

# FABDEC LTD

---

## DATENSCHUTZMAßNAHMEN

### Einleitung

Fabdec Ltd (im Folgenden „Fabdec“) fühlt sich dem Schutz der Rechte und Freiheiten der Betroffenen und der sicheren und verlässlichen Verarbeitung von deren Daten in Übereinstimmung mit allen für uns geltenden rechtlichen Anforderungen verpflichtet.

Wir halten personenbezogene Daten über unsere Mitarbeiter, Kunden, Lieferanten und andere Personen für eine Reihe von geschäftlichen Zwecken vor.

In den vorliegenden Maßnahmen ist dargestellt, wie wir bestrebt sind, personenbezogene Daten zu schützen und zu gewährleisten, dass unsere Mitarbeiter die Regeln kennen, die für die Verwendung personenbezogener Daten, auf die sie in Ausführung ihrer Arbeit Zugriff haben, gelten. Insbesondere fordern die vorliegenden Maßnahmen von den Mitarbeitern, dass vor jeder Aufnahme einer erheblich neuartigen Datenverarbeitungstätigkeit mit dem Datenschutzbeauftragten Rücksprache genommen wird, um zu gewährleisten, dass etwa erforderliche Schritte zur Einhaltung der Vorschriften durchgeführt werden.

### Begriffsbestimmungen

---

<b>Geschäftszwecke</b>	<p>Zwecke, für die wir personenbezogene Daten verwenden könnten, umfassen:</p> <p>Zwecke der Mitarbeiter-, Verwaltungs-, Finanz-, gesetzlichen, Lohn- und Geschäftsentwicklungsbuchhaltung u. -organisation.</p> <p><i>Diese Geschäftszwecke umfassen:</i></p> <ul style="list-style-type: none"><li>- <i>Einhaltung der Vorschriften für uns aus Gesetzen, Verordnungen, Guter Geschäftsführung und -praxis</i></li><li>- <i>Zusammenstellung von Informationen als Teil von</i></li></ul>
------------------------	---

	<p><i>Ermittlungen durch befugte Stellen bzw. in Zusammenhang mit gesetzlichen Verfahren oder Ersuchen</i></p> <ul style="list-style-type: none"> <li>- <i>Gewährleistung, dass Betriebsleitbilder (z.B. Regeln zur Nutzung von E-mail oder Internet) eingehalten werden</i></li> <li>- <i>Durchführung des Betriebs, z.B. Aufzeichnung von Geschäftsvorfällen, Schulung und Qualitätskontrolle, Gewährleistung der Vertraulichkeit schutzwürdiger geschäftlicher Angaben, der Sicherheitsüberprüfungen, Prüfung und Einordnung der Kreditwürdigkeit</i></li> <li>- <i>Abwicklung von Beanstandungen</i></li> <li>- <i>Prüfung von Referenzen, Gewährleistung der Sicherheit am Arbeitsplatz, Überwachung und Verwaltung des Zugriffs von Mitarbeitern auf Systeme und Einrichtungen sowie Mitarbeiterfehlzeiten, deren Verwaltung und Beurteilungen</i></li> <li>- <i>Überwachung von Mitarbeiterverhalten, Disziplinarmaßnahmen</i></li> <li>- <i>geschäftliches Marketing</i></li> <li>- <i>Verbesserung des Services</i></li> </ul>
--	---

<p><b>Personenbezogene Daten</b></p>	<p>„Personenbezogene Daten“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („Betroffener“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.</p> <p><i>Eventuell erhobene personenbezogene Daten sind die Telefonnummer, E-mail-Adresse, Ausbildungsabschluss, Angaben zu Finanzen bzw. Lohn, Angaben zu Bescheinigungen und Zeugnissen, Kenntnisse und Fertigkeiten, Zivilstand, Staatsbürgerschaft, Stellenbeschreibung und Lebenslauf einer Person.</i></p>
<p><b>Besondere Kategorien personenbezogener Daten</b></p>	<p>Besondere Kategorien personenbezogener Daten sind Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder ähnliche Überzeugungen, die Gewerkschaftszugehörigkeit (bzw. -nichtzugehörigkeit), körperlichen und geistigen Gesundheitszustand oder Krankheiten, Vorstrafen bzw. entsprechende Verfahren einer Person sowie genetische und bio-</p>

	metrische Angaben über sie – Angaben besonderer Kategorien, deren Verarbeitung entsprechend den vorliegenden Maßnahmen strikt zu kontrollieren ist.
<b>Für die Daten Verantwortlicher</b>	„Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, wobei die Zwecke und Mittel dieser Verarbeitung durch das Gesetz bestimmt sind.
<b>Datenverarbeiter</b>	„Verarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
<b>Verarbeitung</b>	„Verarbeitung“ meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten oder einer Menge derselben wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
<b>Aufsichtsbehörde</b>	Dabei handelt es sich um die national für den Datenschutz zuständige Stelle. Aufsichtsbehörde im Falle unseres Unternehmens ist das britische Information Commissioner's Office.

## Geltungsbereich

Die vorliegenden Maßnahmen gelten für alle unsere Mitarbeiter, die sich mit ihnen vertraut gemacht haben und sie beachten müssen.

Die vorliegenden Maßnahmen vervollständigen unsere weiteren betreffend Internet- und E-mail-Nutzung. Wir können sie ihrerseits von Zeit zu Zeit durch weitere Maßnahmen oder Leitlinien vervollständigen oder ergänzen. Etwaige neue oder veränderte Maßnahmen werden den Mitarbeitern vor ihrer Anwendbarkeit zur Kenntnis gebracht.

