

# Datenschutz und Datensicherheit bei a+s

## Information

Entity a+s DialogGroup GmbH  
Max-Planck-Straße 7  
D-71254 Ditzingen-Heimerdingen

Contact Kai-Uwe Hesse  
Telefon +49.7152/33000-0  
Telefax +49.7152/33000-20  
hesse@as-dialoggroup.de

Owner DMC Datenschutz Management & Consulting GmbH & Co. KG  
Augustinusstraße 9d  
D-50226 Frechen  
Telefon +49.2234.695890  
Telefax +49.2234.695899

Creating and  
managing Christian Semmler, Dipl.-Wirtsch.Inf.  
Managing Consultant  
semmler@dmc-datenschutz.de

STATUS VERTRAULICH

Version 1.21

Zuletzt  
bearbeitet 18.02.2009 durch Roth

Vermerke

## Datenschutz und Datensicherheit bei A&S

Information

### Wichtiger Hinweis

Dieses Dokument wird lediglich zu Informationszwecken zur Verfügung gestellt und verändert nicht die Bedingungen jedweder Vereinbarung mit a+s. Es kann jederzeit und ohne Vorankündigung geändert werden.

Die hierin enthaltenen Informationen sind als vertraulich klassifiziert und dürfen ohne die schriftliche Genehmigung von a+s keinem Dritten zugänglich gemacht werden.

Mitgeltende Dokumente		
Dokument	Stand/Version	Verfasser
Ehrenkodex des Councils Listbroker		DDV
Qualitäts- und Leistungsstandards (QuLS) der Councils Direct Mail Services und Listbroker		DDV
Verpflichtungserklärung Datenverarbeitung		DDV
Verpflichtungserklärung Datenverarbeitung für Listbroker		DDV
Verpflichtungserklärung Lettershop-Verarbeitung		DDV

# Datenschutz und Datensicherheit bei A&S

Information

## Inhaltsverzeichnis

Wichtiger Hinweis.....	2
<b>1. Vorbemerkungen.....</b>	<b>5</b>
<b>2. Organisation des Datenschutzes .....</b>	<b>6</b>
2.1. Gesetzliche Grundlagen.....	6
2.2. Beauftragter für den Datenschutz.....	7
2.3. Personelle Maßnahmen .....	7
2.3.1. Verpflichtung auf das Datengeheimnis nach § 5 BDSG .....	7
2.3.2. Richtlinie zum Einsatz der Informations- und Kommunikationstechnik.....	7
2.3.3. Information und Schulung.....	8
2.3.4. Regelmäßige Information.....	9
2.4. Formale Voraussetzungen und Maßnahmen.....	9
2.4.1. Interne Verarbeitungsübersicht.....	9
2.4.2. Öffentliches Verzeichnisse.....	10
2.4.3. Auftragsdatenverarbeitung.....	10
<b>3. Gewährleistung der Rechte der Betroffenen und Verbraucherschutz .....</b>	<b>11</b>
<b>4. Technische und organisatorische Sicherheitsmaßnahmen.....</b>	<b>12</b>
4.1. Zutrittskontrolle.....	12
4.2. Zugangskontrolle.....	12
4.2.1. PCs/Netzwerk/Applikationen.....	13
4.2.2. Passwortverfahren.....	13
4.2.3. Zugang von außen .....	13
4.3. Zugriffskontrolle.....	14
4.3.1. Berechtigungs-/Zugriffskonzept .....	14
4.3.2. Löschung von Daten und Entsorgung von Ausdrucken/Listen .....	14
4.3.3. Bewegliche Datenträger .....	15

## Datenschutz und Datensicherheit bei A&S

Information

4.4. Weitergabekontrolle .....	15
4.4.1. Dateneingang .....	15
4.4.2. Datenausgang .....	16
4.5. Eingabekontrolle .....	16
4.6. Auftragskontrolle .....	17
4.7. Verfügbarkeitskontrolle.....	18
4.7.1. Bauliche Maßnahmen (Brandschutz, Stromversorgung, Klimaversorgung) .....	18
4.7.2. Datensicherungskonzept .....	18
4.7.3. Virenschutz.....	18
4.8. Trennungskontrolle (getrennte Verarbeitung) .....	19
<b>5. Ansprechpartner .....</b>	<b>20</b>
5.1. Datenschutzbeauftragter .....	20
5.2. EDV, IT-Sicherheit.....	20

