Vertrag über die Verarbeitung von personenbezogenen Daten im Auftrag (Auftragsverarbeitungsvertrag)

Zwischen

Dropscan GmbH
Ehrenbergstr. 16a
10245 Berlin, Deutschland

- nachfolgend bezeichnet als "Auftragsverarbeiter" -

und

- nachfolgend bezeichnet als "Auftraggeber" -
- beide nachfolgend als "die Vertragsparteien" bezeichnet -
Alle Begrifflichkeiten verstehen sich geschlechtsneutral.

wird der folgende Auftragsverarbeitungsvertrag geschlossen:

Präambel und Anwendungsbereich

Dieser Auftragsverarbeitungsvertrag findet nur insoweit Anwendung, wie der Auftraggeber für den Auftragsverarbeiter Scan- und Bürodienstleistungen erbringt. Der Auftragsverarbeitungsvertrag findet keine Anwendung, wenn die Verarbeitung von personenbezogenen Daten durch den Auftraggeber nicht der DSGVO unterfällt (zum Beispiel bei ausschließlich persönlicher oder familiärer Briefpost von Privatpersonen entsprechend Art. 2 Abs. 2 lit. c DSGVO) und der Auftraggeber daher nicht als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO handelt.
Der Auftragsverarbeitungsvertrag findet ebenfalls keine Anwendung auf die Beförderung von Briefen bis 1.000g auf dem Gebiet der Bundesrepublik Deutschland durch den Auftraggeber, die auf Grundlage einer Postlizenz gem. § 5 Postgesetz erfolgt.
Ausführliche Hinweise zum Gegenstand des Auftragsverarbeitungsvertrages können dem folgenden Auftragsverarbeitungsvertrag entnommen werden.
Der Auftragsverarbeitungsvertrag selbst konkretisiert die Auftragsverarbeitung im Hinblick auf ihren Gegenstand und den sich aus dem Auftragsverarbeitungsverhältnis ergebenden Ansprüche und Pflichten zwischen den Vertragsparteien.

1. Begrifflichkeiten und Definitionen

a. "Auftragsverarbeitung" - Als "Auftragsverarbeitung" ist, im Einklang mit 4 Nr. 8 DSGVO, die im Auftrag des Verantwortlichen, unabhängig von der Zahl dazwischen geschalteter Auftragsverarbeiter, durch den Auftragsverarbeiter entsprechend dem Gegenstand dieses Auftragsverarbeitungsvertrages eine Verarbeitung personenbezogener Daten gem. Art. 4 Nr. 2 DSGVO zu verstehen.
b. "Hauptvertrag" - Der Begriff des Hauptvertrages umfasst alle Arten laufender Geschäftsbeziehungen zwischen dem Auftraggeber und dem

Auftragsverarbeiter, in deren Rahmen der Auftragsverarbeiter personenbezogene Daten im Auftrag und auf Weisung des Auftraggebers entsprechend den Angaben zum Gegenstand der Auftragsverarbeitung in diesem Auftragsverarbeitungsvertrag verarbeitet. Sofern die Geltung dieses Auftragsverarbeitungsvertrages anderweitig (d.h. innerhalb dieser Vereinbarung oder außerhalb, in anderen Verträgen oder Regelungen) auf bestimmte Arten, Typen oder konkrete Geschäftsbeziehungen, Verträge, etc. beschränkt wurde, sind diese jeweils als Hauptvertrag zu verstehen. Der Begriff des Hauptvertrages umfasst auch laufende Einzelaufträge des Auftraggebers an den Auftragsverarbeiter, die von dem Auftraggeber im Rahmen des Hauptvertrages erteilt werden (z. B. im Fall von Rahmenverträgen).

c. "Verantwortlicher" - "Verantwortlicher" ist, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet (Art. 4 Nr. 7 DSGVO).
d. „Personenbezogene Daten“ - "Personenbezogene Daten" (nachfolgend auch kurz als "Daten" bezeichnet) sind im Einklang mit Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
e. "Betroffene Personen" - Als betroffene Personen (kurz "Betroffene") werden entsprechend Art. 4 Nr. 1 DSGVO Personen bezeichnet, die mittels von personenbezogenen Daten zumindest identifizierbar sind. Die von dieser Auftragsverarbeitung betroffenen Personen, ergeben sich aus dem Gegenstand der Auftragsverarbeitung.

f. "Dritte" - „Dritte“ sind entsprechend Art. 4 Nr. 10 DSGVO natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;
g. "Unterauftragsverarbeitung" - Wenn ein Auftragsverarbeiter nicht direkt vom Verantwortlichen beauftragt wurde, sondern von einem Auftragsverarbeiter des Verantwortlichen, liegt eine "Unterauftragsverarbeitung" vor und die dem ersten Auftragsverarbeiter folgenden Auftragsverarbeiter, werden als "Unterauftragsverarbeiter" bezeichnet.
h. "Elektronisches Format" - Erklärungen gelten als im "elektronische Format" entsprechend Art. 28 Abs. 9 DSGVO abgegeben, wenn die erklärende Person erkennbar ist und das elektronische Erklärungsformat sich zum Nachweis der Erklärung eignet. Als "elektronisches Format" werden insbesondere die Textform, eine die auf dauerhaften Datenträgern gespeicherte Vereinbarung (z. B. E-Mail), digitale Signierverfahren oder Verwendung dedizierter Onlinefunktionen (z. B. in Benutzerkonten) verstanden.

2. Gegenstand der Auftragsverarbeitung

a. Die Auftragsverarbeitung erfolgt im Rahmen der folgenden Rechtsbeziehung (Hauptvertrag): Beauftragung mit Scanservices und/oder Bürodienstleistungen auf Grundlage der Allgemeinen Geschäftsbedingungen: https://www.dropscan.de/agb.
b. Detailangaben zum Gegenstand der im Auftrag erfolgenden Verarbeitung, die verarbeiteten personenbezogenen Daten, von der Verarbeitung betroffene Personen sowie Art, Umfang und Zweck der Verarbeitung, richten sich nach den Vorgaben des Anhangs "Gegenstand der Auftragsverarbeitung".

3. Weisungsbefugnis

a. Der Auftragsverarbeiter darf personenbezogene Daten nur im Rahmen des Hauptvertrages sowie der Weisungen des Auftraggebers verarbeiten und nur insoweit die Verarbeitung im Rahmen des Hauptvertrages erforderlich ist.
b. Die Weisungen werden anfänglich durch den Hauptvertrag oder diesen Auftragsverarbeitungsvertrag festgelegt und können vom Auftraggeber danach durch Weisungen in schriftlicher Form oder in einem elektronischen Format (Textform, z. B. E-Mail) an den Auftragsverarbeiter oder die vom Auftragsverarbeiter bezeichnete Stelle geändert, ergänzt oder ersetzt werden.
c. Mündliche Weisungen können erfolgen, wenn sie aufgrund der Umstände (z. B. Eilbedürftigkeit) geboten sind und sind unverzüglich schriftlich oder in elektronischer Form zu bestätigen.
d. Ist der Auftragsverarbeiter aufgrund objektiver Umstände der Ansicht, dass eine Weisung des Auftraggebers gegen geltendes Datenschutzrecht verstößt, wird der Auftragsverarbeiter den Auftraggeber unverzüglich darauf hinweisen und die Ansicht sachlich begründen. In diesem Fall ist der Auftragsverarbeiter berechtigt, die Ausführung der Weisung bis zur ausdrücklichen Bestätigung der Weisung durch den Auftraggeber auszusetzen und offensichtlich rechtswidrige Weisungen abzulehnen.
e. Der Auftragsverarbeiter kann durch das Recht der Union oder der Mitgliedstaaten und behördliche sowie gerichtliche Maßnahmen, denen der Auftragsverarbeiter unterliegt, zur Durchführung von Verarbeitungen oder Mitteilung von Informationen verpflichtet werden. In einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber die rechtlichen Anforderungen der zwingenden gesetzlichen Verpflichtung vor der Verarbeitung mit, sofern das betreffende Gesetz oder die Anordnung eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet; im Fall eines Verbotes der Mitteilung unternimmt der Auftragsverarbeiter die ihm

möglichen und zumutbaren Maßnahmen, um die gesetzlich zwingende Verarbeitung zu verhindern oder einzuschränken.

f. Der Auftragsverarbeiter hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.
g. Der Auftragsverarbeiter benennt die zum Empfang von Weisungen berechtigte Ansprechpartner und ist verpflichtet Änderungen der Ansprechpartner oder deren Kontaktinformationen sowie Vertreter im Fall einer nicht vorübergehenden Abwesenheit oder Verhinderung unverzüglich mitzuteilen.

