Dataforce Verlagsgesellschaft für Business Informationen mbH

Externe Datenschutzrichtlinie

Stand: 3/2023

Dataforce Verlagsgesellschaft
für Business Informationen mbH
Hamburger Allee 14, 60486 Frankfurt
Tel.: +49 69 95930-0
Fax: +49 69 95930-549
www.dataforce.de

Deutsche Bank AG
IBAN: DE07 5007 0010 0852 5768 00
SWIFT: DEUTDEFFXXX

Commerzbank AG
IBAN: DE43 5004 0000 0583 0203 00
SWIFT: COBADEFFXXX

Geschäftsführung:
Marc A. Odinius
UST.-ID.-Nr. DE 213 095 403
HRB 43146 Frankfurt/Main

Inhaltsverzeichnis

I. Ziel der Richtlinie

Die Wahrung des Datenschutzes und der Vertraulichkeit ist seit Gründung der **Dataforce Verlagsgesellschaft für Business Informationen mbH (im Folgenden nur „Dataforce") ** die Basis für unsere Beziehungen zu Kunden und Geschäftspartnern. Wir verfolgen seit je her die Einhaltung von Datenschutzgesetzen und den Grundprinzipien des Datenschutzes. Die folgende Datenschutzrichtlinie soll einen Einblick geben, wie der Datenschutz bei Dataforce organisiert ist und aufzeigen, welche Standards wir bei der Arbeit mit personenbezogenen Daten verfolgen.

II. Geltungsbereich

Diese Datenschutzrichtlinie gilt für Dataforce und seine Mitarbeiter. Sie gilt für alle Fälle der Verarbeitung personenbezogener Daten natürlicher Personen. In Ländern, in denen Daten juristischer Personen in gleicher Weise wie personenbezogene Daten geschützt werden, gilt diese Datenschutzrichtlinie auch in gleicher Weise für Daten juristischer Personen. Diese Datenschutzrichtlinie gilt unbefristet, kann aber jederzeit durch eine aktuellere Richtlinie abgelöst werden, die die Regelung an die jeweiligen Entwicklungen anpasst.

III. Datenschutzorganisation und Kontaktdaten

Der interne **Datenschutzkoordinator (DSK)** des Unternehmens ist unter folgenden Kontaktdaten zu erreichen:

Silke Neubert

silke.neubert@dataforce.de

Das Unternehmen hat einen **Datenschutzbeauftragten (DSB**) bestellt. Diesen erreichen Sie unter folgenden Kontaktdaten:

Oliver Greiner

entplexit GmbH
Kölner Straße 12
65760 Eschborn
Tel +49 6196 97344 - 00
Fax +49 6196 97344 – 29
datenschutz@entplexit.com

Der Datenschutzbeauftragte überwacht die Einhaltung der Datenschutzgrundverordnung (DSGVO) sowie anderer gesetzlichen Vorgaben, einschließlich der Vorgaben dieser und anderer Richtlinien des Unternehmens zum Datenschutz. Der Datenschutzbeauftragte berät und unterrichtet die

Unternehmensleitung hinsichtlich bestehender Datenschutzpflichten und ist zuständig für die Kommunikation mit Aufsichtsbehörden. Ausgewählte Prozesse werden stichprobenartig, risikoorientiert und in angemessenen Zeitabständen auf ihre Datenschutzkonformität hin kontrolliert.

Der Datenschutzbeauftragte nimmt seine Aufgaben weisungsfrei und unter Anwendung seines Fachwissens wahr. Er berichtet in Zusammenarbeit mit dem internen Datenschutzkoordinator an die Dataforce-Unternehmensleitung. Das Unternehmen und seine Mitarbeiter stehen im engen Austausch mit dem Datenschutzbeauftragten und unterstützen diesen bei seiner Arbeit.

IV. Prinzipien für die Verarbeitung personenbezogener Daten

IV.1 Rechtmäßigkeit

Alle personenbezogenen Daten werden bei Dataforce auf ihre rechtmäßige Verarbeitung geprüft und Prozesse entsprechend gestaltet.