# Datenschutz und Datensicherheit bei A&S

Information

## 1. Vorbemerkungen

a+s ist ein unabhängiger Adressdienstleister mit einem echten Full-Service-Angebot. Wir haben uns auf professionelles Dialogmarketing spezialisiert und bieten bei Bedarf alle Leistungen aus einer Hand. Die Kernkompetenz umfasst die gesamten Bereiche Adressbeschaffung, -anreicherung, -optimierung sowie der treuhänderischen Datenbestandsverwaltung. In den Bereichen Werbemittelproduktion, Verarbeitung und Versand, arbeiten wir mit professionellen Partnern zusammen.

Durch unsere Mitgliedschaft im Deutschen Direktmarketing Verband e.V. (DDV) und durch die Auszeichnung mit dem Qualitätssiegel des *Council Listbroker* fühlen wir uns dem dort definierten Ehrencodex bezüglich Qualitäts- und Leistungsstandards und dem Datenschutz besonders verpflichtet. Entsprechend dem jeweiligen Tätigkeitsbereich hat a+s daher die Verpflichtungserklärungen Datenverarbeitung, Datenverarbeitung für Listbroker und Lettershop-Verarbeitung mit weitreichenden Garantien unterzeichnet und beim DDV mit Schutzwirkung zugunsten Dritter hinterlegt.

Datenschutz und Datensicherheit sind für uns von großer Wichtigkeit. Wir respektieren den Schutz persönlicher Daten nicht nur, um gesetzliche Mindestvorgaben zu erfüllen. Über die kostenpflichtige Überprüfung der Qualitäts- und Leistungsstandards durch den DDV hinaus unterwerfen wir uns daher *zusätzlich der kontinuierlichen, unabhängigen* Kontrolle und Beratung durch einen *freiwillig* bestellten, externen Datenschutzbeauftragten. Damit möchten wir zum Ausdruck bringen, dass die Wahrung der Persönlichkeitsrechte bei a+s gelebte Unternehmenskultur und Selbstverständnis unserer Dienstleistungen und Produkte ist. Maßnahmen zum Datenschutz werden daher bei a+s kontinuierlich verbessert, um die Daten und Privatsphäre Ihrer Kunden umfassend zu schützen und deren Rechte zu gewährleisten.

# Datenschutz und Datensicherheit bei A&S

Information

## 2. Organisation des Datenschutzes

### 2.1. Gesetzliche Grundlagen

Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gelten die Vorschriften des Bundesdatenschutzgesetzes (BDSG) gemäß § 1 Abs. 2 Nr. 3 BDSG.

Insbesondere sind für das Listbroking und die Datenverarbeitung folgende Regelungen zu nennen:

- § 4d,e Meldepflicht
- § 4f Beauftragter für den Datenschutz
- § 5 Datengeheimnis
- § 9 Technische und organisatorische Maßnahmen
- § 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag
- § 28 Datenerhebung,- verarbeitung und -nutzung für eigene Zwecke
- § 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung
- § 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung in anonymisierter Form
- § 33 Benachrichtigung des Betroffenen
- § 34 Auskunft an den Betroffenen
- § 35 Berichtigung, Löschung und Sperrung von Daten
- § 38 Aufsichtsbehörde

# Datenschutz und Datensicherheit bei A&S

Information

## 2.2. Beauftragter für den Datenschutz

Gemäß § 4f Abs. 1 BDSG muss a+s keinen Beauftragten für den Datenschutz (betrieblicher Datenschutzbeauftragter) bestellen, da wir weniger als 10 Personen mit der Verarbeitung personenbezogener Daten in automatisierten Verfahren beschäftigen.

Um jedoch unseren hohen Ansprüchen an Datenschutz und Datensicherheit gerecht zu werden, hat a+s unbeschadet dieser Regelung *freiwillig* einen unabhängigen externen Datenschutzbeauftragten bestellt.