**Wer ist für die vorliegenden Maßnahmen zuständig?**

Als unser Datenschutzbeauftragter ist Graham Prince für die tägliche Umsetzung der vorliegenden Maßnahmen insgesamt zuständig. Sprechen Sie hinsichtlich weiterer Informationen zu den vorliegenden Maßnahmen ggf. den Datenschutzbeauftragten an.

## Grundsätze

---

Fabdec hält die Grundsätze des Datenschutzes (im Folgenden „die Grundsätze“) ein, die die Datenschutz-Grundverordnung der EU aufführt. Wir unternehmen jede mögliche Anstrengung, um in allem, was wir tun, diesen Grundsätzen zu folgen. Diese Grundsätze sind:

### **1. Rechtmäßig, in Treu und Glauben, nachvollziehbar**

Die Erhebung von Daten muss sich nach Treu und Glauben richten, für einen rechtmäßigen Zweck erfolgen, und wir haben nachvollziehbar zu sagen, wie die Daten verwendet werden.

### **2. Zweckgebunden**

Daten dürfen nur für einen bestimmten Zweck erhoben werden.

### **3. Minimiert**

Die Datenerhebung muss für den Zweck notwendig sein und darf nicht über das angemessene Maß hinausgehen.

### **4. Sachlich richtig**

Die von uns vorgehaltenen Daten müssen richtig sein und ggf. auf den neuesten Stand gebracht werden.

### **5. Begrenzt aufbewahrt**

Wir dürfen Daten nicht länger als nötig aufbewahren.

### **6. Integer und rechenschaftspflichtig**

Daten, die wir vorhalten, sind sicher und geschützt gegen Einflüsse zu halten.

## Rechenschaft und Nachvollziehbarkeit

Wir haben bei allen Verwendungen von personenbezogenen Daten Rechenschaft abzulegen und nachvollziehbar zu handeln. Wir müssen zeigen können, wie wir jeden der Grundsätze einhalten. Sie sind verantwortlich, ein schriftliches Verzeichnis aller Datenverarbeitungstätigkeiten in der eigenen Zuständigkeit zu führen, das zeigt, wie sie den Grundsätzen entsprechen. Es muss auf aktuellem Stand gehalten werden und vom Datenschutzbeauftragten genehmigt sein.

Die Einhaltung der Datenschutzgesetze und des Grundsatzes von Rechenschaft und Nachvollziehbarkeit der DSGVO geschieht durch den Nachweis, dass man sie einhält. Sie persönlich sind verantwortlich dafür, zu übersehen, was in Ihrer eigenen Zuständigkeit liegt, damit wir unsere folgenden Datenschutzverpflichtungen einhalten können:

- alle angemessenen technischen und organisatorischen Maßnahmen vollständig umsetzen
- auf aktuellem Stand gehaltene, maßgebliche Dokumentation über alle Verarbeitungstätigkeiten vorhalten
- Datenschutz-Folgenabschätzungen erledigen
- Maßnahmen für Datenschutz dank technischer Gestaltung und Voreinstellungen umsetzen, u.a.:
  - Datenminimierung
  - Pseudonymisierung
  - Nachvollziehbarkeit
  - Gelegenheit für Betroffene, die Verarbeitung zu überwachen
  - fortlaufende Erstellung und Verbesserung von Verfahren für Sicherheit und weitergehenden Datenschutz

# Unsere Verfahren

---

## Rechtmäßige Verarbeitung nach Treu und Glauben

Personenbezogene Daten haben wir gemäß dem ersten Grundsatz rechtmäßig, nach Treu und Glauben und unter Wahrung der Betroffenenrechte zu verarbeiten. Im Allgemeinen bedeutet das, dass wir personenbezogene Daten nur verarbeiten, wenn der Betroffene, dessen Daten wir verarbeiten, eingewilligt hat, dass dies geschehen darf.

Lässt sich auf sie keine rechtmäßige Grundlage (vgl. unten) anwenden, entspricht unsere Verarbeitung nicht dem ersten Grundsatz, ist sie also unrechtmäßig. Betroffene haben das Recht, unrechtmäßig verarbeitete Daten löschen zu lassen.

## Verantwortung für und Verarbeitung der Daten

Fabdec ist sowohl als Verantwortlicher als auch als Verarbeiter von Daten anzusehen. Wir haben die entsprechende Eintragung für uns beim Information Commissioner's Office aufrecht zu erhalten, um Daten weiter rechtmäßig als Verantwortlicher und als Verarbeiter vorzuhalten.

Als (Auftrags-) Verarbeiter von Daten haben wir unsere vertraglichen Pflichten einzuhalten und nur gemäß den dokumentierten Weisungen des für die Daten Verantwortlichen zu handeln. Sollten wir zu einem beliebigen Zeitpunkt selbst den Zweck und die Mittel der Verarbeitung unabhängig von den Weisungen des Verantwortlichen bestimmen, gelten wir als der für die Daten Verantwortliche, weil wir insoweit den Vertrag mit dem Verantwortlichen gebrochen haben und uns dann dieselbe Haftung wie den Verantwortlichen trifft. Als (Auftrags-) Verarbeiter haben wir:

- keine Unterbeauftragung ohne schriftliche Zustimmung des Verantwortlichen einzugehen
- mit dem ICO als Aufsichtsbehörde voll zusammenzuarbeiten
- die Sicherheit der Verarbeitung sicherzustellen
- sachlich richtige Aufzeichnungen über die Verarbeitungstätigkeiten zu führen
- den Verantwortlichen von jeder Verletzung des Schutzes personenbezogener Daten zu unterrichten

Haben Sie den geringsten Zweifel, wie wir Daten verwalten, wenden Sie sich an den Datenschutzbeauftragten.

