Technische und organisatorische Maßnahmen des Auftragnehmers (TOM)

1. Zutrittskontrolle

Der Auftragnehmer verwehrt Unbefugten den Zutritt zu den Büro-, Server- und Archivräumen. Die folgenden Maßnahmen verhindern, dass Unbefugte räumlich Zutritt zu den Verarbeitungsanlagen/-räumen personenbezogener Daten oder sonstigen personenbezogenen Unterlagen, z. B. Akten oder Datenträgern erhalten:

- Der Zutritt zu den Gebäuden ist durch Türschlösser gesichert. Das Zutrittskontroll-system gewährleistet den Zutritt nur für autorisierte Mitarbeiter mittels eines Schlüssels.
- Rücknahme von Zugangsmittel (Schlüssel) erfolgt nach Ablauf der Berechtigung und wird von einem Mitarbeiter/einer Mitarbeiterin des Unternehmens schriftlich nachgehalten.
- Die Zugänge des Büros sind mit einem Sicherheitsschloss versehen. Die Zutrittskontrolle zum Büro wird über einen Sicherheitsschlüssel gewährt. Die Verteilung der Schlüssel wird dokumentiert.
- Sensible Datenträger und Papierakten werden in abschließbaren Schränken aufbewahrt.
- Die Besucher-Einlasskontrolle erfolgt durch persönliche Kontrolle. Fremde Besucher haben sich in eine Besucherliste einzutragen und werden bei den Besuchen persönlich zu den betreffenden Räumen begleitet.
- Im Alarmfall ist das Gebäude unverzüglich von allen Mitarbeitern zu verlassen. Die Türen sind in den Büroräumen verschließbar, so dass auch nach Verlassen der Räume sichergestellt ist, dass kein unberechtigter Zutritt durch Dritte erfolgen kann.
- Der Remotezugiff auf Server ist nur ausgewählten Mitarbeiter der Technik gestattet.

2. Zugangskontrolle

Der Auftragnehmer verhindert, dass EDV-Systeme von Unbefugten genutzt werden können. Dies geschieht durch:

- Es wird ein Kennwortverfahren angewendet (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts), mit welchem sichergestellt wird, dass Passwörter die Mindestanforderungen an die Sicherheit erfüllen. Die Passwörter unterliegen genauen Sicherheitsvorgaben.
- Ferner wird sichergestellt, dass nur Mitarbeiter der AL Kompass GmbH zu den Bereich Zugriff erhalten, welche für ihre Arbeit erforderlich sind. Diese wird durch eine entsprechende Rechtevergabe in der IT sichergestellt.
- Ein Passwortwechsel wird alle 3 Monate erzwungen, indem der Mitarbeiter aufgefordert wird, sein Passwort zu ändern. Erfolgt dies nach wiederholter Aufforderung nicht, wird der Zugang gesperrt.
- Ebenso werden externe USB-Schnittstellen gesperrt und nur für Mitarbeiter freigeschaltet, die aufgrund ihrer beruflichen Tätigkeit ein solches Medium benötigen.
- Die IT-Systeme sind mittels einer Firewall vor Viren und Schadsoftware geschützt und werden fortlaufend überwacht. Hierdurch werden unberechtigte Zugriffe erkannt und entsprechend unterbunden. Im Bereich des E-Mail-Zugangs werden die eingehenden E-

Mails auf Viren und Schadsoftware geprüft und erforderlichenfalls in einem Quarantäne-Bereich abgelegtNeben der vorstehend beschriebenen Firewall und dem Virenscanner verfügt die AL Kompass GmbH zusätzlich noch über einen so genannten Schnittstellenschutz.