4. Wahrung des Berufsgeheimnisses

- Die folgenden Verpflichtungen des Abschnitts "Wahrung des Geheimnisses" dieses Auftragsverarbeitungsvertrages, kommen zur Anwendung, falls die im Auftrag verarbeiteten Daten Berufsgeheimnisse im Sinne des § 203 StGB umfassen. Die Verpflichtungen gelten unabhängig von den zeitlichen Regelungen dieses Auftragsverarbeitungsvertrages auch nach Vertragsende zeitlich unbeschränkt.
- Der Auftragsverarbeiter darf sich nur insoweit Kenntnis von Berufsgeheimnissen verschaffen, als dies für die Durchführung des Hauptvertrages sowie dieses Auftragsverarbeitungsvertrages und Erfüllung der vertraglichen Verpflichtungen erforderlich ist.
- Der Auftraggeber belehrt den Auftragsverarbeiter darüber, dass der Verstoß gegen die Vertraulichkeitsverpflichtungen entsprechend dem Gesetz und diesem Auftragsverarbeitungsvertrag durch Bruch der Verschwiegenheit oder die Verwertung fremder Geheimnisse gem. §§ 203 Abs. 1, Abs. 4 S. 1 StGB, § 204 StGB zur Bestrafung des Auftragsverarbeiters, womit auch für den Auftraggeber handelnde Personen mit umfasst sind, mit einer Freiheitsstrafe bis zu einem Jahr, im Fall von § 204 StGB mit Freiheitsstrafe bis zu zwei Jahren, oder mit Geldstrafe bestraft werden kann. Die

Strafandrohung erhöht sich auf eine Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe, sofern der Täter in Bereicherungsabsicht, auch wenn sie zu Gunsten Dritter bestehen sollte, handelt, oder die Absicht hat, durch die Tat einen anderen zu schädigen.

- Sofern der Auftragsverarbeiter Dritte (z. B. Subunternehmer) beauftragt, die an der Auftragsverarbeitung des Auftragsverarbeiters mitwirken und Kenntnis von den Berufsgeheimnissen erlangen können, verpflichtet er die Dritten entsprechend zumindest in Textform zur Verschwiegenheit. Ferner unterrichtet der Auftragsverarbeiter die Dritten über deren Pflichten. Unabhängig von der vorstehenden Verpflichtung, muss der Auftraggeber den Einsatz von Dritten erlaubt haben. Der Auftraggeber belehrt den Auftragsverarbeiter vorsorglich, dass eine Einschaltung Dritter zu einer Freiheitsstrafe von bis zu einem Jahr oder Geldstrafe führen kann, wenn ein Dritter die Verschwiegenheit bricht, und der Auftragsverarbeiter zugleich nicht dafür Sorge getragen hat, dass der Dritte zur Verschwiegenheit verpflichtet wurde (§§ 203 Abs. 1, Abs. 4 S. 2 Nr. 2 StGB). Die Strafdrohung erhöht sich auf Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe, sofern der Täter in Bereicherungsabsicht, auch wenn sie zu Gunsten Dritter bestehen sollte, handelt, oder die Absicht hat, durch die Tat einen anderen zu schädigen.

5. Technische- und organisatorische Maßnahmen (Sicherheits- und Schutzkonzept)

a. Der Auftragsverarbeiter wird die innerbetriebliche Organisation in seinem Verantwortungsbereich entsprechend den gesetzlichen Anforderungen gestalten und wird insbesondere technische und organisatorische Maßnahmen (nachfolgend bezeichnet als „TOMs“) zur angemessenen Sicherung, insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit von Daten des Auftraggebers, unter Beachtung des Stands der Technik, der

Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen treffen sowie deren Aufrechterhaltung, insbesondere durch regelmäßige, mindestens jährliche Evaluation, sicherstellen. Zu den TOMs gehören im Hinblick auf den Schutz der personenbezogenen Daten insbesondere die Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Integritäts- und Verfügbarkeitskontrolle, Trennungskontrolle sowie die Sicherung der Betroffenenrechte.

b. Die bei Vertragsschluss durch den Auftragsverarbeiter mitgeteilten TOMs definieren das vom Auftragsverarbeiter geschuldete Minimum des Sicherheitsniveaus. Die TOMs dürfen entsprechend dem technischen und rechtlichen Fortschritt weiterentwickelt und durch adäquate Schutzmaßnahmen ersetzt werden, sofern sie das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschreiten und wesentliche Änderungen dem Auftraggeber mitgeteilt werden. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, dass das erforderliche gesetzliche Datenschutzniveau und das definierte Minimum des Sicherheitsniveaus nicht unterschritten werden.

c. Der Auftragsverarbeiter gewährleistet, dass es den mit der Verarbeitung der Daten befassten Mitarbeitern, Beauftragten und anderen für den Auftragsverarbeiter tätigen Personen untersagt ist, die personenbezogenen Daten außerhalb der Weisung zu verarbeiten. Der Auftragsverarbeiter stellt ferner sicher, dass die zur Verarbeitung der Daten des Auftraggebers befugten Personen in die gesetzlichen sowie sich aus diesem Auftragsverarbeitungsvertrag ergebenden Datenschutzbestimmungen eingewiesen und auf Vertraulichkeit und Verschwiegenheit verpflichtet worden sind oder einer entsprechenden und angemessenen gesetzlichen

Verschwiegenheitspflicht unterliegen. Der Auftragsverarbeiter trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

d. Der Auftragsverarbeiter sorgt dafür, dass die bei ihm zur Verarbeitung eingesetzten Personen im Hinblick auf den Schutz personenbezogener Daten und Einhaltung gesetzlicher Datenschutzvorschriften angemessen häufig an wiederkehrenden Schulungs- und Sensibilisierungsmaßnahmen teilnehmen.
e. Die Verarbeitung der personenbezogenen Daten außerhalb der Betriebsstätte des Auftragsverarbeiters (z. B. im Home- oder Mobileoffice oder bei Fernzugriff) ist zulässig, sofern die erforderlichen technischen und organisatorischen Maßnahmen ergriffen und dokumentiert werden, die den Besonderheiten dieser Verarbeitungssituationen in angemessener Weise Rechnung tragen und insbesondere auch eine ausreichende Kontrolle der Datenverarbeitung ermöglichen (z. B. Abschluss einer Vereinbarung über Datenschutz im Home- und Mobile-Office mit Mitarbeitern). Der Auftragsverarbeiter legt dem Auftraggeber eine Dokumentation der implementierten technischen und organisatorischen Maßnahmen für derartige Home-, Mobile oder andere Fernverarbeitungen auf Anfrage vor.
f. Die Verarbeitung der personenbezogenen Daten auf Privatgeräten der Beschäftigten des Auftragsverarbeiters und Beauftragten ist nur mit Zustimmung des Auftraggebers zulässig.
g. Sofern durch gesetzliche Vorgaben vorgegeben, benennt der Auftragsverarbeiter eine*n den gesetzlichen Anforderungen entsprechende*n Datenschutzbeauftragte*n. Der Auftragsverarbeiter teilt dem Auftraggeber die Kontaktinformationen des*der Datenschutzbeauftragten und spätere Änderungen mit.
h. Die im Auftrag durchgeführten Verarbeitungsprozesse werden vom Auftragsverarbeiter in einem angemessenen Umfang, in einem Verzeichnis

von Verarbeitungstätigkeiten gesondert dokumentiert und dem Auftraggeber auf Anforderung bereitgestellt.