Diese Funktion wird durch einen Berater der DMC Datenschutz Management & Consulting GmbH & Co. KG (DMC), Augustinusstraße 9d, D-50226 Frechen wahrgenommen. Die Gesellschaft übt für a+s die Aufgaben des betrieblichen Datenschutzbeauftragten als „externer“ Datenschutzbeauftragter gemäß § 4f Abs. 2 Satz 3 BDSG aus und gewährleistet uns eine umfassende Unterstützung in allen rechtlichen, technischen und organisatorischen Fragen und Maßnahmen auf höchstem Niveau.

## 2.3. Personelle Maßnahmen

### 2.3.1. Verpflichtung auf das Datengeheimnis nach § 5 BDSG

Alle Mitarbeiter von a+s sind auf das Datengeheimnis nach § 5 BDSG verpflichtet.

Neben einer allgemeinen Aufklärung über die Bedeutung des Datengeheimnisses enthält diese Verpflichtung auch Hinweise auf weitergehende Informationen zum Datenschutz sowie auf eventuelle Sanktionen.

Im Rahmen der Zusammenarbeit mit externen Partnern (insbesondere im Bereich der Produktion, Verarbeitung, Adressierung/Personalisierung) stellt a+s sicher, dass ebenso alle in die Projekte eingebundenen Subunternehmer bzw. deren Mitarbeiter entsprechend verpflichtet sind.

### 2.3.2. Richtlinie zum Einsatz der Informations- und Kommunikationstechnik

Für alle Mitarbeiter der a+s gilt eine Richtlinie für den Einsatz der Informations- und Kommunikationstechnik, welche alle wesentlichen Aspekte zum datenschutzkonformen Umgang mit personenbezogenen oder personenbeziehbaren Daten im Zusammen-

## Datenschutz und Datensicherheit bei A&S

Information

hang mit der Bearbeitung von Projekten enthält. Die Mitarbeiter werden schriftlich auf die Einhaltung dieser Richtlinie verpflichtet.

### 2.3.3. Information und Schulung

Die bei a+s geltenden Regelungen zu Datenschutz, IT-Sicherheit und Informationsschutz sind in der Richtlinie zum Einsatz der Informations- und Kommunikationstechnik allen Mitarbeitern zugänglich.

Erste Hinweise darauf erhalten die Mitarbeiter bereits bei Einstellung im Arbeitsvertrag. Weitergehende Informationen folgen im Zusammenhang mit der schriftlichen Verpflichtung auf das Datengeheimnis und auf die Einhaltung der Richtlinie sowie im Rahmen der arbeitsplatzbezogenen Einweisung durch die Mitarbeiter der EDV.

Hierdurch wird sichergestellt, dass jeder Mitarbeiter über folgende Punkte informiert ist:

- Grundlagen des Datenschutzes
- Interne Regelungen zum Datenschutz, IT-Sicherheit und Informationsschutz
- Grundzüge technischer und organisatorischer Maßnahmen zur Sicherstellung von Datenschutz, IT-Sicherheit und Informationsschutz
- Verantwortlichkeiten
- Informationsquellen

Ergänzend zu diesen grundsätzlichen Informationen ist vorgesehen, die Mitarbeiter in einer zweiten Stufe einmal jährlich im Rahmen von Präsenzveranstaltungen tiefergehend zu schulen.

Durch dieses Konzept wird sichergestellt, dass sowohl neu eingestellte Mitarbeiter in die Thematik des Datenschutzes eingeführt werden als auch die Kenntnisse der schon länger bei a+s beschäftigten Mitarbeiter regelmäßig aufgefrischt und aktualisiert werden.

Im Übrigen ist der eigentliche Verarbeitungsvorgang von Auftragsdaten durch rechtskonform zu gestaltende Weisungen des Auftraggebers vorgegeben, da der Umgang mit Daten regelmäßig weisungsgebunden im Rahmen eines Auftragsverhältnisses nach § 11 BDSG erfolgt.

## Datenschutz und Datensicherheit bei A&S

Information

### 2.3.4. Regelmäßige Information

a+s erhält über die DMC regelmäßig neueste Informationen über technische und rechtliche Entwicklungen auf den Gebieten des Datenschutzes und der Datensicherheit, so dass ständig eine zeitentsprechende Sensibilisierung bei a+s gegeben ist.

## 2.4. Formale Voraussetzungen und Maßnahmen

### 2.4.1. Interne Verarbeitungsübersicht

Im Rahmen der Verarbeitung personenbezogener Daten stellt a+s dem Datenschutzbeauftragten eine Übersicht über die Verarbeitungen personenbezogener Daten sowie der zugriffsberechtigten Personen gemäß § 4g Abs. 2 BDSG (interne Verarbeitungsübersicht) zur Verfügung.