# Rechtmäßige Grundlage der Datenverarbeitung

Wir müssen für eine rechtmäßige Grundlage der Datenverarbeitung sorgen. Sie haben sich zu vergewissern, dass für alle Daten, für deren Verwaltung Sie zuständig sind, eine schriftliche, rechtmäßige Grundlage der Verarbeitung, die der Datenschutzbeauftragte gutgeheißen hat, vorhanden ist. Es fällt in Ihre Verantwortung, zu prüfen, ob für die Daten, mit denen Sie arbeiten, eine rechtmäßige Grundlage besteht, und sicherzustellen, dass Ihre eigenen Tätigkeiten im Rahmen dieser rechtmäßigen Grundlage erfolgen. Mindestens eine der folgenden Bedingungen muss immer dann erfüllt sein, wenn wir personenbezogene Daten verarbeiten.

## 1. Einwilligung

Wir verfügen über eine klare, eindeutige und genau bezeichnete Einwilligung jüngerer Datums des Betroffenen in die Verarbeitung seiner Daten für einen bestimmten Zweck.

## 2. Vertrag

Die Verarbeitung ist zur Erfüllung oder Vorbereitung eines Vertrags mit der Person erforderlich.

## 3. Rechtliche Verpflichtung

Es besteht für uns eine rechtliche Verpflichtung (außer ein Vertrag) zur Verarbeitung der Daten.

## 4. Lebenswichtige Interessen

Die Datenverarbeitung ist zum Schutz des Lebens einer Person oder im medizinischen Zusammenhang erforderlich.

## 5. Öffentliche Aufgabe

Die Verarbeitung ist zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Ausübung der öffentlichen Gewalt erforderlich oder sie hat eine klare gesetzliche Grundlage.

## 6. Berechtigtes Interesse

Die Verarbeitung ist zur Wahrung unseres berechtigten Interesses erforderlich. Diese Bedingung gilt indes nicht, wenn es Gründe gibt, die personenbezogenen Daten der Person zu schützen, welche diese berechtigten Interessen überwiegen.

## Entscheidung über die Bedingung, auf die sich zu berufen ist

Bei der Beurteilung, ob eine rechtmäßige Grundlage besteht, ist zunächst festzustellen, dass die Verarbeitung erforderlich ist. Das bedeutet, dass die Verarbeitung ein gezielter, angemessener Weg zur Erreichung des formulierten Zwecks sein muss. Sie können sich nicht auf eine rechtmäßige Grundlage berufen, wenn Sie denselben Zweck zumutbar durch andere Mittel erreichen können.

Denken Sie daran, dass mehrere Grundlagen in Frage kommen können, und wählen Sie die am besten zum entsprechenden Zweck passende, nicht die einfachste.

Beurteilen Sie das Folgende und dokumentieren Sie Ihre Antworten:

- Welchen Zweck hat die Verarbeitung der Daten?
- Kann dasselbe zumutbar auf andere Weise erledigt werden?
- Gibt es die Wahl, die Daten zu verarbeiten oder nicht zu verarbeiten?
- Wem kommt die Verarbeitung zugute?
- Wenn ich eine bestimmte rechtmäßige Grundlage wähle, ist es diejenige rechtmäßige Grundlage, welche der Betroffene wohl erwartet hätte?
- Welche Folgen hat die Verarbeitung für die Person?
- Sind Sie in einer Machtposition ihr gegenüber?
- Handelt es sich um eine verletzbare Person?
- Würde sie der Verarbeitung wahrscheinlich widersprechen?
- Sind Sie jederzeit in der Lage, die Verarbeitung auf Ersuchen hin zu beenden, und haben Sie mitberücksichtigt, wie das durchzuführen wäre?

Unsere Einhaltung des ersten Grundsatzes erfordert, dass wir diesen Ablauf dokumentieren und zeigen, dass wir überprüft haben, welche rechtmäßige Grundlage am besten zum jeweiligen Verarbeitungszweck passt, und dass die entsprechenden Entscheidungen vollauf gerechtfertigt sind.

Wir haben zu gewährleisten, dass die Personen, deren Daten durch uns verarbeitet werden, über die rechtmäßige Grundlage dieser Verarbeitung ihrer Daten und den beabsichtigten Zweck unterrichtet werden. Als Mittel dazu ist eine Erklärung zum Datenschutz herzunehmen. Dies gilt, gleich ob wir die Daten direkt bei der Person erheben oder aus anderer Quelle.

Falls es in Ihrer Zuständigkeit liegt, Beurteilungen über die rechtmäßige Grundlage zu erstellen und die Erklärung zum Datenschutz umzusetzen, soweit es eine Verarbeitungstätigkeit betrifft, haben Sie das vom Datenschutzbeauftragten genehmigen zu lassen.



## Was sind besondere Kategorien solcher Daten?

Was früher vertrauliche oder sensible Daten genannt wurde, bezeichnet Daten zu einer Person, die schutzwürdiger sind, also besseren Schutz verdienen. Aus dieser Art von Daten können für die Grundrechte und -freiheiten einer Person größere Risiken entstehen, z.B. indem sie sie rechtswidriger Diskriminierung aussetzen. Zu den besonderen Kategorien von Daten gehören diejenigen zu einer Person über ihre:

- Rasse
- ethnische Herkunft
- politische Anschauung
- Religion
- Zugehörigkeit zu einer Gewerkschaft
- genetische Angaben
- Biometrie (wie im Personalausweis verwendet)
- Gesundheit
- sexuelle Orientierung

In den meisten Fällen der Verarbeitung von Daten besonderer Kategorien durch uns benötigen wir die *ausdrückliche* Einwilligung, es zu tun, durch den Betroffenen, sofern nicht besondere Umstände vorliegen oder wir gesetzlich verpflichtet sind, es zu tun (z.B. um unserer Pflicht zur Erhaltung der Sicherheit am Arbeitsplatz nachzukommen). Jede Einwilligung in der Sache hat eindeutig zu benennen, welche Daten betroffen sind, warum sie verarbeitet werden und wem sie offengelegt werden.

