

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Die Leadinfo B.V., Rivium Quadrant 141, 2909 LC Capelle aan den IJssel, Niederlande (nachfolgend „**Auftragnehmer**“ oder „**Auftragsverarbeiter**“) verarbeitet personenbezogene Daten für Sie (nachfolgend „**Auftraggeber**“ oder „**Verantwortlicher**“) im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage des Hauptvertrages. Hinsichtlich der datenschutzrechtlichen Verpflichtungen der Parteien gelten dabei die nachfolgenden Bestimmungen (nachfolgend die „**Vereinbarung**“):

1. Gegenstand und Dauer der Verarbeitung

- 1.1 Der Auftrag umfasst die Identifikation der B2B-Webseiten-Besucher des Auftraggebers gemäß den Bestimmungen des Hauptvertrags. Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen.
- 1.2 Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages.

2. Art und Zweck der Verarbeitung, Kategorien betroffener Personen, Arten personenbezogener Daten

- 2.1 Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag und umfassen die Identifikation der B2B-Webseiten-Besucher des Auftraggebers zum Zweck der Bereitstellung weiterer Information; sowie ggf. die Bereitstellung weiterer Informationen zum Zweck der Optimierung des Web-Auftritts des Auftraggebers.
- 2.2 Von der Verarbeitung personenbezogener Daten im Rahmen dieser Vereinbarung sind folgende Kategorien von Personen betroffen: Webseitenbesucher des Auftraggebers (einschließlich Bestandskunden, Interessenten, Lieferanten).
- 2.3 Von der Verarbeitung sind folgende Arten personenbezogener Daten betroffen: IP-Adresse.

3. Rechte und Pflichten des Auftraggebers

- 3.1 Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Der Auftragnehmer wird an ihn gerichtete Anfragen, welche erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterleiten.
- 3.2 Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Soweit es der Verantwortliche für erforderlich hält, können weisungsberechtigte Personen benannt werden. Diese wird der Verantwortliche dem Auftragsverarbeiter schriftlich oder in Textform mitteilen. Für den Fall, dass sich diese weisungsberechtigten Personen bei dem Verantwortlichen ändern, wird dies dem Auftragsverarbeiter unter Benennung der jeweils neuen Person schriftlich oder in Textform mitgeteilt.
- 3.3 Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

4. Pflichten des Auftragsverarbeiters

- 4.1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der

Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

- 4.2 Der Auftragsverarbeiter wird den Verantwortlichen bei der Erfüllung der Rechte der Betroffenen, insbesondere im Hinblick auf Berichtigung, Einschränkung der Verarbeitung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen seiner Möglichkeiten unterstützen. Der Auftragsverarbeiter hat auf Weisung des Verantwortlichen die gemäß dieser Vereinbarung verarbeiteten personenbezogenen Daten zu berichtigen, zu löschen oder die Verarbeitung einzuschränken. Soweit sich eine betroffene Person unmittelbar an den Auftragsverarbeiter zwecks Berichtigung, Löschung oder Einschränkung der Verarbeitung der gemäß dieser Vereinbarung verarbeiteten personenbezogenen Daten wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich nach Erhalt an den Verantwortlichen weiterleiten.
- 4.3 Der Auftragsverarbeiter stellt durch geeignete Kontrollen sicher, dass die im Auftrag verarbeiteten personenbezogenen Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des Hauptvertrages und/oder den entsprechenden Weisungen verarbeitet werden. Der Auftragsverarbeiter wird sein Unternehmen und seine Betriebsabläufe so gestalten, dass die gemäß dieser Vereinbarung verarbeitete personenbezogenen Daten im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.
- 4.4 Sofern der Zugriff auf die Daten, die der Verantwortliche dem Auftragsverarbeiter zur Datenverarbeitung übermittelt hat, durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, etc.) gefährdet wird, hat der Auftragsverarbeiter den Verantwortlichen unverzüglich hierüber zu benachrichtigen.
- 4.5 Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine von dem Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter wird den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützen.
- 4.6 Die Verarbeitung der Daten findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Verlagerungen in ein Drittland dürfen nur unter den besonderen Voraussetzungen der Art. 44 ff. DSGVO erfolgen.
- 4.7 Nach Beendigung des Hauptvertrages wird der Auftragsverarbeiter alle im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Verantwortlichen entweder löschen oder zurückgeben, sofern der Löschung dieser Daten keine gesetzlichen Aufbewahrungspflichten des Auftragsverarbeiters entgegenstehen. Die datenschutzgerechte Löschung ist zu dokumentieren und gegenüber dem Verantwortlichen auf Anforderung zu bestätigen.