- Es erfolgt die Sperrung des Benutzerkontos nach drei fehlgeschlagenen Anmeldeversuchen.
- Die PCs im Bereich der IT sind durch automatische, passwortgeschützte Bildschirm- und Rechnersperre gesichert.
- Es erfolgt eine eindeutige Zuordnung von Benutzerkonten zu den Benutzern.
- Sensible Systeme, insbesondere Serversysteme sind nur als Administrator nutzbar.
- Die Übertragung von personenbezogenen Daten erfolgt gesichert (SSH, TLS).
- Der Zugriff auf das firmeninterne VPN ist nur über zertifikatsbasierte Authentifizierung möglich.
- Die Vernichtung von nicht mehr erforderlichen Datenträgern erfolgt mittels kontrollierter Vernichtung.
- Bei Ausscheiden eines Mitarbeiters/einer Mitarbeiterin hat der/die Betroffene alle Zugangsberechtigungen unverzüglich mit Ausscheiden zurückzugeben. Das wird protokolliert.

3. Zugriffskontrolle

Der Auftragnehmer gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies geschieht durch:

- Die Vergabe differenzierter Berechtigungen (z.B. in Form von Profilen, Rollen, Transaktionen, Objekten). Die Mitarbeiter haben nur Zugriff auf Bereich innerhalb der IT, welche für ihre jeweilige Tätigkeit erforderlich und geboten sind. Diese Berechtigungen werden regelmäßig einer Kontrolle unterzogen.
- Die Auswertungen, Kenntnisnahme, Veränderung und Löschung von personenbezogenen Daten erfolgen kontrolliert und werden protokolliert.
- Es erfolgt eine automatische Sperre auf IT-Systeme, sofern eine mehrmalige fehlerhafte Authentifizierung vorgenommen wurde.
- Bei Ausscheiden eines Mitarbeiters/einer Mitarbeiterin werden alle Zugangsberechtigungen des/der Betroffenen unverzüglich mit Ausscheiden gesperrt.

4. Weitergabekontrolle

Der Auftragnehmer gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist. Dies geschieht durch:

- Es erfolgt eine Verschlüsselung bei der Datenübertragung mittels SSH oder SSL bzw.je nach Anwendung auch durch eine Tunnelverbindung (VPN = Virtual Private Network).
- Bei dem Datenaustausch wird die Übertragung standardmäßig mittels Transportprotokolle (SSL) gesichert.
- Im Falle von Remotetätigkeit wird die Datenübertragung mittels VPN verschlüsselt; eine Übertragung von Daten ist ausschließlich durch eine Tunnelverbindung möglich.

5. Eingabekontrolle

Der Auftragnehmer gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies geschieht durch:

- Die Eingabe, wer Daten in die Systeme eingibt erfolgt durch Protokollierungs- und Protokollauswertungssysteme.
- Durch das Berechtigungskonzept ist sichergestellt, dass der Zugriff von Mitarbeitern auf erforderliche Daten nur im Rahmen seiner jeweiligen Funktion im Unternehmen erfolgt und nur in dem Umfang, die für seine Tätigkeit im Unternehmen erforderlich und geboten ist.
- Berechtigungsvergaben auf schützenswerte Ressourcen werden nachvollziehbar nur durch hierfür autorisierte Personen beantragt und vergeben.

6. Auftragskontrolle

Der Auftragnehmer gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers und zur Erfüllung des vertraglich definierten Verwendungszweckes verarbeitet werden. Dies geschieht durch:

- Verpflichtung von Mitarbeitern auf das Datengeheimnis und Datenschutz
- Verarbeitung der Daten erfolgt in der Europäischen Union/EWR
- Vorliegen eines Vertrages zur Auftragsdatenverarbeitung gemäß § 32 DSGVO

7. Verfügbarkeitskontrolle

Der Auftragnehmer gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dies geschieht durch:

- Backup-Verfahren / regelmäßige Sicherungskopien
- Überwachung der Computersysteme
- Getrennte Aufbewahrung
- Ständig aktualisierte/r Virenschutz/Firewall

8. Pseudonymisierung, Speicherung, Löschung

a. Allgemeine Verarbeitungsgrundsätze

Das System der AL Kompass GmbH ist auf die Einhaltung der allgemeinen Grundsätze der DSGVO ausgerichtet. Die folgenden Grundsätze sind einzuhalten:

i. Erlaubnisvorbehalt und Zweckbindung

Daten dürfen von der AL Kompass GmbH bzw. dem Zugriffsberechtigten nur verarbeitet werden, wenn

- dies für den konkreten Zweck gesetzlich erlaubt ist
- oder der Endkunde eingewilligt hat (Erlaubnisvorbehalt).

