Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Zweck der Datenverarbeitung	Versendung von E-Mails und Newslettern
Art und Umfang der Datenverarbeitung	Ergeben sich aus dem Hauptvertrag
Art der Daten	Kommunikationsdaten (E-Mail-Adresse). Die Daten können durch ergänzende Attribute erweitert werden, wenn und soweit der Auftraggeber diese Daten selbst im Zusammenhang mit der E-Mail-Adresse abfragt (z.B. Anrede, Name, Interessen).
Kategorien betroffener Personen	Endkunden, Interessenten, Journalisten oder Abonnenten des Auftraggebers

Anlage 2: Weitere Auftragsverarbeiter

Unterauftragnehmer	Firma, Anschrift
Newsletter System: - Speicherung von Kundendaten - Mailversand	Data Kulturlink AG, Rosenthaler Strasse 38 10178 Berlin
Hosting: - Speicherung von Kundendaten - Mailversand	Serverstandort Deutschland Amazon Web Services, Inc. 410 Terry Avenue North Seattle, WA 98109 United States
Support: - Eigener Kundensupport - Chat Nur Speicherung von B2B Daten (direkte Kunden - es werden keine Newsletter Abonnenten oder Nutzungsdaten von Endkunden verarbeitet)	Intercom Inc. 55 2nd Street 4th Floor San Francisco, CA 94105 United States

Anlage 3:

Technische und organisatorische Maßnahmen (TOM)

gemäß Ziffer 6 des Auftragsverarbeitungsvertrag i.S.d. Art. 32 DSGVO

des Unternehmens eBuch (Stand: 30.08.2019)

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung nachfolgender technischer und organisatorischer Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften sind:

1. Zutrittskontrolle
Maßnahmen, mit denen der Zutritt zur physischen IT-Infrastruktur der eBuch für Unbefugte verwehrt wird:

1.1. Separater und gesicherter Serverraum

1.2. Regelung für die Vergabe von Zutrittsberechtigungen

1.3. Elektronische Zugangskontrolle

1.4. Einbruchmeldeanlage mit Aufschaltung an Sicherheitszentrale

1.5. Videoüberwachung

1.6. Zutritt für Besucher nur in Begleitung von berechtigten Personen

1.7. Zutritt für externe Firmen und Mitarbeiter nur in Begleitung von berechtigten Personen

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

2.1. Beachtung der Vorgaben durch IT-Abteilung (z.B. Vorgaben zur Passwortvergabe)

2.2. Vorgaben zu Benutzer- / Arbeitskonten

2.3. Regelungen für administrative Konten

3. Zugriffskontrolle
Maßnahmen, die gewährleisten, dass der Zugang zur den Datenverarbeitungssystemen nur für Befugte möglich ist:

3.1. Benutzerzuordnungen

3.2. Trennung zwischen Administration und anderen Tätigkeiten

3.3. Vernichtung von Ausdrucken und Datenträgern

4. Weitergabekontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Weitergabe oder beim Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

4.1. Absicherung von Transport und Übermittlung von Daten

4.2. Prüfung auf Vollständigkeit

4.3. Protokollierung der Übertragung

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

5.1. Regelungen zur Durchführung von Aufträgen

5.2. Dokumentation von Aufträgen

5.3. Zuständigkeiten und Verantwortliche

6. Verfügbarkeit

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

6.1. Unterbrechungsfreie Stromversorgung

6.2. Klimatisierung des Serverraums

6.3. Virenschutz

6.4. Firewalls

6.5. Brandschutz

6.6. Sicherung der Daten

6.7. Sofortmaßnahmen bei Notfall

7. Trennungsgebot

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

7.1. Trennung der Dateien durch dedizierte Ordner

7.2. Trennung der Dateien nach Auftraggeber

7.3. Einsicht in Datenschutz- und Sicherheitskonzept