IV.2 Zweckbindung

Die Verarbeitung personenbezogener Daten erfolgt bei Dataforce lediglich zu den festgelegten Zwecken, für welche sie zuvor erhoben wurden. Nachträgliche Änderungen der Zwecke bedürfen grundsätzlich einer eigenständigen Rechtfertigung und unterliegen einer separaten Prüfung durch den Datenschutzbeauftragten.

IV.3 Transparenz

Neben einer stets aktuellen Datenschutzerklärung informieren wir Interessenten und Kunden im Rahmen unserer FAQ sowie über separate Informationsschreiben über die wichtigsten Fragen und Antworten zu unseren Produkten und Angeboten.

IV.4 Datenminimierung und Datensparsamkeit

Dataforce gibt darauf acht, mit personenbezogenen Daten so umzugehen, dass so wenige Daten wie erforderlich erhoben werden („Datenminimierung"). Die Daten werden, soweit es technisch möglich oder sinnvoll ist, anonymisiert oder pseudonymisiert. Wir führen die Datenverarbeitung nur durch, insofern diese für den erhobenen Zweck notwendig und angemessen ist und beschränken die Verarbeitung auf das für uns notwendige Maß.

IV.5 Privacy by Design/Privacy by Default

Unsere Datenverarbeitungssysteme, Datenarchitektur und -prozesse werden von Beginn an so gestaltet, dass jeder Schritt die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes erfüllt.

IV.6 Sachliche Richtigkeit und Datenaktualität

Dataforce bemüht sich die verarbeiteten Daten auf dem neuesten Stand und aktuell zu halten. Unrichtige oder veraltete Daten werden (insbesondere auf Anregung des Betroffenen) aktualisiert.

IV.7 Vertraulichkeit

Jeder bei Dataforce Beschäftigte und Dataforce-Partner arbeitet nach den höchsten Standards der Vertraulichkeit und Integrität der anvertrauten Daten.

IV.8 Datensicherheit

Dataforce hat angemessene technische und organisatorische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung bzw. Weitergabe, versehentlichen Verlust, Veränderung oder Zerstörung ergriffen und implementiert, die neben der Wahrung des Datenschutzes auch der Stärkung der IT-Sicherheit dienen.

V. Zulässigkeit der Datenverarbeitung

Dataforce hat in Anwendung der einschlägigen Datenschutzgesetze die Erlaubnistatbestände definiert, die nur bei Vorliegen eine Datenverarbeitung rechtfertigen:

1. Kunden- und Partnerdaten

V.1 a. Vertragliche Beziehung

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 den definierten Vertragszwecken steht.

V.2 b. Vertragsanbahnung

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. Wir beachten eventuell vom Interessenten geäußerte Einschränkungen und Wünsche.

V.3 c. Einwilligung

Eine Datenverarbeitung kann auf Basis einer Einwilligung stattfinden. Die Einwilligung muss vor der geplanten Verarbeitung eingeholt worden sein. Die Erteilung dokumentieren wir in einem angemessenen Format schriftlich, elektronisch oder mit den dafür angemessenen technischen Hilfsmitteln.

V.4 d. Gesetzliche Erlaubnis

Die Verarbeitung personenbezogener Daten kann auch dann zulässig sein, 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.

V.5 e. Berechtigtes Interesse

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche Interessen (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftliche Interessen (z.B. Vermeidung von Vertragsstörungen). Wir nehmen in jedem Fall eine Interessensabwägung vor. Die Verarbeitung aufgrund eines festgestellten berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen überwiegen.

V.6 f. Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten nehmen wir nur vor, wenn dies gesetzlich erforderlich ist oder ausdrücklich eingewilligt wurde. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig sind, um rechtliche Ansprüche gegenüber den Betroffenen geltend zu machen, auszuüben oder zu verteidigen. Sollten besonders schutzwürdige Daten verarbeitet werden wollen wird der Rat des Datenschutzbeauftragten eingeholt.

