Anlage zum Scanauftrag

Regelungen zur Auftragsdatenverarbeitung

zwischen

.....

- nachstehend Auftraggeber genannt -

und

Dropscan GmbH, Ehrenbergstr. 16a, 10245 Berlin

- nachstehend Auftragnehmer genannt -

1. Einführung

1.1. Die Regelungen zur Auftragsdatenverarbeitung dieser Anlage konkretisieren die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus deren Vertrag über das Scannen von Dokumenten ergeben (nachfolgend bezeichnet als „Hauptvertrag“). Der Inhalt des Hauptvertrages bestimmt sich durch die Allgemeinen Geschäftsbedingungen des Auftragnehmers sowie die konkreten Scanaufträge des Auftraggebers.

1.2. Die Regelungen dieser Anlage findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag im Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrags.

2. Definitionen

2.1. „Personenbezogene Daten“ sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

2.2. „Datenverarbeitung im Auftrag“ ist die Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.

2.3. „Weisung“ ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

3. Gegenstand des Auftrags

3.1. Gegenstand des Auftrags ist das Scannen von Dokumenten und sonstigen Vorlagen durch den Auftragnehmer, die der Auftraggeber im Rahmen des Hauptvertrags eingereicht hat. Die Scanergebnisse werden dem Auftraggeber nach dessen Wahl, entweder in unkörperlicher Form oder gespeichert auf Datenträgern zur Verfügung gestellt. Die Scanvorlagen werden anschließend nach Wahl des Auftraggebers vernichtet oder an diesen zurückgesendet.

3.2. Die Art der Daten bestimmt sich anhand des jeweiligen Scanauftrags des Auftraggebers.

4. Anwendungsbereich und Verantwortlichkeit

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („verantwortliche Stelle“ im Sinne des §3 Abs. 7 BDSG).

4.2. Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Berichtigung, Löschung, Sperrung und Herausgabe von Daten verlangen.

5. Anwendungsbereich und Verantwortlichkeit

5.1. Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

5.2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des

Auftraggebers vor Missbrauch und Verlust treffen, die den Forderungen des Bundesdatenschutzgesetzes (§ 9 BDSG) entsprechen. Dies beinhaltet insbesondere

a) Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),

b) zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

c) dafür Sorge zu tragen, 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 (Zugriffskontrolle),

d) dafür Sorge zu tragen, 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 (Weitergabekontrolle),

e) dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

f) dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

g) dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

h) dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).

5.3. Eine Maßnahme nach b) bis d) ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Eine Darstellung dieser technischen und organisatorischen Maßnahmen wird Anhang zu dieser Anlage.

5.4. Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG notwendigen Angaben zur Verfügung, soweit sich diese nicht bereits aus dieser Anlage und ihrem Anhängen ergeben.

5.5. Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß §5 Bundesdatenschutzgesetz (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen worden sind. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

5.6. Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten des, sofern zutreffend, betrieblichen Datenschutzbeauftragten oder der für den Datenschutz zuständigen Person mit.

5.7. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.

5.8. Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

5.9. Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.

6. Pflichten des Auftraggebers

6.1. Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

6.2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

6.3. Dem Auftraggeber obliegen die aus § 42a BDSG resultierenden Informationspflichten.

6.4. Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

6.5. Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, sofern diese nicht bereits im Hauptvertrag geregelt worden sind, so trägt diese der Auftraggeber.

6.6. Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

7. Anfragen Betroffener an den Auftraggeber

Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen, vorausgesetzt:

- der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert und
- der Auftraggeber erstattet dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten.

8. Kontrollpflichten

8.1. Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers durch Selbstauskünfte des Auftragnehmers und dokumentiert das Ergebnis. Die Selbstauskunft bestimmt sich nach dem Anhang zu dieser Anlage.

8.2. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

9. Subunternehmer

9.1. Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt (s. Anlage Subunternehmer).

9.2. Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit,

Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages.

10. Geheimhaltungspflichten

10.1. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

10.2. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

11. Informationspflichten, Schriftformklausel, Rechtswahl

11.1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortlicher Stelle“ im Sinne des Bundesdatenschutzgesetzes liegen.