5. Kontrollrechte des Verantwortlichen

Der Verantwortliche ist berechtigt, nach rechtzeitiger vorheriger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Geschäftsbetriebes des Auftragsverarbeiters oder Gefährdung der Sicherheitsmaßnahmen für andere Verantwortliche und auf eigene Kosten, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang selbst oder durch Dritte zu kontrollieren. Die Kontrollen können auch durch Zugriff auf vorhandene branchenübliche Zertifizierungen des Auftragsverarbeiters aktuelle Testate oder Berichte einer unabhängigen Instanz (wie z.B. Wirtschaftsprüfer, externer Datenschutzbeauftragter, Revisor oder externer Datenschutzauditor) oder Selbstauskünfte durchgeführt werden. Der Auftragsverarbeiter wird die notwendige Unterstützung zur

Durchführung der Kontrollen anbieten. Der Auftragsverarbeiter wird den Verantwortlichen über die Durchführung von Kontrollmaßnahmen der Aufsichtsbehörde informieren, soweit die Maßnahmen oder Datenverarbeitungen betreffen können, die der Auftragsverarbeiter für den Verantwortlichen erbringt.

6. Unterauftragsverhältnisse

6.1 Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den in der **Anlage 1** benannten Unterauftragnehmern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt.

6.2 Der Auftragsverarbeiter ist berechtigt, weitere Auftragsverarbeiter zu beauftragen oder bereits Beauftragte zu ersetzen. Der Auftragsverarbeiter wird den Verantwortlichen über Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung eines weiteren Auftragsverarbeiters in geeigneter Weise informieren. Der Verantwortliche kann gegen eine beabsichtigte Änderung innerhalb von 2 Wochen nach Zugang der Information über die Änderung Einspruch gegenüber dem Auftragsverarbeiter erheben. Im Fall des Einspruchs kann der Auftragsverarbeiter nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder einen alternativen weiteren Auftragsverarbeiter vorschlagen und mit dem Verantwortlichen abstimmen. Sofern dem Auftragsverarbeiter die Erbringung der Leistung ohne die beabsichtigte Änderung nicht zumutbar ist – etwa aufgrund von damit verbundenen unverhältnismäßigen Aufwendungen für den Auftragsverarbeiter – oder die Abstimmung eines weiteren Auftragsverarbeiters fehlschlägt, können der Verantwortliche und der Auftragsverarbeiter diese Vereinbarung sowie den Hauptvertrag mit einer Frist von einem Monat zum Monatsende kündigen.

6.3 Bei Einschaltung weiterer Auftragsverarbeiter muss stets ein Schutzniveau, welches mit demjenigen dieser Vereinbarung vergleichbar ist, gewährleistet werden. Der Auftragsverarbeiter ist gegenüber dem Verantwortlichen für sämtliche Handlungen und Unterlassungen der von ihm eingesetzten weiteren Auftragsverarbeiter verantwortlich.

7. Vertraulichkeit

7.1 Der Auftragsverarbeiter ist bei der Verarbeitung von Daten für den Verantwortlichen zur Wahrung der Vertraulichkeit verpflichtet. Der Auftragsverarbeiter verpflichtet sich bei der Erfüllung des Auftrags nur Mitarbeiter oder sonstige Erfüllungsgehilfen einzusetzen, die auf die Vertraulichkeit im Umgang mit überlassenen personenbezogenen Daten verpflichtet und in geeigneter Weise mit den Anforderungen des Datenschutzes vertraut gemacht worden sind. Sofern der Verantwortliche besonderen Geheimnisschutzregeln unterliegt, wird er dies dem Auftragsverarbeiter mitteilen. Der Auftragsverarbeiter wird seine Mitarbeiter entsprechend den Anforderungen des Verantwortlichen auf diese Geheimnisschutzregeln verpflichten.

7.2 Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

8. Technische und organisatorische Maßnahmen

8.1 Die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen werden als angemessen vereinbart. Der Auftragsverarbeiter kann diese Maßnahmen aktualisieren und ändern, vorausgesetzt dass das Schutzniveau durch solche Aktualisierungen und/oder Änderungen nicht wesentlich herabgesetzt wird.

8.2 Der Auftragsverarbeiter beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung gemäß Art 32 i.V.m Art. 5 Abs. 1 DSGVO. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen. Er wird alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Standes der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene ergreifen. Die zu treffenden Maßnahmen umfassen insbesondere Maßnahmen

zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Maßnahmen, die die Kontinuität der Verarbeitung nach Zwischenfällen gewährleisten. Um stets ein angemessenes Sicherheitsniveau der Verarbeitung gewährleisten zu können, wird der Auftragsverarbeiter die implementierten Maßnahmen regelmäßig evaluieren und ggf. Anpassungen vornehmen.