V.7 g. Nutzerdaten im Internet

Soweit wir auf Webseiten oder in Apps personenbezogene Daten erheben, verarbeiten oder nutzen, informieren wir hierüber vollumfänglich in der Datenschutzerklärung. Die Datenschutzerklärung ist so gestaltet, dass diese für die Betroffenen unmittelbar erreichbar, ständig verfügbar und leicht verständlich ist. Bei der Erstellung und Anpassung der Datenschutzerklärung wird der Datenschutzbeauftragte der Dataforce miteinbezogen.

2. Mitarbeiterdaten

V.8 Für das Arbeitsverhältnis

Personenbezogene Daten, die im Rahmen des Arbeitsverhältnisses anfallen, verarbeiten wir, soweit diese für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Personenbezogene Daten von Bewerbern verarbeiten wir für die Vorbereitung und Anbahnung eines Arbeitsverhältnisses. Nach Ablehnung eines Bewerbers löschen wir die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen spätestens nach sechs Monaten, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt. Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren oder vor der Weitergabe der Bewerbung an andere Konzerngesellschaften erforderlich.

Im bestehenden Arbeitsverhältnis bezieht sich die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages, sofern nicht einer der nachfolgenden Erlaubnistatbestände die Datenverarbeitung begründet:

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, Kollektivregelungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

V.9 Einwilligung

Eine Verarbeitung von Mitarbeiterdaten kann je nach Konstellation auch auf Basis einer Einwilligung des betroffenen Mitarbeiters stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung wird aus Beweisgründen grundsätzlich schriftlich oder elektronisch eingeholt. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung wird in diesem Fall ordnungsgemäß dokumentiert. Bei einer informierten freiwilligen Angabe von Daten durch den Betroffenen kann eine Einwilligung angenommen werden, wenn nationales Recht keine explizite Einwilligung vorschreibt.

V.10 Gesetzliche Erlaubnis

Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden.

V.11 Berechtigtes Interesse

Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, werden nur durchgeführt, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Bei Vorliegen eines begründeten Anlasses wird die Verhältnismäßigkeit der Kontrollmaßnahme geprüft. 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 werden vor jeder Maßnahme festgestellt und dokumentiert. Dabei werden ggf. nach staatlichem Recht bestehende weitere Anforderungen berücksichtigt.

V.12 Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige personenbezogene Daten werden nur unter bestimmten Voraussetzungen verarbeitet. Besonders schutzwürdige Daten sind Daten über die rassische 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, von staatlichem 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 das Unternehmen den 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 interne Datenschutzkoordinator im Vorfeld zu informieren, der gegebenenfalls den Datenschutzbeauftragten hinzuzieht.

V.13 Automatisierte Entscheidungen

Soweit im Beschäftigungsverhältnis personenbezogene Daten automatisiert verarbeitet werden, durch die einzelne Persönlichkeitsmerkmale bewertet werden (z.B. im Rahmen der Personalauswahl oder der Auswertung von Fähigkeitsprofilen), wird eine solche automatisierte Verarbeitung nicht die ausschließliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für die

betroffenen Mitarbeiter sein. Um Fehlentscheidungen zu vermeiden, wird in automatisierten Verfahren gewährleistet, dass eine inhaltliche Bewertung des Sachverhalts durch eine natürliche Person erfolgt und diese Bewertung Grundlage für die Entscheidung ist. Dem betroffenen Mitarbeiter wird außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben.

V.14 Interne Ermittlungen

Maßnahmen zur Sachverhaltsaufklärung und zur Vermeidung oder Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen im Arbeitsverhältnis werden nur unter genauer Beachtung der einschlägigen gesetzlichen Datenschutzvorschriften durchgeführt. Insbesondere muss die damit einhergehende Datenerhebung und -verwendung zum Erreichen des Ermittlungszwecks erforderlich, angemessen und mit Blick auf die schutzwürdigen Interessen des Betroffenen verhältnismäßig sein.

