TREUHAND|SUISSE Schweizerischer Treuhänderverband

DATENSCHUTZ IN DER TREUHANDBRANCHE

Ein Leitfaden von TREUHAND|SUISSE

Version 1 vom Juli 2018

TREUHAND | SUISSE

DATENSCHUTZ GEHT UNS ALLE AN

Seit dem 25. Mai 2018 gilt in den EU- und EWR-Staaten nach zweijähriger Übergangsfrist die Europäische Datenschutz-Grundverordnung (DSGVO). Aufgrund des sog. Marktortprinzips ist die DSGVO auch auf Unternehmen ausserhalb der EU direkt anwendbar, wenn sie Daten von Personen in der EU (oder im EWR) verarbeiten und die Datenverarbeitung entweder dazu dient, Waren oder Dienstleistungen in der EU oder im EWR anzubieten oder das Verhalten von Personen in der EU oder im EWR zu beobachten.

Nicht jeder grenzüberschreitende Sachverhalt führt automatisch zur Anwendbarkeit der DSGVO. Es empfiehlt sich jedoch, solche Situationen vertiefter abzuklären. Zudem verlangen in der Praxis Unternehmen aus der EU vertraglich häufig explizit die Einhaltung der DSGVO und entsprechende Erklärungen.

Die DSGVO hat das Thema Datenschutz in den Fokus einer breiten Öffentlichkeit gestellt. Die datenschutzrechtlichen Grundsätze sind jedoch weitgehend die gleichen geblieben. Sowohl nach DSGVO als auch nach schweizerischem Datenschutzgesetz (DSG) dürfen Daten nur bearbeitet werden, wenn dies rechtmässig geschieht. Insbesondere müssen bei der Bearbeitung (Terminologie DSG) resp. Verarbeitung (Terminologie DSGVO) von Daten die Grundsätze von Treu und Glauben, der Verhältnismässigkeit und Zweckgebundenheit berücksichtigt werden. Daran ändert auch die DSGVO nichts. Allerdings sind in ihrem Bereich noch zahlreiche Detailfragen ungeklärt. Sie werden sich erst im Laufe der Zeit beantworten lassen.

Datenschutz ist gerade in der Treuhandbranche nicht nur aus rechtlichen, sondern auch aus unternehmerischen Gründen ein zentrales Thema. Deshalb stellt TREUHAND|SUISSE seinen Mitgliedern mit diesem Leitfaden ein Instrument zur Verfügung, sich mit dem Thema Datenschutz zu beschäftigen und das eigene Unternehmen sowie die Kunden für den Datenschutz im Allgemeinen und die DSGVO im Besonderen fit zu machen. Der Leitfaden dient der allgemeinen Information und kann nicht abschliessend sein. Er ersetzt die Auseinandersetzung mit dem Thema im eigenen Unternehmen und nötigenfalls den Beizug von Dritten nicht. Der Leitfaden soll für das Thema Datenschutz sensibilisieren und für Standardsituationen in der Treuhandbranche mögliche Lösungsansätze aufzeigen.

In einem ersten Teil (FAQ Datenschutz und DSGVO) beantwortet der Leitfaden allgemeine Fragen zum Datenschutz und zur DSGVO. Der zweite Teil (Datenschutz in der Treuhandbranche) setzt sich mit den für die Treuhandbranche relevanten Themenbereichen Webseite / Newsletter / Social Media, Personal und Kunden auseinander. Checklisten zum Schluss zeigen typische Geschäftstätigkeiten von Treuhändern und beurteilen allgemein, ob die DSGVO tendenziell anwendbar ist oder nicht, helfen bei der Beurteilung, ob die Datenverarbeitung rechtmässig erfolgt und erläutern den wichtigsten Handlungsbedarf.

Aktuell befindet sich auch die schweizerische Datenschutzgesetzgebung in Revision. Es sind zahlreiche Anpassungen an die DSGVO zu erwarten, so dass selbst Treuhandunternehmen, die nicht in den Anwendungsbereich der EU-Verordnung fallen, gut daran tun, sich mit dem Thema auseinanderzusetzen. Zudem verlangen Kunden und Geschäftspartner vermehrt entsprechende Erklärungen.

FAQ DATENSCHUTZ UND DSGVO

1) Für wen gilt die DSGVO?

Die DSGVO gilt in allen EU- und EWR-Staaten direkt. In Drittstaaten ausserhalb der EU und des EWR (z.B. Schweiz, USA) findet sie aufgrund des sog. Marktortprinzips Anwendung, wenn personenbezogene Daten von Personen, die sich in der EU oder im EWR befinden, verarbeitet werden, sofern die Datenverarbeitung im Zusammenhang steht mit dem Angebot von Waren und Dienstleistungen oder mit der Verhaltensbeobachtung von Personen in der EU oder im EWR (z.B. mittels Cookies und Trackingtools auf einer Webseite). Die Staatsangehörigkeit einer Person und ihr Wohnsitz oder Aufenthalt spielen keine Rolle. Es wird alleine auf den Zielmarkt abgestellt resp. darauf, ob sich eine Person in diesem befindet.

