

Auftragsdatenverarbeitungsbedingungen

in Geltung zwischen der

HEROLD Business Data GmbH

FN 233171 z

Guntramsdorfer Straße 105

A-2340 Mödling

(im Folgenden „*Auftragnehmer*“)

und der dem Nutzer von HEROLD-Dienstleistungen

(im Folgenden „*Auftraggeber*“)

1. Gegenstand, Art und Zweck der Verarbeitung

- 1.1 Der Auftraggeber beauftragt den Auftragnehmer jeweils auf Grundlage gesonderter Aufträge mit der Erbringung von Dienstleistungen gemäß Anhang ./1, bei deren Erbringung der Auftragnehmer personenbezogene Daten für den Auftraggeber verarbeitet (im Folgenden „*Auftragsdatenverarbeitung*“). Der Gegenstand der Auftragsdatenverarbeitung gibt sich aus dem jeweils gesondert an den Auftragnehmer erteilten Auftrag des Auftraggebers, auf den hier verwiesen wird, und dieser Auftragsdatenverarbeitungsvereinbarung (im Folgenden gemeinsam „*Leistungsvereinbarung*“).
- 1.2 Art und Zweck der Auftragsdatenverarbeitung durch den Auftragnehmer für den Auftraggeber sind in der Leistungsvereinbarung konkret beschrieben.

2. Dauer der Verarbeitung

- 2.1 Die Dauer des Auftrags zur Auftragsdatenverarbeitung (Laufzeit) entspricht der Dauer des jeweiligen gesondert erteilten Auftrages zur Erbringung von Dienstleistungen.

3. Art der Daten und Kategorien betroffener Personen

- 3.1 Die Art der verarbeiteten personenbezogenen Daten sind in der Leistungsvereinbarung sowie in Anhang /.1 konkret beschrieben. Die Kategorien der durch die Verarbeitung betroffenen Personen sind der Auftraggeber sowie allenfalls weitere in der Leistungsvereinbarung und in Anhang /.1 konkret beschriebene Personen.

4. Ort der Verarbeitung

- 4.1 Sofern die Erbringung der Auftragsdatenverarbeitung nicht in einem Mitgliedsstaat der EU /des EWR (im Folgenden „*Drittland*“) erfolgt, wird das angemessene Schutzniveau

im jeweiligen Drittland unter Berücksichtigung der besonderen Voraussetzungen der Art. 44 ff. DSGVO hergestellt und dem Auftraggeber vor Beginn der Auftragsdatenverarbeitung in diesem Drittland nachgewiesen.

5. Pflichten des Auftragnehmers

- 5.1 Der Auftragnehmer verpflichtet sich, die Auftragsdatenverarbeitung im Einklang mit den geltenden Datenschutzbestimmungen der EU und deren Mitgliedstaaten sowie ausschließlich im Rahmen der schriftlichen Aufträge und dokumentierten Weisungen des Auftraggebers vorzunehmen, sofern er nicht durch das Recht der EU oder deren Mitgliedstaaten hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese Anforderungen vor der Auftragsdatenverarbeitung mit, sofern eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses rechtlich untersagt ist. Erhält der Auftragnehmer einen behördlichen Auftrag, personenbezogene Daten des Auftraggebers herauszugeben, so hat er – sofern gesetzlich zulässig – den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.
- 5.2 Der Auftragnehmer erklärt, dass er alle mit der Auftragsdatenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Auftragsdatenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.
- 5.3 Der Auftragnehmer erklärt, alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen gemäß Anhang ./2 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 zu berücksichtigen. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.
- 5.4 Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen, sofern solche nur dem Auftragnehmer zur Verfügung stehen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet, lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen

Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

- 5.5 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).
- 5.6 Der Auftragnehmer ist nach Beendigung dieser Leistungsvereinbarung verpflichtet, alle personenbezogenen Daten des Auftraggebers zu löschen oder auf dessen dokumentierte Weisung zurück zu geben, sofern der Auftragnehmer gesetzlich nicht zur Speicherung solcher personenbezogenen Daten nach geltendem Recht der EU oder der Mitgliedstaaten verpflichtet ist.
- 5.7 Dem Auftraggeber wird hinsichtlich der Auftragsdatenverarbeitung der von ihm überlassenen personenbezogenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen des Auftragnehmers, sei es auch durch beauftragte Dritte, eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Auftragsdatenverarbeitungsvereinbarung und der in geltenden Datenschutzbestimmungen enthaltenen Verpflichtungen notwendig sind.
- 5.8 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen geltende Datenschutzbestimmungen der EU oder deren Mitgliedstaaten.
- 5.9 Der Auftragnehmer ist zur Bestellung eines Datenschutzbeauftragten verpflichtet, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Der Datenschutzbeauftragte und dessen jeweils aktuellen Kontaktdaten des sind auf der Website des Auftragnehmers leicht zugänglich hinterlegt.

6. Sub-Auftragsverarbeiter

- 6.1 Der Auftraggeber stimmt der Heranziehung auf <https://www.herold.at/cms/datenschutzerklaerung/#dienstleister> bezeichneten Sub-Auftragsverarbeiter durch den Auftragnehmer zu. Die Auslagerung auf weitere Sub-Auftragsverarbeiter oder der Wechsel des bestehenden Sub-Auftragsverarbeiter sind zulässig, soweit:
 - a) der Auftragnehmer eine solche Auslagerung auf Sub-Auftragsverarbeiter dem Auftraggeber eine angemessene Zeit durch Veröffentlichung auf <https://www.herold.at/cms/datenschutzerklaerung/#dienstleister> vorab anzeigt,

- b) der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der personenbezogenen Daten gegenüber dem Auftragnehmer schriftlich gegen die geplante Auslagerung erhebt, und
- c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis Abs. 4 DSGVO zugrunde gelegt wird.

6.2 Erbringt der Sub-Auftragsverarbeiter die vereinbarte Leistung außerhalb eines Mitgliedsstaates der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen gemäß Art. 44 ff. DSGVO sicher.