Der Betroffene wird hierbei so bald wie möglich über die zu seiner Person durchgeführten Maßnahmen informiert. Bei allen Formen der internen Ermittlungen wird der Datenschutzbeauftragte hinsichtlich der Auswahl und Ausgestaltung der Maßnahmen vorab einbezogen.

VI. Rechte der Betroffenen

Die Betroffenen haben die folgenden Rechte:

- Recht auf **Information** über wesentliche Angaben der Verarbeitung bei Erhebung von personenbezogenen Daten
- Recht auf **Auskunft** über die zu ihrer Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten bezieht, die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden und den Zweck der Speicherung.
- Recht auf **Berichtigung**, wenn unrichtige Daten gespeichert werden.
- Recht auf **Löschung**, wenn die Speicherung der Daten unzulässig ist oder die Daten nicht mehr benötigt werden.
- Recht auf **Schadensersatz** wegen einer unzulässigen oder unrichtigen Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten.
- Recht auf **Sperrung**, soweit die Richtigkeit der Daten vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt. Eine Sperrung kann auch statt einer Löschung vorgenommen werden, soweit Aufbewahrungsfristen entgegenstehen, Grund zur Annahme besteht, dass die Löschung schutzwürdige Interessen der Betroffenen beeinträchtigen würde oder die Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohen Aufwand möglich ist.

- Recht auf **Widerspruch** gegen die Datenverarbeitung wegen der besonderen persönlichen Situation des Betroffenen, sofern die Datenverarbeitung nicht durch eine Rechtsvorschrift verlangt wird.
- Recht auf **Datenübertragbarkeit**
- **Recht auf Beschwerde** bei einer Datenschutz-Aufsichtsbehörde
  Jeder Betroffene hat das Recht, sich über eine Verarbeitung seiner Daten zu beschweren, sollte er sich hierdurch in seinen Rechten verletzt fühlen. Ebenso können Beschäftigte Verstöße gegen diese Unternehmensrichtlinie jederzeit anzeigen.

Diese Rechte können nicht durch Verträge oder sonstige Rechtsgeschäfte ausgeschlossen oder beschränkt werden. Darüber hinaus kann der Betroffene zu Fragen des Datenschutzes sich an den Datenschutzbeauftragten oder die jeweils zuständige Aufsichtsbehörde wenden. Niemand darf benachteiligt oder gemaßregelt werden, weil er sich an den Datenschutzbeauftragten oder die Aufsichtsbehörde gewandt hat.

Sofern ein Betroffener gegenüber einem Mitarbeiter seine Rechte geltend macht (z.B. Auskunfts- oder Löschungsersuchen), hat der Mitarbeiter die Anfrage umgehend an den internen Datenschutzkoordinator weiterzuleiten. Der interne Datenschutzkoordinator bearbeitet sodann die Anfrage, gegebenenfalls mit Unterstützung des Datenschutzbeauftragten.

Sofern die Anfrage des Betroffenen telefonisch erfolgte, hat der Mitarbeiter diesen zwecks Identifizierung zu bitten, die Anfrage erneut in Textform zu stellen. Die Anfrage sollte dabei per E-Mail an den internen Datenschutzkoordinator weitergeleitet werden. Selbstverständlich ist auch eine direkte Anfrage an den Datenschutzbeauftragten möglich.

VII. Übermittlung personenbezogener Daten

VII.1 Übermittlung an Dritte

Eine Übermittlung von personenbezogenen Daten an Dritte unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Abschnitt V. Der Empfänger der Daten wird darauf verpflichtet, diese nur zu den festgelegten Zwecken zu verwenden. Im Falle einer Datenübermittlung in einen Drittstaat werden besondere Maßnahmen zur Wahrung von Rechten und Interessen Betroffener ergriffen. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist oder beispielsweise über besondere Vertragsklauseln nicht hergestellt werden kann.