i. Die im Rahmen des Auftragsverarbeitungsvertrag überlassene Daten sowie Datenträger und sämtliche hiervon gefertigten Kopien, verbleiben im Eigentum, bzw. in Inhaberschaft des Auftraggebers, unterliegen der Verfügungsherrschaft des Auftraggebers, sind durch den Auftragsverarbeiter sorgfältig zu verwahren, vor Zugang durch unberechtigte Dritte zu schützen und dürfen nur mit Zustimmung des Auftraggebers vernichtet werden. Die Vernichtung hat datenschutzgerecht und so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich und nicht zu erwarten ist. Kopien von Daten dürfen nur erstellt werden, wenn sie zur Erfüllung der Leistungshaupt- und Nebenpflichten des Auftragsverarbeiters gegenüber dem Auftraggeber erforderlich sind (z.B. Backups) und das vertragliche sowie das gesetzliche Datenschutzniveau gewährleistet werden.
j. Der Auftragsverarbeiter ist verpflichtet, eine nach diesem Auftragsverarbeitungsvertrag unverzüglich herbeizuführende Rückgabe bzw. Löschung der Daten und Datenträger auch bei Unterauftragsverarbeitern herbeizuführen.
k. Der Auftragsverarbeiter hat den Nachweis, einer im Rahmen dieses Auftragsverarbeitungsvertrages ordnungsgemäß erfolgten Vernichtung, bzw. Löschung von Daten und Dateien zu führen und auf Verlangen dem Auftraggeber zur Verfügung zu stellen.
l. Die Einrede eines Zurückbehaltungsrechts wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
m. Der Auftragsverarbeiter führt im angemessenen Umfang den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit (z. B. durch regelmäßige Kontrollen, Prüfungen, etc.). Der Nachweis ist dem Auftraggeber auf Anforderung zu

überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

n. Der Auftragsverarbeiter ist verpflichtet weitere für ihn im Hinblick auf die im Auftrag verarbeiteten personenbezogenen Daten gesetzlich für ihn geltenden Schutzvorschriften, insbesondere das Fernmeldegeheimnis, das Sozialgeheimnis und Berufsgeheimnispflichten zu beachten.
o. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftragsverarbeiters oder den gesetzlichen Anforderungen nicht oder nicht mehr genügen, benachrichtigt der Auftragsverarbeiter den Auftraggeber unverzüglich.
p. Die bereits zum Abschluss dieses Auftragsverarbeitungsvertrages bestehenden technischen- und organisatorische Maßnahmen, werden vom Auftragsverarbeiter im Anhang „Technische- und organisatorische Maßnahmen“ aufgeführt und von dem Auftraggeber akzeptiert.

6. Informationspflichten und Mitwirkungspflichten des Auftragsverarbeiters

a. Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Zustimmung durch den Auftraggeber oder im Fall zwingender gesetzlicher Pflichten, gerichtlicher oder gesetzlicher Informationen erteilen. Wendet sich eine betroffene Person an den Auftragsverarbeiter und macht ihre Betroffenenrechte geltend (insbesondere Rechte auf Auskunft oder Berichtigung, bzw. Löschung personenbezogener Daten), wird der Auftragsverarbeiter die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragsverarbeiter leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter und unterstützt den Auftraggeber im Rahmen der Zumutbarkeit und Möglichkeit. Der Auftragsverarbeiter haftet nicht, wenn

das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird, soweit dies nicht von dem Auftragsverarbeiter zu vertreten ist.

b. Der Auftragsverarbeiter hat den Auftraggeber unverzüglich und vollständig zu informieren, wenn der Auftragsverarbeiter im Hinblick auf die Verarbeitung der personenbezogenen Daten Fehler oder Unregelmäßigkeiten bei der Einhaltung von Bestimmungen dieses Auftragsverarbeitungsvertrages und/ oder einschlägiger Datenschutzvorschriften feststellt. Der Auftragsverarbeiter trifft die erforderlichen Maßnahmen zur Sicherung der personenbezogenen Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
c. Der Auftragsverarbeiter wird den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde gegenüber dem Auftragsverarbeiter tätig wird und deren Tätigkeit die für den Auftraggeber verarbeiteten Daten betreffen kann. Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Wahrnehmung seiner Pflichten (insbesondere zur Auskunfts- und Duldung von Kontrollen) gegenüber Aufsichtsbehörden.
d. Sollte die Sicherheit der personenbezogenen Daten des Auftraggebers durch Maßnahmen Dritter (z.B. Gläubiger, Behörden, Gerichte, etc.) gefährdet sein (Pfändung, Beschlagnahme, Insolvenzverfahren, etc.) wird der Auftragsverarbeiter die Dritten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei dem Auftraggeber liegen und nach Rücksprache mit dem Auftraggeber, sofern erforderlich, entsprechende Schutzmaßnahmen ergreifen (z.B. Widersprüche, Anträge, etc. stellen).
e. Der Auftragsverarbeiter stellt dem Auftraggeber Informationen betreffend die Verarbeitung von Daten im Rahmen dieses Auftragsverarbeitungsvertrages, die für die Erfüllung von gesetzlichen Pflichten des Auftraggebers (zu denen insbesondere Anfragen Betroffener

oder Behörden und die Einhaltung seiner Rechenschaftspflichten einer Datenschutz-Folgenabschätzung gehören können) notwendig sind, zur Verfügung und unterstützt diesen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

f. Die Informationspflichten des Auftragsverarbeiters erstrecken sich zunächst auf Informationen, die dem Auftragsverarbeiter, seinen Beschäftigten und Beauftragten vorliegen. Die Informationen müssen nicht von dritten Quellen beschafft werden, wenn die Beschaffung durch den Auftraggeber im zumutbaren Rahmen erfolgen könnte und keine anderweitige Vereinbarung getroffen wurde.

7. Maßnahmen bei Gefährdung oder Verletzung des Datenschutzes

a. Für den Fall, dass der Auftragsverarbeiter Tatsachen feststellt, welche die Annahme begründen, dass der Schutz der für den Auftraggeber verarbeiteten personenbezogenen Daten im Sinne des Art. 4 Nr. 12 DSGVO verletzt sein könnte, hat der Auftragsverarbeiter den Auftraggeber unverzüglich und vollständig zu informieren, unverzüglich erforderliche Schutzmaßnahmen zu ergreifen, und bei der Erfüllung der dem Auftraggeber obliegenden Pflichten, insbesondere im Zusammenhang mit der Meldung an zuständige Behörden oder betroffene Personen zu unterstützen.
b. Die Meldung des Auftragsverarbeiters muss entsprechend Art. 33 Abs. 3 DSGVO, mindestens die folgenden Angaben beinhalten:
    a. Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der betroffenen Kategorien von Daten und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

   b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlauf- oder Kontaktstelle für weitere Informationen;
   c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (z. B. unter Angabe weiterer Details: Identitätsdiebstahl, Vermögensnachteile, etc.);
   d. eine Beschreibung der vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

c. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen oder von ihm Beauftragten gegen datenschutzrechtliche Bestimmungen oder die in diesem Auftragsverarbeitungsvertrag getroffenen Festlegungen.