6.3 Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

Anhang /.1

Dienstleistung	Art der Daten und Kategorien von betroffenen Personen	Art und Zweck der Verarbeitung
Werbeeintragungen	Daten zur Gestaltung der Werbemittel, insbesondere Personenstammdaten (Firma, Vor- und Nachname, Anrede, Titel und Zustelladresse), Kommunikationsdaten (E-Mail-Adresse, Website, Telefax- und Telefonnummer), Öffnungszeiten, Fotos des Auftraggebers und von dessen Unternehmen.	Gestaltung und Verarbeitung von Werbeeintragungen.
Website und Online Shop	Daten zur Gestaltung der Website und des Online Shop, insbesondere Personenstammdaten (Firma, Vor- und Nachname, Anrede, Titel und Zustelladresse), Kommunikationsdaten (E-Mail-Adresse, Website, Telefax- und Telefonnummer), Öffnungszeiten, Fotos und Website-Texte des Auftraggebers und von dessen Unternehmen.	Gestaltung und Hosting der Websites und Online Shop.
Kundenzähler	Informationen zu eingehenden Anrufen, insbesondere anonymisierte Rufnummer des eingehenden Anrufers, geografische Zuweisung des eingehenden Anrufers, Anrufdatum und Anrufzeitpunkt, Anrufdauer.	Messungen und Auswertungen zu beauftragten Analysezwecken.
Bereitstellung Kontaktformular Website	Name und Kontaktdaten des Users der eine Nachricht schickt samt Freitext und Anfragentexte, die in ein Kontaktformular vom User eingegeben werden.	Speicherung und Übermittlung von Informationen an den Websitebetreiber.
Customer Reporting	Personenstammdaten (Firma, Vor- und Nachname, Anrede, Titel und Zustelladresse) und Kommunikationsdaten (E-Mail-Adresse, Website, Telefax- und Telefonnummer) des Auftraggebers und von dessen Unternehmen, Anzahl von Kontaktaufnahmen aufgrund einer Werbeleistung, Anzahl von Aufrufe der Detailseiten eines Werbeeintrages, Anzahl an Eintragungsinteraktionen der Werbeleistung auf www.herold.at, insbesondere Klicks auf Öffnungszeiten, Routenplanung, Kontaktdaten, etc., Anzahl von Suchanfragen, Angabe der häufigsten Suchbegriffe, Durchschnittliche Sternebewertung, Anzahl der Sternebewertungen, Informationen zur Öffnung des Report-E-Mails an den Kunden und über die Auswahl von Services auf der Reporting-Seite.	Verarbeitung von Daten und Bereitstellung auf der Reporting-Seite.
Online Complete	Unternehmensname, Kategorie / Branche, Adresse (Straße, PLZ, Ort, Bundesland), Kartenmarker (X/Y Koordinaten), Telefonnummer, Mein Highlight (Werbebotschaft), Unternehmensbeschreibung, Geschäftszeiten, Zusätzliche Infos zu den Geschäftszeiten, Geschäftszeiten an Feiertagen, Zahlungsmethoden, Kontakt-E-Mail-Adresse, Websites, iOS-App-URL, Android-App-URL, Geschäftslogo, Fotos, Youtube Video Verlinkung, Foursquare-Extra Verlinkung, Twitter-Handle, Instagram-Handle, Produkte und Services, Kalender, über uns Beschreibung, Speisekarten, Gründungsjahr, Produkte, Dienstleistungen, Spezialgebiete, Mitgliedschaften in Kammern u. Ä., geführte Marken, Sprachen, Stichwörter, Google-Coverfoto, Google-Profilfoto, Facebook-Coverfoto, Facebook-Profilbild, Facebook Call-to-Action, Link zum Start von Uber, Uber Link, Uber Fahrt-Branding, Info ob Unternehmen geschlossen wurde, weitere Stichwörter (Labels), Ladenkontakt, Foursquare Verlinkung, Google+ Verlinkung, Facebook Verlinkung, Google My Business Verlinkung, Kontaktinformationen, Benachrichtigungen bei Reviews	Veröffentlichung von Daten auf diversen Internet-Plattformen über einen Dienstleister.
Suchmaschinenwerbung	Daten zur Gestaltung, Auslieferung und Optimierung von Google AdWords Kampagnen; insbesondere Personenstammdaten (Firma, Vor- und Nachname, Anrede, Titel und Zustelladresse) und Kommunikationsdaten (E-Mail-Adresse, Website, Telefax- und Telefonnummer), Ansprechpersonen, Informationen zu Produkten und Dienstleistungen und Informationen zu Zielgruppen und Ausrichtung des Auftraggebers und von dessen Unternehmen.	Verwendung von Daten zum Zweck des Setups, der Auslieferung, der Optimierung sowie der Ergebnismessung von Google AdWords Kampagnen.