Auf den Punkt gebracht:

- Sie fallen in den Anwendungsbereich der DSGVO, wenn Sie Ihre Dienstleistungen oder Waren Kunden in der EU oder im EWR anbieten (gilt auch für Gratisangebote), oder wenn Ihre in der EU oder im EWR zugängliche Webseite Cookies, Analyse- und Trackingtools etc. benützt.

2) Welche Daten sind geschützt?

Im Gegensatz zum schweizerischen Datenschutzgesetz (DSG) schützt die DSGVO nur Daten von natürlichen Personen. Der Schutz des DSG erstreckt sich auch auf juristische Personen. Für verstorbene Personen gilt weder die DSGVO noch das DSG.
Geschützt sind im Weiteren nur «personenbezogene Daten» (DSGVO) resp. «Personendaten» (DSG). Als solche gelten alle Informationen und Angaben, die sich auf eine identifizierte oder identifizierbare Person beziehen und einer bestimmten Person zugeordnet werden können.

Auf den Punkt gebracht:

- Nach DSGVO sind nur Daten von bestimmten oder bestimmbaren natürlichen Personen (Name, AHV-Nummer, IP-Adressen, Standortdaten etc.) geschützt.
- Daten von *juristischen* Personen sind nach DSVO nicht geschützt, wohl aber nach DSG.

3) Was bedeutet Verarbeitung von Daten?

Die DSGVO spricht von Verarbeitung von Daten, das DSG von Bearbeitung. Gemeint ist weitestgehend dasselbe. Der Begriff ist weit zu fassen: Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Umgang mit Personendaten als Verarbeitung, namentlich fallen darunter das Erheben, Erfassen, Organisieren, Abfragen, Übermitteln, Verbreiten, Speichern, Ändern, Löschen oder Vernichten.
Die Verarbeitung von Daten muss rechtmässig erfolgen. Dabei dürfen grundsätzlich nur diejenigen Daten bearbeitet werden, die für den entsprechenden Verarbeitungszweck nötig sind.

Auf den Punkt gebracht:

- Jeder Umgang mit personenbezogenen Daten, der nicht zu rein privaten/familiären Zwecken erfolgt, gilt als Datenverarbeitung und fällt unter den Datenschutz. Das DSG schützt die Daten von natürlichen und juristischen, die DSGVO nur von natürlichen Personen.

4) Welche Grundsätze gelten für die Verarbeitung von Personendaten?

Daten dürfen sowohl nach DSG als auch nach DSGVO ausschliesslich rechtmässig, nach Treu und Glauben, zweckgebunden und erkennbar/transparent verarbeitet werden. Nach DSGVO muss die Einhaltung der Grundsätze nachgewiesen werden können (Rechenschaftspflicht).

Es gelten die folgenden Grundsätze:

Rechtmässigkeit: Rechtmässig ist eine Datenverarbeitung, wenn a) eine Einwilligung vorliegt, b) sie für die Erfüllung eines Vertrags erforderlich ist, c) sie für die Erfüllung einer rechtlichen Pflicht erforderlich ist, d) zur Wahrung lebenswichtiger Interessen erforderlich ist, e) sie zur Erfüllung einer Aufgabe im öffentlichen Interesse erforderlich ist, oder f) zur Wahrung berechtigter Interessen erforderlich ist.

Transparenz: Der Verantwortliche informiert präzise, verständlich und transparent über Name und Kontaktdaten des Verantwortlichen, den Zweck der Datenverarbeitung und allenfalls weitere Punkte wie Dauer der Datenspeicherung, Auskunfts- oder Löschungsrecht.

Zweckbindung: Daten dürfen nur für den angegebenen, legitimen Zweck verarbeitet werden.

Datenminimierung: Die Datenverarbeitung ist auf das für den Zweck notwendige Mass zu beschränken («so viel wie nötig, sowenig wie möglich»).

Richtigkeit: Die verarbeiteten Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Unrichtige Daten müssen unverzüglich gelöscht oder berichtigt werden.

Speicherbegrenzung: Die Speicherung von Daten muss in einer Form geschehen, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für den Zweck erforderlich ist.

Datensicherheit: Personendaten müssen vor unbefugter oder unrechtmässiger Verarbeitung geschützt werden.

Auf den Punkt gebracht:

- Wenn Sie die datenschutzrechtlichen Grundsätze bei der Datenbearbeitung bereits bisher beachtet haben, bringt die DSGVO in diesem Bereich nichts grundsätzlich Neues.
- Es dürfen nur diejenigen Daten bearbeitet werden, die für den entsprechenden Zweck notwendig sind.

5) Welche Rechte hat die betroffene Person?

Sowohl nach DSG als auch nach DSGVO hat die betroffene Person namentlich ein Auskunftsrecht sowie ein Recht auf Berichtigung oder Löschung unrichtiger resp. nicht mehr erforderlicher Daten.