8. Überprüfungen und Inspektionen

a. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorgaben und der Regelungen dieses Auftragsverarbeitungsvertrag, insbesondere der TOMs beim Auftragsverarbeiter jederzeit im erforderlichen Umfang selbst oder durch Dritte zu kontrollieren und die erforderlichen Überprüfungen, einschließlich Inspektionen, durchzuführen.
b. Der Auftragsverarbeiter hat den Auftraggeber bei den Kontrollen und Inspektionen im erforderlichen Rahmen zu unterstützen (z. B. durch Bereitstellung von Personal und Gewährung von Zugangs- und Zugriffsrechten).
c. Vor-Ort-Kontrollen erfolgen innerhalb üblicher Geschäftszeiten, sind vom Auftraggeber mit einer angemessenen Frist (mindestens 14 Tage)

anzumelden. In Notfällen, d.h., wenn ein Zuwarten die Rechte der Betroffenen und/oder des Auftraggebers für diese in einem nicht zumutbaren Maße gefährden würde, kann eine angemessen kürzere Frist gewählt werden. Umgekehrt kann eine längere Frist erforderlich sein (wenn z. B. umfangreiche Vorbereitungen erfolgen müssen oder während der Urlaubszeit). Die Abweichungen von der Frist sind jeweils von der sie in Anspruch nehmenden Vertragspartei zu begründen.

d. Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters sowie den Schutz von personenbezogenen Daten Dritter (z.B. anderer Kunden oder Mitarbeiter des Auftragsverarbeiters) Rücksicht nehmen. Vermeidbare Betriebsstörungen sind zu vermeiden. Soweit dem Anlass und Zweck der Prüfung genügend, soll sich eine Kontrolle auf Stichproben beschränken.
e. Zur Durchführung der Kontrolle sind nur fachkundige Personen zugelassen, die sich legitimieren können und im Hinblick auf die Betriebs- und Geschäftsgeheimnisse sowie interne Prozesse des Auftragsverarbeiters und personenbezogene Daten zur Vertraulichkeit- und Verschwiegenheit verpflichtet sind. Der Auftragsverarbeiter kann den Nachweis einer entsprechenden Verpflichtung verlangen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragsverarbeiter stehen oder sonst ein begründeter Anlass zur seiner Ablehnung vorliegen, hat der Auftragsverarbeiter gegen diesen ein Einspruchsrecht.
f. Statt der Einsichtnahmen und der Vor-Ort-Kontrollen, darf der Auftragsverarbeiter den Auftraggeber auf eine gleichwertige Kontrolle durch unabhängige Dritte (z.B. neutrale Datenschutzauditoren), Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder geeignete Datenschutz- oder IT-Sicherheitszertifizierungen gem. Art. 42 DSGVO verweisen. Dies gilt nur, wenn der Verweis dem Auftraggeber zuzumuten ist und die Art sowie Umfang der Prüfung und Verweise der Art und dem Umfang des

berechtigten Kontrollvorhabens des Auftraggebers entsprechen. Der Auftragsverarbeiter verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

g. Der Auftraggeber übt sein Kontrollrecht grundsätzlich nicht häufiger als alle 12 Monate aus, es sei denn ein konkreter Anlass (insbesondere eine Verletzung des Datenschutzes, ein Sicherheitsvorfall oder das Ergebnis einer Auditierung) macht Kontrollen vor Ablauf dieses Zeitraums erforderlich.

9. Unterauftragsverhältnisse

a. Der Auftraggeber erklärt sich unbeschadet etwaiger Einschränkungen durch den Hauptvertrag ausdrücklich damit einverstanden, dass der Auftragsverarbeiter im Rahmen der Auftragsverarbeitung Unterauftragsverarbeiter einsetzen darf. Der Auftragsverarbeiter informiert den Auftraggeber mit einer angemessenen Vorfrist, die regelmäßig 14 Werktage beträgt, über neue Unterauftragsverarbeiter und gibt dem Auftraggeber die Möglichkeit die Unterauftragsverarbeiter vor deren Einsatz im angemessenen Rahmen überprüfen und beim berechtigten Interesse Einspruch gegen den Einsatz der Unterauftragsverarbeiter erheben zu können. Erhebt der Auftraggeber keinen Einspruch innerhalb der Vorfrist, darf der Unterauftragsverarbeiter eingesetzt werden. Der Auftraggeber macht von seinem Recht auf Einspruch im Hinblick auf die Änderungen nur unter Beachtung der Grundsätze von Treu und Glauben sowie der Angemessenheit und Billigkeit Gebrauch.
b. Nimmt der Auftragsverarbeiter die Dienste eines Unterauftragsverarbeiters (z. B. eines Subunternehmers) in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, dann

muss er dem Unterauftragsverarbeiter im Wege eines Vertrags oder eines gesetzlich zulässigen anderen Rechtsinstruments dieselben Datenschutzpflichten zu denen sich der Auftragsverarbeiter in diesem Auftragsverarbeitungsvertrag verpflichtet hat, auferlegen (insbesondere im Hinblick auf die Befolgung von Weisungen, Einhaltung der TOMs, Erteilung von Informationen und Duldung von Kontrollen).

c. Der Auftragsverarbeiter wählt den Unterauftragsverarbeiter unter besonderer Berücksichtigung der Eignung und der Zuverlässigkeit zur Einhaltung der Pflichten aus diesem Auftragsverarbeitungsvertrag sowie der Eignung der vom Unterauftragsverarbeiter getroffenen TOMs, sorgfältig aus.
d. Die Weiterleitung von im Auftrag verarbeiteten personenbezogenen Daten an Unterauftragsverarbeiter ist erst zulässig, wenn der Auftragsverarbeiter sich davon überzeugt hat, dass der Unterauftragsverarbeiter seine Verpflichtungen vollständig erfüllt hat. Die Prüfung ist zu dokumentieren und die Dokumentation dem Auftraggeber auf Aufforderung vorzulegen.
e. Der Auftragsverarbeiter hat die Einhaltung der Pflichten der Unterauftragsverarbeiter, insbesondere der TOMs regelmäßig, spätestens alle 12 Monate, in einem angemessenen Umfang zu überprüfen. Die Prüfung und ihr Ergebnis sind so nachvollziehbar zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen. Statt eigener Überprüfung darf der Auftragsverarbeiter auf eine Überprüfung durch unabhängige Dritte (z.B. neutrale Datenschutzauditoren), Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder geeignete Datenschutz- oder IT-Sicherheitszertifizierungen gem. Art. 42 DSGVO verweisen. Der Auftragsverarbeiter verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise beim Subunternehmer unverzüglich zu unterrichten.

f. Die Verantwortlichkeiten zur Wahrnehmung der Pflichten aus diesem Auftragsverarbeitungsvertrag und aus dem Gesetz sind zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter eindeutig zu regeln und voneinander abzugrenzen.
g. Die Rechte des Auftraggebers müssen auch gegenüber den Unterauftragsverarbeitern wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem, im Rahmen dieses Auftragsverarbeitungsvertrages festgelegten Umfang Kontrollen auch bei Unterauftragsverarbeitern durchzuführen oder durch Dritte durchführen zu lassen.
h. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragsverarbeiter gegenüber dem Auftraggeber.
i. Verarbeitungen von personenbezogenen Daten, die keinen direkten Zusammenhang mit der Erbringung der Hauptleistung aus dem Hauptvertrag aufweisen und bei denen der Auftragsverarbeiter die Leistungen Dritter als reine Nebenleistung in Anspruch nimmt um seine geschäftliche Tätigkeit auszuüben (z.B. Reinigungs-, Bewachungs-, Wartungs-, Telekommunikations- oder Transportleistungen) stellen keine Unterauftragsverarbeitung im Sinne der vorstehenden Regelungen dieses Auftragsverarbeitungsvertrages dar. Gleichwohl hat der Auftragsverarbeiter sicher zu stellen, z.B. durch vertragliche Vereinbarungen oder Hinweise und Instruktionen, dass hierbei die Sicherheit der Daten nicht gefährdet wird und die Vorgaben dieses Auftragsverarbeitungsvertrages und der Datenschutzvorschriften eingehalten werden.
j. Unterauftragsverhältnisse, die dem Auftraggeber bei Abschluss dieses Auftragsverarbeitungsvertrages mitgeteilt wurden, gelten in dem mitgeteilten Umfang unter Geltung der Regelungen dieses Auftragsverarbeitungsvertrages zu Unterauftragsverhältnissen als genehmigt.

