Auftragsverarbeitungsvereinbarung
„Reichweitenverlängerung mit Retargeting“

Die Verarbeitung personenbezogener Daten im Rahmen der Nutzung des Produkts „Reichweitenverlängerung mit Retargeting“ erfolgt im Auftrag des Werbungtreibenden (nachfolgend „**Auftraggeber**“) durch die Axel Springer SE (nachfolgend „**Auftragsverarbeiter**“) nach Maßgabe dieser Auftragsverarbeitungsvereinbarung.

§ 1 Gegenstand der Vereinbarung

1.1 Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag von Auftraggeber unter Beachtung nachfolgender Regelungen.

1.2 Zweck und Umfang des Auftrags sind in **Anhang A** zu dieser Vereinbarung konkretisiert. Auftraggeber hat im Rahmen dieser Vereinbarung ein umfassendes Weisungsrecht gegenüber Auftragsverarbeiter. Dies gilt insbesondere hinsichtlich Berichtigung, Löschung (auch bzgl. Daten im Back-Up-Speicher), Einschränkung und Weitergabe der Daten sowie über Art, Umfang und Verfahren der Datenverarbeitung. Dieses umfassende Weisungsrecht von Auftraggeber kann dieser durch Einzelanweisung konkretisieren.

1.3 Die Inhalte dieser Vereinbarung gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 2 Allgemeine Pflichten von Auftraggeber

2.1 Auftraggeber ist gemäß Art. 4 Nr. 7 DSGVO Verantwortlicher im datenschutzrechtlichen Sinne für die bei Auftragsverarbeiter vertragsgemäß verarbeiteten personenbezogenen Daten.

2.2 Auftraggeber informiert Auftragsverarbeiter unverzüglich und vollständig, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

2.3 Auftraggeber führt ein Verzeichnis für Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO.

§ 3 Allgemeine Pflichten von Auftragsverarbeiter

3.1 Auftragsverarbeiter ist bezüglich der zu verarbeitenden Daten für die Einhaltung der jeweils einschlägigen Datenschutzgesetze, insbesondere für eine im Einklang mit der DSGVO erfolgte Verarbeitung verantwortlich. Er darf die Daten nur im Rahmen dokumentierter Weisungen von Auftraggeber verarbeiten. Ist er der Ansicht, dass eine Verletzung des Schutzes personenbezogener Daten vorliegt oder eine Weisung von Auftraggeber gegen ein Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er Auftraggeber darauf hinzuweisen.

3.2 Auftragsverarbeiter stellt Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der gemäß Art. 28 DSGVO und dieser Vereinbarung niedergelegten Pflichten sowie die für das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO notwendigen Angaben zur Verfügung und führt soweit gesetzlich vorgeschrieben gemäß Art. 30 Abs. 2 bis 5 DSGVO ein eigenes Verzeichnis zu allen Kategorien von im Auftrag von Auftraggeber durchgeführten Tätigkeiten der Verarbeitung.

3.3 Auftragsverarbeiter hat soweit gesetzlich vorgeschrieben, einen Datenschutzbeauftragten bestellt.

3.4 Alle Personen, die auftragsgemäß auf personenbezogene Daten von Auftraggeber zugreifen können, sind gemäß Art. 28 Abs. 3 b) DSGVO zur Vertraulichkeit zu verpflichten und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung zu belehren.

§ 4 Unterstützungspflichten von Auftragsverarbeiter

4.1 Auftragsverarbeiter gewährleistet den Schutz der Rechte betroffener Personen und unterstützt Auftraggeber im notwendigen Umfang bei der Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten gemäß Art. 12 – 23 DSGVO.

4.2 Auftragsverarbeiter unterstützt Auftraggeber bei der Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO und der daraus resultierenden Konsultation der Aufsichtsbehörde gemäß Art. 36 DSGVO im notwendigen Umfang.

4.3 Auftragsverarbeiter unterstützt Auftraggeber im Hinblick auf die Gewährleistung der Melde- und Benachrichtigungspflichten im Fall von Datenschutzverletzungen im Sinne von Art. 33 und 34 DSGVO. Hierfür ist entsprechend der Meldekette zur Störungsmeldung sowohl seitens Auftragsverarbeiter als auch seitens Auftraggeber ein Notfallkontakt mit 24-stündiger Erreichbarkeit vorzuhalten.