9. Haftung

- 9.1 Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen gemäß den gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diese Vereinbarung sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen, die der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen. Eine Ersatzpflicht des Auftragsverarbeiters besteht nicht, sofern der Auftragsverarbeiter nachweist, dass er die ihm überlassenen Daten des Verantwortlichen ausschließlich nach den Weisungen des Verantwortlichen verarbeitet und seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nachgekommen ist.
- 9.2 Der Verantwortliche stellt den Auftragsverarbeiter von allen Ansprüchen Dritter frei, die aufgrund einer schuldhaften Verletzung der Verpflichtungen aus dieser Vereinbarung oder geltenden datenschutzrechtlichen Vorschriften durch den Verantwortlichen gegen den Auftragsverarbeiter geltend gemacht werden.

10. Sonstiges

- 10.1 Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor.
- 10.2 Änderungen und Ergänzungen dieser Vereinbarung setzen die beidseitige Zustimmung der Vertragsparteien voraus unter konkreter Bezugnahme auf die zu ändernde Regelung dieser Vereinbarung. Mündliche Nebenabreden bestehen nicht und sind auch für künftige Änderungen dieser Vereinbarung ausgeschlossen. Dies gilt auch für Änderungen der Regelung in dieser Ziffer 10.2.
- 10.3 Anwendbares Recht und Gerichtsstand richten sich nach dem Hauptvertrag.

Anlage 1: Unterauftragsverhältnisse gemäß § 9 der Vereinbarung zur Auftragsverarbeitung

Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den folgenden weiteren Auftragsverarbeitern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt:

- **Amazon Web Services EMEA SARL (Luxemburg):**
Cloud-Infrastruktur; Server-Standort in Irland

Anlage 2: Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

Der Auftragsverarbeiter sichert zu, folgende technische und organisatorische Maßnahmen getroffen zu haben:

A. Maßnahmen zur Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren:

- Verarbeitung pseudonymer Online-Kennungen der Webseitenbesucher

B. Maßnahmen zur Verschlüsselung

Maßnahmen oder Vorgänge, bei denen ein klar lesbarer Text / Information mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird:

- Verschlüsselung der serverseitig verarbeiteten Daten
- Verschlüsselung (und Passwortschutz) der Endbenutzergeräte
- Verschlüsselung der Datenübertragungen per https
- Bereitstellung der unternehmensbezogenen Informationen der Webseitenbesucher in einem Passwort-gesicherten Online-Bereich

C. Maßnahmen zur Sicherung der Vertraulichkeit

1. Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren:

- Ausweisleser, kontrollierte Schlüsselvergabe, Chipkarte
- Türsicherung (elektronischer Türöffner)
- gesicherter Serverraum

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können:

- Kennwortverfahren mit Komplexitätsanforderungen
- Begrenzung der Zahl der berechtigten Mitarbeiter
- Verschlüsselung von Datenträgern
- Protokollierung der Anmeldeversuche und Abbruch des Anmeldevorgangs nach festgelegter Zahl von erfolglosen Zahl von Versuchen
- Aktueller Antivirenschutz

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Benutzerberechtigungskonzept mit entsprechender Dokumentation
- Protokollierung von Zugriffen und Missbrauchsversuchen
- Verschlüsselung von Datenträgern

4. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist:

- Benutzerberechtigungskonzept
- verschlüsselte Speicherung personenbezogener Daten
- Trennung von Test- und Produktivsystemen

D. Maßnahmen zur Sicherung der Integrität

1. Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden:

- Einspielen neuer Releases und Patches mit Release-/Patchmanagement
- Funktionstests

2. Übertragungskontrolle

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:

- Transportprozesse mit individueller Verantwortlichkeit

3. Transportkontrolle

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

- Übermittlung von Daten über verschlüsselte Datennetze oder Tunnelverbindungen
- Transportprozesse mit individueller Verantwortlichkeit

E. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle

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

- Datensicherungsverfahren
- Unterbrechungsfreie Stromversorgung
- Notfallpläne
- Brandmelde-, Klima- und Alarmanlage

2. Zuverlässigkeit

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

- Automatisches Monitoring mit automatischen E-Mail-Benachrichtigungen
- regelmäßige Tests der Datenwiederherstellung

- Notfallpläne mit Verantwortlichkeiten

F. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

1. Überprüfungsverfahren

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen:

- Datenschutz- und Informationssicherheitsmanagement
- Weisungen des Auftraggebers werden dokumentiert
- formalisiertes Auftragsmanagement

2. Auftragskontrolle

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

- Weisungen des Auftraggebers werden dokumentiert
- formalisiertes Auftragsmanagement
