
# Datenschutz Management System

Version: 00

dataplan
enterprise solutions

**dataplan**
Stahltwiete 23
D-22761 Hamburg
+49/40/398442-0

www.dataplan.de
info@dataplan.de

25. April 2018

**- Vertrauliche Informationen -**

## 1 Präambel

Das Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOM) im Sinne eines Systems, wie bei dataplan die personenbezogenen Daten (pbD) gemäß EU-DS-GVO geschützt verarbeitet werden. Die TOMs bilden in ihrer Gesamtheit das dataplan-spezifische Datenschutz-Management-System (DSMS).
Das Dokument insgesamt ist als Datenschutzverpflichtung zu verstehen, die sich dataplan zur Einhaltung der DSGVO selbst auferlegt hat. Individuelle Vereinbarungen mit einzelnen Kunden sind auf dieser Basis nicht erforderlich.

Die Grundsätze der Verordnung werden wie folgt praktisch umgesetzt:

- Rechtmäßigkeit der Verarbeitung personenbezogener Daten (VpbD)
  Eine VbpD erfolgt auf der Basis
  - einer Einwilligung einer Person (Art 6 Abs. 1a DSGVO)
  - einer Beauftragung durch eine Person (z.B. Anfrage per Mail, Telefon o.a.) oder eines Vertrages zur Erbringung einer Dienstleistung wie Systeminstallation, Wartung und Pflege, Beratung, Schulung u.ä. (Art 6 Abs. 1b DSGVO)

- Sparsamkeit
  Es werden nur Kontaktdaten verarbeitet, die für kommunikative oder kaufmännische Zwecke nötig sind. Sie werden nicht an Dritte (Empfänger) weitergeleitet oder für andere Zwecke (z.B. Profiling) missbraucht.

- Zweckbindung
  Die pbD werden ausschließlich zur Erfüllung eines Auftrages oder Vertrages verwendet. Eine Umwidmung für einen anderen Zweck (Werbung) ist unzulässig und wird nicht vorgenommen.
  Nicht als Werbung verstanden werden die Informationsblätter zu dataplan-Produkten und –Leistungen, an denen unsere Interessenten, Kunden und Anwender ein eigenes Interesse haben.

- Sicherheit
  Die VpbD erfolgt auf sichere Art und Weise, indem TOMs ergriffen werden, die fälschliche oder missbräuchliche Verwendung wirksam verhindern.
  Da **ausschließlich** Kontaktdaten verarbeitet werden, kann das Risiko für eine Person als sehr niedrig eingeschätzt werden. Die Schutzklasse 1 gilt dafür als ausreichend.

- Übermittlung in Drittstaaten
  Eine Übermittlung in andere Länder erfolgt grundsätzlich nicht, außer es liegt eine ausdrückliche Einwilligung und Beauftragung vor.

- Betroffenenrechte
  Die Rechte der betroffenen Personen werden vollumfänglich gewahrt und proaktiv umgesetzt. Auf Verlangen werden
  - Auskünfte erteilt,
  - Daten berichtigt, gelöscht, eingeschränkt oder ausgehändigt,
  - Widersprüche respektiert.

Die pbD werden während ihrer Verarbeitung durch diverse TOMs geschützt. Folgende TOMs werden eingesetzt, um die Anforderungen der Schutzklasse 1 zu gewährleisten:

- Privacy by Design: Verschlüsselung
- Privacy by Default: Voreinstellungen

Die VpbD erfolgt unter Anwendung und Einhaltung genehmigter, branchenspezifischer Verhaltensregeln (Art 40 DSGVO).

Eine Verletzung des Datenschutzes, sollte sie ungewollt dennoch auftreten, wird unverzüglich der zuständigen Aufsichtsbehörde gemeldet, soweit ein Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person entstehen.
In einem solchen Fall werden außerdem der Auftraggeber sowie die Person informiert. Zugleich wird bestmöglich für Schadensbegrenzung und –überwindung gesorgt.

Da die VpbD bei dataplan kein hohes Risiko für die persönlichen Rechte und Freiheiten einer Person bedeutet, ist eine Abschätzung von Folgen nicht erforderlich. Dies wird untermauert durch die Tatsache, dass keine der Verarbeitungsarten gemäß Art 35 Abs. 3a,b,c vorgenommen wird.
Da außerdem keine „neuen Technologien“ oder massenhaft pbD verarbeitet werden, ist eine Folgenabschätzung gemäß DSGVO entbehrlich.