k. Die aktuelle Liste der Unterauftragsverhältnisse ist unter der folgenden Webadresse abrufbar:
https://www.dropscan.de/datenschutz/subunternehmer

10. Räumlicher Bereich der Auftragsverarbeitung

a. Personenbezogene Daten werden im Rahmen der Auftragsverarbeitung in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) verarbeitet.
b. Die Verarbeitung darf in Drittstaaten erfolgen, sofern die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, d. h. insbesondere die EU-Kommission ein angemessenes Datenschutzniveau festgestellt hat; b) auf Grundlage von wirksamen Standardschutzklauseln (sog. Standard Contractual Clauses, SCC); oder c) auf Grundlage von anerkannten verbindlichen internen Datenschutzvorschriften.
c. Die Auftragsverarbeitung in einem anderen, als den vorstehend genannten Ländern, auch durch Unterauftragsverarbeiter, bedarf der vorherigen Genehmigung des Auftraggebers.

11. Pflichten des Auftraggebers

a. Der Auftraggeber hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen, Weisungen oder Verarbeitungsprozessen Fehler oder Unregelmäßigkeiten im Hinblick auf datenschutzrechtliche Bestimmungen feststellt.
b. Die Auftraggeber benennt die zum Empfang von Weisungen berechtigte Ansprechpartner und ist verpflichtet Änderungen der Ansprechpartner oder deren Kontaktinformationen sowie Vertreter im Fall einer nicht vorübergehenden Abwesenheit oder Verhinderung unverzüglich mitzuteilen.

c. Im Falle einer Inanspruchnahme des Auftragsverarbeiters durch betroffene Personen, dritte Unternehmen, Stellen oder Behörden hinsichtlich etwaiger Ansprüche aufgrund der Verarbeitung von personenbezogenen Daten im Rahmen dieses Auftragsverarbeitungsvertrages, verpflichtet sich der Auftraggeber den Auftragsverarbeiter bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten und unter Berücksichtigung des Verschuldensgrades der Vertragsparteien zu unterstützen.

12. Haftung

Es gelten die gesetzlichen Haftungsregelungen, insbesondere Art. 82 DSGVO sowie im Falle des Einsatzes eines Unterauftragsverarbeiters Art. 28 Abs. 4. S. 2 DSGVO.

13. Laufzeit, Fortgeltung nach Vertragsende und Datenlöschung

a. Dieser Auftragsverarbeitungsvertrag wird mit dessen Unterzeichnung, bzw. Abschluss in einem elektronischen Format wirksam.
b. Laufzeit und Ende dieses Auftragsverarbeitungsvertrages richten sich nach der Laufzeit und dem Ende des Hauptvertrages.
c. Das Recht auf außerordentliche Kündigung bleibt den Vertragsparteien vorbehalten, insbesondere im Fall eines schwerwiegenden Verstoßes gegen die Pflichten und Vorgaben dieses Auftragsverarbeitungsvertrages und des geltenden Datenschutzrechts. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragsverarbeiter die in dem Auftragsverarbeitungsvertrag bestimmten Pflichten und die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
d. Der außerordentlichen Kündigung hat bei unerheblichen Pflichtverstößen eine Abmahnung der Verstöße mit angemessener Frist zur Abhilfe vorauszugehen, wobei die Abmahnung nicht erforderlich ist, wenn nicht

damit zu rechnen ist, dass die beanstandeten Verstöße behoben werden oder diese derart schwer wiegen, dass ein Festhalten am Auftragsverarbeitungsvertrag der kündigenden Vertragspartei nicht zuzumuten ist.

e. Die Kündigung dieses Auftragsverarbeitungsvertrages, als auch die Aufhebung dieser Formklausel müssen zumindest im elektronischen Format erfolgen.

f. Nach Abschluss der Erbringung der Verarbeitungsleistungen im Rahmen dieses Auftragsverarbeitungsvertrages, wird der Auftragsverarbeiter alle personenbezogenen Daten und deren Kopien (sowie sämtliche im Zusammenhang mit dem Auftragsverhältnis in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände), nach Wahl des Auftraggebers entweder vernichten oder zurückgeben, sofern nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht; in diesem Fall informiert der Auftragsverarbeiter den Auftraggeber über die Verpflichtung und deren Umfang, es sei denn dass die Kenntnis der Verpflichtung seitens des Auftraggebers erwartet werden kann. Die Vernichtung, bzw. Löschung hat datenschutzgerecht und so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich und nicht zu erwarten ist. Die Einrede eines Zurückbehaltungsrechts wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Im Hinblick auf die Löschung oder Rückgabe, gelten die Auskunfts-, Nachweis und Kontrollrechte des Auftraggebers entsprechend diesem Auftragsverarbeitungsvertrag.

g. Die sich aus dem Auftragsverarbeitungsvertrag ergebenden Pflichten zum Schutz vertraulicher Informationen gelten auch nach Ende des Auftragsverarbeitungsvertrages fort, sofern der Auftragsverarbeiter weiterhin die vom Auftragsverarbeitungsvertrag umfassten

personenbezogenen Daten verarbeitet und die Einhaltung der Pflichten für den Auftragsverarbeiter auch nach Vertragsende zumutbar ist.

h. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung und Sicherstellung der TOMs dienen, sind durch den Auftragsverarbeiter den jeweiligen, ihm bekannten Aufbewahrungs- und Löschungsfristen (oder solchen, die ihm bekannt sein müssten) des Auftraggebers entsprechend, zumindest drei Jahre auch über das Vertragsende hinaus aufzubewahren. Der Auftragsverarbeiter kann die Dokumentationen zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

14. Schlussbestimmungen

a. Das anwendbare Recht bestimmt sich nach dem Hauptvertrag.
b. Der Gerichtsstandort bestimmt sich nach dem Hauptvertrag.
c. Der vorliegende Auftragsverarbeitungsvertrag stellt die vollständige, zwischen den Vertragsparteien getroffene Vereinbarung dar. Nebenabreden bestehen nicht.
d. Mit Zustandekommen dieses Auftragsverarbeitungsvertrages werden alle etwaigen früheren Verträge aufgehoben, die zwischen den Vertragsparteien dieses Vertrages abgeschlossen wurden und die die Verarbeitung personenbezogener Daten im Auftrag regeln, wenn und soweit diese den gleichen Gegenstand der Auftragsverarbeitung betreffen und wenn und soweit zwischen den Vertragsparteien nicht ausdrücklich schriftlich etwas anderes vereinbart wurde.
e. Änderungen sowie Ergänzungen dieses Auftragsverarbeitungsvertrages, als auch die Aufhebung dieser Formklausel müssen zumindest im elektronischen Format erfolgen.

f. Bei etwaigen Widersprüchen gehen Regelungen dieses Auftragsverarbeitungsvertrages zum Datenschutz den Regelungen des Hauptvertrages vor.

g. Sollten eine oder mehrere Bestimmungen dieses Auftragsverarbeitungsvertrages unwirksam oder undurchführbar sein, so wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Die unwirksamen Bestimmungen werden vielmehr im Wege der ergänzenden Auslegung eine solche Regelung ersetzt, die von den Vertragsparteien mit der/den unwirksamen Bestimmung/en erkennbar verfolgten wirtschaftlichen Zweck möglichst nahekommt. Sofern die vorbenannte ergänzende Auslegung aufgrund gesetzlich zwingender Vorgaben nicht möglich ist, werden die Vertragsparteien eine ihr entsprechende Regelung vereinbaren.

