Vereinbarung zur Auftragsdatenverarbeitung

gemäß Art. 28 DS-GVO

Versand von Präsenten
(nachfolgend „**Hauptvertrag**“ genannt)

zwischen
Firma/Institution _____
Straße und Hausnummer _____
PLZ und Ort _____
(als „**Verantwortlicher**“, nachfolgend „**Auftraggeber**“ genannt)

und

graphodata GmbH
Benefizshoppen
Karl-Friedrich-Straße 74
52072 Aachen
Vertreten durch die Geschäftsführer Mario Pauly und Martina Henrichs
(nachfolgend „**Auftragsverarbeiter**“ genannt)

gemeinsam Auftraggeber und Auftragsverarbeiter einzeln jeweils „Vertragspartei“
und gemeinsam: „Vertragsparteien“

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Versand von Präsenten

(2) Dauer

Bis zur abschließenden Durchführung des Auftrags

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftraggeber stellt dem Auftragsverarbeiter Adressdaten Excel für den Versand von Präsenten zur Verfügung.

Der Auftragsverarbeiter konfiguriert diese Datensätze entsprechend den Vorgaben des Paketdienstes DHL, lädt die Daten über das DHL-Portal zwecks Versanddurchführung hoch und druckt Versandetiketten.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(2) Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-Kategorien
(bitte anklicken)

- ☐ Firmen-/Institutionsname
- ☐ Name
- ☐ Vorname
- ☐ Adresse
- ☐ Email-Adresse
- ☐ Geburtsdatum

(3) Kategorien betroffener Personen (bitte anklicken)

- ☐ Kunden
- ☐ Partner
- ☐ Mitarbeiter

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragsverarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu

übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

(2) Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen (Einzelheiten in **Anlage 1**).

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragsverarbeiter sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; 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.
b) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten in Anlage 1).
d) Der Auftraggeber und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.
f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.
g) Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.
i) Als Ansprechpartner beim Auftragsverarbeiter ist Frau Martina Henrichs benannt und ist unter info@benefizshoppen.de erreichbar.

6. Unterauftragsverhältnisse (Subunternehmer)

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragsverarbeiter darf Unterauftragsverarbeiter (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragsverarbeiter stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, erfolgt durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO.

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragsverarbeiter einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragsverarbeiter hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter die vom Auftraggeber bereitgestellten Datensätze zu löschen. Zwecks Nachvollziehbarkeit von Versendungen, Rückläufern, Reklamationen erfolgt die Löschung der Daten 6 Wochen nach Durchführung des Versandes.

11. Freistellung

Der Auftragsverarbeiter verpflichtet sich, den Auftraggeber von Schadenersatzansprüchen Dritter wegen der Verletzung von Datenschutzvorschriften durch den Auftragsverarbeiter im Rahmen des Auftragsdatenverarbeitungsverhältnisses freizustellen. Dies gilt nicht, wenn der Auftragsverarbeiter die Verletzung der Datenschutzvorschriften nicht zu vertreten hat.

12. Schlussbestimmungen

Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

_____	28/06/22
Ort, Datum	
	
_____	
(als Verantwortlicher / Auftraggeber)	graphodata GmbH, Benefizshoppen

Anlage 1: Technische und organisatorische Maßnahmen zum Datenschutz

graphodata GmbH
Karl-Friedrich-Str. 74
52072 Aachen
Vertreten durch die Geschäftsführer Mario Pauly und Martina Henrichs

Datum der letzten Bearbeitung: 11.02.2021

1. Zutrittskontrolle
1.1 Dokumentation der Vergabe von Schlüsseln
1.2 Rückgabe von Schüsseln nach Austritt von Mitarbeitern
1.3 Verwendung einer Alarmanlage

2. Zugangskontrolle
2.1 Ggfls. Anwendung von Maßnahmen zur Verschlüsselung von lokalen Daten (z. B. Festplatten, Server)
2.2 Automatisches Sperren von PCs nach 10 Minuten
2.3 Verwendung personalisierter Logins im Unternehmensnetzwerk
2.4 Verwendung sicherer und individueller Passwörter

3. Zugriffskontrolle
3.1 Dokumentation eingerichteter Zugänge für Mitarbeiter
3.2 Einführung von Benutzer- und Rollenkonzepten für interne Systeme
3.3 Sperrung von Zugängen nach Austritt von Mitarbeitern
3.4 Zentrale Verwaltung von Benutzerzugängen und -rechten

4. Weitergabekontrolle
4.1 Nutzung SSL-verschlüsselter Übertragungswege im Internet
4.2 Sicherung von Dokumenten beim Versand auf dem Postweg (z. B. undurchsichtige Versandhüllen)
4.3 Verwendung von VPN-Systemen zum Login in das Firmennetzwerk

5. Trennungskontrolle
5.1 Einführung von Zugriffsberechtigungen für interne Systeme
5.2 Ggfls. Trennung von Live- und Entwicklungssystemen

6. Verschlüsselung
6.1 Verwendung verschlüsselter Übertragungswege für den Datenaustausch
6.2 Ggfls. Verwendung von Maßnahmen zur verschlüsselten Datenspeicherung
6.3 Verwendung von SSL-Zertifikaten für Hostingumgebungen

7. Eingabekontrolle
7.1 Einführung von Benutzer- und Rollenkonzepten für interne Systeme
7.2 Einführung individueller Zugänge für interne Systeme
7.3 Verwendung personalisierter Logins im Unternehmensnetzwerk

8. Verfügbarkeitskontrolle
8.1 Ggfls. Nutzung einer Versionskontrolle GIT in der Entwicklung
8.2 Regelmäßige Aktualisierung der Virendefinitionen
8.3 Regelmäßige Durchführung von Datensicherungen
8.4 Regelmäßige Durchführung von Updates (Windows, Desktopanwendungen)
8.5 Verwendung einer Firewall (Debian Linux)
8.7 Verwendung eines Virenscanners (Avira)
8.8 Verwendung einer unterbrechungsfreien Stromversorgung für File- und Entwicklungsserver
8.9 Verwendung von RAID-Systemen für File- und Entwicklungsserver

9. Rasche Wiederherstellbarkeit
9.1 Tägliches Backup, redundant, gebäudlich getrennt
9.2 Ggfls. Nutzung einer Versionskontrolle GIT in der Entwicklung

10. Datenschutz-Managementsystem
10.1 Löschen nicht mehr benötigter Daten
10.2 Sichere Entsorgung defekter/nicht mehr benötigter Hardware
10.3 Sichere Entsorgung von Dokumenten (z. B. Aktenvernichter, Reisswolf)

11. Auftragskontrolle
11.1 Abschluss von AV-Verträgen mit Dienstleistern, Partnern und Kunden
11.2 Kommunikation von Verhaltensrichtlinien zum Thema Datenschutz an alle Mitarbeiter
11.3 Unterzeichnung einer Verschwiegenheitserklärung durch alle Mitarbeiter