Dataplan ist bestrebt, den Schutz pbD bestmöglich zu gewährleisten. Deswegen wird ein Datenschutzbeauftragter berufen, obwohl dies nicht notwendig wäre gemäß Art. 37 Abs. 1 DSGVO. Denn das Kerngeschäft von dataplan besteht in der Erstellung, Pflege und Weiterentwicklung sowie Beratung und Betreuung von Anwendern der entwickelten Softwarelösungen für die Planung im Produktionsbereich.
Nur nebenbei werden pbD lediglich in Form von Kontaktdaten (Name, Tel., E-Mail u.ä.) verarbeitet für rein kommunikative oder kaufmännische Zwecke (wie Besprechungen, Abstimmungen, Angebots- und Rechnungsschreibung). Dies stellt eine reine Nebentätigkeit dar und gilt umso mehr, als dass **nicht** „in der Regel mindestens 10 Personen ständig mit der automatisierten VpbD beschäftigt sind.(Art 38 BDSG)“.

Zum Datenschutzbeauftragten bestellt wird Herr Olaf Schumann, der in besonderer Weise für diese Aufgabe qualifiziert ist. Er ist ein sehr erfahrener IT-Systemspezialist, der die technischen Belange im Hinblick auf Datenschutz richtig und vollständig umzusetzen versteht und darüber hinaus auch die organisatorischen Fragen beantworten kann.

Dataplan orientiert sich bei der Umsetzung der DSGVO an branchenspezifischen Verhaltensregeln (Art 40,41 DSGVO), die vom EU-Datenschutzausschuss registriert und veröffentlicht sind. Eine Zertifizierung darüber hinaus ist nicht erforderlich.

Dataplan bestätigt allen Kunden und mit ihr im Kontakt stehenden Personen die unbedingte Einhaltung der Grundsätze gemäß Art 5 Abs. 1 DSGVO und kann dies jederzeit nachweisen.

Hamburg, den 25. April 2018

Dr. Wolfgang Zetsche (Geschäftsführer)

_____

## 2 Grundsätze

Die bereits in der Präambel kurz genannten und in einen Gesamtzusammenhang eingeordneten Grundsätze werden nachfolgend, soweit erforderlich, näher spezifiziert.

### 2.1 Rechtmäßigkeit der Verarbeitung personenbezogener Daten (VpbD)

Eine VbpD erfolgt auf der Basis
- einer Einwilligung einer Person (Art 6 Abs. 1a DSGVO)
- einer Beauftragung durch eine Person (z.B. Anfrage per Mail, Telefon o.a.) oder eines Vertrages mit einem Kunden zur Erbringung einer Dienstleistung wie Systeminstallation, Wartung und Pflege, Beratung, Schulung u.ä. (Art 6 Abs. 1b DSGVO)

### 2.2 Sparsamkeit

Es werden nur Kontaktdaten verarbeitet, die für kommunikative oder kaufmännische Zwecke nötig sind. Sie werden nicht an Dritte (Empfänger) weitergeleitet oder für andere Zwecke (z.B. Profiling) missbraucht. Die Anzahl von auszufüllenden Pflichtfeldern ist auf ein Minimum reduziert.

### 2.3 Zweckbindung

Die pbD werden ausschließlich zur Erfüllung eines Auftrages oder Vertrages verwendet. Eine Umwidmung für einen anderen Zweck ist unzulässig und wird nicht vorgenommen.

### 2.4 Sicherheit

Die VpbD erfolgt auf sichere Art und Weise, indem TOMs ergriffen werden, die fälschliche oder missbräuchliche Verwendung wirksam verhindern.
Da **ausschließlich** Kontaktdaten verarbeitet werden, kann das Risiko für eine Person als sehr niedrig eingeschätzt werden. Die Schutzklasse 1 gilt dafür als ausreichend.

- Die Arbeitsplätze sind vor unautorisiertem Zugriff abgesichert
- Die Arbeitsplätze werden bei Inaktivität gesperrt
- Es werden automatisiert aktuelle Sicherheitsupdates der Betriebssysteme installiert
- pbD werden verschlüsselt gespeichert

### 2.5 Übermittlung in Drittstaaten

Eine Übermittlung in andere Länder erfolgt grundsätzlich nicht, außer es liegt eine ausdrückliche Einwilligung und Beauftragung vor.