Der Inhalt dieser Angaben ergibt sich aus § 4e Satz 1 Nr. 1 bis 9 BDSG:

1. Name der verantwortlichen Stelle,
2. Leiter der verantwortlichen Stelle und der Datenverarbeitung,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. Geplante Datenübermittlung an Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 BDSG (i.V.m. der Anlage dazu) zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

Dabei dokumentieren wir auf der Ebene der Verarbeitung bzw. des Verfahrens eine Reihe weiterer Umstände. Dies betrifft z.B. Zugriffsberechtigungen, die Meldepflicht, das Ergebnis der Vorabkontrolle (§ 4d Abs. 5, 6 BDSG) und den Grund des Verzichts auf die Benachrichtigung des Betroffenen.

Die unternehmensweit für a+s vorliegende Übersicht wird im Rahmen regelmäßiger Statusgespräche bei Bedarf aktualisiert.

## Datenschutz und Datensicherheit bei A&S

Information

### 2.4.2. Öffentliches Verzeichnisse

Der Datenschutzbeauftragte hat auf Antrag die Angaben des öffentlichen Verzeichnisses (§ 4e Satz 1 Nr. 1 bis 8 BDSG) jedermann in geeigneter Weise verfügbar zu machen.

Ein derartiges öffentliches Verzeichnisse für a+s liegt vor und wird auf Antrag jedermann zur Verfügung gestellt.

### 2.4.3. Auftragsdatenverarbeitung

a+s erbringt ihre Dienstleistungen gegenüber ihren Kunden regelmäßig als Auftragsdatenverarbeitung gemäß § 11 BDSG (z.B. als Generalunternehmer im Bereich des Direktmarketing sowie insbesondere im Bereich der Beschaffung und Vermarktung von Adressen verschiedener Listeigner an Werbetreibende).

Dabei nimmt a+s regelmäßig Dienstleistungen externer Unternehmen in Anspruch, die in den Bereich der Auftragsdatenverarbeitung fallen. Insbesondere im Projektgeschäft im Bereich der Produktion, Verarbeitung, Adressierung/Personalisierung und Versand von Werbemitteln sowie der maschinellen Responsebearbeitung werden Unterauftragnehmer eingesetzt.

Die Auftragnehmer werden dabei unter besonderer Berücksichtigung der Eignung der getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt. Für die betroffenen Auftragsverhältnisse wird die Verpflichtungserklärung Lettershop-Verarbeitung (DDV-Standard) zugrunde gelegt. Diese Regelung entspricht grundsätzlich den Vorgaben des § 11 BDSG.

## Datenschutz und Datensicherheit bei A&S

Information

### 3. Gewährleistung der Rechte der Betroffenen und Verbraucherschutz

Im Interesse der Verbraucher und der Direktmarketing-Anwender unterstützen wir aktiv die Robinson-Datei. Wir empfehlen unseren Kunden immer, soweit technisch möglich und wirtschaftlich vertretbar, den Abgleich gegen die Robinson-Datei. Werbeverweigerer setzen wir außerdem in unsere interne Werbverweigererliste und nehmen sie von weiteren Aktionen aus.

Darüber hinaus verpflichten wir uns, alle Wünsche Betroffener nach Auskunft, Berichtigung, Löschung oder Sperrung von Daten schnellstens, zuvorkommend und ausführlich zu bearbeiten.

Als zusätzlichen Service bieten wir unseren Kunden dabei nicht nur an, beim Werbetreibenden eingehende Anfragen an den>Listeigner weiterzuleiten, sondern wickeln auf Wunsch (und Anordnung) gerne auch die gesamte Korrespondenz für und zwischen allen Beteiligten ab (Betroffener-Werbetreibender-Auftragsdatenverarbeiter-Listeigner).