VII.2 Datenübermittlung innerhalb einer Unternehmensgruppe

Personenbezogene Daten von Mitarbeitern einer Unternehmensgruppe können innerhalb der Europäischen Union übermittelt und verarbeitet werden. Dasselbe gilt für die Verarbeitung personenbezogener Daten von Kunden, potenziellen Kunden, Bewerbern und Businesspartnern. Die Gruppen-Gesellschaften haben hieran ein berechtigtes Interesse, insbesondere soweit die administrativen (inkl. der Personal-) Angelegenheiten zentral für alle Gesellschaften bearbeitet werden. Ein angemessenes Schutzniveau ist innerhalb der Unternehmensgruppe in der Europäischen Union gegeben. Die Interessen der Betroffenen werden im Rahmen von internen Datenschutzbestimmungen und Verhaltensregeln innerhalb des Unternehmens hinreichend berücksichtigt.

Die Datenübermittlung erfolgt demnach auf der Grundlage des Art. 6 Abs. 1 S.1 lit. f DSGVO, Art. 4 Nr.19 DSGVO, i.V.m. Erwägungsgrund 48 der DSGVO, aufgrund des berechtigten Interesses der verantwortlichen Stelle. Eine Interessenabwägung zwischen den Interessen der Betroffenen und der Unternehmensgruppe fällt zu Gunsten dieser aus.

VIII. Internetauftritt: Datenschutzerklärung

Es wurde eine umfassende Datenschutzerklärung erstellt und über die Internetseite zugänglich gemacht. Die Datenschutzerklärung, die AGB sowie das Impressum werden aktuell gehalten und sind auf der Internetpräsenz von jeder Seite aus abrufbar sein. Bei der Erstellung und Anpassung der Datenschutzerklärung wird der Datenschutzbeauftragte (DSB) miteinbezogen.

IX. Auftragsverarbeitungen

Auftragsverarbeitung im Sinne des Datenschutzrechts bedeutet die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter (regelmäßig ein entsprechender Dienstleister) im Auftrag und nach Weisung des Verantwortlichen. Soll ein Dienstleister personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, bedarf es des Abschlusses eines Vertrags zur Auftragsverarbeitung (Auftragsverarbeitungsvertrag / AVV). Hierin werden die in Art- 28 DSGVO vorgegebenen Datenschutz- und IT-Sicherheitsaspekte geregelt.

Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten werden vor der Auftragserteilung sorgfältig ausgewählt. Die Auswahl wird dokumentiert und berücksichtigt insbesondere die folgenden Aspekte:

- Fachliche Eignung des Auftragnehmers für den konkreten Datenumgang
- Technisch-organisatorische Sicherheitsmaßnahmen

– Erfahrung des Anbieters im Markt

– Sonstige Aspekte, die auf eine Zuverlässigkeit des Anbieters schließen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten etc.)

Der Dienstleister ist im Hinblick auf die mit ihm vertraglich vereinbarten technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen und das Ergebnis zu dokumentieren.

Bei reinen „Nebenleistungen" ist regelmäßig kein Auftragsverarbeitungsvertrag abzuschließen. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Das Unternehmen ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten.

Sofern eine Auftragsverarbeitung geplant wird, ist im Vorfeld der interne Datenschutzkoordinator zu informieren, der gegebenenfalls den Datenschutzbeauftragten hinzuzieht.

X. Verzeichnis von Verarbeitungstätigkeiten

Das Unternehmen hat ein Verzeichnis über alle Datenverarbeitungen zu führen. Jede Fachabteilung hat eine verantwortliche Person zu benennen, die alle notwendigen Informationen zu den Verfahren der jeweiligen Abteilung nach den gesetzlichen Anforderungen des Art. 30 DS-GVO dokumentiert. Der Datenschutzbeauftragte kann zur Beratung hinsichtlich der gesetzlich geforderten Informationen hinzugezogen werden.

Das Unternehmen stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung. Zuständig hierfür ist der Datenschutzbeauftragte im Einvernehmen mit der Unternehmensleitung.

XI. Technische und organisatorische Maßnahmen

Dataforce hat alle erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um die Einhaltung der Bestimmungen des Datenschutzes und der Art. 25, 32 DSGVO zu gewährleisten. Die Maßnahmen umfassen u.a.

a) die Pseudonymisierung und Verschlüsselung von Daten

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
c) Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung
e) sowie ergriffene Maßnahmen zur Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle.