### 2.6 Betroffenenrechte

Die Rechte der betroffenen Personen werden vollumfänglich gewahrt und pro-aktiv umgesetzt. Auf Verlangen werden
- Auskünfte erteilt,
- Daten berichtigt, gelöscht, eingeschränkt oder ausgehändigt,
- Widersprüche respektiert.

### 2.7 Verhaltensregeln

Dataplan orientiert sich bei der Umsetzung der DSGVO an branchenspezifischen Verhaltensregeln (Art 40,41 DSGVO), die vom EU-Datenschutzausschuss registriert und veröffentlicht sind. Eine Zertifizierung darüber hinaus ist nicht erforderlich.

# 3 Technische und organisatorische Maßnahmen (TOM)

Dataplan ergreift folgende technische- und organisatorische Maßnahmen zur sachgerechten Umsetzung der DSGVO:

## 3.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b) und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

### 3.1.1 Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

- Eingangstüren werden stets verschlossen gehalten.
- Anwesenheitsaufzeichnungen für Mitarbeiter (Zeiterfassungseinrichtungen).
- Besucher/Externe werden begleitet bzw. abgeholt und stets beaufsichtigt.
- Schlüssel
- Elektrische Türöffner mit Personenkontrolle

### 3.1.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

- Alle IT-Programme laufen auf eigenen Servern im Rechenzentrum (Housing)
- Externer Zugang ist besonders gesichert (Verschlüsselung, VPN)
- Abschottung des Netzwerkes gegen ungewollte Zugriffe von außen (Firewall).
- Zutritt zum Rechenzentrum nur mit hardwaregestützter Sicherheitskontrolle
- Zugang zu EDV-Systemen nur mit Benutzerkennung und individuellem Passwort möglich.
- Zugangsberechtigungen werden dokumentiert.
- Mobile Datenträger sind verschlüsselt (Hardwareverschlüsselung).
- Bildschirmsperre an Arbeitsstationen, automatische Sperrung bei längerer Abwesenheit.

### 3.1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

- Individuelle Zugriffsrechte für jeden einzelnen Benutzer (in einem schriftlichen Berechtigungskonzept dokumentiert),
  zentrale Verwaltung und Steuerung.
- Zugriffsberechtigungen werden aufgabenbezogen und nach dem Need-to-know-Prinzip erteilt.
- Regelmäßige Überprüfung der Zugriffsberechtigungen. Nicht mehr erforderliche Berechtigungen werden unverzüglich entzogen.
- Daten auf mobilen IT-Systemen sind verschlüsselt (komplettes System, Hardwareverschlüsselung).
- Aufzeichnung von Zugriffen auf das IT-System

### 3.1.4 Trennungskontrolle / Zweckbindungskontrolle

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

- Trennung von Produktiv- und Testsystemen (in getrennten Datenbanken).

## 3.2 Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

### 3.2.1 Weitergabekontrolle

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

- Datenspeicherung und -verarbeitung erfolgt auf IT-Systemen im Rechenzentrum. Verbindung zwischenexternen Client und Server ist besonders gesichert (Verschlüsselung, VPN).
- Mitbringen und verwenden privater Datenträger ist untersagt. Es dürfen nur verschlüsselte betriebliche Datenträger genutzt werden.
- Wiederbeschreibbare Datenträger werden vor der Wiederverwendung sicher gelöscht.
- Bei Hardwaretausch werden Festplatten vorher ausgebaut.
- Kontrollierte Vernichtung von Datenträgern mit Protokollierung (physische Vernichtung, zertifizierter Entsorger).
- Besucher haben keinen Zugriff auf betriebliches LAN/WLAN.

### 3.2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

- Automatisierte Protokollierung der Dateneingabe, Änderung oder Löschung.
- Protokollierung gescheiterter Zugriffsversuche.
- Protokollierung der Aktivitäten des Systemverwalters und sämtlicher Benutzer.
- Protokollierung der Aktivitäten auf dem Server.
- Sicherung der Protokolldaten gegen Verlust oder Veränderung.
- Dokumentation der Eingabeprogramme.