Die Bedingung, auf der die Verarbeitung von personenbezogenen Daten besonderer Kategorien fußt, muss eine gesetzliche Grundlage haben. Falls es uns an einer rechtmäßigen Grundlage für die Verarbeitung von Daten besonderer Kategorien mangelt, ist diese Verarbeitungstätigkeit einzustellen.

# Verantwortung

---

## Unsere Verantwortung

- die Art vorgehaltener personenbezogener Daten bewerten und dokumentieren
- Verfahren prüfen, die gewährleisten, dass alle Rechte des Betroffenen gewahrt sind
- die rechtmäßige Grundlage der Verarbeitung der Daten kennen
- gewährleisten, dass die Verfahren zur Einwilligung rechtmäßig sind
- Verfahren umsetzen und überwachen, um Verletzungen des Schutzes personenbezogener Daten zu erkennen, zu melden und zu untersuchen
- Daten sicher und geschützt speichern
- das Risiko abschätzen, das sich für die Rechte und Freiheiten einer Person ergeben könnte, wenn der Datenschutz gefährdet wäre

## Ihre persönliche Verantwortung

- alle Ihre Pflichten bezüglich des Datenschutzes vollständig erfassen
- prüfen, dass alle Datenverarbeitungstätigkeiten, mit denen Sie zu tun haben, unsere Datenschutzmaßnahmen einhalten und gerechtfertigt sind
- Daten keinesfalls unrechtmäßig nutzen
- Daten nicht unrichtig speichern, mit ihnen nicht nachlässig sein oder auf andere Weise eine Verletzung durch uns der Datenschutzgesetze oder unserer Maßnahmen heraufbeschwören, welche sich aus Ihren Handlungen ergäbe
- die vorliegenden Maßnahmen jederzeit einhalten
- Unverzüglich alle Fragen aufwerfen, von Verletzungen oder Fehlern unterrichten und alles melden, was verdächtig erscheint oder den vorliegenden Maßnahmen oder unseren gesetzlichen Pflichten widerspricht

## Verantwortung des Datenschutzbeauftragten

- die Geschäftsführung über Zuständigkeiten, Risiken und Fragen rund um den Datenschutz auf dem Laufendem halten
- alle Datenschutzverfahren und -maßnahmen regelmäßig überwachen
- Datenschutzbildung und -unterweisung für alle Mitarbeiter und die in den vorliegenden Maßnahmen Genannten organisieren
- Fragen der Mitarbeiter, der Geschäftsführung und anderer Teilhaber zum Datenschutz beantworten
- auf Anfragen von Personen, z.B. Kunden, Lieferanten, dahingehend, welche Daten über sie von uns vorgehalten werden, reagieren

- mit Dritten, die Daten des Unternehmens verwalten, Verträge und Vereinbarungen zur Auftragsverarbeitung überprüfen und genehmigen

## Verantwortung des IT-Leiters

- gewährleisten, dass alle Systeme, Dienste, Software und Hardware angemessene Sicherheitsstandards erfüllen
- Sicherheitshardware und -software regelmäßig überprüfen und testen, um zu gewährleisten, dass sie wie vorgesehen funktionieren
- Dienste von Dritten, z.B. Cloud-Dienste, welche das Unternehmen für die Speicherung und Verarbeitung von Daten in Erwägung zieht, analysieren

## Verantwortung des Vertriebsleiters

- Datenschutzerklärungen, die an E-mails angehängt werden oder sich in anderem Vertriebsmaterial finden, genehmigen
- auf Datenschutzanfragen von Kunden, Zielgruppen oder Presseredaktionen reagieren
- sich mit dem Datenschutzbeauftragten so koordinieren, dass Marketingaktionen die Datenschutzgesetze und die Datenschutzmaßnahmen des Unternehmens einhalten

## Sachliche Richtigkeit und Erheblichkeit

Wir gewährleisten, dass personenbezogene Daten, die wir verarbeiten, sachlich richtig, angemessen, erheblich und auf das für den Zweck, für den sie erhoben wurden, Notwendige beschränkt sind. Wir verarbeiten Daten, die für einen Zweck erhoben wurden, für keinen damit nicht in Zusammenhang stehenden Zweck, sofern nicht der Betroffene seine Einwilligung dazu erteilt hat oder dies aus anderen Gründen vernünftigerweise erwartet.

Personen dürfen von uns die Berichtigung von sie betreffenden personenbezogenen Daten, die sachlich unrichtig sind, verlangen. Falls Sie meinen, dass Informationen unrichtig sind, notieren Sie, dass die sachliche Richtigkeit der Information zweifelhaft ist, und unterrichten Sie den Datenschutzbeauftragten davon.

## Datensicherheit

Sie haben personenbezogene Daten vor Verlust und Missbrauch geschützt aufzubewahren. Soweit andere Unternehmen in unserem Auftrag als Dienstleistung personenbezogene Daten verarbeiten, legt der Datenschutzbeauftragte fest, welche zusätzlichen, spezifischen Datensicherheitsabreden ggf. in Verträge mit diesen Drittunternehmen aufzunehmen sind.