Facebook Marketing	Daten zur Gestaltung von Facebook Fanpages und Facebook Content Posts sowie zur Gestaltung, Auslieferung und Optimierung von Facebook Werbekampagnen; insbesondere Personenstammdaten (Firma, Vor- und Nachname, Anrede, Titel und Zustelladresse) und Kommunikationsdaten (E-Mail-Adresse, Website, Telefax- und Telefonnummer), Öffnungszeiten, Fotos, Videos, Website-Texte, Ansprechpersonen, Informationen zu Produkten und Dienstleistungen und Informationen zu Zielgruppen und Ausrichtung des Auftraggebers und von dessen Unternehmen.	Verwendung von Daten zum Aufsetzen von Facebook Fanpages, zum Kreieren und Veröffentlichen von Facebook Content Posts sowie zum Aufsetzen, zur Auslieferung, Optimierung und Messung von Facebook Werbekampagnen.
Erklärvideo	Daten zur Gestaltung des Erklärvideos, insbesondere Personenstammdaten (Firma, Vor- und Nachname, Anrede, Titel und Zustelladresse) und Kommunikationsdaten (E-Mail-Adresse, Website, Telefax- und Telefonnummer), Öffnungszeiten, Ansprechpersonen, Fotos, Videos, Musik, Stimmen, Texte, Informationen zu Produkten und Dienstleistungen und Informationen zu Zielgruppen und Ausrichtung des Auftraggebers und von dessen Unternehmen.	Erstellung und Ausspielung eines animierten Erklärvideos.
Firmenvideo	Daten zur Gestaltung des Firmenvideos, insbesondere Personenstammdaten (Firma, Vor- und Nachname, Anrede, Titel und Zustelladresse) und Kommunikationsdaten (E-Mail-Adresse, Website, Telefax- und Telefonnummer), Öffnungszeiten, Ansprechpersonen, Fotos, Videos, Musik, Stimmen, Texte, Informationen zu Produkten und Dienstleistungen und Informationen zu Zielgruppen und Ausrichtung des Auftraggebers und von dessen Unternehmen.	Erstellung und Ausspielung eines animierten Firmenvideos.
Ranking-Boost	Daten zur Gestaltung der Website und der Kampagne, insbesondere Personenstammdaten (Firma, Vor- und Nachname, Anrede, Titel und Zustelladresse) und Kommunikationsdaten (E-Mail-Adresse, Website, Telefax- und Telefonnummer), Öffnungszeiten, Ansprechpersonen, Fotos, Videos, Musik, Stimmen, Texte, Informationen zu Produkten und Dienstleistungen und Informationen zu Zielgruppen und Ausrichtung des Auftraggebers und von dessen Unternehmen.	Verwendung von Daten zum Zweck des Setups und der Umsetzung von Werbe-Kampagnen.
MDOonline und MDOoffline	Ermittlung des Nutzerverhaltens des Auftraggebers als Lizenznehmer von MDOonline Consumer und Business und MDOoffline (Feststellung der bereitgestellten Datensätze) sowie zur Gewährleistung der Datensicherheit.	Verwendung von Daten zu Abrechnungszwecken.
Online-Terminbuchungslösung	Firma, Adresse, E-Mail-Adresse, URL, Telefonnummer, Telefax, Personenstammdaten von Ansprechpersonen (Name, Anrede, E-Mail, Telefon), Instagram-Handle, Facebook Fanpage URL, Geschäftslogo, Fotos, Öffnungszeiten, Leistungen, Preise sowie Daten der Kunden des Auftraggebers, insbesondere Name, Adresse, Telefonnummer, E-Mail-Adresse, gegebenenfalls kundenspezifische Informationen zur Terminbuchung bzw. zu einem Vertragsabschluss.	Bereitstellung der Online-Terminbuchungslösung

Anhang ./2 – Technisch-organisatorische Maßnahmen

Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

- **Zutrittskontrolle**
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen: Chipkarten, Schlüssel, elektrische Türöffner, besetzter Empfangsbereich, Alarmanlage, Videoanlage;
- **Zugangskontrolle**
Keine unbefugte Systembenutzung: sichere Kennwörter und Passwortregelungen, automatische Sperrmechanismen, Verschlüsselung von Datenträgern, Firewall, Virenschutz, regelmäßige Sicherheitsupdates und Patches;
- **Zugriffskontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, VPN Technologie, Protokollierung von Zugriffen;
- **Trennungskontrolle**
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden: Mandantenfähigkeit, getrennte Datenbanken, Sandboxing.

2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

- **Weitergabekontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport: Verschlüsselung, Virtual Private Networks (VPN), Intrusion-Detection-System;
- **Eingabekontrolle**
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind: Protokollierung.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO)

- **Verfügbarkeitskontrolle**
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust: Backup-Strategie, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- **Rasche Wiederherstellbarkeit** (Art. 32 Abs. 1 lit. c) DSGVO): Disaster Recovery Plan.

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

- **Datenschutz-Management;**
- **Incident-Response-Management;**
- **Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DSGVO);
- **Auftragskontrolle**
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Kontrollrechte, Verpflichtung auf Datengeheimnis, Weisungsrecht.