## 3.3 Verfügbarkeit, Belastbarkeit (Art. 32 Abs. 1 lit. b), Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c)

### 3.3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (die Angaben beziehen sich auf eigene IT-Systeme des Auftragnehmers):

- Datensicherheitskonzept.
- Versionierte Daten- und Systembackups nach Backup-Plan (täglich/wöchentlich).
- Festplattenspiegelung (RAID)

- Schadsoftwareschutz. Sicherheitsrelevante Updates und Patches werden regelmäßig und zeitnah eingespielt.
- Erhaltene und auszuliefernde Datenträger sowie Mails werden Schadsoftwarechecks unterzogen.
- Unterbrechungsfreie Stromversorgung

### 3.4 regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) Art. 25 Abs. 1

#### 3.4.1 Auftragskontrolle

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

- Auftragnehmer werden sorgfältig ausgesucht.
- Klare und unzweifelhafte vertragliche Regelungen zur Datenverarbeitung
- Formalisiertes Weisungsmanagement
- Weisungen werden grundsätzlich schriftlich erteilt.
- Kontrolle des Auftragnehmers durch die Geschäftsführung oder den Datenschutzbeauftragten.

### 3.5 Betroffenenrechte

Die Rechte Betroffener werden vollumfänglich gewahrt:

- Anfragen seitens betroffener Personen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, werden unverzüglich an diesen weitergeleitet.
- Anfragen werden unverzüglich bearbeitet

### 3.6 Beschäftigtenpflichten

Alle Mitarbeiter von dataplan sind ebenfalls der Einhaltung der DSGVO verpflichtet:

- Eine Verpflichtungserklärung (Vertraulichkeit, Verschwiegenheit u.ä.) ist unterschrieben.
- Ein Merkblatt zur Verpflichtungserklärung wurde ausgehändigt.

### 3.7 Dokumentationspflichten

Dataplan kommt den Pflichten zur Dokumentation nach, indem alle Maßnahmen zur Sicherheit der Datenverarbeitung sowie und Schutz der pbD in dem Dokument „Datenschutz-Management System“ beschrieben werden. Darüber hinaus findet statt die

- Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig und Mitteilung an Auftraggeber
- Erstellung der Verzeichnisse von Verarbeitungstätigkeiten

### 3.8 Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO, Art. 25 Abs. 1 DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten in einer Weise verarbeitet werden, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

- Pseudonymisierung ist nicht erforderlich, da alle personenbezogenen Daten in verschlüsselter Form gespeichert werden.

### 3.9 Internetauftritt und Website

Der Internetauftritt von dataplan wird im Impressum erweitert um den bestellten Datenschutzbeauftragten sowie die zuständige Aufsichtsbehörde, die hinsichtlich der DSGVO zu kontakten wäre:

Freie und Hansestadt Hamburg
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Prof. Dr. Johannes Caspar
Klosterwall 6 (Block C), 20095 Hamburg
Tel.: 040 / 428 54 - 4040
Fax: 040 / 428 54 - 4000
E-Mail: mailbox@datenschutz.hamburg.de

Außerdem wird dieses Dokument auf der Website zum Herunterladen bereitgestellt.

Alle Pflichtangaben gemäß Telemediengesetz und Rundfunkstaatsvertrag sind ebenfalls enthalten.

---

Telemediengesetz (TMG)
§ 5 Allgemeine Informationspflichten
(1) Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. den Namen und die Anschrift, unter der sie niedergelassen sind,
   bei juristischen Personen zusätzlich die Rechtsform, den Vertretungsberechtigten
   und, sofern Angaben über das Kapital der Gesellschaft gemacht werden, das Stamm- oder Grundkapital
   sowie, wenn nicht alle in Geld zu leistenden Einlagen eingezahlt sind, der Gesamtbetrag der ausstehenden Einlagen,
2. Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post,
3. soweit der Dienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, Angaben zur zuständigen Aufsichtsbehörde,
4. das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind, und die entsprechende Registernummer,
5. soweit der Dienst in Ausübung eines Berufs im Sinne von Artikel 1 Buchstabe d der Richtlinie 89/48/EWG des Rates vom 21. Dezember 1988 über eine allgemeine Regelung zur Anerkennung der Hochschuldiplome, die eine mindestens dreijährige Berufsausbildung abschließen (ABl. EG Nr. L 19 S. 16), oder im Sinne von Artikel 1 Buchstabe f der Richtlinie 92/51/EWG des Rates vom 18. Juni 1992 über eine zweite allgemeine Regelung zur Anerkennung beruflicher Befähigungsnachweise in Ergänzung zur Richtlinie 89/48/EWG (ABl. EG Nr. L 209 S. 25, 1995 Nr. L 17 S. 20), zuletzt geändert durch die Richtlinie 97/38/EG der Kommission vom 20. Juni 1997 (ABl. EG Nr. L 184 S. 31), angeboten oder erbracht wird, Angaben über
   a)die Kammer, welcher die Diensteanbieter angehören,
   b)die gesetzliche Berufsbezeichnung und den Staat, in dem die Berufsbezeichnung verliehen worden ist,
   c)die Bezeichnung der berufsrechtlichen Regelungen und dazu, wie diese zugänglich sind,
6. in Fällen, in denen sie eine Umsatzsteueridentifikationsnummer nach § 27a des Umsatzsteuergesetzes oder eine Wirtschafts-Identifikationsnummer nach § 139c der Abgabenordnung besitzen, die Angabe dieser Nummer,
7. bei Aktiengesellschaften, Kommanditgesellschaften auf Aktien und Gesellschaften mit beschränkter Haftung, die sich in Abwicklung oder Liquidation befinden, die Angabe hierüber.