## Sichere Speicherung der Daten

- Geschieht die Speicherung ausgedruckt auf Papier, ist dieses an einem gegen Zugang von unberechtigten Mitarbeitern geschützten Ort aufzubewahren.
- Ausgedruckte Daten sind zu vernichten, wenn sie nicht mehr erforderlich sind.
- Auf Computern gespeicherte Daten sind durch starke, regelmäßig geänderte Passwörter zu schützen. Wir ermuntern alle Mitarbeiter, für die Erstellung und Verwaltung ihrer Passwörter einen Passwortmanager zu verwenden.
- Auf CD-Rom oder Speichersticks gespeicherte Daten sind zu verschlüsseln oder mit Passwort zu schützen, das Medium sodann geschützt wegzuschließen, wenn es nicht verwendet wird.
- Speicherung von Daten in der Cloud ist stets vom Datenschutzbeauftragten genehmigen zu lassen.
- Server, auf denen sich personenbezogene Daten befinden, sind an einem geschützten Ort abseits der allgemeinen Büroräume aufzustellen.
- Daten sind regelmäßig und entsprechend den Datensicherungsvorgaben des Unternehmens zu sichern.
- Daten sind niemals direkt auf mobile Geräte wie Laptop, Tablet oder Smartphone zu speichern.
- Alle Server, auf denen sich sensible/besondere Daten befinden, sind genehmigen zu lassen und durch Sicherheitssoftware zu schützen.
- Alle möglichen technischen Maßnahmen zum Schutz der Daten müssen ergriffen und eingerichtet werden.

## Aufbewahrung der Daten

Wir haben personenbezogene Daten nur so lange wie erforderlich aufzubewahren. Was erforderlich ist, hängt von den Umständen des Einzelfalles ab, wobei die Zwecke, zu denen die personenbezogenen Daten erhoben wurden, zu beachten sind, und ist auf eine Weise zu bestimmen, die mit unseren Leitlinien zur Datenaufbewahrung im Einklang steht.

## Internationale Weitergabe von Daten

Die internationale Weitergabe von personenbezogenen Daten unterliegt Beschränkungen. Sie dürfen personenbezogene Daten ohne ausdrückliche Erlaubnis durch den Datenschutzbeauftragten weder ins Ausland noch sonst außerhalb der normalen Regeln und Verfahren weitergeben.

# Rechte des Betroffenen

---

Personen haben Rechte an ihren Daten, die wir so gut es uns möglich ist zu respektieren und einzuhalten haben. Wir haben wie folgt zu gewährleisten, dass Personen ihre Rechte ausüben können:

## 1. Recht, informiert zu werden

- Bereitstellung von Datenschutzerklärungen, die präzise gefasst, nachvollziehbar, verständlich und leicht zugänglich sowie gratis sind, welche in klarer und einfacher Sprache abgefasst sind, besonders wenn sie sich an Kinder richten
- Aufzeichnungen darüber, wie wir personenbezogene Daten verwenden, zum Nachweis der Einhaltung der Rechenschafts- und Nachvollziehbarkeitspflicht

## 2. Recht auf Auskunft

- Möglichkeit für Personen, über ihre personenbezogenen Daten und zusätzliche Informationen Auskunft zu erhalten
- Gelegenheit für Personen, Kenntnis von der Rechtmäßigkeit der Verarbeitungstätigkeiten zu erlangen und diese zu überprüfen

## 3. Recht auf Berichtigung

- Pflicht für uns, personenbezogene Daten einer Person auf Ersuchen zu berichtigen oder zu ergänzen, wo sie unrichtig oder unvollständig sind
- Erledigung unverzüglich, spätestens binnen eines Monats; Möglichkeit der Verlängerung auf zwei Monate mit Erlaubnis des Datenschutzbeauftragten

## 4. Recht auf Löschung

- Pflicht für uns, Daten einer Person auf Ersuchen zu löschen oder zu entfernen, sofern kein zwingender Grund für die weitere Verarbeitung besteht

## 5. Recht auf Einschränkung der Verarbeitung

- Pflicht für uns, einem Ersuchen zur Einschränkung, Blockierung oder sonstigen Unterdrückung der Verarbeitung personenbezogener Daten zu entsprechen
- Erlaubnis an uns, personenbezogene Daten, deren Verarbeitung eingeschränkt wurde, zu speichern, aber nicht weiterhin zu verarbeiten; Pflicht für uns, ausreichend Daten aufzubewahren, um das Recht auf Einschränkung auch in Zukunft wahren zu können

## 6. Recht auf Datenübertragbarkeit

- Pflicht für uns, Personen ihre Daten so bereitzustellen, dass sie sie für eigene Zwecke oder über verschiedene Dienste hinweg selbst weiterverwenden können
- Pflicht für uns, sie in einem gängig verwendeten, maschinenlesbaren Format bereitzustellen und auf Ersuchen direkt an einen anderen Verantwortlichen zu senden

## **7. Recht auf Widerspruch**

- Pflicht für uns, das Recht einer Person zu wahren, der Datenverarbeitung aus berechtigtem eigenem Interesse oder im Rahmen der Durchführung einer Aufgabe im öffentlichen Interesse zu widersprechen
- Pflicht für uns, das Recht einer Person zu wahren, der Direktwerbung, einschließlich Profiling zu widersprechen
- Pflicht für uns, das Recht einer Person zu wahren, der Verarbeitung ihrer Daten für wissenschaftliche oder historische Forschung und Statistik zu widersprechen

## **8. Rechte in Bezug auf automatisierte Entscheidungen und Profiling**

- Pflicht für uns, die Rechte, welche Personen in Bezug auf automatisierte Entscheidungen und Profiling haben, zu wahren
- Aufrechterhalt durch die und bei der Person ihres Rechts, solcher automatisierten Verarbeitung zu widersprechen, sich deren Begründung erläutern zu lassen und menschliches Eingreifen zu fordern

# Datenschutzerklärungen

---

## Fälle, wo eine Datenschutzerklärung erforderlich ist

Eine Datenschutzerklärung muss im Zeitpunkt des Erhalts der Daten direkt vom Betroffenen bereitgestellt werden. Falls die Daten nicht direkt vom Betroffenen erhalten werden, muss die Datenschutzerklärung binnen einer angemessenen Frist nach Erhalt der Daten bereitgestellt werden, was einen Monat meint.