§ 5 Informationspflichten von Auftragsverarbeiter

5.1 Auftragsverarbeiter unterrichtet Auftraggeber unverzüglich in Textform bei Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen gemäß Art. 4 Nr. 12 DSGVO im Zusammenhang mit der Datenverarbeitung oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten von Auftraggeber.

5.2 Auftragsverarbeiter hat im Benehmen mit Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen, soweit die Datenschutzverletzung in seiner Verantwortung lag.

5.3 Bei Ermittlungen der Datenschutzbehörde bei Auftragsverarbeiter ist, soweit diese den Vertragsgegenstand betreffen, Auftraggeber unverzüglich zu informieren.

5.4 Für den Fall, dass Auftragsverarbeiter eine Verarbeitung von Daten von Auftraggeber – einschließlich einer Übermittlung in ein Drittland oder an eine internationale Organisation – beabsichtigt, ohne hierzu von Auftraggeber angewiesen worden zu sein, z.B. weil er hierzu gesetzlich verpflichtet ist, wird Auftragsverarbeiter Auftraggeber unverzüglich über Zweck, Rechtsgrund und betroffene Daten informieren, soweit und solange ihm eine solche Mitteilung nicht gesetzlich untersagt ist.

§ 6 Sicherheit der Verarbeitung

6.1 Auftragsverarbeiter wird durch eine ordnungsgemäße Umsetzung und Einhaltung der in **Anhang C** genauer beschriebenen geeigneten technischen und organisatorischen Maßnahmen ein dem Risiko angemessenes Schutzniveau sowie die Sicherung der Daten vor Missbrauch und Verlust sicherzustellen.

6.2 Diese Maßnahmen sollen unter Berücksichtigung von Implementierungskosten, dem Stand der Technik, Art, Umfang und Zweck der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen beispielsweise einschließen:

6.2.1 die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

6.2.2 die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

6.2.3 die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

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

6.3 Auftragsverarbeiter hat die Umsetzung der von Auftraggeber vor Erteilung des Auftrags dargelegten technischen und organisatorischen Maßnahmen für diese Auftragsverarbeitung vor Beginn der Verarbeitung zu dokumentieren (Datenschutz- und Sicherheitskonzept) und Auftraggeber auf Anfrage zur Prüfung zur Verfügung zu stellen. Bei Akzeptanz werden diese als **Anhang C** Grundlage der Vereinbarung. Soweit die Prüfung / ein Audit von AUFTRAGGEBER einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

6.4 Die getroffenen technischen und organisatorischen Maßnahmen sind gegenüber Auftraggeber nachzuweisen. Hierzu kann Auftragsverarbeiter auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) vorlegen.

6.5 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist Auftragsverarbeiter zur Wirkungsüberprüfung und entsprechender Anpassung bei Fortschritten nach dem Stand der Technik verpflichtet. Alternative Sicherheitsmaßnahmen sind gestattet, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

6.6 Wesentliche Änderungen nach Vertragsschluss sind AUFTRAGGEBER unverzüglich anzuzeigen. Werden die Maßnahmen so geändert, dass aus der Sicht von AUFTRAGGEBER AUF-TRAGSVERARBEITER keinen gleichwertigen oder einen höheren Schutz der Daten garantieren kann, hat AUFTRAGGEBER nach

erfolgloser Erteilung von Weisungen das Recht zur außerordentlichen Kündigung. Gleiches gilt bei unterlassener Anzeige solcher Änderungen.