(2) Weitergehende Informationspflichten nach anderen Rechtsvorschriften bleiben unberührt.

---

Rundfunkstaatsvertrag (RStV) in der Fassung des 13. Rundfunkänderungsstaatsvertrags
Gesetzestext (Materialien)
VI. Abschnitt: Telemedien
§55
(1) Anbieter von Telemedien, die nicht ausschließlich persönlichen oder familiären Zwecken dienen, haben folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:
1. Namen und Anschrift sowie
2. bei juristischen Personen auch Namen und Anschrift des Vertretungsberechtigten.

(2) Anbieter von Telemedien mit journalistisch-redaktionell gestalteten Angeboten, in denen insbesondere vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben werden,
haben zusätzlich zu den Angaben nach den §§ 5 und 6 des Telemediengesetzes einen Verantwortlichen mit Angabe des Namens und der Anschrift zu benennen.
Werden mehrere Verantwortliche benannt, so ist kenntlich zu machen, für welchen Teil des Dienstes der jeweils Benannte verantwortlich ist. Als Verantwortlicher darf nur benannt werden, wer
1. seinen ständigen Aufenthalt im Inland hat,
2. nicht infolge Richterspruchs die Fähigkeit zur Bekleidung öffentlicher Ämter verloren hat,
3. voll geschäftsfähig ist und
4. unbeschränkt strafrechtlich verfolgt werden kann.

(3) Für Anbieter von Telemedien nach Absatz 2 Satz 1 gilt § 9 a entsprechend.

## 4 Datenstruktur <person>

Die Datenstruktur <person> zur Speicherung personenbezogener Daten umfasst Attribute, die in 4 Teile gegliedert sind.

Die Attribute in Teil 1 beziehen sich auf den Datensatz an sich, indem sie seine effiziente Verwaltung ermöglichen und unterstützen. Sie beschreiben nicht die Person selbst.

Die Attribute im Teil 2 beschreiben eine Kontaktperson, die für die Erfüllung eines Auftrages bekannt sein muss. Es werden nur solche Informationen gespeichert, die für kommunikative bzw. kaufmännische Zwecke (z.B. Rechnungsschreibung) nötig sind. Darüber hinaus wird nichts Beschreibendes zur Kontaktperson gespeichert.

Verarbeitet werden die Daten über eine Auflistung, die die personenbezogenen Daten zu Kontaktpersonen liefert.
Ob diese Auflistung von einem Anwender aufgerufen werden kann und in welchem Umfang, ist über die Definition von Rollen und Rechten geregelt.
Die Auflistung ist konfigurierbar hinsichtlich sichtbarer Spalten (Attribute) und Sortierung. Dies sind ebenfalls benutzerabhängig konfigurierbare Sichten auf die Daten, die beschränkt werden können.

Die Verarbeitung der personenbezogenen Daten erfolgt über einen Dialog, der je nach Personen-Kategorie unterschiedlich aussieht.

