Salubris UG
(haftungsbeschränkt) & Co. KG
Meindersstraße 1a
33615 Bielefeld
Fon: 0521-5577.2126
Fax: 0521-5577.2135

Büro Witten:
Kellerstraße 3
58456 Witten
Mobil: 0172-6548573

info@salubris.de
www.salubris.de

Technische und organisatorische Maßnahmen

für den Datenschutz nach Art. 32 DSGVO

Salubris UG (haftungsbeschränkt) & Co. KG

Meindersstraße 1a

33615 Bielefeld

Fon: 0521 - 5577.2126

E-Mail: info@salubris.de

(im Folgenden Salubris genannt)

1. Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Die Verarbeitung von Daten erfolgt in den Räumlichkeiten der Firma Salubris in Bielefeld (Anschrift: Meindersstraße 1a, 33615 Bielefeld).
- Der Zutritt zu den Räumen erfolgt nur über eine Haustür sowie drei Bürotüren. Die Türen sind mit Sicherheitsschlössern versehen. Nur die Mitarbeitenden von Salubris haben eigenständigen Zugang zu den Räumlichkeiten. Die Ausgabe der Schlüssel wird dokumentiert.
- Besucher, die Geschäftsführer sowie externe Mitarbeitende der Firma Salubris melden sich über eine Gegensprechanlage an und haben somit keinen eigenen Zutritt zu den Räumlichkeiten, sondern nur in Begleitung eines Mitarbeitenden von Salubris.

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Der Zugang zu den datenverarbeitenden Rechnern ist standardmäßig durch eine Benutzeridentifikation (Benutzername und Passwort) geschützt.
- Die Daten sind auf passwort-geschützen Rechnern gespeichert. Zugang zu den verschlüsselten Ordnern haben nur die bearbeitenden Mitarbeitende.
- Auf den datenverarbeitenden Rechnern ist ein Bildschirmschoner mit Passwortschutz aktiviert. Bei Verlassen der Räume sind die Mitarbeitenden dazu verpflichtet, ihre Rechner zu sperren oder herunterzufahren.
- Mitarbeitende haben nur Zugang zu den Daten, die sie bearbeiten.
- Alle Mitarbeitenden haben eine Schulung zum Umgang mit Passwörtern erhalten: Ein sicheres Passwort sollte mindestens zehn Zeichen lang sein und sowohl Buchstaben, Zahlen als auch Sonderzeichen enthalten. Dabei werden Wortkombinationen oder logische Zahlen- oder Buchstabenreihen vermieden. Ihre persönlichen Passwörter können die Mitarbeitenden selbst ändern.

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Die Daten sind in der beschriebenen Form nur lokal auf dem Rechner des bearbeitenden Mitarbeitenden gespeichert. Zugang zu und Zugriff auf einen jeweiligen Datensatz hat immer nur der befugte Mitarbeitende.

- In Papierform vorliegende personenbezogene Daten (z. B. ausgefüllte Fragebögen) werden nach der Erfassung und Verarbeitung gemäß AV-Vertrag vernichtet. Die Vernichtung richtet sich nach den Vorgaben der DIN 66399 und wird protokolliert.
- Interne und externe Speichermedien, die nach ihrem bisherigen Gebrauch für einen erneuten Gebrauch freigegeben werden sollen, werden nach den geltenden Standards mit Hilfe geeigneter Software so sicher überschrieben, dass keine Daten mehr rekonstruiert werden können.
- Daten auf intakten Festplatten werden nach den geltenden Standards mit Hilfe geeigneter Software so sicher überschrieben, dass keine Daten mehr rekonstruiert werden können.
- Interne und externe Speichermedien, die nicht mehr verwendet werden können, werden gemäß DIN 66399 vernichtet.

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Die Daten werden in Form von Projekten auf dem Rechner des bearbeitenden Mitarbeitenden gespeichert. Auf den einzelnen Rechnern wiederum erfolgt die Ablage und Verarbeitung in getrennten Ordnerstrukturen.

1.5 Pseudonymisierung/Anonymisierung

Maßnahmen, die nötig sind, um personenbezogene Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zuzuordnen sind.

- Bei Prozessen - in denen keine Zuordnung von einzelnen Datensätzen zu einer Person notwendig ist - werden diese mit einer Nummer oder einem nicht personenbezogenen Namen versehen.
- Pseudonymisierte Daten werden getrennt von den Informationen zur Identifizierung der einzelnen Personen aufbewahrt (z. B. in getrennten Datenbanken, Räumen und Aktenschränken).
- Nur die Mitarbeitenden, die an der Datenverarbeitung betraut sind, haben Zugriff auf die zur Identifizierung notwendigen Daten.

2. Integrität

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Externen Speichermedien, die zur Datensicherung und zum Transport der Daten genutzt werden, werden mit einer geeigneten Software verschlüsselt.