Auf den Punkt gebracht:

- **Auskunftsrecht:** Die betroffene Person kann namentlich darüber Auskunft verlangen, ob über sie Personendaten verarbeitet werden, wenn ja welche, von welcher Herkunft und zu welchem Zweck.
- **Berichtigungsrecht:** Die betroffene Person kann die sofortige Berichtigung unrichtiger Personendaten verlangen.
- **Löschungsrecht:** Die betroffene Person kann die Löschung der Personendaten verlangen, wenn die Datenverarbeitung nicht mehr erforderlich ist, wenn die Einwilligung in die Datenverarbeitung der einzige Rechtfertigungsgrund war und nun widerrufen wird, wenn Widerspruch nach DSGVO eingelegt wird, oder wenn die Daten unrechtmässig bearbeitet werden.

6) Was ist eine Datenschutzerklärung?

Wer im Anwendungsbereich der DSGVO Daten bearbeitet, muss die betroffenen Personen «in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache» darüber informieren. Diese Datenschutzerklärung hat insbesondere den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls eines Vertreters oder eines Datenschutzbeauftragten zu enthalten. Im Weiteren sind namentlich der Zweck der Datenverarbeitung, die Rechtsgrundlage, die Rechte der betroffenen Person sowie wenn möglich die Dauer der Datenspeicherung anzugeben. Die Erklärung erfolgt in der Regel schriftlich oder (vor allem bei Webseiten oder im E-Mail-Kontakt) in elektronischer Form.

Diese Informationspflicht besteht im Gegensatz zur Pflicht zum Führen eines Verzeichnisses (s. FAQ 7) unabhängig der Unternehmensgrösse.

Auf den Punkt gebracht:

- Mit der Datenschutzerklärung kommt das datenverarbeitende Unternehmen seiner Informationspflicht gegenüber der betroffenen Person gemäss DSGVO nach.
- Die Informationspflicht umfasst namentlich die Angabe der Kontaktdaten, des Datenverarbeitungszwecks, der Rechtsgrundlage und der Rechte der betroffenen Person.

7) Welche Dokumentation ist nach DSGVO erforderlich?

Nach DSGVO muss jeder, der Personendaten verarbeitet, ein Verzeichnis über seine Verarbeitungstätigkeiten führen. Dieses Verzeichnis muss folgende Angaben enthalten: a) Name und Kontaktdaten des Verantwortlichen, b) Zweck der Datenverarbeitung, c) Beschreibung der Kategorie betroffener Personen und Daten, d) Kategorie allfälliger Datenempfänger, e) gegebenenfalls Datenübermittlung an ein Drittland, f) wenn möglich Fristen für die Löschung verschiedener Datenkategorien und g) wenn möglich eine allgemeine Beschreibung der technischen und organisatorischen Massnahmen bezüglich Datensicherheit.

KMU-Artikel: Die Pflicht zum Führen des Verzeichnisses entfällt, wenn

- das Unternehmen weniger als 250 Mitarbeiter beschäftigt,
- die Datenverarbeitung kein Risiko für die Rechte der betroffenen Personen birgt,
- die Verarbeitung nur gelegentlich erfolgt oder
- keine besondere Datenkategorie betroffen ist.

Auf den Punkt gebracht:

- Die Pflicht zum Führen des Verzeichnisses von Verarbeitungstätigkeiten entfällt bei Unternehmen mit weniger als 250 Mitarbeitern.

- Die DSGVO schreibt nur den Inhalt nicht die Form des Verzeichnisses vor. Es sind sowohl tabellarische Darstellungen als auch Erläuterungen in Lauftextform oder Kombinationen denkbar. Das Verzeichnis wird oft als Teil einer Datenschutzrichtlinie oder eines Datenschutzkonzepts geführt. Wichtig ist dabei insbesondere, dass dieses Dokument stets aktuell gehalten wird.

DATENSCHUTZ IN DER TREUHANDBRANCHE
THEMENBEREICH 1: WEBSEITEN / NEWSLETTER / SOCIAL MEDIA

1) Anwendbarkeit der DSGVO

Die DSGVO ist anwendbar, wenn Unternehmen aus Drittstaaten wie der Schweiz entweder ihre Dienstleistungen oder Produkte in der EU oder im EWR anbieten oder wenn sie das Verhalten von Personen in der EU oder im EWR beobachten. Webseiten und Angebote über Webseiten sind daher ein häufiger Anknüpfungspunkt für die Unterstellung unter die DSGVO. Einerseits kann ein Unternehmen über Webseiten seine Produkte und Dienstleistungen auch in der EU und im EWR anbieten, andererseits nutzen heute die meisten Webseiten-Cookies, Tracking- und Analysetools, die der Verhaltensbeobachtung dienen. Die Zugänglichkeit der Webseite in der EU oder im EWR führt nach aktuellem Wissensstand allein nicht zur Anwendbarkeit. Sobald jedoch ein Angebot (auch) für Kunden in der EU oder im EWR erfolgt, Preise in Euro angegeben oder Domains in der EU oder im EWR verwendet werden, deutet dies auf ein Angebot mit dem Zielmarkt EU/EWR und auf die Anwendbarkeit der DSGVO hin. Sobald die Webseite Daten über Besucher aus der EU oder dem EWR sammelt, ist die DSGVO anwendbar.