Eine Datenverarbeitung für einen bestimmten Zweck ist deshalb nur zulässig,

- wenn dies in diesen Handlungsanweisungen vorgesehen ist oder
- der Endkunde in diese konkrete Datenverarbeitung wirksam eingewilligt hat. In diesem Fall ist jeweils im Einzelfall zu prüfen, ob eine ausreichende schriftliche oder

elektronische Einwilligungserklärung des Kunden vorliegt (Art. 6 ff. DSGVO).

Hierbei ist insbesondere das Zweckbindungsgebot zu beachten. Eine gesetzliche Erlaubnis zur Datenverarbeitung oder die Einwilligung des Endkunden gilt nur für den konkreten Zweck, den die gesetzliche Erlaubnis oder die Einwilligung des Endkunden ausdrücklich vorsieht. Für die Verarbeitung der Daten für weitere Zwecke ist dem entsprechend ein neuer Erlaubnistatbestand (gesetzliche Erlaubnis oder die Einwilligung des Endkunden) erforderlich. Bei der konkreten Verarbeitung von Daten ist deshalb auch immer noch zu prüfen, ob die gesetzliche Erlaubnis oder die Einwilligung den vorgesehenen Verarbeitungszweck umfasst.

ii. Koppelungsverbot

Die Angebote der AL Kompass GmbH beachten das sog. Koppelungsverbot nach § 7 Abs. 4 DSGVO. Den Betroffenen muss es effektiv freistehen, in weitere Datenverarbeitung zum Zwecke der Werbung einzuwilligen oder diese Einwilligung zu verweigern, bzw. eine einmalig erteilte Einwilligung zu widerrufen.

iii. Datenvermeidung und Datensparsamkeit

Das Angebot von AL Kompass GmbH richtet sich an den Zielen der Datenvermeidung und Datensparsamkeit aus.

iv. Datenübermittlung

Die Datenübermittlung an Dritte ist nach den nachfolgenden Ablaufplänen an den gesetzlichen Erfordernissen ausgerichtet (z.B. Übermittlung an Überwachungsbehörden). Eine über die gesetzlichen Erlaubnistatbestände hinausgehende Weitergabe von personenbezogenen Daten an Dritte ist ohne ausdrückliche Einwilligung der Kunden nicht zulässig.

v. Einbindung Dritter

Eine Einbindung Dritter bei der Erhebung und Verarbeitung personenbezogener Daten darf nur aufgrund einer Rechtsgrundlage im Sinne des Datenschutzrechts (DSGVO) oder aufgrund einer Einwilligung des Betroffenen erfolgen.

Eine Einbindung Dritter ist demnach möglich, wenn

- mit dem Dritten eine Vereinbarung über die Auftragsdatenverarbeitung nach Maßgabe der DSGVO (Art. 28 DSGVO) geschlossen wurde.

Die Voraussetzungen sind vor der Einbindung in Datenverarbeitung zu prüfen.

vi. Besondere Verarbeitungstatbestände

Vorgabe der Verarbeitungsabläufe

Das nachfolgende Datenschutzkonzept orientiert sich an den Datenverarbeitungsabläufen, wie sie bei der Realisierung der Dienste entstehen und vorzunehmen sind. Die folgenden Vorschriften und Regelungen sind zwingend einzuhalten.

