

VEREINBARUNG

über eine

Auftragsverarbeitung nach Art 28 DSGVO gemäß dem Muster der WKO

Der Verantwortliche:

Der Auftragsverarbeiter:

x-files Druck,-Consulting-und
Produktionsagentur GmbH
Gewerbzeile 14
4040 Lichtenberg

(im Folgenden Auftraggeber)

(im Folgenden Auftragnehmer)

1. GEGENSTAND DER VEREINBARUNG

[1] Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben: Standardauftrag. Diese Vereinbarung ist als Ergänzung zu einem Standardauftrag zu verstehen.

[2] Folgende Datenkategorien werden verarbeitet: Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Entgelt Daten, usw.

[3] Folgende Kategorien betroffener Personen werden unterliegen der Verarbeitung: Kunden, Interessenten, Lieferanten, Ansprechpartner, Beschäftigte, usw.

2. DAUER DER VEREINBARUNG

Die Vereinbarung ist befristet abgeschlossen und endet mit dem in Verbindung stehenden Auftrag.

3. PFLICHTEN DES AUFTRAGNEHMERS

[1] Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des

Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

[2] Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

[3] Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage .1 zu entnehmen).

[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. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und 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] 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).

[6] Der Auftragnehmer wird darauf hingewiesen, dass er für die

vorliegende Auftragsverarbeitung ein Verzeichnis nach Art 30 DSGVO zu errichten hat.

[7] Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

[8] Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, die Daten bis zum Ende

der gesetzlichen oder vertraglichen Verpflichtungen zu Verfügung zu halten. Nach Ablauf dieser Fristen werden die Daten gelöscht.

[9] Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt

5. SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer kann Sub-Auftragsverarbeiter seines Vertrauens, jeder Zeit hinzuziehen.

Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

.....
[Ort], am [Datum]

Für den Auftraggeber:

.....
[Ort], am [Datum]

Für den Auftragnehmer:

.....
[Name samt Funktion]

.....
[Name samt Funktion]

ANLAGE ./1 –

TECHNISCH-ORGANISATORISCHE MASSNAHMEN

VERTRAULICHKEIT

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, Schlüssel, , usw.
- **Zugangskontrolle:** Schutz vor unbefugter Systembenutzung, Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, usw.
- **Zugriffskontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Standard-Berechtigungsprofile auf „need to know-Basis“, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten;
- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung [geheim/vertraulich/intern/öffentlich].

INTEGRITÄT

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

VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle:** Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall; Security Checks auf Infrastruktur-

- und Applikationsebene, Mehrstufiges Sicherungskonzept, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
- Rasche **Wiederherstellbarkeit;**

VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters, Vorabüberzeugungspflicht, Nachkontrollen.