Der Auftragsverarbeitungsvertrag wird im elektronischen Format abgeschlossen und ist ohne Unterschriften der Vertragsparteien wirksam.

15. Anhang: Gegenstand der Auftragsverarbeitung

Zwecke der Auftragsverarbeitung

Personenbezogene Daten des Auftraggebers werden auf Grundlage dieses Auftragsverarbeitungsvertrages zu den folgenden Zwecken verarbeitet:

- Empfang von postalischen Sendungen, Scannen, Speicherung und digitale Bereitstellung sowie Vernichtung von Postsendungen, Aktenordnern und anderen Unterlagen sowie Bereitstellung einer postalischen Empfangsadresse.

Arten und Kategorien von Daten

Zu den auf Grundlage dieses Auftragsverarbeitungsvertrages verarbeiteten Arten und Kategorien von personenbezogenen Daten gehören:

- Sofern der Auftragsverarbeiter Bestands-, Vertragsdaten sowie Zahlungs- und Nutzungsdaten des Auftraggebers zu Zwecken der Begründung, Durchführung oder Beendigung der Kundenbeziehung verarbeitet, erfolgt dies in eigener Verantwortlichkeit gem. Art. 4 Nr. 7 DSGVO zu Zwecken der Vertragsdurchführung, zur Erfüllung gesetzlicher Pflichten und berechtigter Interessen gem. Art. 6 Abs. 1 S. 1 lit. b., c. und f. DSGVO.
- Der Auftragsverarbeiter verarbeitet keine besonderer Kategorien von personenbezogener Daten. Soweit Angaben sensibler Natur in den eingescannten Inhalten enthalten sind, werden sie unterschiedslos alleine mit dem Zweck der Bereitstellung an den Auftraggeber verarbeitet.
- Im Rahmen der Auftragserfüllung werden Postsendungen und andere Unterlagen eingescannt sowie die hierbei gewonnenen Daten betreffend die Absender und Adressaten sowie den Inhalt, dem Auftraggeber bereitgestellt.

Kategorien der betroffenen Personen

Zu den durch die Verarbeitung von personenbezogenen Daten auf Grundlage dieses Auftragsverarbeitungsvertrages betroffenen Personengruppen gehören:

- Sich aus den gescannten Postsendungen, Unterlagen oder empfangenen Informationen ergebende Angaben zu Personen oder sie betreffende Informationen, werden unterschiedslos wie andere Inhalte verarbeitet.
- Angaben zu Absendern oder Empfängern von postalischen Sendungen oder sonst anderweitig vom Auftraggeber bestimmte Datenkategorien werden gesondert verarbeitet und dem Auftraggeber bereitgestellt.

Quellen der verarbeiteten Daten

Die auf Grundlage dieses Auftragsverarbeitungsvertrages verarbeiteten Daten werden aus den im Folgenden genannten Quellen, bzw. im Rahmen genannter Verfahren erhoben oder sonst empfangen:

- Die von dem Auftragsverarbeiter verarbeiteten Daten werden im Rahmen der Entgegennahme und der Scanleistungen aus Postsendungen und anderen Unterlagen gewonnen oder dem Auftragsverarbeiter direkt durch den Auftraggeber, z.B. in Eingabeformularen, bereitgestellt.

Anhang: Zuständige Personen und Ansprechpartner

Dr. Thomas Schwenke: Externer Datenschutzbeauftragter, datenschutz@dropscan.de.
Martin Güther: Vertretungsberechtigter Geschäftsführer, Tel: (030) 346 493 15, E-Mail: service@dropscan.de.

Die im folgenden benannten Ansprechpersonen sind für die Erteilung, bzw. den Empfang von Weisungen des Auftraggebers berechtigt. Änderungen der Ansprechpersonen, deren nicht nur vorübergehende Verhinderung oder ihrer Kontaktinformationen müssen der anderen Vertragspartei angezeigt werden.

Anhang: Technisch-organisatorische Maßnahmen (TOMs)

Es wird für die konkrete Auftragsverarbeitung und die in ihrem Rahmen verarbeiteten personenbezogenen Daten ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau Gewähr geleistet. Dazu werden insbesondere die Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Organisatorische Maßnahmen

Es sind organisatorische Maßnahmen ergriffen worden, die ein angemessenes Datenschutzniveau und dessen Aufrechterhaltung gewährleisten.

a. Der Auftragsverarbeiter hat ein angemessenes Datenschutzmanagementsystem, bzw. ein Datenschutzkonzept implementiert und gewährleistet dessen Umsetzung.
b. Eine geeignete Organisationsstruktur für die Datensicherheit und Datenschutz ist vorhanden und die Informationssicherheit ist integriert in unternehmensweite Prozesse und Verfahren integriert.
c. Es sind interne Sicherheitsricht- bzw. -leitlinien definiert, die unternehmensintern gegenüber Mittarbeitern als verbindliche Regeln kommuniziert werden.
d. Es werden regelmäßig und auch anlasslos System- und Sicherheitstests, wie z. B. Code-Scan und Penetrationstests, durchgeführt.
e. Der Auftragsverarbeiter führt bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durch. Das Verfahren ist entsprechend dem

PDCA-Zyklus aufgebaut und besteht aus einer kontinuierlichen Beobachtung der technischen und organisatorischen Maßnahme sowie Festlegung des Istzustandes, als auch des zu erreichenden Soll-Zustandes mit folgender Umsetzungs- und sich daran anschließenden Überprüfungsphase sowie Evaluierung der Umsetzung und Ableitung der gewonnenen Erfahrungen für künftige Optimierungen und Vorgehen im Hinblick auf die Sicherheitsstandards.

f. Die Entwicklung des Standes der Technik und sowie der Entwicklungen, Bedrohungen und Sicherheitsmaßnahmen werden fortlaufend beobachtet und in geeigneter Art und Weise auf das eigene Sicherheitskonzept abgeleitet.
g. Es besteht ein Konzept, das die Wahrung der Betroffenenrechte durch den Auftraggeber gewährleistet (insbesondere im Hinblick auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche). Zu dem Konzept gehört die Unterrichtung der Mitarbeiter über die Informationspflichten gegenüber dem Auftraggeber, Einrichtung von Umsetzungsverfahren und die Benennung zuständiger Personen sowie regelmäßige Kontrolle und Evaluierung der ergriffenen Maßnahmen.
h. Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Gefährdungen und Verletzungen des Schutzes personenbezogener Daten gewährleistet. Zu dem Konzept gehört die Unterrichtung der Mitarbeiter über die Informationspflichten gegenüber dem Auftraggeber, Einrichtung von Umsetzungsverfahren und die Benennung zuständiger Personen sowie regelmäßige Kontrolle und Evaluierung der ergriffenen Maßnahmen.
i. Sicherheitsvorkommnisse werden konsequent dokumentiert, auch wenn sie nicht zu einer externen Meldung (z. B. an die Aufsichtsbehörde, betroffene Personen) führen (sogenanntes "Security Reporting").

j. Ausreichende fachliche Qualifikation des Datenschutzbeauftragten für sicherheits-relevante Fragestellungen und Möglichkeiten zur Fortbildung in diesem Fachbereich.
k. Ausreichende fachliche Qualifikation des IT-Sicherheitsbeauftragten für sicherheits-relevante Fragestellungen und Möglichkeiten zur Fortbildung in diesem Fachbereich.
l. Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden (Wartungs-, Wach-, Transport- und Reinigungsdienste, freie Mitarbeiter, etc.), werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten. Sofern die Dienstleister im Rahmen ihrer Tätigkeit Zugang zu personenbezogenen Daten des Auftraggebers erhalten oder sonst das Risiko eines Zugriffs auf die personenbezogenen Daten besteht, werden sie speziell auf Verschwiegenheit und Vertraulichkeit verpflichtet.
m. Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt.
n. Eingesetzte Software und Hardware wird stets auf dem aktuell verfügbaren Stand gehalten und Softwareaktualisierungen werden ohne Verzug innerhalb einer angesichts des Risikograd es und eines eventuellen Prüfnotwendigkeit angemessenen Frist ausgeführt. Es wird keine Software und Hardware eingesetzt, die von den Anbietern im Hinblick auf Belange des Datenschutzes- und Datensicherheit nicht mehr aktualisiert wird (z. B. abgelaufene Betriebssysteme).

o. Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen.
p. Es wird ein „papierloses Büro“ geführt, d. h. Unterlagen werden grundsätzlich nur digital gespeichert und nur in Ausnahmefällen in Papierform aufbewahrt.
q. Unterlagen im Papierformat werden nur dann aufbewahrt, wenn keine im Hinblick auf die Auftragsverarbeitung, ihrem Zweck und den Interessen der von den Inhalten der Unterlagen betroffenen Personen adäquate digitale Kopie vorliegt oder eine Aufbewahrung mit dem Auftraggeber vereinbart wurde oder gesetzlich erforderlich ist.
r. Es liegt ein den Datenschutzanforderungen der Auftragsverarbeitung und dem Stand der Technik entsprechendes Lösch- und Entsorgungskonzept vor. Die physische Vernichtung von Dokumenten und Datenträgern erfolgt datenschutzgerecht und entsprechend den gesetzlichen Vorgaben, Branchenstandards und dem Stand der Technik entsprechenden Industrienormen (z. B. nach DIN 66399). Mitarbeiter wurden über gesetzliche Voraussetzungen, Löschfristen und soweit zuständig, über Vorgaben für die Datenvernichtung oder Gerätevernichtung durch Dienstleister unterrichtet.
s. Die Verarbeitung der Daten des Auftraggebers, die nicht entsprechend den Vereinbarungen dieses Auftragsverarbeitungsvertrages gelöscht wurden (z.B. in Folge der gesetzlichen Archivierungspflichten), wird im erforderlichen Umfang durch Sperrvermerke und/oder Aussonderung eingeschränkt.

Datenschutz auf Mitarbeiterebene

Es sind Maßnahmen ergriffen worden, die gewährleisten, dass die mit der Verarbeitung personenbezogener Daten beschäftigten Mitarbeiter, über die datenschutzrechtlich nötige Sachkenntnis und Zuverlässigkeit verfügen.

a. Mitarbeiter werden auf Vertraulichkeit und Verschwiegenheit (Datenschutzgeheimnis) verpflichtet.

b. Mitarbeiter werden im Hinblick auf den Datenschutz entsprechend den Anforderungen ihrer Funktion sensibilisiert und unterrichtet. Die Schulung und Sensibilisierung wird in angemessenen Zeitabständen oder wenn es die Umstände erfordern wiederholt.
c. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden (Home- und Mobileoffice), werden Mitarbeiter über die speziellen Sicherheitsanforderungen sowie Schutzpflichten in diesen Konstellationen unterrichtet, sowie auf deren Einhaltung unter Vorbehalt von Kontroll- und Zugriffsrechten verpflichtet.
d. Die an Mitarbeiter ausgegebene Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus den Diensten des Auftragsverarbeiters, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.
e. Mitarbeiter werden verpflichtet, ihre Arbeitsumgebung aufgeräumt zu hinterlassen und so insbesondere den Zugang zu Unterlagen oder Datenträgern mit personenbezogenen Daten zu verhindern (Clean Desk Policy).

Zutrittskontrolle

- Der Zutritt bei aktiver Alarmanlage ist durch ein Schließsystem mit Codesperre (Zugangscode) gesichert.
- Unterlagen (Akten, Dokumente, etc.) werden sicher, z. B. in Aktenschränken oder sonstigen angemessen gesicherten Regalen aufbewahrt und angemessen vor Zugriff durch unbefugte Personen gesichert.
- Fenster, Schächte und ähnliche Zugangsmöglichkeiten, die eine potentielle Zutrittsmöglichkeit bieten könnten (z. B. Fenster im Erdgeschoss) sind mit einer Alarmanlage gegen den unberechtigten Zutritt gesichert.

Es sind Maßnahmen zur physischen Zutrittskontrolle ergriffen worden, die es Unbefugten verwehren, sich den Systemen, Datenverarbeitungsanlagen oder Verfahren physisch zu nähern, mit denen personenbezogene Daten verarbeitet werden.

a. Der Zutritt zu Datenverarbeitungsanlagen ist zusätzlich gesichert und nur befugten Mitarbeitern möglich.
b. Es findet eine Personenkontrolle beim Pförtner oder am Empfang statt.
c. Die Besucher werden protokolliert.
d. Die Besucher dürfen sich nicht frei, sondern nur in Begleitung von Mitarbeitern bewegen.
e. Um den Zutritt durch Unbefugte zu verhindern, wird Videoüberwachungstechnologie eingesetzt.
f. Um den Zutritt durch Unbefugte zu verhindern, wird eine Alarmanlage eingesetzt.
g. Eine geeignete Umzäunung des Betriebsgeländes.
h. Nach den Betriebsstunden finden regelmäßige Kontrollgänge durch das Sicherheitspersonal statt.
i. Der Zutritt ist durch ein elektronisches Schließsystem mit Sicherheitsschlössern gesichert.
j. Die Ausgabe und Rückgabe von Schlüsseln und/ oder Zugangskarten wird protokolliert.
k. Mitarbeiter werden verpflichtet, Geräte zu sperren oder sie besonders zu sichern, wenn sie ihre Arbeitsumgebung oder die Geräte verlassen.
l. Unterlagen (Akten, Dokumente, etc.) werden sicher, z. B. in Aktenschränken oder sonstigen angemessen gesicherten Containern aufbewahrt und angemessen vor Zugriff durch unbefugte Personen gesichert.
m. Datenträger werden sicher aufbewahrt und angemessen vor Zugriff durch unbefugte Personen gesichert.

Zugangskontrolle

Es sind Maßnahmen zur elektronischen Zugangskontrolle ergriffen worden, die gewährleisten, dass ein Zugang (d. h. bereits die Möglichkeit der Nutzung, Verwendung oder Beobachtung) durch Unbefugte zu Systemen, Datenverarbeitungsanlagen oder Verfahren verhindert wird.

a. Ein Passwortkonzept legt fest, dass Passwörter eine dem Stand der Technik und den Anforderungen an Sicherheit entsprechende Mindestlänge und Komplexität haben müssen.
b. Sämtliche Datenverarbeitungsanlagen sind passwortgeschützt.
c. Passwörter werden grundsätzlich nicht im Klartext gespeichert und nur gehashed oder verschlüsselt übertragen.
d. Es wird eine Passwort-Management-Software eingesetzt.
e. Für den Zugang zu Daten des Auftraggebers wird eine Zwei-Faktor-Authentifizierung verwendet.
f. Fehlversuche beim Login auf betriebsinterne Systeme werden auf eine angemessene Anzahl beschränkt (z.B. Sperrung von Logindaten).
g. Zugangsdaten werden, wenn deren Benutzer das Unternehmen oder Organisation des Auftragsverarbeiters verlassen haben, gelöscht oder deaktiviert.
h. Es werden Serversysteme und Dienste eingesetzt, die über Angriffserkennungssysteme ("Intrusion-Detection-Systeme") verfügen.
i. Es wird auf dem aktuellen Stand gehaltene Anti-Viren-Software eingesetzt.
j. Einsatz von Hardware-Firewall(s).
k. Einsatz von Software-Firewall(s).
l. Backups werden verschlüsselt gespeichert.

