


<b>Anlage A zum AV-Vertrag - TOMs</b>			
Dokumentverantwortung: DSB		Datum: 15.01.2020	Seite: 1 von 6
Informationsklassifizierung: vertraulich	Dokumentstatus: freigegeben		
Geltungsbereich: ALL	Datei: TPL_Foncloud_TOMs_v1.1.docx1		

## Anlage A

### zum Auftragsverarbeitungsvertrag (AVV)

## Technische und organisatorischen Maßnahmen (TOM's)

### nach Art. 32 Abs 1 lit. B DSGVO der foncloud GmbH & Co.KG

#### Dokumentenlenkung


Autor	Abteilung	Datum	Unterschrift
Sandra Effertz		11.04.2019	S.E.

#### Freigabe

Freigegeben durch	Abteilung	Datum	Unterschrift
Peter Krug	GF	16.04.2019	P.K.
Stephan Reich	Technik	16.04.2019	S.R.


#### Änderungskontrolle

Version	Datum	Autor	Änderung
1.0	16.04.2019	Peter Krug	Erstbefüllung
1.1	15.01.2020	Peter Krug	10.1. Liste der Unterauftragnehmer erweitert

<b>Anlage A zum AV-Vertrag - TOMs</b>			
Dokumentverantwortung: DSB		Datum: 15.01.2020	Seite: 2 von 6
Informationsklassifizierung: vertraulich		Dokumentstatus: freigegeben	
Geltungsbereich: ALL		Datei: TPL_Foncloud_TOMs_v1.1.docx1	

## Inhaltsverzeichnis

1. Zutrittskontrolle .....	3
2. Zugangskontrolle .....	3
3. Zugriffskontrolle .....	3
4. Trennungskontrolle .....	4
5. Pseudonymisierung .....	4
6. Weitergabekontrolle .....	4
7. Eingabekontrolle .....	5
8. Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit .....	5
9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung .....	5
10. Auftragskontrolle .....	6
10.1. Liste der Unterauftragnehmer des AN .....	6

<b>Anlage A zum AV-Vertrag - TOMs</b>			
Dokumentverantwortung: DSB		Datum: 15.01.2020	Seite: 3 von 6
Informationsklassifizierung: vertraulich	Dokumentstatus: freigegeben		
Geltungsbereich: ALL	Datei: TPL_Foncloud_TOMs_v1.1.docx1		

## 1. Zutrittskontrolle

Bei der Zutrittskontrolle handelt es sich um Maßnahmen, die geeignet sind, „Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren“.

umgesetzt	Anforderung
X	Verschlussmöglichkeiten von Büros und DV-Räumen
X	Prozess Berechtigungsmanagement (physische und elektronische Schlüssel, Berechtigungen)
X	Überprüfung Berechtigungsmanagement und vergebener Berechtigungen
X	Besucherregelung (An- Abmeldung, Begleitung)
X	Clear-Desk-Policy

## 2. Zugangskontrolle

Bei der Zugangskontrolle handelt es sich um Maßnahmen, die geeignet sind „zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden“.


umgesetzt	Anforderung
X	Vergabeprinzip „Need-to-Know“
X	Verbot von Gruppenaccounts
X	Prozess Berechtigungsmanagement
X	Überprüfung Berechtigungsmanagement und vergebener Berechtigungen
X	Clear-Desk-Policy
X	Session-Timeouts
X	Verschlüsselung mobiler Geräte und -Datenträger
X	Passwortrichtlinie
X	Datenschutzkonforme Vernichtung gemäß DIN 66399
X	Verschlüsselte Anmeldung
X	Verschlüsselte Ablage von Passwörtern
X	Verwendung von Firewalls

## 3. Zugriffskontrolle

Zugriffskontrolle sind Maßnahmen, 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, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können“.

Die Zugriffsberechtigungen sind in der Praxis oft an die Zugangsberechtigungen gekoppelt, sodass die Maßnahmen zum Zugang auch indirekte Auswirkungen auf den Zugriff haben.

umgesetzt	Anforderung
X	Vergabeprinzip „Need-to-Know“
X	Verbot von Gruppenaccounts

<b>Anlage A zum AV-Vertrag - TOMs</b>			
Dokumentverantwortung: DSB		Datum: 15.01.2020	Seite: 4 von 6
Informationsklassifizierung: vertraulich	Dokumentstatus: freigegeben		
Geltungsbereich: ALL	Datei: TPL_Foncloud_TOMs_v1.1.docx1		