- Nach Erhalt der Originaldaten (z. B. durch den Download aus der Befragungssoftware) werden die Daten physisch übertragen. Dies betrifft zum einen die Speicherung auf externen Speichermedien, um die Daten vor Verlust oder Zerstörung zu schützen, zum anderen den Transport zwischen Rechnern der Mitarbeitenden von Salubris, sofern dies notwendig sein sollte (Urlaub, Krankheit etc.).
- Die Verschlüsselung von E-Mails erfolgt über den vom Host-Anbieter angebotene Sicherheitsverfahren und entspricht den datenschutzrechtlichen Vorgaben. Mit dem Host-Anbieter wurde ein entsprechender AV-Vertrag geschlossen.

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Original-Datendateien (Rohdaten) werden verschlüsselt auf Festplatten gespeichert. Eine Verarbeitung der Daten erfolgt nur anhand einer Kopie der Originaldaten (Arbeitsdatei).
- Alle Änderungen, die an der ursprünglichen Rohdaten-Datei vorgenommen werden müssen, werden dokumentiert. Die Dokumentation enthält die vorgenommene Veränderung und einen Hinweis auf die Person, die die Veränderung vorgenommen hat.
- Zu dem beschriebenen Vorgehen der Eingabekontrolle haben alle Mitarbeitenden eine Richtlinie erhalten.

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Die gespeicherten Daten sind in der oben beschriebenen Form gegen ungewollte Zugriffe geschützt (siehe Punkt 1).
- Die gespeicherten Daten sind vor Stromausfall (unterbrechungsfreie Stromversorgung) und Feuerschäden (Rauchmelder und Feuerlöschgeräte) geschützt. Es liegt kein Hochwassergebiet vor.
- Mithilfe eines geeigneten Backup-Programmes auf den Rechnern der Mitarbeitenden wird ein tägliches Backup durchgeführt und Daten verschlüsselt gespeichert (AES-Verfahren). Das Backup wird automatisiert durchgeführt. Die Sicherungen stellen ein identisches Abbild der ursprünglichen Daten dar. Bei einem Ausfall des ursprünglichen Systems können die Daten über die Sicherung problemlos rekonstruiert werden.
- Die datenverarbeitenden Rechner sind durch Firewall-Programme sowie Anti-Viren-Programme geschützt. Die Programme werden durch automatisierte Updates regelmäßig aktualisiert.
- Bei Bedarf wird für Einrichtung und Wartung von IT-bezogenen Sicherheitsmaßnahmen ein externes Fachunternehmen beauftragt und ein entsprechender AV-Vertrag gem. Art. 28 DSGVO abgeschlossen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutzmanagement

Maßnahmen, die geeignet sind, ein funktionierendes Datenschutzmanagement zu gewährleisten.

- Mitarbeitende werden regelmäßig zum Thema Datenschutz durch den/die Datenschutzbeauftragte/n geschult und sensibilisiert. Die Teilnahme ist verpflichtend.
- Mitarbeitende sind verpflichtet, sofort nach Kenntnisnahme einer Datenpannen den/die Datenschutzbeauftragte/n zu informieren.
- Mitarbeitende sind verpflichtet, vor Einsatz einer neuen Software oder eines neuen Dienstleisters den/die Datenschutzbeauftragte/n einzubinden.
- Ein Verfahrensverzeichnis von Verarbeitungstätigkeiten wird nach Art. 30 DSGVO kontinuierlich nachgehalten.
- Mitarbeitende sind auf die Vertraulichkeit und den Datenschutz verpflichtet worden.
- Das Vorgehen zur Wahrnehmung von Betroffenenrechten ist in der Vereinbarung zur Auftragsverarbeitung von Daten nach Art. 28 DSGVO geregelt.
- Bei Störungen technischer Systeme, die nur durch Fachpersonal behoben werden können, wird unverzüglich ein externes Fachunternehmen mit der Beseitigung der Störungen beauftragt. Mit dem Unternehmen wird dann gem. Art. 28 DSGVO ein AV-Vertrag abgeschlossen.
- Es finden regelmäßige Datenschutzaudits durch den/die Datenschutzbeauftragte/n (mindestens jährlich) statt.

4.2 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Bei Bedarf beauftragt Salubris in Abstimmung mit dem Auftraggeber einen weiteren Unterauftragnehmer für die Erhebung oder Erfassung von Daten.
- In diesen Fällen schließt Salubris mit dem Unterauftragnehmer einen AV-Vertrag gemäß Art. 28 DSGVO ab. Salubris stellt seinem Auftraggeber Kopien dieser Verträge sowie die Erklärungen zu den technischen und organisatorischen Maßnahmen zum Datenschutz gemäß Art. 32 DSGVO zur Verfügung.
- Gemäß DSGVO behält Salubris in diesen Fällen die Verantwortung für die Einhaltung der vereinbarten datenschutzrechtlichen Vorschriften. Bei der Auswahl des Unterauftragnehmers wird daher insbesondere auf den Gesichtspunkt Datensicherheit bzw. Datenschutz geachtet.
- Die Unterauftragnehmer werden gemäß der jeweiligen AV-Verträge nach Art. 28 DSGVO verpflichtet, erhobenen Daten unwiederbringlich zu löschen.