Interne Zugriffskontrolle und Eingabekontrolle (Berechtigungen für Benutzerrechte auf Zugang zu und Änderung von Daten)

Es sind Maßnahmen zur Zugriffskontrolle ergriffen worden, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Ferner sind Maßnahmen zur Eingabekontrolle ergriffen worden, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert, entfernt oder sonst verarbeitet worden sind.

a. Ein Rechte- und Rollenkonzept (Berechtigungskonzept) sorgt dafür, dass der Zugriff auf personenbezogenen Daten nur für einen nach Erforderlichkeitsmaßstäben ausgewählten Personenkreis und nur in dem erforderlichen Umfang möglich ist.
b. Das Rechte- und Rollenkonzept (Berechtigungskonzept) wird regelmäßig, innerhalb einer angemessenen zeitlichen Frequenz sowie wenn ein Anlass es erfordert (z. B. Verstöße gegen die Zugriffsbeschränkungen), evaluiert und bei Bedarf aktualisiert.
c. Die Zugriffe auf einzelne Dateien des Auftraggebers werden protokolliert.
d. Die Eingabe, Veränderung und Löschung einzelner Daten des Auftraggebers wird protokolliert.
e. Anmeldungen in den Datenverarbeitungsanlagen, bzw. Verarbeitungssystemen werden protokolliert.
f. Die Protokoll-, bzw. Logdateien werden vor Veränderung sowie vor Verlust und gegen unberechtigten Zugriff geschützt.
g. Die Tätigkeiten der Administratoren werden im Rahmen rechtlich zulässiger Möglichkeiten und im Rahmen technisch vertretbaren Aufwandes angemessen überwacht und protokolliert.

h. Es wird sichergestellt, dass nachvollziehbar ist, welche Beschäftigten oder Beauftragten auf welche Daten wann Zugriff hatten (z.B. durch Protokollierung der Softwarenutzung oder Rückschluss aus den Zugriffszeiten und dem Berechtigungskonzept).

Weitergabekontrolle

Es sind Maßnahmen zur Weitergabekontrolle ergriffen worden, die gewährleisten dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern 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.

a. Beim Zugriff auf betriebsinterne Systeme von außen (z.B. bei Fernwartung), werden verschlüsselte Übertragungstechnologien verwendet (z.B. VPN).
b. E-Mails werden während der Übertragung verschlüsselt, was bedeutet, dass die E-Mails auf dem Weg vom Absender zum Empfänger davor geschützt sind, von jemandem gelesen zu werden, der Zugang zu den Netzwerken hat, durch die die E-Mail gesendet wird.
c. Die Übermittlung und Verarbeitung von personenbezogenen Daten des Auftraggebers über Onlineangebote erfolgt geschützt mittels der SSL/TLS-Technologie. Weitere Hinweise: https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-policy-table.html.
d. Die im Auftrag verarbeiteten Daten werden im Ruhezustand mittels der AES-256-Technologie verschlüsselt. Die Verschlüsselung umfasst den zugehörigen Speicherplatz von Datenbankinstanzen sowie deren automatisierte Backups, Lesereplikate und Snapshots. Weitere Informationen: https://docs.aws.amazon.com/de_de/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

Auftragskontrolle, Zweckbindung und Trennungskontrolle

Es sind Maßnahmen zur Auftragskontrolle ergriffen worden, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Die Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten des Auftraggebers getrennt verarbeitet werden und keine Vermengung, Verschnitt oder sonstige dem Auftrag widersprechende gemeinsame Verarbeitung dieser Daten erfolgt.

a. Die für den Auftraggeber durchgeführten Verarbeitungsprozesse werden in einem angemessenen Umfang, in einem Verzeichnis von Verarbeitungstätigkeiten gesondert dokumentiert.
b. Sorgfältige Auswahl von Unterauftragsverarbeitern und sonstigen Dienstleistern.
c. Der Auftragsverarbeiter darf keine weiteren Unterauftragsverarbeiter ohne Zustimmung oder ohne Information des Auftraggebers (dieser hat dann ein Widerspruchsrecht) aufnehmen.
d. Mitarbeiter und Beauftragte werden verständlich und deutlich über die Weisungen des Auftraggebers und den zulässigen Verarbeitungsrahmen informiert und entsprechend instruiert. Eine gesonderte Information und Instruktion sind nicht erforderlich, wenn die Einhaltung des zulässigen Rahmens ohnehin, z. B. aufgrund anderweitiger Vereinbarungen oder betrieblicher Übung, verlässlich zu erwarten ist.
e. Die Einhaltung von Weisungen des Auftraggebers und des zulässigen Rahmens der Verarbeitung der personenbezogenen Daten durch Mitarbeiter und Beauftragte wird in angemessenen Abständen überprüft.
f. Die für die Verarbeitung der personenbezogenen Daten des Auftraggebers geltenden Löschfristen werden innerhalb des Löschkonzepts des Auftragsverarbeiters, sofern erforderlich gesondert, dokumentiert.

g. Die personenbezogenen Daten des Auftraggebers werden von Daten anderer Verarbeitungsverfahren des Auftragsverarbeiters logisch getrennt verarbeitetet und vor unberechtigtem Zugriff oder Verbindung oder Verschneidung mit anderen Daten geschützt (z.B. in unterschiedlichen Datenbanken oder durch angemessene Attribute).
h. Produktiv- und Testdaten werden streng getrennt voneinander in unterschiedlichen Systemen gespeichert. Die Produktivsysteme werden getrennt und unabhängig von den Entwicklungs- und Testsystemen betrieben.

Sicherung der Integrität und Verfügbarkeit von Daten sowie der Belastbarkeit von Verarbeitungssystemen

Es sind Maßnahmen ergriffen worden, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und in Notfällen zügig wiederhergestellt werden können.

a. Es werden ausfallsichere Serversysteme und Dienste eingesetzt, die doppelt, bzw. mehrfach ausgelegt sind.
b. Die Verfügbarkeit der Datenverarbeitungssysteme wird permanent, insbesondere auf Verfügbarkeit, Fehler sowie Sicherheitsvorfälle überwacht und kontrolliert.
c. Die personenbezogenen Daten werden bei externen Hosting-Anbietern gespeichert. Die Hosting-Anbieter werden sorgfältig ausgewählt und erfüllen die Vorgaben an den Stand der Technik, im Hinblick den Schutz vor Schäden durch Brand, Feuchtigkeit, Stromausfälle, Katastrophen, unerlaubte Zugriffe sowie an Datensicherung und Patchmanagement, als auch an die Gebäudesicherung.
d. Die Verarbeitung von personenbezogenen Daten erfolgt auf Datenverarbeitungssystemen, die einem regelmäßigen und dokumentierten

Patch-Management unterliegen, d. h. insbesondere regelmäßig aktualisiert werden.

e. Die zur Verarbeitung eingesetzten Serversysteme und Dienste werden in angemessenen Abständen Belastbarkeitstests und Hardwaretests unterzogen.
f. Die zur Verarbeitung eingesetzten Serversysteme verfügen über einen Schutz gegen Denial of Service (DoS) Angriffe.
g. Die zur Verarbeitung eingesetzten Serversysteme verfügen über einen angemessenen Brandschutz (Feuer- und Rauchmeldeanlagen sowie entsprechende Feuerlöschvorrichtungen oder Feuerlöschgeräte).
h. Es werden Serversysteme eingesetzt, die über einen Schutz vor Feuchtigkeitsschaden (z. B. Feuchtigkeitsmelder) verfügen.
i. Es werden Serversysteme und Dienste eingesetzt, die ein Backupsystem an anderen Orten, auf dem die aktuellen Daten vorgehalten werden und so ein lauffähiges System auch im Katastrophenfall zur Verfügung stellen, bereithalten.
j. Die Datensätze des Auftraggebers werden systemseitig vor versehentlicher Änderung oder Löschung geschützt (z. B. durch Zugriffsbeschränkungen, Sicherheitsabfragen und Backups).
k. Es werden Serversysteme und Dienste eingesetzt, die über ein angemessenes, zuverlässiges und kontrolliertes Backup- & Wiederherstellungskonzept verfügen.