X	Prozess Berechtigungsmanagement
X	Überprüfung Berechtigungsmanagement und vergebener Berechtigungen
X	Clear-Desk-Policy
X	Session-Timeouts
X	Verschlüsselung mobiler Geräte und -Datenträger
X	Passwortrichtlinie
X	Datenschutzkonforme Vernichtung gemäß DIN 66399
X	Verschlüsselte Anmeldung
X	Verschlüsselte Ablage von Passwörtern

#### 4. Trennungskontrolle

Maßnahmen, die „gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können“.

umgesetzt	Anforderung
X	Logische Mandantentrennung

#### 5. Pseudonymisierung


„Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.

umgesetzt	Anforderung
X	Umsetzung der hier genannten TOMs zum Schutz der Zuordnungsinformationen
X	Zentrale Speicherung der Zuordnungsinformationen

#### 6. Weitergabekontrolle

Unter Weitergabekontrolle versteht man Maßnahmen, die geeignet sind „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“.

umgesetzt	Anforderung
X	Alle Mitarbeiter sind vertraglich auf das Datengeheimnis verpflichtet.

<b>Anlage A zum AV-Vertrag - TOMs</b>			
Dokumentverantwortung: DSB		Datum: 15.01.2020	Seite: 5 von 6
Informationsklassifizierung: vertraulich	Dokumentstatus: freigegeben		
Geltungsbereich: ALL	Datei: TPL_Foncloud_TOMs_v1.1.docx1		

X	Mobile Datenträger, sowie die Datenträger von Laptops / Notebooks werden verschlüsselt
X	Der Zugang zu den Rechnersystemen erfolgt mittels VPN-Technologie
X	Bei Kommunikation mit externen Geschäftspartnern, Kunden und Diensten werden Verschlüsselungen nach dem Stand der Technik eingesetzt
X	Protokollierung der Übertragung
X	Verschlüsselung bei der Übertragung
X	Schutz bei physischen Transport
X	Protokollierung der Übertragung

## 7. Eingabekontrolle

Unter Eingabekontrolle versteht man Maßnahmen, die geeignet sind „zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind“.

umgesetzt	Anforderung
X	Festlegung, was protokolliert wird, insbesondere die Eingabe, Änderung und Löschung von Daten werden protokolliert
X	Sichere Aufbewahrung von Protokollinformationen

## 8. Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit


Maßnahmen, die „gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind“.

umgesetzt	Anforderung
X	Brandschutzeinrichtungen (Feuerlöscher, Rauch- oder Brandmelder), Rauchverbot, Wasserschutzeinrichtungen
X	Verwendung eines Virenschutzes
X	Automatische tägliche Datensicherung

## 9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

„Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“.

umgesetzt	Anforderung
X	Auditplanung und Durchführung von internen- und externen Audits
X	Durchführung von Sensibilisierungsmaßnahmen

<b>Anlage A zum AV-Vertrag - TOMs</b>			
Dokumentverantwortung: DSB		Datum: 15.01.2020	Seite: 6 von 6
Informationsklassifizierung: vertraulich	Dokumentstatus: freigegeben		
Geltungsbereich: ALL	Datei: TPL_Foncloud_TOMs_v1.1.docx1		

X	Maßnahmenplanung
X	Reporting bzw. Berichterstattung
X	Prozess zur Behandlung von Datenschutzvorfällen
X	Datenschutzfreundliche Voreinstellungen

## 10. Auftragskontrolle

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

umgesetzt	Anforderung
X	Die Unterauftragnehmer sind sorgfältig ausgewählt.
X	Sorgfältige Vertragsgestaltung (z.B. Kontrollrechte, Verpflichtung Mitarbeiter, AV-Verträge, relevante Aspekte des TKG, etc.).
X	Durchführung von Kontrollen
X	Einholen von Nachweisen (z.B. Zertifikate)

### 10.1. Liste der Unterauftragnehmer des AN

Folgenden Unterauftragnehmer werden vom AN zu Vertragsbeginn genutzt und gelten als freigegeben:

Name und Anschrift	Gegenstand	D, EWR, Drittland
<b>outbox AG</b> Emil-Hoffmann-Straße 1a 50996 Köln	Terminierung, Originierung, Portierungsvorabstimmung, Portierung	D
<b>3U TELECOM GmbH</b> Frauenbergstraße 31–33 35039 Marburg	Terminierung, Originierung, Portierungsvorabstimmung, Portierung	D
<b>Hetzner Online GmbH</b> Industriestr. 25 91710 Gunzenhausen	Serverinfrastruktur	D
<b>Amazon Web Services, Inc.</b> 410 Terry Avenue North Seattle WA 98109	Serverinfrastruktur	D
<b>Telefaks Services GmbH</b> Bartholomäus-Arnoldi-Strasse 97 61250 Usingen	Entwicklung Application Server	D