre IP-Adresse, Name und Version Ihres Web-Browsers, die Webseite (URL), die Sie vor dem Aufruf dieser Website besucht haben, bestimmte Cookies (siehe Punkt 2 unten) und jene Informationen, die Sie selbst durch zB Ausfüllen des Kontaktformulars, Registrierung auf unserer Website zur Verfügung stellen.

Es besteht keine Verpflichtung, jene Daten, um deren Angabe wir Sie auf unserer Website bitten, tatsächlich anzugeben. Wenn Sie dies jedoch nicht tun, wird es Ihnen nicht möglich sein, alle Funktionen der Website zu nutzen.

2. Cookies/Google Analytics

Diese Website benutzt Google Analytics, einen Webanalysedienst von Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA („Google"). Google Analytics verwendet sogenannte „Cookies", Textdateien, die auf Ihrem Computer gespeichert werden und eine Analyse Ihrer Nutzung der Website ermöglichen. Wir verarbeiten Ihre Daten auf Grundlage unseres überwiegenden berechtigten Interesses, auf kosteneffiziente Weise, um eine leicht zu verwendende Website-Zugriffstatistik zu erstellen (Art 6 Abs 1 lit. f Datenschutz-Grundverordnung).

Die durch das Cookie erzeugten Informationen über Ihre Nutzung dieser Website (einschließlich Ihrer IP-Adresse und die URLs der aufgerufenen Webseiten) werden an den Server von Google in den USA übertragen und dort gespeichert. Wir speichern keine Ihrer Daten, die in Zusammenhang mit Google Analytics erhoben werden.

Diese Website verwendet die von Google Analytics gebotene Möglichkeit der IP-Anonymisierung. Ihre IP-Adresse wird daher von Google gekürzt/anonymisiert, sobald Google Ihre IP-Adresse erhält. In unserem Auftrag wird Google die Informationen verwenden, um Ihre Nutzung der Website auszuwerten, um Reports über die Websiteaktivitäten zusammenzustellen und um weitere mit der Websitenutzung und der Internetnutzung verbundenen Dienstleistungen an uns zu erbringen. Die im Rahmen von Google Analytics von Ihrem Browser übermittelte IP-Adresse wird von Google nicht mit anderen Daten zusammengeführt.

Sie können die Speicherung der Cookies durch eine entsprechende Einstellung Ihrer Browser-Software verhindern. Wir weisen Sie jedoch darauf hin, dass Sie in diesem Fall unter Umständen nicht sämtliche Funktionen dieser Website vollumfänglich nutzen können. Sie können darüber hinaus verhindern, dass Google Ihre Daten im Zusammenhang mit Google Analytics erhebt, indem Sie das unter dem folgenden Link verfügbare Browser-Plugin herunterladen und installieren: http://tools.google.com/dlpage/gaoptout?hl=de.

Sie können die Erhebung Ihrer Daten durch Google Analytics auf dieser Website auch verhindern, indem Sie die Checkbox bei „alle Cookies" deaktivieren und mit „Auswahl speichern" bestätigen.

Cookie Einstellungen

Formularbeginn

☑ Notwendige Cookies ☐ Alle Cookies

Formularende

Nähere Informationen zu den Nutzungsbedingungen von Google sowie zur Google Datenschutzerklärung finden Sie unter http://www.google.com/analytic/terms/de.html bzw. unter https://www.google.at/intl/at/policies/.

3. Zwecke der Datenverarbeitung

Wir werden Ihre personenbezogenen Daten zu folgenden Zwecken verarbeiten:

- um Ihnen diese Website zur Verfügung zu stellen und um diese Website weiter zu verbessern und zu entwickeln;
- um Nutzungsstatistiken erstellen zu können;
- um Angriffe auf unsere Website erkennen, verhindern und untersuchen zu können;
- um Ihnen ein webbasiertes Shopsystem zur Verfügung zu stellen

4. Rechtsgrundlagen der Verarbeitung
Die rechtliche Grundlage für die Verarbeitung Ihrer personenbezogenen Daten ist unser überwiegendes berechtigtes Interesse (gemäß Art 6 Abs 1 lit f EU Datenschutz-Grundverordnung), welches darin besteht, die oben unter Punkt 3 genannten Zwecke zu erreichen.