# Datenschutz und Datensicherheit bei A&S

Information

## 4. Technische und organisatorische Sicherheitsmaßnahmen

*Allgemeine Beschreibung gemäß § 4e Satz 1 Nr. 9 BDSG, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 BDSG (i.V.m. der Anlage dazu) zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.*

### 4.1. Zutrittskontrolle

*Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Nr. 1 der Anlage zu § 9 BDSG).*

*Ziel der Zutrittskontrolle ist es, zu gewährleisten, dass nur Berechtigte Personen Zutritt zu Grundstücken, Gebäuden, Bereichen und Räumen haben, in welchen sich Einrichtungen für die Datenverarbeitung (DV-Anlagen, Server, PCs/Terminals, Systemkomponenten usw.) befinden.*

Die Datenverarbeitungsräume der a+s befinden sich in einem abgeschlossenen Gebäude des *Grafischen Zentrums Drucktechnik* (GZD) in Ditzingen-Heimerdingen. Getrennte und abgestufte Sicherheitsbereiche (Foyer, Büroräume, Serverraum, Archiv) gewährleisten, dass nur gemäß ihrem Aufgabenbereich befugte Personen Zutritt zu den jeweiligen Räumen haben.

Als zusätzliche Schutzmaßnahme ist unser klimatisierter Serverraum durch ein mechanisches Code-Schließsystem gesichert. Die Server auf denen Ihre Daten lagern, befinden sich wiederum in einem nochmals abgeschlossenen Server-Rack.

### 4.2. Zugangskontrolle

*Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Nr. 2 der Anlage zu § 9 BDSG).*

*Ziel der Zugangskontrolle ist es, durch technische Maßnahmen sicherzustellen, dass nur berechtigte Personen Zugang zu Rechnern, Servern, Systemkomponenten etc. haben. Dies gilt sowohl für die Inbetriebnahme als auch für den laufenden Betrieb.*

## Datenschutz und Datensicherheit bei A&S

Information

### 4.2.1. PCs/Netzwerk/Applikationen

Als Zugangskontrolle wird auf den PCs die Zugangskontrolle zu Windows verbunden mit der Zugangskontrolle zum Netz genutzt.

Vor der Benutzung der PCs müssen sich die Mitarbeiter durch die Eingabe einer Benutzerkennung und eines Passwortes im Netzwerk identifizieren und authentifizieren. Jeder Mitarbeiter verfügt nur über die Anwendungen, die er für seinen Aufgabenbereich benötigt. Ferner ist für bestimmte Anwendungen (z.B. Datenbereitstellung und -versand) ein zusätzlicher Login erforderlich.

Damit auch bei einer kürzeren Abwesenheit des IT-Benutzers ein Zugriffsschutz für das IT-System gewährleistet ist, wird nach 15 Minuten Inaktivität automatisch eine Bildschirmsperre aktiv, welche nur durch eine erfolgreiche Benutzerauthentifikation deaktiviert werden kann. Die Benutzer sind angehalten diese Bildschirmsperre allerdings auch schon vor Ablauf dieser 15 Minuten selbst zu aktivieren.

### 4.2.2. Passwortverfahren

Die minimale Passwortlänge beträgt 8 Zeichen. Ein Passwortwechsel wird alle drei Monate erzwungen. Eine Wiederverwendung kann frühestens nach zehn Wechseln erfolgen. User werden nach der dreimaligen Falscheingabe ihres Passwortes gesperrt und können nur vom Administrator wieder aktiviert werden. Dies muss an einem Server im Server-Raum geschehen.

### 4.2.3. Zugang von außen

Der Zugang von außen wird durch den Einsatz aktueller Technologien und Best-Practices abgesichert. Beispielhaft seien genannt:

- Cisco PIX-Firewall
- IP Masquerading
- VPN-Einwahl
- Demilitarisierte Zone (DMZ) für Virenschutz und E-Mail-Server

## Datenschutz und Datensicherheit bei A&S

Information

### 4.3. Zugriffskontrolle

*Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Nr. 3 der Anlage zu § 9 BDSG).*

*Ziel der Zugriffskontrolle ist es, über ein Berechtigungskonzept sicherzustellen, dass der Zugriff auf personenbezogene Daten nur in dem Umfang ermöglicht wird, wie es für die jeweilige Aufgabenerledigung erforderlich ist. Aus dem Berechtigungskonzept muss zweifelsfrei hervorgehen, welche Benutzer auf welche Benutzer(gruppen) auf welche Daten, Funktionen, Objekte usw. Zugriff haben.*

#### 4.3.1. Berechtigungs-/Zugriffskonzept

Berechtigungen werden bei a+s auf Ebene PCs/Netzwerk, Netzwerk-Laufwerken und Applikationen differenziert nach Aufgabenbereich vergeben. Zugriff auf die Datenbanken sowie die Datenein- bzw. -ausgangsrechner und somit auf die personenbezogenen Daten haben nur autorisierte Mitarbeiter der EDV.

