Datenschutz-Leitlinie

der

INNOCEPT engineering GmbH

INNOCEPT engineering GmbH, Kronach - Neuses
INNOCEPT engineering GmbH, Winterhausen

Version: 1.1 / Stand 10.09.2018

Vorwort

Liebe INNOCEPT Mitarbeiter,

die Themen gesetzlicher Datenschutz und Informationssicherheit werden für uns, unsere Kunden und Interessenten immer wichtiger und bedeutsamer. Wir als Ingenieurdienstleister im Bereich der Produktentwicklung und des Produktdesign, genießen ein hohes Vertrauen bei unseren Kunden.

Vertrauen bedeutet jedoch auch Verantwortung für unser Handeln, für unsere Arbeit, für die Systeme und Daten der Kunden. Unsere Kunden legen ihre persönlichen und betriebswirtschaftlichen Daten in unsere Hände und damit auch unternehmenswichtige sowie kritische Informationen.

Für uns bei INNOCEPT engineering GmbH ist es besonders wichtig, mit diesen Daten verantwortungsbewusst umzugehen. Daher liegt es sehr nahe, dass wir das Thema gesetzlicher Datenschutz in der Praxis sehr ernst nehmen und uns auch entsprechend organisieren.

Diese Leitlinie soll helfen, die Bedeutung und Wichtigkeit des gesetzlichen Datenschutzes zu verdeutlichen und auch den Mitarbeitern dieses Thema transparenter zu machen.

Geschäftsführung:

Birgit Partheymüller, Jürgen Gäbelein, Ralf Fischbach

1. Ziel der Datenschutzleitlinie

INNOCEPT engineering GmbH verpflichtet sich im Rahmen ihrer gesellschaftlichen Verantwortung zur Einhaltung von Datenschutzrechten. Diese Datenschutzleitlinie gilt für die gesamte INNOCEPT engineering GmbH, Kronach – Neuses und Winterhausen in Bezug auf die Grundprinzipien des Datenschutzes. Die Wahrung des Datenschutzes ist die Basis für vertrauensvolle und wertschätzende Geschäftsbeziehungen und die Reputation der INNOCEPT engineering GmbH als attraktiver Arbeitgeber.

Die Datenschutzleitlinie schafft eine der notwendigen Rahmenbedingungen für die Datenübermittlungen zwischen INNOCEPT engineering GmbH, Mitarbeitern, Kunden und Interessenten, sowie sonstigen Geschäftspartnern. Sie gewährleistet das von der EU-Datenschutz-Grundverordnung und den nationalen Gesetzen verlangte angemessene Datenschutzniveau.

Wir definieren dazu ergänzend unsere eigenen Datenschutzziele als Selbstverpflichtung.
Dazu gehören:

- Unbedingte Einhaltung der Vorgaben der EU-Datenschutz-Grundverordnung durch die gesamte Belegschaft
- Unbedingte Einhaltung der unternehmenseigenen Datenschutzvorschriften durch die gesamte Belegschaft.
- Strikte Verpflichtung zur Geheimhaltung und Vertraulichkeit.
- Datenschutzkonforme Arbeitsplatzgestaltung
- Unbedingter Schutz vor Dateneinsicht durch Unbefugte
- usw.

2. Geltungsbereich und Änderung der Datenschutzleitlinie

Diese Datenschutzleitlinie gilt für INNOCEPT engineering GmbH, Kronach-Neuses und Winterhausen. Die Datenschutzleitlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten. Anonymisierte Daten, z.B. für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser Datenschutzleitlinie. Die aktuellste Version der Datenschutzleitlinie kann unter den Datenschutzhinweisen auf der Internetseite der INNOCEPT engineering GmbH, www.Innocept-engineering.de abgerufen werden.

3. Geltung staatlichen Rechts

Diese Datenschutzleitlinie fußt auf den Vorgaben der EU-Datenschutz-Grundverordnung und den dazugehörigen nationalen Gesetzen.

4. Prinzipien für die Verarbeitung personenbezogener Daten

1. **Rechtmäßigkeit**
   Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise erhoben und verarbeitet werden.

2. **Zweckbindung**
   Die Verarbeitung personenbezogener Daten darf lediglich für die Zwecke erfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung oder Einwilligung des Betroffenen.

3. **Transparenz**
   Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:
   - Die Identität der verantwortlichen Stelle
   - Den Zweck der Datenverarbeitung
   - Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden.

4. **Datenvermeidung und Datensparsamkeit**
   Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

5. **Löschung**
   Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen dieser Daten, müssen die Daten gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt und durch INNOCEPT engineering GmbH geprüft werden konnte.