§ 7 Überprüfungen einschließlich Inspektionen

Auftragsverarbeiter stellt Auftraggeber auf Anfrage alle erforderlichen Informationen zum Nachweis der in diesem Vertrag niedergelegten Pflichten zur Verfügung und ermöglicht Auftraggeber vor Beginn und während der Laufzeit dieser Vereinbarung nach angemessener vorherige Ankündigung und während der üblichen Geschäftszeiten (9:00-18.00 Uhr) die Durchführung von Überprüfungen, einschließlich Inspektionen nach Maßgabe des Art. 28 Abs. 3 h) DSGVO. Auftragsverarbeiter verpflichtet sich insbesondere, Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Auftraggeber ist darüber hinaus berechtigt, sich selbst oder durch geeignete, zur Berufsverschwiegenheit verpflichtete Dritte vor Beginn und während der Auftragsverarbeitung, nach rechtzeitiger Anmeldung in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, von der Einhaltung der gemäß Art. 28 DSGVO niedergelegten und in dieser Vereinbarung nebst dokumentierten Weisungen spezifizierten Pflichten zu überzeugen. Das Ergebnis dieser Überprüfungen wird jeweils dokumentiert und ist von beiden Parteien zu unterschreiben.

§ 8 Weitere Auftragsverarbeiter

8.1 Auftragsverarbeiter kann Aufträge an weitere Auftragsverarbeiter („Unterauftragsverarbeiter“) vergeben, wenn er Auftraggeber vorab über die Hinzuziehung oder Ersetzung neuer Unterauftragsverarbeiter schriftlich informiert und Auftraggeber binnen 4 Wochen keinen Einspruch erhebt. Bei Erteilung des Auftrags werden die in **Anhang B** aufgelisteten Unterauftragsverarbeiter genehmigt.

8.2 Auftragsverarbeiter hat den Unterauftragsverarbeitern im Wege eines Vertrags dieselben Datenschutzpflichten aufzuerlegen, die in dieser Vereinbarung festgelegt sind bzw. prüft bei Unterauftragsverarbeitern, die in einem Drittland in Bezug auf die Datenverarbeitung gemäß dieser Vereinbarung tätig werden, dass die eingesetzten Unterauftragsverarbeiter zumindest vollinhaltlich die Verpflichtungen aus den geltenden Standardvertragsklauseln erfüllen, welche die EU-Kommission erlässt oder von einer Aufsichtsbehörde festgelegt werden (gem. Art. 28 Abs. 6 bis 8 DSGVO), wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung den Anforderungen der DSGVO entspricht. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet Auftragsverarbeiter gemäß Art. 28 Abs. 4 S. 2 DSGVO gegenüber Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragsverarbeiters.

8.3 Bei der Unterbeauftragung sind Auftraggeber Überprüfungsrechte entsprechend dieser Vereinbarung beim Unterauftragsverarbeiter durch Einbeziehung dieser Vereinbarung einzuräumen. Insbesondere hat Auftraggeber gegenüber dem Unterauftragsverarbeiter ein gesetzliches Weisungsrecht gemäß Art. 29 DSGVO.

8.4 Dienstleistungen, die bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch genommen werden, gelten nicht als Unterauftragsverarbeiter. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten von Auftraggeber auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Überprüfungsmaßnahmen zu ergreifen.

§ 9 Löschung und Rückgabe

9.1 Alle überlassenen Datenträger sowie hiervon gefertigte Kopien oder Reproduktionen verbleiben im Eigentum von Auftraggeber. Sie sind vor dem Zugriff unberechtigter Dritter zu sichern. Nach Abschluss der Erbringung der Verarbeitungsleistungen – spätestens mit Beendigung dieser Vereinbarung - hat Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände und Kopien, die im Zusammenhang mit dem Auftragsverhältnis stehen, Auftraggeber auszuhändigen und danach in seinen Systemen datenschutzgerecht zu vernichten. Die Parteien können stattdessen vereinbaren, auf die Aushändigung zu verzichten, und die sofortige datenschutzgerechte Vernichtung durch Auftragsverarbeiter vornehmen zu lassen. Gleiches gilt für Test- und Ausschussmaterial. Über die Rückgabe oder Löschung der Daten nach Vertragsende wird Auftraggeber innerhalb einer von Auftragsverarbeiter gesetzten Frist entscheiden.

9.2 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch Auftragsverarbeiter entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren, sofern Auftraggeber dazu keine anderen Weisungen getroffen hat. Er kann sie aber auch bei Vertragsende an Auftraggeber übergeben.

