**Beispiel Auftragsverarbeiterverzeichnis Direktmarketing**

1. **Stammblatt des Auftragsverarbeiters**
2. **Name und Kontaktdaten des Auftragsverarbeiters/der Auftragsverarbeiter**
	1. **Name und Anschrift:** Kreativ GmbH, Müllerstraße 1a 1040 Wien
	2. **E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie zB Tel.Nr.):**

Max Müller, 0043 664 123 45 67

* 1. **Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Datenschutzbeauftragten des Auftragsverarbeiters[[1]](#footnote-1):**
1. **Stammblatt zum Verantwortlichen, in dessen Namen Daten verarbeitet werden, und Angaben zur Auftragsdatenverarbeitung**
2. **Name und Kontaktdaten des (der) für die Verarbeitung (gemeinsam) Verantwortlichen (=Auftraggeber)**
	1. **Name(n) und Anschrift(en): XXX Möbel GmbH, Funderstraße 4, 1020 Wien**
	2. **E-Mail-Adresse(n) (und allenfalls weitere Kontaktdaten wie zB Tel.Nr.): DI Reinhard Gruber, GF der XXX Möbel GmbH**
	3. **Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Datenschutzbeauftragten:1**
	4. **Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Vertreters des (der) Verantwortlichen:[[2]](#footnote-2)**
3. **Kategorien von Verarbeitungen, die im Auftrag des konkreten Verantwortlichen durchgeführt werden**

Versand des XXX Möbel GmbH Newsletter, Direct Marketing Zusendungen an Bonuscard-Kunden

1. **Übermittlung von personenbezogenen Daten in Drittländer, inkl. internationale Organisationen**
	1. Ja 🞎 Nein

Wenn ja, Angabe des betreffenden Drittlandes bzw. der internationalen Organisation:

* 1. Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Abs 1 Unterabsatz 1 DSGVO erfolgt (vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Binding Corporate Rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt):[[3]](#footnote-3)
1. **Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen**
* **Vertraulichkeit (Pseudonymisierung und Verschlüsselung)[[4]](#footnote-4):**

Der Zugang zum Rechenzentrum sowie anderen sicherheitskritischen Bereichen ist geregelt und nur befugten Personen möglich. Alle Systeme sind vor unbefugter Systembenutzung zumindest durch Einsatz von Passwörtern, im Regelfall aber durch Zwei-Faktor-Authentifizierung geschützt. Festplatten der Endgeräte (PC, Notebooks) sind zusätzlich verschlüsselt. Allen Benutzern steht einerseits ein persönliches Laufwerk, das nur von diesen selbst einsehbar ist, sowie zusätzliche Serverlaufwerke, die nur berechtigten und authentifizierten anderen Benutzern zugänglich sind, zur Verfügung.

* **Integrität [[5]](#footnote-5):**

Die Integrität verarbeiteter Daten wird einerseits durch die vorhandenen Berechtigungssysteme, andererseits durchgeregelte Testmethoden vor Implementierung neuer Anwendungen sichergestellt. Zusätzlich kommen technische Maßnahmen wie Transportverschlüsselung, durchgehender Einsatz von VPN-Verbindungen und flächendeckender Einsatz von Virenschutzprogrammen zum Einsatz. Soweit aufgrund des Schutzbedarfs der Daten notwendig und technisch umsetzbar, werden Protokollierungsmaßnahmen eingesetzt.

* **Verfügbarkeit und Belastbarkeit:**

Der Sicherstellung der Verfügbarkeit erfolgt über das zentrale Monitoring der kritischen Systeme mit Hilfe automatisierter Lösungen. Zur Wiederherstellung der Funktionsfähigkeit sind umfassende Datensicherungen sowie Wiederherstellungsdokumentationen verfügbar.

* **Periodische Evaluierung:**

Es erfolgen regelmäßige Checks, gegebenenfalls auch externe Audits der eingesetzten Sicherheitsmaßnahmen. Zumindest jährlich werden die Sicherheitsstandards überprüft und aktualisiert.

* **Awareness und Benutzerschulungen:**

Die angemessene Information der BenutzerInnen wird einerseits durch das IT-Sicherheitshandbuch für MitarbeiterInnen, andererseits durch entsprechende Kurse und Veranstaltungen zu Sicherheit und Datenschutzsichergestellt. Eine umfassende Auflistung der Sicherheitsvorkehrungen ist dem Dokument „IT Security Standard“ zu entnehmen.

1. Sofern ein Datenschutzbeauftragter verpflichtend oder auf freiwilliger Basis bestellt wurde.
**HINWEIS:** Wenn keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht, der Verantwortliche aber freiwillig einen bestellen möchte, müssen trotzdem alle den Datenschutzbeauftragten betreffenden Bestimmungen der DSGVO eingehalten werden; möchte man das nicht, darf die bestellte Person nicht „*Datenschutzbeauftragter*“ genannt werden, sondern sollte eine andere Bezeichnung gewählt werden (zB „*Datenschutzkoordinator*“). Dieser kann, muss aber nicht ins Verarbeitungsverzeichnis aufgenommen werden. Siehe dazu das WKO-Merkblatt [„Datenschutzbeauftragter“](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Der-Datenschutzbeauftragt.html). [↑](#footnote-ref-1)
2. Darunter sind Vertreter von nicht in der EU niedergelassenen Verantwortlichen zu verstehen. [↑](#footnote-ref-2)
3. Siehe das Merkblatt der WKO [„Internationalen Datenverkehr“](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Internationaler-Datenverk.html). [↑](#footnote-ref-3)
4. Verhinderung von (unbeabsichtigter) Offenlegung oder unbefugten Zugang zu personenbezogenen Daten. [↑](#footnote-ref-4)
5. Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten. [↑](#footnote-ref-5)