6. **Anonymisierung**
   Wo möglich und wirtschaftlich zumutbar, sind Verfahren zur Löschung der Identifikationsmerkmale der Betroffenen (Anonymisierung) bzw. zur Ersetzung der Identifikationsmerkmale durch andere Kennzeichen (Pseudonymisierung) einzusetzen. Anonymisierung und Pseudonymisierung haben so zu erfolgen, dass die tatsächliche Identität des Betroffenen nicht oder nur mit unverhältnismäßigen Aufwand wieder festgestellt werden kann.

7. **Sachliche Richtigkeit und Datenaktualität**
   Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

8. **Vertraulichkeit und Datensicherheit**
   Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigtem Zugriff, unrechtmäßiger Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

5. Zulässigkeit der Datenverarbeitung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

1. Kunden-, Interessenten- und Partnerdaten

a) Datenverarbeitung bei Anbahnung, Abschluss und Vertragskündigung
Personenbezogene Daten des betroffenen Interessenten, Kunden oder Partners dürfen zur Begründung, zur Durchführung und zur Beendigung eines Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht. Im Vorfeld eines Vertrages – also in der Vertragsanbahnungsphase – ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Kaufanträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten erlaubt. Interessenten dürfen während der Vertragsanbahnung unter Verwendung der Daten kontaktiert werden, die sie mitgeteilt haben.

b) Datenverarbeitung zu Werbezwecken
Kundenbindungs- oder Werbemaßnahmen bedürfen zusätzlicher rechtlicher Voraussetzungen. Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. Der Betroffene ist über die Verwendung seiner Daten für Zwecke der Werbung zu informieren. Sofern Daten ausschließlich für Werbezwecke erhoben werden, ist deren Angabe durch den Betroffenen freiwillig. Der Betroffene soll über die Freiwilligkeit der Angabe von Daten für diese Zwecke informiert werden und dass er jederzeit der Verarbeitung zu Werbezwecken widerrufen kann.

c) Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene gemäß IV.3 dieser Datenschutzleitlinie informiert werden. Die Einwilligung kann vom Betroffenen jederzeit schriftlich widerrufen werden.

d) Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

e) Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses von INNOCEPT engineering GmbH erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z.B. Vermeidung von Vertragsstörungen) Tatbestände. Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen.

f) Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Beauftragte für den Datenschutz im Vorfeld zu informieren.

g) Nutzerdaten und Internet

Wenn auf Webseiten oder in Apps personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzhinweisen und ggf. Cookie Hinweisen zu informieren. Die Datenschutzhinweise und ggf. Cookie-Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind. Werden zur Auswertung des Nutzungsverhaltens von Webseiten und Apps Nutzungsprofile erstellt (Tracking), so müssen die Betroffenen darüber in jedem Fall in den Datenschutzhinweisen informiert werden. Ein personenbezogenes Tracking darf nur erfolgen, wenn das nationale Recht dies zulässt oder der Betroffene eingewilligt hat. Erfolgt das Tracking unter einem Pseudonym, so soll dem Betroffenen in den Datenschutzhinweisen eine Widerspruchsmöglichkeit eröffnet werden (Opt-out). Werden bei Webseiten oder Apps, in einem registrierungspflichtigen Bereich Zugriffe auf personenbezogene Daten ermöglicht, so sind die Identifizierung und Authentifizierung der Betroffenen so zu gestalten, dass ein für den jeweiligen Zugriff angemessener Schutz erreicht wird.

2. Mitarbeiterdaten

a) Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt.
Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift.
Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen.
Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen oder eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

b) Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Mitarbeiterdaten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

c) Einwilligung in die Datenverarbeitung

Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung des Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung muss in jedem Fall ordnungsgemäß dokumentiert werden. Bei einer informierten freiwilligen Angabe von Daten durch den Betroffenen kann eine Einwilligung angenommen werden, wenn nationales Recht keine explizite Einwilligung vorschreibt. Vor der Einwilligung muss der Betroffene gemäß IV.3. dieser Datenschutzleitlinie informiert werden.

d) Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses von INNOCEPT engineering GmbH erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z.B. Bewertung von Mitarbeitern) begründet.

Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen. Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen.

Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahme (z.B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechtigte Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Maßnahme festgestellt und dokumentiert werden. Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen (z.B. Informationsrechte der Betroffenen) berücksichtigt werden.

e) Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Besonders schutzwürdige Daten sind Daten über die rassistische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, vom staatlichen Recht aufgestellten Voraussetzungen verarbeitet werden. Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann. Der Mitarbeiter kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragte im Vorfeld zu informieren.

f) Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, Intranet und Internet sowie interne soziale Netzwerke werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Richtlinien genutzt werden. Im hier vorliegenden Fall der erlaubten Nutzung zu privaten Zwecken sind das Fernmeldegeheimnis und das jeweils nationale geltende Telekommunikationsrecht zu beachten, soweit diese Anwendung finden.
Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Internet-Nutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur können Schutzmaßnahmen implementiert werden, die schadhafte Inhalte blockieren.
Aus Gründen der Sicherheit kann eine Nutzung der Telefonanlagen, der E-Mail-Adressen, des Internets zeitlich befristet protokolliert werden. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien von INNOCEPT engineering GmbH erfolgen. Diese Kontrollen dürfen nur durch ermittelnde Bereiche unter Wahrung des Verhältnismäßigkeitsprinzips und durch Kontrolle des Datenschutzbeauftragten erfolgen. Die jeweiligen nationalen Gesetze sind zu beachten.

6. Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb des Unternehmens INNOCEPT engineering GmbH oder an Empfänger innerhalb des Unternehmens unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Abschnitt V. Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden.

Im Falle einer Datenübermittlung von Dritten an das Unternehmen INNOCEPT engineering GmbH muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

7. Auftragsdatenverarbeitung

Eine Auftragsdatenvereinbarung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. In diesen Fällen ist mit externen Auftragnehmern eine Vereinbarung über eine Auftragsdatenvereinbarung abzuschließen. Dabei behält das beauftragende Unternehmen die Verantwortung für die korrekte Durchführung der Datenverarbeitung.

Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrages sind die nachfolgenden Vorgaben einzuhalten; der beauftragende Fachbereich muss ihre Umsetzung sicherstellen.

1. Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen. Der Auftragnehmer hat die Sicherheit gem. Art.28 Abs.3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art.5 Abs. 2 DSGVO herzustellen.

2. Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.

3. Die vom Beauftragten für den Datenschutz bereitgestellten Vertragsstandards müssen beachtet werden.

4. Der Auftraggeber muss sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen. Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmäßig zu wiederholen.

5. An zahlreichen Stellen der DSGVO finden sich **selbstständige datenschutzrechtliche Pflichten,** die sich ebenfalls an den Auftragsverarbeiter richten.

6. Art.27 Abs.1 DSGVO; Die Pflicht zur **Bestellung eines „Repräsentanten“** trifft auch den Auftragsverarbeiter.

7. Art.30 Abs.2 DSGVO: Der Auftragsverarbeiter ist zur **Führung von Verfahrensverzeichnissen** verpflichtet.

8. Art.31 DSGVO: Die Pflicht zur **Zusammenarbeit mit der Datenschutzaufsicht** trifft auch den Auftragsverarbeiter.

9. Art.32 Abs.1 DSGVO: Die Pflicht zu **technischen und organisatorischen Maßnahmen** der Datensicherheit gilt auch für den Auftragsverarbeiter.

10. Art.37 Abs.1 DSGVO: Die Pflicht zur Bestellung eines **betrieblichen Datenschutzbeauftragten** trifft auch den Auftragsverarbeiter.

11. Art.44 DSGVO: Die Beschränkungen für den **Datentransfer in Drittländer** sind auch vom Auftragsverarbeiter zu beachten.

8. Betroffenenrechte

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen. Folgendes ist zu beachten:

1. Informationsrecht – Offenlegung

a) Name und Kontaktdaten des Verantwortlichen (ggf. auch des Vertreters)
b) Kontaktdaten des Datenschutzbeauftragten
c) Zweck und Rechtsgrundlage der Verarbeitung
d) Berechtigte Interessen (bei Verarbeitung nach Art.6 DSGVO)
e) Empfänger bzw. Kategorien von Empfängern
f) Übermittlung in Drittland oder an internationale Organisation
g) Dauer der Speicherung
h) Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch und auf Datenübertragbarkeit
i) Bestehen eines Rechts auf Widerspruch der Einwilligung
j) Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
k) Information, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und mögliche Folgen der Nichtbereitstellung
l) Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling
m) Informationen über eine mögliche Zweckänderung der Datenverarbeitung

2. Auskunftsrecht

a) Zwecke der Datenverarbeitung
b) Kategorien der Daten
c) Empfänger oder Kategorien von Empfängern
d) Dauer der Speicherung
e) Recht auf Berichtigung, Löschung und Widerspruch
f) Beschwerderecht bei einer Aufsichtsbehörde
g) Herkunft der Daten (wenn nicht bei Betroffenen erhoben)
h) Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling
i) Übermittlung in Drittland oder an internationale Organisation

3. Recht auf Berichtigung und Löschung

a) Wenn die Speicherung der Daten nicht mehr notwendig ist.
b) Wenn der Betroffene seine Einwilligung zur Datenverarbeitung widerrufen hat.
c) Wenn die Daten unrechtmäßig verarbeitet wurden.
d) Wenn eine Rechtspflicht zum Löschen nach EU- oder nationalen Recht besteht.

9. Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgabe betraut und entsprechend berechtigt zu sein. Es gilt das Need-to-know-Prinzip: Mitarbeiter dürfen Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.

Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andre Weise zugänglich machen. Vorgesetzte müssen Ihre Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses unterrichten. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

10. Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt abhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten zu orientieren. Der verantwortliche Fachbereich kann dazu insbesondere seinen Datenschutzbeauftragten zu Rate ziehen. Die technisch- organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des Informationssicherheitsmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

11. Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze muss regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft werden. Die Durchführung obliegt dem Datenschutzbeauftragten und weiteren, mit Auditrechten ausgestatteten Unternehmensbereichen.

Die Ergebnisse der Datenschutzkontrollen sind dem Datenschutzbeauftragten mitzuteilen. Die Geschäftsführung ist über wesentliche Ergebnisse zu informieren. Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zustehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Leitlinie durchführen.

12. Datenschutzvorfälle

Jeder Mitarbeiter soll dem Datenschutzbeauftragten unverzüglich Fälle von Verstößen gegen diese Datenschutzleitlinie oder andere Vorschriften zum Schutz personenbezogener Daten melden. Die für die Funktion oder die Einheit verantwortliche Führungskraft ist verpflichtet, den zuständigen Datenschutzbeauftragten umgehend über Datenschutzvorfälle zu unterrichten.

In Fällen von

a) Unrechtmäßiger Übermittlung personenbezogener Daten an Dritte,
b) Unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten oder
c) Bei Verlust personenbezogener Daten
d) Verlust von Speichermedien (USB-Stick, Laptop, Tablet etc.)

sind die im Unternehmen vorgesehenen Meldungen unverzüglich vorzunehmen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen unverzüglich, jedoch spätestens innerhalb von 72 Stunden, erfüllt werden können.

13. Verantwortlichkeiten und Sanktionen

Die Geschäftsführung ist verantwortlich für die Datenverarbeitung. Damit ist sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzleitlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden (z.B. nationale Meldepflichten). Es ist eine Managementaufgabe der Führungskraft, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Betrachtung des Datenschutzes sicherzustellen. Die Umsetzung dieser Vorgaben liegt in der Verantwortung des zuständigen Mitarbeiters. Bei Datenschutzkontrollen durch Behörden ist der Datenschutzbeauftragte umgehend zu informieren.

Die Geschäftsführung ist verpflichtet, den Datenschutzbeauftragten in seiner Tätigkeit zu unterstützen. Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen den Datenschutzbeauftragten rechtzeitig über neue Verarbeitungen personenbezogener Daten informieren. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Datenschutzbeauftragte schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten. Die Führungskräfte müssen sicherstellen, dass ihre Mitarbeiter im erforderlichen Umfang zum Datenschutz geschult werden. Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht werden in vielen Staaten auch strafrechtlich verfolgt und können Schadenersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

14. Der Datenschutzbeauftragte

Der Datenschutzbeauftragte als externes, fachlich weisungsunabhängiges Organ wirkt auf die Einhaltung der nationalen und internationalen Datenschutzvorschriften hin. Er ist verantwortlich für die Leitlinien zum Datenschutz und überwacht deren Einhaltung. Der Datenschutzbeauftragte wurde von der Geschäftsführung der INNOCEPT engineering GmbH bestellt.

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Datenschutzbeauftragten wenden. Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt.

Kann der zuständige Datenschutzbeauftragte einer Beschwerde nicht abhelfen oder einen Verstoß gegen Datenschutzleitlinien nicht abstellen, muss zur Abhilfe der Datenschutzverletzung die Geschäftsführung benachrichtigt werden.

Anfragen von Aufsichtsbehörden sind immer auch dem Datenschutzbeauftragten zur Kenntnis zu bringen. Der Datenschutzbeauftragte kann wie folgt erreicht werden:

SCHNEIDER

Dipl. Ing. Sandra Schneider

Beratung zu Managementsystemen

Bamberger Straße 5a I 96342 Stockheim

www.schneider-qm.de

Tel.: 09261-965090 I 0171-308 10 41

E-Mail: audit@schneider-qm.de

Geschäftsführung:
Birgit Partheymüller, Ralf Fischbach, Jürgen Gäbelein