Falls die Daten zur Kommunikation mit der Person verwendet werden, muss die Datenschutzerklärung bereitgestellt werden, wenn die erste solche Kommunikation erfolgt.

Falls die Weitergabe an einen anderen Empfänger ins Auge gefasst ist, muss die Datenschutzerklärung vor der Weitergabe bereitgestellt werden.

## Inhalt einer Datenschutzerklärung

Eine Datenschutzerklärung muss präzise, nachvollziehbar, verständlich und leicht zugänglich sein. Sie hat gratis zu sein und in klarer und einfacher Sprache geschrieben zu sein, insbesondere wenn sie sich an Kinder richtet.

Folgende Angaben muss eine Datenschutzerklärung, die sich an alle Betroffenen richtet, enthalten:

- Angabe und Kontaktinformationen des Verantwortlichen und seines Datenschutzbeauftragten
- Zweck der Datenverarbeitung und rechtmäßige Grundlage derselben
- berechtigtes Interesse des Verantwortlichen und ggf. der Dritten
- so zutreffend, Hinweis auf des Recht zum jederzeitigen Einwilligungswiderruf
- Kategorien personenbezogener Daten (nur für Daten, die nicht direkt beim Betroffenen erhoben werden)
- etwaige Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- Details zu etwaigen Übertragungen in Drittländer und eingerichteten Sicherheitsmaßnahmen
- Zeitdauer, die die Daten aufbewahrt werden, bzw. Kriterien, die diese Zeitdauer bestimmen, einschließlich Angaben zur Vernichtung nach der Zeitdauer der Aufbewahrung

- Hinweis auf das Recht, sich mit Beanstandungen an das ICO zu wenden, und auf interne Verfahren zur Bearbeitung von Beanstandungen
- Quelle der personenbezogenen Daten und ob sie aus öffentlich zugänglicher Quelle stammen (nur für Daten, die nicht direkt beim Betroffenen erhoben werden)
- Hinweis auf etwaige automatisierte Entscheidungen, einschließlich Profiling, mit Angaben, wie solche Entscheidungen getroffen werden und welche Bedeutung und Folgen sie für den Betroffenen haben
- Hinweis, ob die Bereitstellung der personenbezogenen Daten Teil eines Erfordernisses oder einer Pflicht aus Vorschrift oder Vertrag ist, und welche möglichen Folgen bei Nichtbereitstellung entstehen (nur für Daten, die nicht direkt beim Betroffenen erhoben werden)

## Auskunftsersuchen des Betroffenen

---

### Was ist ein Auskunftsersuchen des Betroffenen?

Jede Person hat das Recht, sich bestätigen zu lassen, dass ihre Daten verarbeitet werden, und Auskunft über ihre personenbezogenen Daten und die zugehörigen Angaben, worunter die Informationen in einer Datenschutzerklärung zu verstehen sind, zu erhalten.

### Unser Verfahren für Auskunftsersuchen

Wir haben einer Person eine Kopie der Angaben, um die sie ersucht, gratis bereitzustellen. Dies hat unverzüglich zu geschehen, spätestens einen Monat nach Zugang. Wir sind bestrebt, Betroffenen die Auskunft über ihre Angaben in einem gängig verwendeten elektronischen Format und wo möglich durch direkten Zugriff auf die Angaben als Fernzugriff über ein abgesichertes System zu gewähren.

Falls es komplex oder aufwändig ist, dem Ersuchen zu entsprechen, kann die Frist um zwei Monate verlängert werden, ist aber dennoch die Person binnen eines Monats zu informieren. Für die Verlängerung der Frist haben Sie die Genehmigung des Datenschutzbeauftragten einzuholen.

Wir dürfen bei bestimmten Ersuchen verweigern, ihnen zu entsprechen, bzw. in den Fällen, wo ein Ersuchen eindeutig unbegründet oder überzogen ist, eine Gebühr berechnen. Betrifft das Ersuchen eine große Menge Daten, dürfen wir von der Person verlangen, die Angaben, um die sie ersucht, näher zu bezeichnen. Dies darf mit der ausdrücklichen Erlaubnis des Datenschutzbeauftragten geschehen.



Sobald ein Auskunftersuchen eines Betroffenen gestellt ist, dürfen Sie die Daten, um die ersucht wird, nicht mehr ändern oder ergänzen. Dies wäre eine strafbare Handlung.

## Ersuchen um Datenübertragbarkeit

Wir haben Daten, um die ersucht wird, in einem strukturierten, gängig verwendeten und maschinenlesbaren Format bereitzustellen. Normalerweise handelt es sich um eine CSV-Datei, wenngleich andere Formate zulässig sind. Diese Daten sind entweder der Person, die ersucht hat, oder dem Verantwortlichen, an den sie gemäß Ersuchen zu übermitteln sind, bereitzustellen. Es hat gratis und unverzüglich zu geschehen, spätestens binnen eines Monats. Im Falle von komplexen oder aufwändigen Ersuchen kann die Frist auf zwei Monate verlängert werden, doch muss die Person von der Verlängerung binnen eines Monats unterrichtet werden, und Sie haben zunächst die ausdrückliche Erlaubnis des Datenschutzbeauftragten einzuholen.