§ 10 Laufzeit

10.1 Die Regelungen dieser Vereinbarung gelten auch nach einer Beendigung des primären Leistungsverhältnisses bis zur vollständigen Vernichtung oder Rückgabe aller personenbezogenen Daten durch Auftragsverarbeiter an Auftraggeber fort.

10.2 Ein grober Verstoß gegen eine der vorstehenden Regelungen oder der sonstigen datenschutzrechtlichen Pflichten durch Auftragsverarbeiter berechtigt Auftraggeber im Übrigen zu einer außerordentlichen Kündigung der Verträge, die der Auftragsverarbeitung zugrunde liegen. Weitere gesetzliche Gründe zur außerordentlichen Kündigung bleiben unberührt.

§ 11 Sonstiges

11.1 Mündliche Nebenabreden sind nicht getroffen. Änderungen und Ergänzungen dieses Vertrages und seiner Anlagen (einschließlich der Aufhebung des hier beschriebenen Formerfordernisses) bedürfen der Schriftform. Ausgenommen von dem Formerfordernis sind Weisungen von Auftraggeber. Mündlich erteilte Weisungen sind von Auftragsverarbeiter unverzüglich zu dokumentieren.

11.2 Es gilt deutsches Recht. Ausschließlicher Gerichtsstand ist Berlin, Deutschland.

11.3 Anhänge A, B und C sind wesentlicher Bestandteil dieser Vereinbarung.

§ 12 Kontaktdaten für die Meldekette im Störungsfall

Media Impact GmbH & Co. KG	Ansprechpartner, Kontaktdaten
Datenschutzbeauftragte-/r	Andreas Macke, +49 30 2591 - 72701 Andreas.Macke@axelspringer.de
Ansprechpartner Fachbereich / Projekt	1. Volker Mieß, 0151 42125762 volker.miess@axelspringer.com 2. Wenke Hammler, 0151 44047685 wenke.hammler@axelspringer.com
Kontakt bei Datenpannen (24 h erreichbar) (Bitte jeweils unter Nennung Stichwort „Datenpanne“ und Nennung Ansprechpartner Fachbereich / Projekt.)	datenschutz@axelspringer.de Zentrale Notrufnummer: +49 30 5858 5379

Der Auftraggeber teilt dem Auftragsverarbeiter die Kontaktdaten seines Datenschutzbeauftragten mit, soweit vorhanden. Ferner teilt der Auftraggeber dem Auftragsverarbeiter Kontaktdaten zur Meldung von Datenpannen mit.

Anhang A zur Auftragsverarbeitungsvereinbarung

Gegenstand und Dauer der Verarbeitung:	Die Plattformen (z. B. Webseiten) des Auftraggebers auf die von den vertragsgegenständlichen Werbeanzeigen von Auftraggeber verlinkt wird, werden zum Zwecke der Performance-Optimierung für den Auftraggeber verpixelt.
Art und Zweck der Verarbeitung:	Bei der Verpixelung werden Cookies (DV360) auf den Webseiten des Auftraggebers eingesetzt. Der Einsatz erfolgt vorbehaltlich der Einwilligung des Nutzers, die gemäß einer geeigneten technischen Lösung auf den Webseiten des Auftraggebers eingeholt und an den von Auftragsverarbeiter eingesetzten Unterauftragsverarbeiter (EPROFESSIONAL) übermittel werden muss. Auf Basis der mittels der Cookies gesammelten Daten wird die weitere Kampagnenausspielung für den Auftraggeber optimiert. Optimierung auf KPIs erfolgt auf Wunsch von Auftraggeber (z. B. Leads, Registrierungen, Klicks etc.) Personenbezogene Daten werden in einem separaten Daten-Silo für den Auftraggeber gespeichert. Die Daten werden ausschließlich zur Optimierung der gebuchten Kampagne genutzt und nach Kampagnenende gelöscht.
Art der personenbezogenen Daten:	Trackingdaten, IP-Adresse, Cookie ID
Kategorien betroffener Personen:	Nutzer der Website des Auftraggebers
Löschung von Daten:	Die Daten werden nach Kampagnenende gelöscht.