XII. Datenschutz-Folgenabschätzung

Jede Fachabteilung ist zur Durchführung von Datenschutz-Folgenabschätzungen für Verfahren, die unter ihrer Verantwortung erfolgen, verpflichtet, wenn ein hohes Risiko für Rechte und Freiheiten von Betroffen aufgrund der Datenverarbeitung zu erwarten ist. Die Datenschutz-Folgenabschätzung enthält alle gesetzlich geforderten Beschreibungen des Art. 35 Abs. 7 DSGVO. Der Datenschutzbeauftragte berät die Fachabteilungen bei der Durchführung der Datenschutz-Folgenabschätzung sowie bezüglich der Frage, wann Verarbeitungen ein hohes Risiko für Betroffene beinhalten können.

XIII. Datenschutzvorfälle, Datenschutzverletzungen

Trotz großer Sorgfalt kann es zu Sicherheitsvorfällen kommen, die personenbezogene Daten betreffen. Das Unternehmen ist bestrebt, die internen Abläufe im Rahmen von möglicherweise auftretenden Datenschutzverletzungen im Unternehmen zu optimieren und so den gesetzlichen Pflichten nach Art. 33 und 34 DSGVO angemessen nachzukommen. Dazu muss das Unternehmen Verletzungen des Schutzes personenbezogener Daten („Datenschutzverletzungen“) gegebenenfalls den zuständigen Behörden melden und die von der Datenschutzverletzung betroffenen Personen benachrichtigen.

Eine Datenschutzverletzung liegt bei jeder Verletzung der Datensicherheit vor, die zur Vernichtung, zum Verlust oder zur Veränderung, der unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führt. Eine potenzielle Datenschutzverletzung kann also in vielen verschiedenen Formen auftreten. Beispielsweise:

- Die Offenlegung von Kundendaten infolge eines Hackerangriffs, Phishing

- Ein Bug im Webserver, der einen Vollzugriff auf Systeme ermöglicht
- Ein verloren gegangener USB-Stick, Laptop oder sonstiger Datenträger
- Eine fehlerhafte Entsorgung von Kreditkartenbelegen
- Übermittlung personenbezogener Daten an den falschen Empfänger, Versand einer E-Mail mit offenem Verteilerkreis
- Verlorengegangene Postsendung
- Nicht datenschutzkonforme Entsorgung von Datenträgern
- Unbeabsichtigte Veröffentlichung

Sollten der Verdacht bestehen, dass eine mögliche Datenschutzverletzung vorliegt, hat das Unternehmen eine Frist von max. 72 Std. darauf zu reagieren. Um den vorliegenden Fall bewerten zu können, sind die Mitarbeiter angehalten wie folgt vorzugehen:

1) Feststellung der betroffenen Daten, Feststellung der betroffenen Personen

2) Beweissicherung und Entfernung/Behebung der Datenschutzverletzung

3) Sofortige Benachrichtigung des DSK sowie ggf. DSB

4) Dokumentation des Vorfalls und Weiterleitung an den DSK sowie ggf. DSB zur Festlegung von Folgemaßnahmen

XIV. Schulung der Mitarbeiter

Um auch in der Praxis sicherzustellen, dass die Vorgaben und Grundsätze des Datenschutzes eingehalten werden, werden Mitarbeiter, die mit personenbezogenen Daten arbeiten, in regelmäßigen Abständen geschult. Hierbei wird der Datenschutzbeauftragte miteinbezogen.

XV. Vertraulichkeit

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 Aufgaben betraut und entsprechend berechtigt zu sein.

Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.

Jeder Mitarbeiter hat zu Beginn des Beschäftigungsverhältnisses eine Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen zu unterzeichnen, welche auch die Wahrung des Datengeheimnisses beinhaltet. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

XVI. Meldungen interner Verstöße

Jeder Mitarbeiter soll unverzüglich Fälle von Verstößen oder potenziellen Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle) melden. Grundsätzlich erfolgt die Meldung an den internen Datenschutzkoordinator. Dieser zieht bei Bedarf den Datenschutzbeauftragten hinzu.