Berechtigungen werden von den Mitarbeitern der EDV auf Weisung der Geschäftsführung angelegt. Beim Ausscheiden eines Mitarbeiters wird der entsprechende User gelöscht. Das Hinzufügen, Ändern und Löschen von Berechtigungen ist nur autorisierten Mitarbeitern der EDV möglich.

#### 4.3.2. Löschung von Daten und Entsorgung von Ausdrucken/Listen

Nach Wegfall des Verarbeitungszwecks werden alle im Zusammenhang mit der Verarbeitung angefallenen Daten gelöscht. Dies geschieht unmittelbar bzw. nach Ablauf der gesetzlichen, satzungsmäßigen oder vertraglichen Aufbewahrungsfristen.

Falsche bzw. veralteter Datenträger werden mit einem hauseigenen speziell dafür vorgesehenen Reißwolf vernichtet.

Die Löschung bzw. Vernichtung dokumentieren wir in speziellen Löschprotokollen, die von einem Zeugen bestätigt werden müssen. Diese Löschprotokolle werden sowohl auf dem Server gespeichert als auch ausgedruckt abgelegt. Wenn vom Auftraggeber gewünscht, wird die Löschung ebenfalls an diesen bestätigt.

Gleiches gilt analog für etwaige angefallene Ausdrücke oder Listen.

## Datenschutz und Datensicherheit bei A&S

Information

### 4.3.3. Bewegliche Datenträger

Um unbefugten Zugriff auf Datenträger mit personenbezogenen Daten zu verhindern, werden CDs, DVDs und Disketten wie auch Sicherungsbänder etc. bei a+s ausschließlich zum Zwecke der Verarbeitung während der Arbeitszeit am Arbeitsplatz genutzt. Ansonsten werden diese grundsätzlich in einem feuerfesten Safe im abgeschlossenen Archivraum des Kellers verwahrt, der nur autorisierten Mitarbeitern und der Geschäftsführung zugänglich ist.

### 4.4. Weitergabekontrolle

*Es ist zu 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 (Nr. 4 der Anlage zu § 9 BDSG).*

*Ziel der Weitergabekontrolle sind einerseits die Sicherung der Daten gegen unbefugte Kenntnisnahme auf dem Übertragungsweg. Andererseits die Protokollierung zum Nachweis, durch wen, von welcher Stelle Daten zu welchem Ziel übertragen bzw. transportiert wurden.*

Um zu verhindern, dass private Datenträger von den Mitarbeitern genutzt werden, wurden an allen Rechnern außerhalb des Serverraums die CD-, DVD- und Disketten-Laufwerke, die USB-Anschlüsse und die CD-Brenner wirksam deaktiviert. Daten auf oder von Datenträgern zu kopieren ist ausschließlich auf einem speziell hierzu vorgesehen Arbeitsplatz im Server-Raum möglich und wird protokolliert.

#### 4.4.1. Dateneingang

Personenbezogene Daten gehen bei a+s per E-Mail, FTP, ISDN, HTTPS oder auch auf Datenträgern ein.

Bewegliche Datenträger wie CDs, DVDs und Disketten werden bei a+s grundsätzlich nur von den Mitarbeitern der EDV entgegengenommen und ausschließlich auf einem speziell protokollierten Dateneingangsrechner im Serverraum ausgelesen. Sie werden mit dem Namen des Auftraggebers sowie dem Datum des Eingangs versehen und im

## Datenschutz und Datensicherheit bei A&S

Information

Anschluss im Safe im abgeschlossenen Archivraum des Kellers verwahrt (siehe auch Abschnitt 4.3.3 oben).

Möchte ein Auftraggeber Daten per Email schicken, wird er darauf hingewiesen, diese verschlüsselt an die Adresse [daten@as-dialoggroup.de](mailto:daten@as-dialoggroup.de) zu richten. Dieses Postfach und auch die Zugänge für alle anderen elektronischen Übertragungswege sind auf einem speziell für den Datenein- und -ausgang vorgesehenen Arbeitsrechner im Server-Raum eingerichtet und nur für autorisierte Mitarbeiter der EDV bzw. den Geschäftsführer zugänglich.