# Recht auf Löschung

---

## Was ist das Recht auf Löschung?

Personen haben unter den folgenden Umständen das Recht, ihre Daten löschen und die Verarbeitung beenden zu lassen:

- Die personenbezogenen Daten sind für den Zweck, für den sie ursprünglich erhoben und/oder verarbeitet wurden, nicht mehr erforderlich.
- Die Einwilligung wurde widerrufen.
- Die Person widerspricht der Verarbeitung und es gibt kein überwiegendes berechtigtes Interesse an der Fortsetzung der Verarbeitung
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet oder Datenschutzgesetze wurden auf andere Weise verletzt.
- Es besteht eine gesetzliche Verpflichtung.
- Die Verarbeitung betrifft ein Kind.

## Unser Verfahren hinsichtlich des Rechts auf Löschung

Dem Recht auf Löschung zu entsprechen, können wir nur unter folgenden Umständen verweigern:

- Ausübung des Rechts auf Meinungs- und Informationsfreiheit
- Einhaltung einer gesetzlichen Pflicht hinsichtlich der Wahrnehmung einer Aufgabe in öffentlichem Interesse oder Ausübung der öffentlichen Gewalt
- aus Zwecken der öffentlichen Gesundheit im öffentlichen Interesse
- aus Archivzwecken im öffentlichen Interesse, für wissenschaftliche Forschung, historische Forschung und statistische Zwecke
- zur Ausübung oder Verteidigung von Rechtsansprüchen

Soweit personenbezogene Daten zu löschen sind, die an andere Teilhaber oder Empfänger weitergegeben wurden, sind diese anzusprechen und von ihrer Pflicht, die Daten zu löschen, zu unterrichten. Falls die Person nachfragt, haben wir sie von diesen Empfängern zu unterrichten.

## Recht auf Widerspruch

Personen haben das Recht, der Nutzung ihrer Daten aus Gründen, die sich aus ihrer besonderen Situation ergeben, zu widersprechen. Wir haben die Verarbeitung zu beenden sofern nicht:

- wir schutzwürdige Gründe für die Verarbeitung haben, die die Interessen, Rechte und Freiheiten des Betroffenen überwiegen;
- die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

Wir haben die Person stets bei der ersten Gelegenheit zur Kommunikation von ihrem Recht auf Widerspruch zu unterrichten, d.h. in der Datenschutzerklärung. Wir müssen Personen eine Möglichkeit online zum Widerspruch geben.

## Recht auf Einschränkung automatisierter Entscheidungen und Profiling

Automatisiertes Profiling oder Entscheidungen, die auf eine Person rechtliche Wirkung oder eine ähnlich erhebliche Folge entfalten, dürfen wir nur unter folgenden Umständen vornehmen:

- Es ist für den Abschluss oder die Erfüllung eines Vertrags erforderlich.
- Es erfolgt mit ausdrücklicher Einwilligung.
- Es ist auf andere Art und Weise rechtlich zulässig.

Unter diesen Umständen müssen wir:

- den Personen detaillierte Angaben über die automatisierte Verarbeitung machen;
- ihnen einfache Möglichkeiten anbieten, den Eingriff eines Menschen zu fordern oder eine etwaige Entscheidung über sie anzufechten;
- regelmäßige Prüfungen und Nutzertests durchführen, um zu gewährleisten, dass unsere Systeme wie beabsichtigt funktionieren.

# Dritte

---

## Zusammenarbeit mit Dritten als Verantwortliche und Verarbeiter

Als Datenverantwortlicher und (Auftrags-) Verarbeiter haben wir über schriftliche Verträge mit allen Drittverantwortlichen und -verarbeitern zu verfügen, mit denen wir zusammenarbeiten. In dem Vertrag müssen eindeutige Bestimmungen enthalten sein, die unsere und ihre Haftung, Pflichten und Zuständigkeiten definieren.

Als für Daten Verantwortlicher habe wir nur auf (Auftrags-) Verarbeiter zurückzugreifen, die ausreichend Gewähr entsprechend DSGVO dafür bieten, dass die Rechte der Betroffenen geachtet und geschützt werden.

Als (Auftrags-) Datenverarbeiter haben wir nur gemäß den dokumentierten Weisungen des für die Daten Verantwortlichen zu handeln. Wir erkennen unsere Verantwortung als Auftragsdatenverarbeiter gemäß DSGVO an und achten und schützen die Rechte der Betroffenen.

## Verträge

Unsere Verträge haben die Normen des ICO einzuhalten und, soweit möglich, den standardisierten Vertragsbestimmungen zu folgen, die verfügbar sind. Unsere Verträge mit Verantwortlichen und Auftragsdatenverarbeitern müssen den Gegenstand und die Dauer der Verarbeitung, die Art und ausdrücklichen Zweck der Verarbeitungstätigkeiten, die Arten personenbezogener Daten und Kategorien von Betroffenen bestimmen sowie die Pflichten und die Rechte des Verantwortlichen.