9. Trennungskontrolle

Der Auftragnehmer gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Es besteht keine Notwendigkeit zu einer physischen Trennung; eine logische Trennung der Datenträger ist ausreichend. Dies geschieht durch:

- Sofern Daten zu verschiedenen Zwecken verarbeitet werden, wird sichergestellt, dass

die Verarbeitung jeweils nur mandantenbezogen für den/die jeweils betroffene Person erfolgt. Die Systeme für die Endkundenbearbeitung verfügen über eine interne Mandantenfähigkeit und richten sich nach dem jeweiligen Zweck der Verarbeitung der personenenbezogenen Daten (Zweckbindung).

- Logische Trennung personenbezogener Daten verschiedener Auftraggeber.

10. Organisationskontrolle

Im Rahmen der Organisationskontrolle wurden folgende Maßnahmen vom Auftragnehmer umgesetzt:

- Die mit der Datenverarbeitung betrauten Mitarbeiter*innen wurden auf das Datengeheimnis und den Datenschutz verpflichtet.
- Die mit der Datenverarbeitung betrauten Mitarbeiter*innen wurden auf ihre Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse hingewiesen.
- Die mit der Datenverarbeitung betrauten Mitarbeiter/-innen wurden in Datenschutzschulungen mit den Vorschriften der DSGVO und des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz vertraut gemacht.

11. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die Beschäftigten werden regelmäßig zum Datenschutz geschult. Mindestens einmal im Kalenderjahr.

Die Beschäftigten werden durch ihren zum vertraulichen Umgang mit personenbezogenen Daten und auf das Fernmeldegeheimnis durch ihren Arbeitsvertrag verpflichtet.

Anfragen von Betroffenen werden an einen externen Rechtsanwalt weitergeleitet, der diese Anfragen zeitnah bearbeitet.

12. Fernwartungskontrolle

Nur zutreffend, sofern der Auftragnehmer Tätigkeiten via Fernwartungszugang ausführt:

Der Auftraggeber stellt durch technische und organisatorische Maßnahmen sicher, dass nur auf die für die Wartung unbedingt erforderlichen personenbezogenen Daten zugegriffen werden kann.

Die vom Auftragnehmer mit Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses gemäß DSGVO und BDSG verpflichtet worden. Bei Wartungsarbeiten ist sicherzustellen, dass der Zugriff auf die Systeme des Auftraggebers und die Übertragung/ Übermittlung von Daten nur in verschlüsselter, pseudonymisierter oder anonymisierter Form erfolgen kann.

Folgende Maßnahmen wurden vom Auftragnehmer umgesetzt:

- Fernwartungszugriff wird über eine verschlüsselte Verbindung realisiert.
- Protokollierung von Fernwartungen (Mitarbeiter, Dauer, Grund).
- Ausschluss von Fremdzugriff im Bereich des technisch möglichen.

13. Standorte der Datenverarbeitung

Die von dem Auftragnehmer ausgeführte Datenverarbeitung findet an folgenden Standorten statt:

Eine Veränderung der Standorte, in denen Daten des Auftraggebers verarbeitet und/ oder genutzt werden, bedarf der schriftlichen Zustimmung des Auftraggebers.

Standort der Geschäftsräume des Auftragnehmers:

- Merkenicher Straße 132, 50735 Köln

Standort der Rechenzentren des Auftragnehmers (für das Hosting der Software):

- Hetzner Online GmbH, Am Datacenter-Park 1, 08223 Falkenstein

Standort der Rechenzentren des Auftragnehmers (für das Hosting des Online-Shops):

- Elopage GmbH (Anbieter Online-Shop): Host Europe GmbH, Hansestrasse 111, 51149 Köln

14. Verpflichtungserklärung zur Umsetzung der TOM

Der Auftragnehmer bestätigt, dass er die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten des Auftraggebers vor Beginn der Datenverarbeitung umgesetzt hat. Der Auftragnehmer verpflichtet sich, die Erfüllung dieser Anforderungen für die Dauer der Zusammenarbeit sicherzustellen, regelmäßig zu kontrollieren, zu dokumentieren und auf Nachfrage des Auftraggebers zur Verfügung zu stellen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insofern ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber unverzüglich mitzuteilen.