2) Zulässigkeit der Datenverarbeitung im Bereich Webseiten / Newsletter / Social Media

Da mit den Besuchern der Webseite regelmässig keine vertraglichen Beziehungen bestehen, müssen diese auf die Verwendung von Cookies, Tracking- und Analysetools hingewiesen werden, und die betroffene Person muss aktiv ihr Einverständnis erklären (Kästchen, in denen bereits Häkchen gesetzt sind, sind nicht zulässig). Die Einwilligung muss nachgewiesen werden können und die betroffene Person kann sie jederzeit widerrufen (z.B. bei Newslettern). Im Bereich Webseiten / Newsletter / Social Media besteht mitunter der grösste Handlungsbedarf für Treuhandunternehmen.

3) Datenminimierung

Es dürfen nur diejenigen Daten verarbeitet werden, die für den entsprechenden Zweck erforderlich sind. Aus diesem Grund ist gerade im Bereich der Webseiten / Newsletter / Social Media der Zweck zu bezeichnen. Tendenziell werden zu viele Daten erhoben. So ist z.B. für den Versand eines nicht personalisierten elektronischen Newsletters in der Regel die Angabe des Geburtsdatums einer Person, der Postanschrift oder des Namens nicht nötig.

4) Privacy by default und privacy by design

Webseiten müssen so ausgestaltet sein, dass durch technische Voreinstellungen der grösstmögliche Datenschutz der Besucher gewährleistet ist. Die DSGVO verlangt «Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen» (privacy by design und privacy by default). Bereits bei der Planung der Datenverarbeitung muss das Unternehmen durch geeignete technische und organisatorische Massnahmen sicherstellen, dass nur Daten verarbeitet werden, die für den jeweiligen Zweck erforderlich sind, und dass die Datenschutzgrundsätze wirksam umgesetzt werden.

5) Aufbewahrung und Löschung von Daten

Die Daten dürfen solange aufbewahrt werden, wie es für den Zweck erforderlich ist. Nicht mehr erforderliche Daten sind zu löschen. Werden Daten für den Versand eines elektronischen Newsletters verarbeitet, sind diese z.B. zu löschen, wenn die betroffene Person den Newsletter abbestellt.

6) Datenschutzerklärung nach DSGVO

Die Datenschutzerklärung betreffend Datenverarbeitung via Webseite muss auf dieser unentgeltlich leicht zugänglich abrufbar sein. Sie hat insbesondere den Namen und die Kontaktdaten des Verantwortlichen (Treuhandunternehmen) sowie gegebenenfalls eines Vertreters oder eines Datenschutzbeauftragten zu enthalten. Im Weiteren sind namentlich der Zweck der Datenverarbeitung, die Rechtsgrundlage, die Rechte der betroffenen Person sowie wenn möglich die Dauer der Datenspeicherung anzugeben.

7) Verzeichnis von Verarbeitungstätigkeit nach DSGVO

Wer in den Anwendungsbereich der DSGVO fällt, muss ein Verzeichnis führen über alle Verarbeitungstätigkeiten im entsprechenden Bereich. Dieses Verzeichnis enthält den Namen und die Kontaktdaten des Verantwortlichen (Treuhandunternehmen und gegebenenfalls interner Datenschutzbeauftragter), den Zweck der Verarbeitung, eine Umschreibung der Kategorie betroffener Personen (Besucher der Webseite), die Kategorie von Empfängern gegenüber denen die personenbezogenen Daten offengelegt werden, wenn möglich vorgesehene Fristen für die Löschung der Datenkategorien und wenn möglich eine allgemeine Beschreibung der verschiedenen Datenkategorien.

KMU-Artikel: Die Pflicht zum Führen des Verzeichnisses entfällt, wenn

- das Unternehmen weniger als 250 Mitarbeiter beschäftigt
- die Datenverarbeitung kein Risiko für die Rechte der betroffenen Personen birgt
- die Verarbeitung nur gelegentlich erfolgt oder
- keine besondere Datenkategorie betroffen ist

8) Weitere Informationen: Institut 4.0 von TREUHAND|SUISSE

Praxisguide und weitere Informationen:

Die sich aus der DSGVO ergebenden Anforderungen im Bereich Webseiten / Newsletter / Social Media sowie deren Umsetzung kann fallweise juristisch und technisch sehr komplex sein. Aus diesem Grund hat das Institut Treuhand 4.0 einen umfangreichen Praxisguide erarbeitet, welcher auf die vorgenannten Punkte und weitere Themen (z.B. Share Buttons, Kontaktformulare, Social Login, etc.) im Detail eingeht und hilfreiche Checklisten und Tipps für die Umsetzung in der Praxis liefert. Der Praxisguide kann auf der Website des Instituts Treuhand 4.0 (www.treuhand40.ch) bezogen werden. Zudem steht das Institut Treuhand 4.0 für weiterführende Fragen gerne zur Verfügung.