Zumindest müssen unsere Verträge Bestimmungen enthalten über:

- Handeln nur auf schriftliche Weisung
- Vertraulichkeitsverpflichtung für die mit der Verarbeitung Betrauten
- Ergreifen angemessener Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung
- Inanspruchnahme weiterer Auftragsverarbeiter nur nach vorheriger Einwilligung des Verantwortlichen und auf Grundlage eines schriftlichen Vertrags
- Unterstützung des Auftragsverarbeiters durch den Verantwortlichen bei Auskunftersuchen von Betroffenen und bei der Durchführung der Ausübung ihrer Rechte nach DSGVO durch Betroffene
- Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Erfüllung der Pflichten nach DSGVO betreffs Sicherheit der Verarbeitung, Unter-

richtung von Verletzungen des Schutzes der Daten und Durchführung von Datenschutz-Folgenabschätzung

- Löschung oder Rückgabe aller personenbezogenen Daten am Ende der Vertragslaufzeit
- Einhaltung regelmäßiger Überprüfungen und Inspektionen und Bereitstellung jedweder Informationen, die zur Einhaltung der gesetzlichen Pflichten seitens des Verantwortlichen und des Auftragsverarbeiters erforderlich sind
- Verpflichtung seitens sowohl des Verantwortlichen als auch des Auftragsverarbeiters, nichts zu tun, was die DSGVO verletzen würde

# Daten über strafbare Handlungen

---

## Einsicht ins Vorstrafenregister

Etwaige Einsicht ins Vorstrafenregister beruht auf einer gesetzlichen Grundlage. Solche Einsicht ist nicht allein aufgrund der Einwilligung des Betroffenen zulässig. Wir dürfen keine umfassenden Aufzeichnungen aus Vorstrafendaten führen. Alle Daten betreffs strafbarer Handlungen gelten als eine besondere Kategorie personenbezogener Daten und sind als solche zu behandeln. Sie haben vor jeder Einsicht in das Vorstrafenregister die Genehmigung des Datenschutzbeauftragten einzuholen.

## Überprüfung, Überwachung und Schulung

---

### Datenüberprüfung

Regelmäßige Datenüberprüfungen zum Umgang mit und zur Minderung von Risiken speisen das Datenregister. Es enthält Angaben über die vorgehaltenen Daten, den Ort ihrer Speicherung, die Art ihrer Nutzung, die dafür Verantwortlichen sowie etwaige weitere Regeln und Aufbewahrungsdauer, die relevant sein könnten. Sie haben gemäß den Vorgaben des Datenschutzbeauftragten und den normalen Abläufen regelmäßige Datenüberprüfungen durchzuführen.

## Überwachung

Jeder hat sich an die vorliegenden Maßnahmen zu halten. Die Gesamtverantwortung obliegt dem Datenschutzbeauftragten. Unser Unternehmen beobachtet diese Maßnahmen ständig und wird sie ggf. ergänzen oder ändern. Sie haben den Datenschutzbeauftragten über jede Verletzung dieser Maßnahmen zu unterrichten. Sie selbst haben diese Maßnahmen vollständig und stets einzuhalten.

## Schulung

Sie erhalten angemessene Schulung über die gesetzlichen Bestimmungen zum Datenschutz, die für Ihre Rolle von Belang sind. Sie haben an allen Schulungen so wie gefordert teilzunehmen. Bei einem Wechsel Ihrer Rolle oder Zuständigkeit obliegt es Ihnen, um eine neue Datenschutzeschulung, die für Ihre neue Rolle oder Zuständigkeit von Belang ist, nachzusuchen.

Sollten Sie weiterer Schulung zu Angelegenheiten des Datenschutzes bedürfen, sprechen Sie den Datenschutzbeauftragten an.

# Unterrichtung von Schutzverletzungen

---

Jede Verletzung der Bestimmungen in den vorliegenden Maßnahmen oder in den Datenschutzgesetzen muss so schnell wie praktisch möglich gemeldet werden. Dies bedeutet, sobald die Schutzverletzung zu Ihrer Kenntnis gekommen ist. Fabdec ist gesetzlich verpflichtet, das Information Commissioner's Office (ICO) von jeder Verletzung des Datenschutzes binnen 72 Stunden zu unterrichten.

Alle Mitglieder der Belegschaft sind verpflichtet, tatsächliche oder potenzielle Nichteinhaltungen der Datenschutzmaßnahmen zu melden. Uns erlaubt das:

- Untersuchung der Nichteinhaltung und ggf. Korrekturschritte
- Führung einer Aufzeichnung der Fälle von Nichteinhaltung
- Unterrichtung des ICO von materiellen Nichteinhaltungen entweder als Einzelfälle oder als einzelnes Auftreten in einem Muster der Nichteinhaltung

Gegen jedes Mitglied der Belegschaft, das eine Schutzverletzung nicht meldet oder dem nachgewiesen werden kann, von einer aufgetretenen Schutzverletzung gewusst oder sie vermutet zu haben, ohne das ordnungsgemäße Meldeverfahren eingehalten zu haben, werden Disziplinarmaßnahmen ergriffen.

Unterrichten Sie bitte den Datenschutzbeauftragten sofort von Schutzverletzungen.

## Nichteinhaltung

Wir nehmen die Einhaltung der vorliegenden Maßnahmen sehr ernst. Die Nichteinhaltung setzt sowohl Sie selbst als auch das Unternehmen Risiken aus.

Die Bedeutung der vorliegenden Maßnahmen drückt sich darin aus, dass die Nichteinhaltung einer beliebigen enthaltenen Bestimmung zu Disziplinarmaßnahmen führen kann, in deren Ergebnis auch eine Entlassung ausgesprochen werden kann.

Falls Sie Fragen oder Sorgen hinsichtlich was auch immer in den vorliegenden Maßnahmen haben, zögern Sie nicht, den Datenschutzbeauftragten anzusprechen.