5. Übermittlung Ihrer personenbezogenen Daten

Zu den oben genannten Zwecken werden wir Ihre personenbezogenen Daten an folgende Empfänger übermitteln:

Rosenbauer International AG
Asseco Solutions AG
Logistikpartner und Online-Bezahldienste

6. Dauer der Speicherung

Wir werden Ihre Daten grundsätzlich für eine Dauer von drei Monaten speichern. Eine längere Speicherung erfolgt nur, soweit dies erforderlich ist, um festgestellte Angriffe auf unserer Website zu untersuchen.

Wenn Sie sich auf unserer Website registrieren, werden wir Ihre Daten jedenfalls so lange speichern, so lange Ihr Account besteht und danach für nur so lange, wie rechtliche Verpflichtungen dies vorsehen.

7. Ihre Rechte im Zusammenhang mit personenbezogenen Daten

Sie sind unter anderem berechtigt (unter den Voraussetzungen anwendbaren Rechts), (i) zu überprüfen, ob und welche personenbezogenen Daten wir über Sie gespeichert haben und Kopien dieser Daten zu erhalten, (ii) die Berichtigung, Ergänzung oder das Löschen Ihrer personenbezogenen Daten, die falsch sind oder nicht rechtskonform verarbeitet werden, zu verlangen, (iii) von uns zu verlangen, die Verarbeitung Ihrer personenbezogenen Daten einzuschränken, und (iv) unter bestimmten Umständen der Verarbeitung Ihrer personenbezogenen Daten zu widersprechen oder die für das Verarbeiten zuvor gegebene Einwilligung zu widerrufen, (v) Datenübertragbarkeit zu verlangen, (vi) die Identität von

Dritten, an welche Ihre personenbezogenen Daten übermittelt werden, zu kennen und (vii) bei der zuständigen Behörde Beschwerde zu erheben.

Kontaktdaten Datenschutzbehörde:

Österreichische Datenschutzbehörde
Barichgasse 40-42
1030 Wien
Telefon: +43 1 52 152-0
E-Mail: dsb@dsb.gv.at

8. Unsere Kontaktdaten

Sollten Sie zu der Verarbeitung Ihrer personenbezogenen Daten Fragen oder Anliegen haben, wenden Sie sich bitte an uns:

ISTAC Promotion GmbH
A-4062 Kirchberg-Thening
Titanstraße 3
office@istac-service.at
+43(0)7221 / 63 760