Beim Eintreffen von neuen elektronisch übermittelten Daten werden die Mitarbeiter der EDV automatisch über ein firmeneigenes Tool benachrichtigt. Alle wichtigen Informationen zu den eingetroffenen Daten, wie Empfangsdatum und -Uhrzeit, die Anhänge der Emails, Dateigröße, etc. wie auch Löschdatum und -Uhrzeit, zu der die Daten aus den jeweiligen Ordnern oder aus dem Posteingang des E-Mail-Programms gelöscht wurden und in die Verarbeitung gingen werden protokolliert.

### 4.4.2. Datenausgang

Je nach Auftrag werden Daten von a+s per E-Mail, FTP, ISDN oder HTTPS verschickt bzw. bereitgestellt. Die elektronische Übertragung bzw. Bereitstellung erfolgt dabei ausschließlich verschlüsselt und passwortgeschützt bzw. getrennt nach Berechtigungsbereichen und wird nur von geschulten Mitarbeitern der EDV durchgeführt.

Sämtliche Datenbereitstellungen und -übertragungen werden umfassend protokolliert.

Von a+s ausgehende Datenträgertransporte zu Auftraggebern bzw. Auftragnehmern finden nicht statt.

## 4.5. Eingabekontrolle

*Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Nr. 5 der Anlage zu § 9 BDSG).*

*Ziel der Eingabekontrolle ist die Sicherstellung der Nachvollziehbarkeit einzelner Benutzeraktionen im Bezug auf Eingabe, Veränderung und Löschung von Daten im Nachhinein. Voraussetzung hierfür ist, dass nach dem Prinzip der minimalen Berechtigung jeder nur auf die Daten zugreifen kann, die er für seine eigene Arbeit benötigt.*

## Datenschutz und Datensicherheit bei A&S

Information

Um diese Nachvollziehbarkeit bei a+s im Nachhinein zu gewährleisten, werden sämtliche Aktivitäten auf allen Systemen (Rechner/Server) benutzerbezogen sowohl auf System- als auch auf Anwendungsebene protokolliert. Dabei wird jede Art von Objektzugriff registriert (wer/wann auf was zugegriffen hat) und sicherheitsrelevante Ereignisse in einem separaten Sicherheitsprotokoll protokolliert. Die Protokolle aller Rechner/Server werden von einem weiteren Server gesichert und im Rahmen des Datensicherungskonzepts drei Monate gespeichert.

### 4.6. Auftragskontrolle

*Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Nr. 6 der Anlage zu § 9 BDSG).*

*Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag (z.B. durch ein Rechenzentrum) verarbeitet werden, nur nach den Weisungen des Auftraggebers ausgeführt werden. Die Auftragskontrolle ist als Ergänzung der §§ 11 und 29 BDSG zu sehen. Insbesondere sind im Vertrag die Art und Weise der Auftragserteilung zu formalisieren.*

Um im Rahmen der ordnungsgemäßen Vertragsausführung zu gewährleisten, dass personenbezogene Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden, erhalten die Auftraggeber vor Auftragserfüllung eine individuelle, schriftliche Auftragsbestätigung von dem zuständigen Kundenbetreuer, in der sämtliche Arbeitsschritte entsprechend den Weisungen aufgeführt sind.

Nach Bestätigung durch den Auftraggeber beginnt die Bearbeitung des Auftrages. Der Kundenbetreuer übergibt einen Workflow mit den entsprechenden Anweisungen aus der Auftragsbestätigung an den zuständigen Mitarbeiter der EDV. Dieser erhält die Auftragsdaten vom Auftraggeber, führt den Auftrag gemäß den Anweisungen des Workflows aus und versendet dann die bearbeiteten Daten an eine vom Auftraggeber gewünschte Stelle.

Der komplette Auftrag vom Angebot bis zur Rechnungsstellung wird vom zuständigen Kundenbetreuer im Warenwirtschaftssystem dokumentiert. Die gesamte Prozedur dient auch der Absicherung der Rechtsverbindlichkeit.