Sofern der (potenzielle) Verstoß durch den internen Datenschutzkoordinator erfolgte, ist die Geschäftsleitung zu informieren.

Sofern der Verstoß durch die Geschäftsleitung erfolgte, ist der Datenschutzbeauftragte zu informieren.

Die Meldung einer Datenschutzverletzung kann auch jederzeit an den Datenschutzbeauftragten gerichtet werden.

Die Meldung soll grundsätzlich unter dem Namen des Meldenden erfolgen, um insbesondere Rückfragen zu ermöglichen. Dem Mitarbeiter dürfen aus der Meldung keine negativen Folgen erwachsen, es sei denn, es handelt sich um völlig unbegründete Meldungen gegen einen anderen Mitarbeiter ohne jeden Anhaltspunkt oder Meldungen, die einen Charakter aufweisen, die für beabsichtigtes Mobbing oder Verleumdung sprechen.

Für den Fall, dass der Mitarbeiter dennoch Repressalien aufgrund einer Meldung befürchtet, kann diese Meldung auch anonym an den internen Datenschutzkoordinator oder den Datenschutzbeauftragten erfolgen.

Sofern für bestimmte Fälle gesonderte Prozesse festgelegt sind, sind diese einzuhalten. Der interne Datenschutzkoordinator entscheidet sodann, ob und wie der Datenschutzbeauftragte zu unterrichten ist.

XVI.1 Bildschirmsperre

Jeder Mitarbeiter hat seinen Bildschirm vor Verlassen seines Arbeitsplatzes zu sperren und eine automatische Bildschirmsperre einzurichten. Dies gilt sowohl für Laptops,

Tablets, Handys und andere Devices, sofern eine Bildschirmsperre hier technisch möglich ist.

XVI.2 Meldung bei Diebstahl oder Verlust

Bei Diebstahl oder Verlust eines Devices muss die Geschäftsleitung, die IT-Abteilung sowie möglichst der interne Datenschutzkoordinator innerhalb von 2 Stunden nach erkanntem Diebstahl bzw. Verlust informiert werden.

XVI.3 Zugangskontrolle

Passwörter, Schlüssel, Tokens und sonstige Zugangsmöglichkeiten zu personenbezogenen Daten sind stets sicher aufzubewahren. Im Fall von Passwörtern sind sichere Passwörter zu wählen. Bei der Auswahl von Passwörtern sind die Maßgaben der internen Passwortrichtlinie zu befolgen.

XVI.4 Entsorgung von Datenträgern

Alle Daten mit personenbezogenen Daten müssen datenschutzgerecht nach aktuellem Stand der Technik entsorgt werden. Datenträger sind insbesondere Papier, Magnetbänder, Magnetplatten, Flash-Speicher, Disketten, optische Speicher oder Filmmaterial.

Papier mit personenbezogenen Daten ist in den Aktenvernichter zu geben.

Elektronische, elektromagnetische und sonstige Datenträger sind stets zur Entsorgung an die IT-Abteilung zu geben.

XVII. Verantwortlichkeit

Die Geschäftsführung ist verantwortlich für die Datenverarbeitungen im Unternehmen. Damit ist sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzrichtlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden.

XVIII. Folgen von Verstößen

Ein fahrlässiger oder gar mutwilliger Verstoß gegen diese Richtlinie kann arbeitsrechtliche Maßnahmen nach sich ziehen, einschließlich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

XIX. Rechenschaftspflicht

Die Einhaltung der Vorgaben dieser Richtlinie muss jederzeit nachgewiesen werden können. Hierbei ist insbesondere auf die Nachvollziehbarkeit und Transparenz getroffener Maßnahmen zu achten, so beispielsweise über zugehörige Dokumentationen.

XX. Aktualisierung der Richtlinie; Nachweisbarkeit

Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.

Änderungen an dieser Richtlinie sind formlos wirksam. Die Beschäftigten und leitenden Angestellten sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.