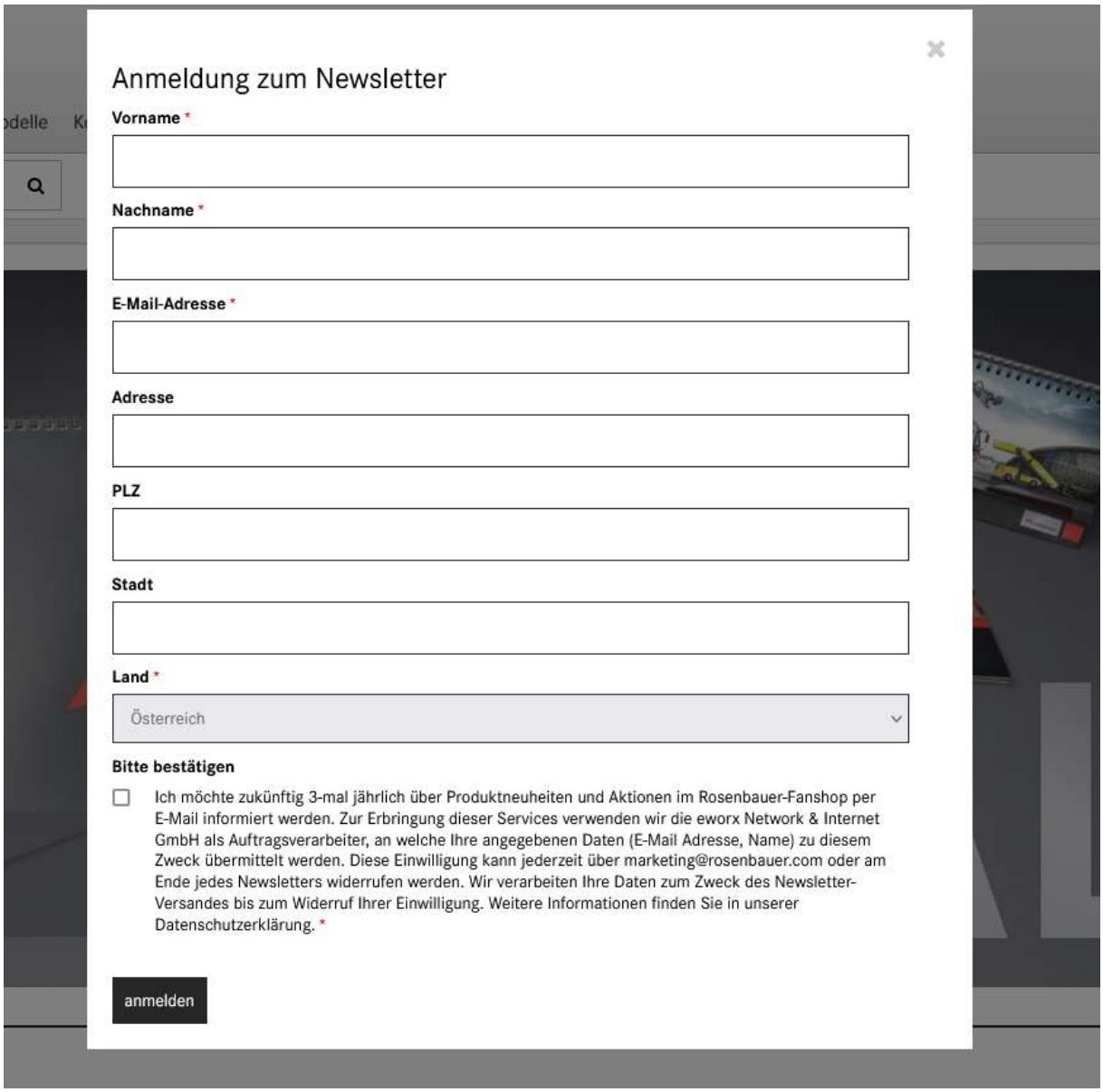
Alternativ können Sie sich auch an unseren Datenschutzbeauftragten wenden:

Datenschutzbeauftragter der Firma ISTAC Promotion GmbH
A-4062 Kirchberg-Thening
Titanstraße 3
jkupfer@istac.at
0660 / 88 77 037

Zuletzt aktualisiert am 03.08.2021

Newsletter Anmeldung / Doble-Opt-in

Meldet sich ein User in weiterer Folge für den Newsletter an, wird er noch einmal ausführlich über die erhobenen Daten und deren Nutzung informiert. Außerdem ist bei den Newsletter Anmeldungen ein Doble-Opt in Prozess implementiert, weshalb der User die Anmeldung noch via per Mail zugeschicktem Link bestätigen muss.



Bitte bestätigen Sie Ihre Newsletteranmeldung

Vollansicht

Von: Rosenbauer International AG

10.06.2021 um 15:03 Uhr

Information wird nicht korrekt dargestellt? Klicken Sie bitte hier

rosenbauer

Sehr geehrte Damen und Herren!

Vielen Dank für Ihr Interesse am Rosenbauer Newsletter.

Um Ihre Registrierung zu vervollständigen, klicken Sie bitte auf folgenden Link. Damit können wir sicherstellen, dass Sie den Newsletter nicht unbeabsichtigt erhalten und Sie in den Verteiler aufnehmen.

Anmeldung bestätigen

Ohne Bestätigung sind Sie nicht angemeldet und erhalten auch keine weiteren Nachrichten.