Anhang B zur Auftragsverarbeitungsvereinbarung

Die im folgenden aufgelisteten Unterauftragsverarbeiter von Auftragsverarbeiter werden bei Erteilung des Auftrags genehmigt.

	Firma, Anschrift:	Art der erbrachten Tätigkeit:
1.	EPROFESSIONAL GmbH, Heidenkampsweg 74-76, 20097 Hamburg Deutschland	Performance Optimierung
2.	Google DV 360, Google Inc.1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	

Anhang C zur Auftragsverarbeitungsvereinbarung

Technische und organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter gewährleistet im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die gesetzlich geforderten Sicherheitsmaßnahmen. Hierzu kommen folgende technische und organisatorische Maßnahmen zur Anwendung:

a.) Zutrittskontrolle (für Gebäude, Geschäftsräume, Serveranlagen und Schränke)

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

- Alarmanlage & Bewegungsmelder
- Automatische Zugangskontrollsystem

- Chipkarten- & Transponder-Schließsystem
- Manuelles Schließsystem
- Schlüsselregelung & Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal.

b.) Zugangskontrolle (Anmeldung am System, Verhinderung unerlaubten Hochfahrens und Eindringens in das DV-System)

Maßnahmen, mit denen die Nutzung von DV-Systemen durch Unbefugte verhindert wird:

- Erstellen von Benutzerprofilen & Zuordnung von Benutzerrechten
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Passwortvergabe & Authentifikation mit Benutzername / Passwort
- Spezielle / Individuelle Benutzermenüs
- Automatische Sperrung / Log-off
- Einsatz von Intrustion-Detection-Systemen
- Einsatz von Anti-Viren-Software, Hardware-Firewall & Software-Firewall
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum Fernlöschen von Daten)
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Schlüsselregelung & Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal.

c.) Zugriffskontrolle (Kontrollierte Ausführung von Anwendungen, Beschränkung von Tätigkeiten in DV-Systemen und Zugriffen auf Daten, Applikationen und Schnittstellen)

Maßnahmen, die gewährleisten, dass die zur Benutzung eines DV-Systems 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:

- Berechtigungskonzept & Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf einzelne Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Einsatz von Aktenvernichtern durch zertifizierte Dienstleister
- Protokollierung der Vernichtung.

d.) Trennungsgebot

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

- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem.

e.) Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

f.) 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:

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Regelung des Kommunikationsverkehrs.

g.) Eingabekontrolle (Nachvollziehbarkeit, Dokumentation)

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

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können, insb. in Form eines Verfahrensverzeichnisses
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts.

h.) Verfügbarkeitskontrolle und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust, gegen technische Störungen durch Versagen der Betriebs-/Anwendungssoftware, vor fahrlässigen/vorsätzlichen Handlungen und vor schadenstiftender Software geschützt sind:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen & besondere Feuerlöschgeräte für Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen im Rechenzentrum
- Backup- & Recoverykonzept & Testen von rascher Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Erstellen eines Notfallplans
- Serverräume nicht unter sanitären Anlagen und über der Wassergrenze.

i.) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

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

- / Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen
- / Incident-Response-Management
- / Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- / schriftliche Weisungen an den Auftragsverarbeiter (z. B. durch ADV-Vertrag)
- / formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters, Vorabüberzeugungspflicht, Nachkontrollen
- / Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
- / Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.

Ergänzende Angaben:

	Dokumentierter Prozess zur Erkennung/Meldung von Datenpannen / Sicherheitsvorfällen
	Gibt es einen formalen, definierten Prozess zur erkennung und Meldung von Datenpannen? Wird dieser Prozess regelmäßig getestet und geprobt, um die gesetzliche Frist von 72 Stunden zu garantieren? *Sind die Kontaktwege zu den jeweiligen Behörden bekannt und dokumentiert?*
x	/ Es gibt einen dokumentierter Prozess zur Erkennung/Meldung von Datenpannen / Sicherheitsvorfällen
x	/ Dieser Prozess wird regelmäßig geprüft und ggf. verbessert/angepasst
x	/ Dieser Prozess ermöglicht die Einhaltung der Meldefrist von 72 Stunden an die Aufsichtsbehörden
	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
	Gibt es einen Plan zur Reaktion bei Sicherheitsvorfällen: *-Kommunikationsplan für interne Kommunikation* *-Einbindung von Ressourcen (intern und ggf. extern)* *-Beweissicherung und Forensiche Untersuchung des Vorfalls* *-Festgelegte Entscheidungswege um ggf. Systeme und Maschinen vorübergehend abzuschalten* *-Externe Kommunikation zu Kunden, Vertragspartnern, Aufsichtsbehörden, u.a.* *- ggf. abgestimmte Kommunikation an Strafverfolgungsbehörden und Presse*
x	/ Ja
	/ Teilweise
	/ Nein
	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen
	Gibt es einen formalen Prozess zur Auswertung von Sicherheitsvorfällen ("lesson learned")? Werden die Erkenntnisse des Sicherheitsvorfalls in die jeweiligen Pläne und Prozesse eingearbeitet, um zukünftig eine optimierte Reaktion aufzuweisen?
x	/ Ja
	/ Teilweise
	/ Nein
	Härtung der Backendsysteme

	Die Sicherheit der Systeme wurde durch folgende Maßnahmen erhöht: *Alle Systeme und Anwendungen sind stets auf dem aktuellen Patchstand.* *Alle nicht benötigten Dienste wurden deaktiviert.* *Nicht benötigte Hardwareschnittstellen wurden deaktiviert.* *Voreingestellte Dienstkonten/Passworte wurden deaktiviert.* *Es existieren Handlungsanweisungen bei Missbrauchsverdacht.* *Es existiert ein aktueller Virenschutz.*
x	/ Alle Systeme und Anwendungen sind stets auf dem aktuellen Patchstand
x	/ Voreingestellte Dienstkonten/Passworte (defaults) wurden deaktiviert
x	/ Es existieren Handlungsanweisungen bei Missbrauchsverdacht
x	/ Es existiert ein aktueller Virenschutz
	Firewall
	Jede verantwortliche Stelle, die personenbezogene Daten erhebt, verarbeitet und / oder nutzt, ist verpflichtet, technische und organisatorische Maßnahmen (TOM) zu treffen, um die Anforderungen aus Artikel 32 Abs. 1 DSGVO zu erfüllen. Der Einsatz einer Firewall sollte als technische Maßnahme fest integriert sein, da der Einsatz für den Schutz von Daten eine erhebliche Rolle spielen kann.
x	/ Es existieren Firewalls an Netzwerk-Übergabepunkten
x	/ Die Firewalls sind ständig aktiviert
x	/ Die Firewalls sind durch den Nutzer nicht deaktivierbar
	Backup & Recovery Konzept (ausformuliert)
	Erfolgt die Datensicherung nach einem detailliert ausformulierten Plan? *Werden Sicherheitskopien der Datenbestände nach dem Generationsprinzip in geeigneten zeitlichen Abständen erstellt?* *Wurde beachtet, dass die Sicherungsdateien zu schützen sind, etwa durch ein Passwort, Schutzbit oder Freigabedatum?* *Wird neben einer manuellen Datensicherung systemseitig eine automatische Sicherung erzwungen?* *Erfolgt ein Schreiben von Prüfpunkten (Synchronisationspunkten) zur Erzeugung genau definierter Dateizustände (für späteren Wiederanlauf des Verfahrens)?* *Bestehen Maßnahmen zur Vermeidung der Verwendung falscher Sicherungsbänder (z.B. eindeutige Beschriftung, geregelte Ausgabe)?*
x	/ Es existiert ein ausformuliertes Backup- & Recovery Konzept
	/ Es gibt ein Mehrgenerationenkonzept zur Sicherung (Großvater/Vater/Sohn)
x	/ Eine für das Backup verantwortliche Person und deren Vertreter sind benannt
x	/ Die Datenpartitionen und auch die Systempartitionen sind gesichert
x	/ Die Sicherungsmedien sind durch Sicherungsmaßnahmen (z.B. Password) geschützt
x	/ es ist sichergestellt, dass ein Backup nicht auch als Archiv genutzt wird