Allen Kategorien gemeinsam ist die Karteikarte „Einstellungen“. In ihr werden die grundlegenden Informationen wie Name, Anrede usw. erfasst bzw. geändert und dann gespeichert.
Ebenfalls gemeinsam ist die Karteikarte „Adressen“. In ihr werden gegebenenfalls die Anschrift (Firmenadresse bei Kontaktperson / Privatanschrift bei Beschäftigten) erfasst bzw. geändert und dann gespeichert.
Eine dritte Karte „Eigenschaften“ rundet den Dialog ab. Auf ihr kann festgehalten werden, ob die Person bestimmte Informationen (Messeeinladungen, Weihnachtsgrüße u.ä.) erhalten hat. Informationen also, die nicht die Person an sich beschreibt, sondern dataplan-interne Betriebsabläufe dokumentiert.

Für eine Kontaktperson werden keine weiteren Daten erfasst.

Die Teile 3+4 beziehen sich auf personenbezogene Daten von Mitarbeitern, die nicht von allgemeinem Interesse sind und daher hier nicht näher beschrieben werden, sondern Gegenstand eines erweiterten Dokumentes sind.

Die personenbezogenen Daten werden verschlüsselt gespeichert. Die Verschlüsselung erfolgt nach einem symmetrischen Verfahren, dessen Schlüssel länger als 4096 bit ist.

Sämtliche Verarbeitungsvorgänge hinterlassen Einträge in der Betriebsdatenerfassung. Zu einer Meldung gehört standardmäßig von welchem Anwender, Arbeitsplatz und wann was geändert wurde.Auf diese Weise ist jederzeit detailliert nachweisbar, welche personenbezogenen Daten wie und durch wen verarbeitet wurden.

## 5 Datenstruktur <benutzer>

Neben Daten zu natürlichen Personen werden bei dataplan auch Informationen zu sogenannten „Benutzern“ gespeichert.
Wegen ihrer Bezeichnung als „Benutzer“ könnten diese Informationen fälschlicherweise auch für personenbezogene Daten gehalten werden. Das ist aber genau nicht der Fall, denn die Datenstruktur <benutzer> speichert nur die rein technischen Informationen zu einer Zugangsberechtigung. Diese ist völlig unabhängig von „Personen“ und beschreibt lediglich, welche technischen Zugangsberechtigungen es gibt.

Jede Zugangsberechtigung verfügt über einen „Namen“. Aber das ist der Name des Login, nicht einer Person! Die gespeicherten Attribute sind rein technischer Natur zum erfolgreichen Einloggen in ein System. Damit fallen „Benutzer“ nicht unter die Anforderungen an den Schutz personenbezogener Daten, sondern sind im Rahmen der allgemeinen IT-Sicherheit richtig zu verwalten.

Die Datenstruktur <benutzer> könnte daher in diesem Dokument eigentlich völlig fehlen. Um aber für jedermann zu dokumentieren, dass es sich um reine Zugangsdaten handelt, die von einer konkreten Person völlig losgelöst sind, wird sie hier der Klarheit halber dennoch aufgeführt.

## 6 Sonstiges

Für die Abwicklung des dataplan-Geschäftsbetriebes sind E-Mails ein außerordentlich wichtiges Kommunikationsmittel, das in folgender Weise organisiert ist:

- E-Mails werden auf zentralen Rechnern im dataplan-Rechenzentrum verwaltet. Es werden keine Kopien auf anderen, gar externen Servern gehalten.
- Ein Zugriff auf E-Mails von extern ist nur verschlüsselt mit Authentifizierung möglich.
- E-Mails des Empfängers werden nur intern zusätzlich auf dem vom Empfänger zur Mailbearbeitung genutzten und gesichertem Rechner gespeichert.

## 7 Zusammenfassung

Das vorliegende Dokument „Datenschutz Management System“ legt detailliert dar, wie dataplan im Sinne einer **Selbstverpflichtung** mit dem Datenschutz natürlicher Personen umgeht. Es vermittelt, dass alle Verpflichtungen aus der DSGVO sowie dem BDSG sehr ernst genommen und nach dem aktuellen Stand der Technik bestmöglich in die betriebliche Praxis umgesetzt werden. Dataplan wird dauerhaft bestrebt sein dies zu gewährleisten. Selbstverständlich nehmen wir Kritik jederzeit gern entgegen und werden kontinuierlich an Verbesserungen arbeiten.
Dataplan möchte sich so für alle Kunden, Partner sowie Freunde als zuverlässiger Dienstleister heute und in der Zukunft präsentieren.