## Datenschutz und Datensicherheit bei A&S

Information

### 4.7. Verfügbarkeitskontrolle

*Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Nr. 7 der Anlage zu § 9 BDSG).*

#### 4.7.1. Bauliche Maßnahmen (Brandschutz, Stromversorgung, Klimaversorgung)

Ein Feuerlöscher ist in zentraler Lage vorhanden. Im Serverraum wird zudem darauf geachtet, keine leicht brennbaren Materialien zu lagern. Um bei Überspannung, Unterspannung oder Stromausfall die Versorgung der Server sicherzustellen, sind zwei UPS vorhanden, die in den Serverschrank integriert sind. Der Server-Raum verfügt zudem über eine Klimaanlage, die den Raum auf konstanter Betriebstemperatur hält.

#### 4.7.2. Datensicherungskonzept

Ein Datensicherungsplan legt fest, welche Daten/Systeme in welchen Abständen und zu welchem Zeitpunkt auf welche Medien bzw. anderen Systeme gesichert werden und wie die Verantwortlichkeiten hierfür geregelt sind. Die Datensicherung erfolgt dabei mehrstufig sowohl auf Servern als auch auf externen Wechseldatenträgern.

Diese werden im Safe im abgeschlossenen Archivraum des Kellers verwahrt (siehe auch Abschnitt 4.3.3 oben). Zusätzlich wird ein täglich rollierendes Sekundärbackup an einem entfernten Standort verwahrt und am darauf folgenden Tag durch ein aktuelleres ersetzt. Alle Wechseldatenträger sind durch Verschlüsselung vor Zugriffen unbefugter geschützt.

Im Falle einer Wiederherstellung ist sichergestellt, dass zwischen dem Zeitpunkt des letzten Backups und dem Schadenfall etwaig gelöschte Daten anhand der Löschprotokolle nachvollzogen werden können, so dass jederzeit eine konsistente Rekonstruktion des Datenbestandes möglich ist.

#### 4.7.3. Virenschutz

Sämtliche Systeme (Arbeitsplatzrechner und Server) sind durch eine aktuelle Virenschutz-Lösung gesichert. Diese Software wird automatisch bei Bereitstellung neuer Updates aktualisiert und ständig überprüft. Weiterhin werden sämtliche Arbeitsplatzrechner wöchentlich einer vollständigen Überprüfung unterzogen.

## Datenschutz und Datensicherheit bei A&S

Information

### 4.8. Trennungskontrolle (getrennte Verarbeitung)

*Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Nr. 8 der Anlage zu § 9 BDSG).*

Bei a+s gibt es zwei verschiedene Arten von Daten:

- Business-to-Business-Adressen
- Privat-Adressen

Die Maßnahmen, die ergriffen werden um die Daten von verschiedenen Auftraggebern getrennt zu halten unterscheiden sich hier aufgrund der gewählten Speicherform.

Business-to-Business-Adressen werden in von einander getrennten Datenbanken gespeichert, d.h. es existiert für jeden Auftraggeber eine separate Datenbank in der sowohl die Adressen als auch die Selektionsinformationen zu diesen Adressen gespeichert werden. So kann es zu keiner Vermischung der einzelnen Bestände kommen.

Privat-Adressen werden in einen vorgegebenen Datensatzaufbau gebracht und in eine SQL-Datenbank eingespielt. Bei jeder dieser Adressen wird über eine eindeutige Nummer hinterlegt, von welchem Auftraggeber bzw. aus welchem Bestand eines Auftraggebers die jeweilige Adresse stammt.

## Datenschutz und Datensicherheit bei A&S

Information

### 5. Ansprechpartner

#### 5.1. Datenschutzbeauftragter

DMC Datenschutz Management & Consulting GmbH & Co. KG

Augustinusstraße 9d

D-50226 Frechen

Telefon +49.2234.695890

Telefax +49.2234.695899

Christian Semmler, Dipl.-Wirtsch.Inf.

Managing Consultant

semmler@dmc-datenschutz.de

#### 5.2. EDV, IT-Sicherheit

a+s DialogGroup GmbH

Max-Plank-Straße 7

D-71254 Ditzingen-Heimerdingen

Chris-Holger Riemer

Telefon +49.7152/33000-12

Telefax +49.7152/33000-20

riemer@as-dialoggroup.de