THEMENBEREICH 2: PERSONAL: PERSONAL

1) Anwendbarkeit der DSGVO

Das Bearbeiten von Bewerbungsunterlagen und das Führen eines Personaldossiers gelten sowohl unter DSGVO als auch unter DSG als Datenverarbeitung. Solange sich Arbeitgeber und Arbeitnehmer in der Schweiz befinden und die Datenverarbeitung (Personaldossier) in

der Schweiz vorgenommen wird, findet die DSGVO keine Anwendung. Sobald sich der Arbeitnehmer in der EU oder im EWR befindet, spielt die Auslegung des Begriffs des Angebots von Dienstleistung eine zentrale Rolle. Denn sobald die Datenverarbeitung des Arbeitgebers im Zusammenhang steht mit dem Angebot einer Dienstleistung in der EU oder im EWR, findet die DSGVO Anwendung auf den Schweizer Arbeitgeber und seine Datenverarbeitung.

Der Begriff der Dienstleistung wird grundsätzlich weit gefasst, allerdings ist zurzeit unklar und umstritten, was darunterfällt und was nicht. So ist aktuell unklar, ob bereits die reine Lohnzahlung in die EU oder in den EWR genügt (nach der hier vertretenen Meinung eher nicht).

Tendenziell als Dienstleistung qualifiziert werden dürfte allerdings beispielsweise das Zurverfügungstellen eines Geschäftsfahrzeugs zu privaten Zwecken in der EU oder im EWR.

2) Zulässigkeit der Datenverarbeitung im Rekrutierungsverfahren und im Anstellungsverhältnis

Sowohl im Rekrutierungsverfahren als auch im Anstellungsverhältnis sind die datenschutzrechtlichen Grundsätze zu beachten. Insbesondere dürfen sowohl nach DSG als auch nach DSGVO nur diejenigen Personendaten verarbeitet werden, die zum Zweck der Rekrutierung resp. zum Zweck der Abwicklung des Arbeitsverhältnisses erforderlich sind.

Rekrutierungsverfahren:

- Die betroffene Person muss der Datenverarbeitung grundsätzlich zustimmen. Das Einreichen eines Bewerbungsdossiers gilt als Einwilligung zur Datenverarbeitung zum Zweck des Rekrutierungsverfahrens.
- Im Rekrutierungsverfahren dürfen nur Personendaten erhoben werden, die erforderlich sind, um die Qualifikationen des Arbeitnehmers und seine Eignung für die ausgeschriebene Stelle abzuklären. So dürfen etwa folgende Daten im Rekrutierungsstadium in der Regel nicht erhoben werden: AHV-Nummer, Kontonummer, Familienverhältnisse etc.

Anstellungsverhältnis:

- Die Datenverarbeitung («Führen des Personaldossiers») ist rechtmässig, soweit sie für die Erfüllung des konkreten Arbeitsvertrags und der rechtlichen Verpflichtungen daraus erforderlich ist (Zweckgebundenheit).
- Im Anstellungsverhältnis dürfen Personendaten erhoben werden, die erforderlich sind für die Erfüllung einer rechtlichen Verpflichtung (z.B. Arbeitszeiten, krankheitsbedingte Absenzen, AHV-Nummer), für die Personaladministration (z.B. Geburtsdatum, Familienstand, Bankverbindung) oder für die Arbeitsorganisation (z.B. Freitage, geplante Absenzen, Krankheiten/Unverträglichkeiten).

3) Datenminimierung und Datensicherheit

Das Personaldossier darf nur Personaldaten enthalten, die für die Abwicklung des konkreten Arbeitsverhältnisses (inkl. vor- und nachvertragliches Stadium) erforderlich sind. Personaldaten, die keine Relevanz (mehr) aufweisen (z.B. alte Verwarnungen des Arbeitnehmers) sind zu löschen. Elektronisch geführte Personaldossiers müssen durch geeignete technische und organisatorische Massnahmen vor Zugriff durch Unbefugte sowie unbefugter und unrechtmässiger Verarbeitung oder Verlust geschützt sein.

4) Aufbewahrung und Löschung von Daten

Die Daten dürfen solange aufbewahrt werden, wie es für den Zweck erforderlich ist. Im Rekrutierungsverfahren sind die Daten zu löschen, sobald feststeht, dass der entsprechende Kandidat die Stelle nicht erhält oder nicht antritt. Personaldossiers sollten regelmässig darauf überprüft werden, ob die darin enthaltenen Daten noch erforderlich sind oder nicht. Nicht mehr erforderliche Daten sind zu löschen. Nach Austritt des Arbeitnehmers sind nur noch diejenigen Daten aufzubewahren, die für nachvertragliche Ansprüche resp. die Abwehr entsprechender Forderungen erforderlich sind.