Freundliche Grüße,

Rosenbauer Newsletter Team

Personenbezogene Daten Mitarbeiter

Aber auch bei den Mitarbeitern werden personenbezogene Daten erhoben. Neben den personenbezogenen Daten, welche für die Vertragsaufsetzung und die Anmeldung des Mitarbeiters benötigt werden, werden die Mitarbeiter während des Jahres auch fotografiert und durch die Videokameras aufgezeichnet.

Für die Mitarbeiterfotos und für die Aufzeichnung durch Videokameras wird von den Mitarbeitern eine zusätzliche Zustimmungsvereinbarung eingeholt. Hier ist hervorzuheben, dass die Mitarbeiter diesen Vereinbarungen nicht zustimmen müssen und diese auch jederzeit wiederruft werden können.

Zustimmungsvereinbarung Mitarbeiterfotos

Istac, Titanstraße 3 4062 Kirchberg Thening („wir") beabsichtigt Fotoaufnahmen der MitarbeiterInnen für folgende Zwecke zu veröffentlichen: Veröffentlichung im Internet zur bildlichen Darstellung des Ansprechpartners, sowie für Inserate und Broschüren für die Dauer des Arbeitsverhältnisses der Firma Istac GmbH.

Der Unterzeichner _____ erklärt sein Einverständnis mit der (unentgeltlichen) Verwendung der fotografischen Aufnahmen seiner Person für die oben beschriebenen Zwecke. Eine Verwendung der fotografischen Aufnahmen für andere als die beschriebenen Zwecke oder ein Inverkehrbringen durch Überlassung der Aufnahmen an Dritte ist unzulässig. Die fotographischen Aufnahmen werden ausschließlich intern verwendet und lediglich an Partnerunternehmen zur Herstellung der Webseite oder Erstellung einer Broschüre übermittelt. Sämtliche fotografischen Aufnahmen werden nach Beendigung des Arbeitsverhältnisses oder nach erfolgtem Löschantrag durch den Betroffenen aus allen Anwendungsorten entfernt und unwiederbringlich vernichtet. Die Aktualisierung der fotografischen Aufnahme durch den Verantwortlichen erfolgt in neuerlicher Abstimmung mit dem Betroffenen. Diese Einwilligung ist freiwillig. Wird sie nicht erteilt, entstehen keine Nachteile. Diese Einwilligung kann jederzeit mit Wirkung für die Zukunft beim Datenschutzbeauftragten unter jkupfer@istac.at widerrufen werden

_____ _____

Ort, Datum Unterschrift des Arbeitnehmers

istac

istac

Zustimmung zum Einsatz von Videokameras

Istac, Titanstraße 3 4062 Kirchberg Thening („wir") beabsichtigen, im Außenbereich zum Zweck des vorbeugenden Schutzes von Personen und Sachen Videokameras anzubringen und einzusetzen, deren Blickfeld den gesamten Außenbereich des Firmengeländes abdeckt.
Ausdrücklich festgehalten wird, dass die Videokameras nicht dazu dienen, die Leistungen und das Verhalten der Arbeitnehmer zu kontrollieren.

Da die Videokameras allerdings abstrakt dazu geeignet wären, Arbeitnehmer beim Betreten und Verlassen des Firmengebäudes zu kontrollieren, ist der Einsatz der Videokameras nur mit Zustimmung der Arbeitnehmer zulässig.

Festgehalten wird, dass die Aufzeichnungen der Videoüberwachung nach 72 stunden gelöscht werden. Fällt das Ende dieser 72-stündigen Frist auf einen Samstag, Sonntag, gesetzlichen Feiertag, Karfreitag oder 24. Dezember, so ist der nächste Tag, der nicht einer der vorgenannten Tage ist, als letzter Tag der Frist anzusehen. Eine über diese Zeit hinaus dauernde Aufbewahrung findet nur dann statt, soweit dies zu Beweissicherungszwecken im Falle strafbarer Handlungen erforderlich ist.

Durch Ihre Unterschrift erteilen Sie _____ uns Ihre Zustimmung zu Videoüberwachung in der oben beschriebenen Weise. Diese Zustimmungserklärung ist für eine Dauer von 10 Jahren unwiderruflich.

_____ _____

Ort, Datum Unterschrift des Arbeitnehmers