11.2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

11.3. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

11.4. Es gilt deutsches Recht.

Anhang – Verzeichnis über das Verfahren sowie technische und organisatorische Maßnahmen

1. Zuständige Person

Verantwortliche Stelle für die Datenverarbeitung:

Dropscan GmbH
Ehrenbergstr. 16a
10245 Berlin – Deutschland

Vertreten durch die Geschäftsführer: Christian Schulte, Stephan Lindow
Handelsregister: Amtsgericht Berlin / HRB 136188 B

Zuständige Person und Ansprechpartner für den Datenschutz: Stephan Lindow

Email: datenschutz@dropscan.de
Telefon: (030) 34 64 93 15

2. Zweckbestimmung der Datenverarbeitung, Kreis Betroffener Personengruppen, Empfänger und Art der Daten

2.1. Gegenstand der Datenverarbeitung ist das Scannen von Dokumenten und sonstigen Vorlagen (nachfolgend „Scanvorlagen“) durch die verantwortliche Stelle. Die Scanvorlagen werden der verantwortlichen Stelle durch deren Kunden (nachfolgend „Auftragnehmer“) eingereicht, nachdem diese sich zuvor auf der Website der verantwortlichen Stelle registriert und dieser einen Scanauftrag erteilt haben. Die Art der Daten und der Kreis der Betroffenen bestimmt sich anhand des jeweiligen Scanauftrags des Auftraggebers. Die Scanergebnisse werden dem Auftraggeber nach dessen Wahl, entweder in unkörperlicher Form oder gespeichert auf Datenträgern zur Verfügung gestellt. Sie werden anschließend bei der verantwortlichen Stelle gelöscht. Die Scanvorlagen werden anschließend nach Wahl des Auftraggebers vernichtet oder an diesen zurückgesendet.

2.2. Die Scanvorgänge werden durch die ODS-Office Data Service GmbH, Ehrenbergstr. 16a, 10245 Berlin vorgenommen. Zwischen dieser und der verantwortlichen Stelle wurde ein Rahmenvertrag zur Auftragsdatenverarbeitung abgeschlossen, der die datenschutzrechtliche Sicherheit im Rahmen der Scanvorgänge garantiert.

3. Weiterleitung in Drittstaaten

Eine Weiterleitung der Daten in Drittstaaten findet grundsätzlich nicht statt. Nur wenn der Auftragnehmer eine Weiterleitung seines Scanergebnisses ins Drittland wünscht bzw. selbst veranlasst, findet eine Weiterleitung statt.

4. Art der eingesetzten Datenverarbeitungsanlagen und Software

Für das Scannen wird insbesondere Technik des Unternehmens Kodak Alaris Inc. eingesetzt. Die Verarbeitung der Daten erfolgt in einem serverbasierten Computer-Netzwerk. Dabei wird Software der Unternehmen Kodak Document Imaging/ Opco Inc., LuraTech Solutions GmbH und anderer Anbieter genutzt.

5. Zutrittskontrolle

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

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

- elektrischer Türschließer: Jeder Mitarbeiter erhält Zutritt in die Betriebsräume mit individuell eingerichtetem Transponder (individuelle Festlegung von Zutrittsberechtigungen für jeden Mitarbeiter für die von ihm zu benutzenden Räume)
- schriftliche Betriebsanweisung für Schlüsselregelung für die Produktionsräume
- Anwesenheitsaufzeichnungen über ein elektronisches Zeiterfassungssystem
- Sicherung der Büroeingangsbereiches mit Kameraüberwachung und angeschlossener externer Sicherheitsfirma
- Sicherung der Betriebsräume außerhalb der Arbeitszeit über externe Sicherheitsfirma (Rundgänge, Verschließen der Toranlage zum Innenhof ab 20.00 Uhr)
- schriftliche Festlegung für Empfangsbereich für Umgang mit betriebsfremden Personen
- An- und Ablieferung erfolgt über gesicherten Eingang

6. Zugangskontrolle

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

Es existieren folgende Maßnahmen zur Zugangskontrolle:

- verschlossener Serverraum – Zutrittsberechtigung über Transponder nur für Geschäftsführung und Mitarbeiter der EDV
- Bildschirm-Kennwortschutz an jedem Arbeitsplatz
- Festlegung von individuellen Benutzerberechtigungen für jeden Mitarbeiter bzw. Mitarbeitergruppen
- serverseitige Datenverschlüsselung.

7. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung 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:

Es existieren folgende Maßnahmen zur Zugriffskontrolle:

- Festlegung von Zugriffsberechtigungen für jeden Mitarbeiter
- Daten sind grundsätzlich servergespeichert, nicht lokal am Arbeitsplatz.

8. 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:

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

- Verschlüsselung der Daten
- bei Abholung über Kurierdienst – schriftliche Verpflichtung auf § 5 BDSG
- Gesonderter Verschluss vertraulicher Datenträger (Tresor)
- Vernichtung von Datenträgern in Sicherheitsbehälter Sicherheitsstufe 3, die von zertifizierter Entsorgungsfirma im 2-Wochenrhythmus bzw. nach Anforderung entsorgt werden
- Verschlüsselter Datentransport (HTTPS, SFTP)

9. Eingabekontrolle

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

Es existieren folgende Maßnahmen zur Eingabekontrolle:

- Eingaben sind nur nach explizierter Anmeldung möglich
- Protokollierung der Nutzer-ID pro Datensatz
- Verfahrens- und Arbeitsanweisungen definiert

10. Auftragskontrolle

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

- Die Scanaufträge erfolgen im Rahmen eines eindeutig gestalteten Vertrages, dessen Umfang sowie die sich für die Vertragsparteien ergebenden Rechte und Pflichten in den Allgemeinen Bedingungen geregelt sind.
- Die konkrete Erteilung des Scanauftrags erfolgt in einem formalisierten Verfahren.
- Die verantwortliche Stelle hat keinen Spielraum bei der Verarbeitung der Daten, der Ihr zum Beispiel die Möglichkeit der Auswahl und Klassifizierung der Daten lässt. Vielmehr werden alle Scanvorlagen in einem automatisierten Verfahren eingescannt.

11. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

- Unternehmensnotfall-Vorsorgeplan (Backup-Restore)
- tägliches Backup (Verwahrung an externer Stelle)
- Gespiegelter Datenbestand der Produktionsdaten

12. Gewährleistung der Zweckbindung/Trennungsgebot

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

Es existieren folgende Maßnahmen zur Verwendungszweckkontrolle:

- Kundentrennung – Daten werden in kunden- und auftragsspezifischen Verzeichnissen gespeichert
- Festlegung von Dateinamenskonvention – eindeutige Identifizierung eines jeden Auftrags möglich
- Die mit der Verarbeitung der Scanaufträge befassten Systeme dienen alleine diesen Zwecken.
- Die Verarbeitung erfolgt auf Serversystemen, die durch ein System von logischen und physischen Zugriffskontrollen im Netzwerk logisch getrennt sind.

_____, den _____

Ort Datum

_____, den _____

Ort Datum

_____

Unterschrift Auftraggeber

_____

Unterschrift Auftragnehmer

Anhang – Subunternehmer

Als Subunternehmer werden von Dropscan werden beauftragt:

Amazon Web Services (AWS), Inc., 410 Terry Avenue North, Seattle, Washington 98109-5210, USA, mit Webhostingleistungen auf Grundlage einer von der Artikel-29-Datenschutzgruppe der EU-Datenschutzbehörden bestätigten Auftragsdatenverabeitungsvereinbarung erbracht, wobei die Daten ausschließlich in Deutschland/Frankfurt gespeichert werden. AWS ist entspr. ISO 27001 zertifiziert und wird mind. jährlich durch unabhängige Dritte auditiert.

ODS-Office Data Service GmbH, Ehrenbergstr. 16 A, 10245 Berlin mit Scanleistungen sowie Management des Postein- und Postausgangs auf Grundlage eines ADV-Vertrages.

Mailjet GmbH, c/o RBS RoeverBroennerSusat GmbH & Co. KG, Rankestraße 21, 10789 Berlin mit E-Mail-Versand, auf Grundlage eines Agreement on commissioned data processing in accordance with Art 2e European Data Protection Directive 95/46 and section 11 Federal Data Protection Act (FDPA).

Help Scout, Anbieter Help Scout Inc., 131 Tremont St, Boston, MA 02111-1338, USA, mit CRM-Leistungen, auf Grundlage von Model Contracts for the transfer of personal data to third countries on the basis of Article 26 (4) of directive 95/46/EC.