Der Arbeitnehmer kann die Löschung von Daten verlangen, wenn diese für den Zweck, zu dem sie erhoben wurden, nicht mehr notwendig sind, oder wenn sie unrechtmässig verarbeitet wurden. Der Arbeitgeber muss die Daten nicht löschen, soweit die Verarbeitung nötig ist für die Vertragsabwicklung sowie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

5) Datenschutzerklärung nach DSGVO

Die Datenschutzerklärung betreffend Datenverarbeitung für das Personalwesen muss in der Regel schriftlich (Vertrag, Reglement, Merkblätter) oder elektronisch (Intranet) erfolgen. Sie hat insbesondere den Namen und die Kontaktdaten des Verantwortlichen (Arbeitgeber) sowie gegebenenfalls eines Vertreters oder eines Datenschutzbeauftragten zu enthalten. Im Weiteren sind namentlich der Zweck der Datenverarbeitung, die Rechtsgrundlage, die Rechte der betroffenen Person sowie wenn möglich die Dauer der Datenspeicherung anzugeben.

6) Verzeichnis von Verarbeitungstätigkeiten nach DSGVO

Wer in den Anwendungsbereich der DSGVO fällt, muss ein Verzeichnis führen über alle Verarbeitungstätigkeiten im entsprechenden Bereich. Dieses Verzeichnis enthält den Namen und die Kontaktdaten des Verantwortlichen (Arbeitgeber und gegebenenfalls interner Datenschutzbeauftragter), den Zweck der Verarbeitung (Personaladministration), eine Umschreibung der Kategorie betroffener Personen (Arbeitnehmer), die Kategorie von Empfängern gegenüber denen die personenbezogenen Daten offengelegt werden, wenn möglich vorgesehene Fristen für die Löschung der Datenkategorien und wenn möglich eine allgemeine Beschreibung der verschiedenen Datenkategorien.

KMU-Artikel: Die Pflicht zum Führen des Verzeichnisses entfällt, wenn

- das Unternehmen weniger als 250 Mitarbeiter beschäftigt,
- die Datenverarbeitung kein Risiko für die Rechte der betroffenen Personen birgt,
- die Verarbeitung nur gelegentlich erfolgt oder
- keine besondere Datenkategorie betroffen ist.

THEMENBEREICH 3: KUNDEN

1) Anwendbarkeit der DSGVO

Für reine Binnenverhältnisse gilt das DSG. Die DSGVO ist anwendbar, wenn das Treuhandunternehmen seine Waren oder Dienstleistungen in der EU oder im EWR anbietet. Die Tätigkeit des Treuhänders gilt dabei grundsätzlich als Dienstleistung im Sinne der DSGVO. Ist die betroffene Person (Kunde) eine juristische Person, findet die DSGVO keine Anwendung. Achtung: Sobald personenbezogene Daten einer natürlichen Person erhoben werden (z.B. Name, E-Mail und Telefonnummer Ansprechpartner), fallen diese gegebenenfalls unter die DSGVO.

2) Zulässigkeit der Datenverarbeitung im Kundenverhältnis

Im Verhältnis zwischen Treuhandunternehmen und Kunde sind die datenschutzrechtlichen Grundsätze zu beachten. Insbesondere dürfen sowohl nach DSG (von natürlichen und juristischen Personen) als auch nach DSGVO (von natürlichen Personen) nur diejenigen Personendaten verarbeitet werden, die zum Zweck der Abwicklung des konkreten Auftrags erforderlich sind. Die Datenverarbeitung ist rechtmässig sofern und soweit sie für die Erfüllung des Vertrags oder einer rechtlichen Verpflichtung erforderlich ist. Eine separate Einwilligung des Betroffenen ist zwingend.

3) Datenminimierung

Der Treuhänder darf nur Daten erheben, die für die Abwicklung des konkreten Vertragsverhältnisses (inkl. vor- und nachvertragliches Stadium) erforderlich sind. Personaldaten, die keine Relevanz (mehr) aufweisen sind zu löschen, oder es ist eine explizite Einwilligung der betroffenen Person einzuholen.

Elektronisch geführte Datensammlungen müssen durch geeignete technische und organisatorische Massnahmen vor Zugriff durch Unbefugte sowie unbefugter und unrechtmässiger Verarbeitung oder Verlust geschützt sein.

4) Aufbewahrung und Löschung von Daten

Die Daten dürfen solange aufbewahrt werden, wie es für den Zweck erforderlich ist. Nicht mehr erforderliche Daten sind zu löschen. Nach Beendigung des Vertragsverhältnisses sind nur noch diejenigen Daten aufzubewahren, für deren Aufbewahrung eine rechtliche Verpflichtung besteht (z.B. Aufbewahrungspflichten nach Obligationenrecht).
Der Kunde kann die Löschung von Daten verlangen, wenn diese für den Zweck, zu dem sie erhoben wurden, nicht mehr notwendig sind oder wenn sie unrechtmässig verarbeitet wurden. Der Treuhänder muss die Daten nicht löschen, sofern und soweit ihn eine rechtliche Verpflichtung trifft, oder die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

5) Datenschutzerklärung nach DSGVO

Die Datenschutzerklärung betreffend Datenverarbeitung im Hinblick auf die Erfüllung der Verträge mit Kunden wird in der Regel schriftlich (Vertrag) erfolgen. Wenn der Kunde dies verlangt, und seine Identität nachgewiesen ist, kann die Information auch mündlich erfolgen. Die Datenschutzerklärung hat insbesondere den Namen und die Kontaktdaten des Verantwortlichen (Treuhandunternehmen) sowie gegebenenfalls eines Vertreters oder eines Datenschutzbeauftragten zu enthalten. Im Weiteren sind namentlich der Zweck der Datenverarbeitung, die Rechtsgrundlage, die Rechte der betroffenen Person sowie wenn möglich die Dauer der Datenspeicherung anzugeben.

6) Verzeichnis von Verarbeitungstätigkeiten nach DSGVO

Wer in den Anwendungsbereich der DSGVO fällt, muss ein Verzeichnis führen über alle Verarbeitungstätigkeiten im entsprechenden Bereich. Dieses Verzeichnis enthält den Namen und die Kontaktdaten des Verantwortlichen (Treuhandunternehmen und gegebenenfalls interner Datenschutzbeauftragter), den Zweck der Verarbeitung, eine Umschreibung der Kategorie betroffener Personen (Treuhandkunden), die Kategorie von Empfängern gegenüber denen die personenbezogenen Daten offengelegt werden, wenn möglich vorgesehene Fristen für die Löschung der Datenkategorien und wenn möglich eine allgemeine Beschreibung der verschiedenen Datenkategorien.

KMU-Artikel: Die Pflicht zum Führen des Verzeichnisses entfällt, wenn

- das Unternehmen weniger als 250 Mitarbeiter beschäftigt,
- die Datenverarbeitung kein Risiko für die Rechte der betroffenen Personen birgt,
- die Verarbeitung nur gelegentlich erfolgt oder
- keine besondere Datenkategorie betroffen ist.

DSGVO-CHECKLISTEN FÜR TREUHÄNDER

ANWENDBARKEIT DSGVO

DSGVO (tendenziell) nicht anwendbar	DSGVO (tendenziell) anwendbar
☐ Treuhandunternehmen hat Arbeitnehmer aus EU-/EWR-Staaten mit Arbeitsort CH.	☐ Treuhandunternehmen hat eine Tochtergesellschaft, Zweigniederlassung, Filiale oder Betriebsstätte in EU-/EWR-Staaten.
☐ Webseite des Treuhandunternehmens ist nur auf den Schweizer Markt ausgerichtet und verwendet keine Cookies, Tracking- und Analysetools etc. (Verhaltensbeobachtung).	☐ Webseite des Treuhandunternehmens ist in EU-/EWR-Staaten zugänglich und verwendet Cookies, Tracking- und Analysetools etc. (Verhaltensbeobachtung).
☐ Geschäftstätigkeit des Treuhandunternehmens ist ausschliesslich auf Kunden in der Schweiz ausgerichtet.	☐ Geschäftstätigkeit des Treuhandunternehmens ist (auch) auf Kunden in EU-/EWR-Staaten ausgerichtet.
☐ Treuhandunternehmen führt Lohnbuchhaltung/Saläradministration für Kunden in CH mit Arbeitnehmern aus EU-/EWR-Staaten	☐ Treuhandunternehmen hat Kunden in EU-/EWR-Staaten, über die es Daten (auch) natürlicher Personen wie Ansprechperson, persönliche E-Mailadressen etc. verarbeitet (Kundendatenbank).
☐ Die Kundendatenbank des Treuhandunternehmens enthält ausschliesslich Daten von natürlichen oder juristischen Personen in der Schweiz oder ausschliesslich Daten juristischer Personen in EU-/EWR-Staaten (keine Daten zu Ansprechpersonen, persönlichen E-Mailadressen etc.).	☐ Treuhandunternehmen bietet (Gratis-) Dienstleistungen in EU-/EWR-Staaten an wie z.B. Beratungen, Kurse, Newsletter etc. oder bewirbt seine Dienstleistungen in EU-/EWR-Staaten.

RECHTSMÄSSIGKEIT DATENVERARBEITUNG DSGVO

Mindestens eine der nachstehenden Bedingung muss erfüllt sein, damit die Datenverarbeitung rechtmässig ist.

	Bedingung
☐	**Die betroffene Person hat ihre Einwilligung zur Verarbeitung für den entsprechenden Zweck erteilt**. *So muss z.B. beim Gebrauch der Webseite auf die Verwendung von Cookies, Tracking- und Analysetools hingewiesen werden und die betroffene Person muss aktiv ihr Einverständnis erklären (Kästchen, in denen bereits Häkchen gesetzt sind, sind nicht zulässig). Die Einwilligung muss nachgewiesen werden können und die betroffene Person kann sie jederzeit widerrufen.*
☐	**Die Verarbeitung ist für die Erfüllung eines Vertrags oder vorvertraglicher Massnahmen erforderlich**. *Die Datenverarbeitung des Treuhandunternehmens basiert regelmässig auf einem Vertrag mit dem Kunden (Auftrag), mit dem Arbeitnehmer (Arbeitsvertrag) oder allenfalls mit Dritten, ist also grundsätzlich rechtmässig.*
☐	**Die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich**. *Rechtliche Verpflichtungen für Treuhandunternehmen ergeben sich insbesondere aus dem Rechnungslegungsrecht, dem Revisionsrecht oder dem öffentlichen Arbeitsrecht (Arbeitsgesetz inkl. Verordnungen).*
☐	**Die Verarbeitung ist zur Wahrung lebenswichtiger Interessen erforderlich**. *Dieser Rechtfertigungsgrund dürfte regelmässig dort gegeben sein, wo Leib und Leben einer betroffenen Person in Gefahr sind.*
☐	**Die Verarbeitung ist für die Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich oder in Ausübung öffentlicher Gewalt**. *Vorstellbar ist hier allenfalls die Ausübung eines öffentlichen Amtes.*
☐	**Die Verarbeitung ist zur Wahrung berechtigter Interessen erforderlich**. *Zu denken ist hier beispielsweise an die Durchsetzung oder Abwehr von Ansprüchen.*

HANDLUNGSBEDARF DSGVO

	Handlungsbedarf
☐	**Abklären, ob Ihr Treuhandunternehmen in den Anwendungsbereich der DSGVO fällt, wenn ja für welche Tätigkeiten**. *Häufig werden insbesondere Webseiten und die damit verbundene Datenverarbeitung in den Anwendungsbereich der DSGVO fallen, wenn sie Cookies, Analyse- und Trackingtools verwenden oder Newsletter anbieten.*
☐	**Webseite / Newsletter / Social Media DSGVO-konform ausgestalten**. *Webseite mit Kontaktdaten und Datenschutzerklärung über die Art, Form und Zweck der verarbeiteten Daten (Cookies, Analyse- und Trackingtools etc.) sowie die Rechte der betroffenen Personen (Auskunft, Berichtigung, Löschung).*
☐	**Einwilligung der betroffenen Person einholen.** *Sofern sich die Rechtmässigkeit der Datenverarbeitung ausschliesslich auf die Einwilligung der betroffenen Person stützt, d.h. die Legitimation sich nicht aus Vertrag*

	oder Gesetz ergibt, muss die betroffene Person der Datenverarbeitung aktiv explizit zustimmen. Die Zustimmung kann auch formlos erfolgen, allerding muss das Unternehmen sie nachweisen können. Die Einwilligung ist für die Treuhandbranche namentlich im Zusammenhang mit Webseiten / Newsletter / Social Media wichtig.
☐	**Anwendbares Datenschutzrecht (DSGVO oder DSG) einhalten.** *Hier gilt es, das Bewusstsein für Datenschutz zu stärken und sich der datenschutzrechtlichen Grundsätze bewusst zu werden. Insbesondere sollte jedes Unternehmen wissen, welche Daten es zu welchem Zweck erhebt und ob der Umfang der erhobenen Daten durch den Zweck der Datenverarbeitung gedeckt sind.*
☐	**Privacy by design und Privacy by default sicherstellen.** *Die DSGVO verlangt «Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen» (privacy by design und privacy by default). Bereits bei der Planung der Datenverarbeitung muss das Treuhandunternehmen durch geeignete technische und organisatorische Massnahmen sicherstellen, dass nur Daten verarbeitet werden, die für den jeweiligen Zweck erforderlich sind, und dass die Datenschutzgrundsätze wirksam umgesetzt werden.*
☐	**Datenschutzerklärung verfassen.** *Die DSGVO verlangt eine Information «in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache». Darin ist festzuhalten, wer welche Daten zu welchem Zweck und auf welcher Rechtsgrundlage erhebt und welche Rechte die betroffene Person hat.*
☐	**Ernennen eines Vertreters in der EU.** *Treuhandunternehmen in Drittstaaten, auf die die DSGVO anwendbar ist, müssen einen Vertreter in der EU benennen. Die Pflicht entfällt, wenn die Datenverarbeitung nur gelegentlich erfolgt, keine besondere Datenkategorie (sensible Daten) betrifft und kein Risiko für die Rechte und Freiheiten der betroffenen Person birgt.*
☐	**Verzeichnis von Verarbeitungstätigkeiten erstellen.** *Die DSGVO verlangt ein Verzeichnis der Verarbeitungstätigkeiten. Darin müssen Namen und Kontaktdaten des Treuhandunternehmens, Zweck der Datenverarbeitung, Beschreibung der Kategorie betroffener Personen und Daten etc. aufgeführt sein. Die Pflicht zur Führung des Verzeichnisses entfällt bei Treuhandunternehmen mit weniger als 250 Mitarbeitern (KMU-Artikel).*
☐	**Verantwortlich für den Datenschutz ist die natürliche oder juristische Person, Behörde, Einrichtung oder Stelle, die über die Datenverarbeitung entscheidet**. *Gemäss schweizerischem Aktienrecht ist der Verwaltungsrat verantwortlich für die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen (Compliance). Die betriebliche Umsetzung der Datenschutzgesetzgebung kann der Verwaltungsrat auf die operative Ebene delegieren. Er bleibt aber verantwortlich für die Kontrolle.*

Für den Verband **TREUHAND|SUISSE:**

Institut Treuhand und Recht
Monbijoustrasse 20
Postfach
3001 Bern
Telefon: 031 380 64 30
treuhand@treuhandsuisse.ch | www.treuhandsuisse.ch