**Beispiel für ein Verarbeitungsverzeichnis: Newsletter-Versand, Publikationen und Veranstaltungseinladungen (alles Online) für das eigene Unternehmen**

1. **Angaben zum Verantwortlichen**

|  |  |  |  |
| --- | --- | --- | --- |
| Verantwortlicher: | Kreativ GmbH, Müllerstraße 1a 1040 Wien | Vertreter: |  |
| Kontakt | Max Müller | Kontakt |  |
| Tel.-Nr. | +43 123 456 78 | Tel.-Nr. |  |
| Mobil-Nr. |  | Mobil-Nr. |  |
| Fax |  | Fax |  |
| E-Mail |  | E-Mail |  |
| Für die Verarbeitung zuständige Organisationseinheit: | Kreativ GmbH, Marketing-Abteilung |  |  |

|  |  |
| --- | --- |
| Datenschutzbeauftragter (DSBA): |  |
| Tel.-Nr. |  |
| Mobil.-Nr. |  |
| Fax |  |
| E-Mail |  |

**Auftragsverarbeiter:**

|  |  |
| --- | --- |
| Auftragsverarbeiter 1: | Muster IT-Solution |
| Kontakt | Ing. Werner Müller |
| Tel.-Nr. |  |
| Mobil.-Nr. |  |
| Fax |  |
| E-Mail |  |

**Auftragsverarbeiter 2: Sonstige Auftragsverarbeiter für Adressierung und Zustellung**

|  |  |
| --- | --- |
| Auftragsverarbeiter: |  |
| Kontakt |  |
| Tel.-Nr. |  |
| Mobil.-Nr. |  |
| Fax |  |
| E-Mail |  |



Datenschutz- Folgenabschätzung: Nicht erforderlich für dieses Verfahren

Wurde durchgeführt

1. **Zweckbestimmung und Rechtsgrundlagen**

Zweckbestimmung: Versand von Newslettern, Publikationen und Einladungen zu Veranstaltungen einschließlich des Führens von Anwesenheitslisten und Korrespondenzen, Gewinnspiele, Werbeauftritte durch Verwendung von Kunden- und Interessentendaten für die eigene Geschäftsanbahnung

Rechtsgrundlage(n): Art. 6 Abs. 1 lit. a DSGVO (Rechtmäßigkeit der Verarbeitung)

1. **Personengruppen (Kategorien betroffener Personen)**

|  |  |  |
| --- | --- | --- |
| Nr. | Personengruppe | Anmerkung |
| 10 | Kunden |  |
| 20 | Interessenten |  |
| 30 | Lieferanten |  |
| 40 | Besucher der Website/Webshop |  |

1. **Kategorien von Empfängern, an die personenbezogene Daten weitergegeben werden, speziell bei Empfängern in Drittländern sowie Art und Herkunft empfangener Daten (inkl. Auftragsverarbeitung)**

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Empfängerkategorie | Kürzel | Rechtsgrundlage für Datenübermittlung |
| 1 | Muster IT-Solution (Hoster für Homepage/Webshop, Online-Tracking-Anbieter) | DL | Art. 28 DSGVO iVm DL-Vereinbarung Muster IT-Solution |
| 2 | Sonstige Auftrags-verarbeiter für Adressierung und Zustellung | DL | Art. 28 DSGVO iVm DL-Vereinbarung mit jew. Auftragsverarbeiter |
| 3 | Werbeunternehmen/Event-Veranstalter | DL | Art. 28 DSGVO iVm DL-Vereinbarung mit jew. Auftragsverarbeiter |

1. **Übermittlung an Empfängern in Drittländern**

Es findet keine Übermittlung in ein Drittland statt.

1. **Datenkategorien**

**10 Kunden**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Datenkategorie | Bes. Kat | Straf. Rel. | Datenherkunft | Aufbew.-  dauer | Empfänger |
| 10 | Name |  |  | int | Ende | 1, 2, 3 |
| 20 | Geschlecht |  |  | int | Ende | 1, 2, 3 |
| 30 | Funktion im Unternehmen oder Behörde |  |  | int | Ende | 1 |
| 40 | Unternehmen, Behörde, etc. |  |  | int | Ende | 1, 2 |
| 50 | Spezifische Fach- und Interessengebiete |  |  | int | Ende | 1 |
| 60 | Adresse |  |  | int | Ende | 1, 2, 3 |
| 70 | Elektronische Kontaktdaten /Tel., Fax, E-Mail-Adresse) |  |  | int | Ende | 1 |
| 80 | Erhaltene Newsletter, Publikationen oder Einladungen |  |  | int | Ende | 1 |
| 90 | Vermerke zu Zu-/Absagen sowie Anwesenheiten bei Veranstaltungen |  |  | int | Ende | 1, 3 |
| 100 | Korrespondenzen |  |  | int | Ende | 1 |

**20 Interessenten**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Datenkategorie | Bes. Kat | Straf. Rel. | Datenherkunft | Aufbew.-  dauer | Empfänger |
| 10 | Name |  |  | selbst | Wid | 1, 2, 3 |
| 20 | Geschlecht |  |  | selbst | Wid | 1, 2, 3 |
| 30 | Spezifische Fach- und Interessengebiete |  |  | selbst | Wid | 1 |
| 40 | Adresse |  |  | selbst | Wid | 1, 2, 3 |
| 50 | Elektronische Kontaktdaten /Tel., Fax, E-Mail-Adresse) |  |  | selbst | Wid | 1 |
| 60 | Vermerke zu Einwilligung oder Abbestellung |  |  | selbst | Wid | 1 |
| 70 | Erhaltene Newsletter, Publikationen oder Einladungen |  |  | selbst | Wid | 1 |
| 80 | Vermerke zu Zu-/Absagen sowie Anwesenheiten bei Veranstaltungen |  |  | selbst | Wid | 1, 3 |
| 90 | Korrespondenzen |  |  | selbst | Wid | 1 |

1. **Technisch-organisatorische Maßnahmen**

**7.1 Allgemeine sicherheitsrelevante Informationen**

**Zertifizierungen:** Zertifizierung des IT-Betreibers (Muster IT-Solution) nach ISO/IEC 27001:2013

**Betroffene Assets:** Basisdienst Client-Betrieb / Basisdienst Dateiservices / Media Standard - E-Mail Marketing (mailworx)

**Risikoanalyse durchgeführt:**

Unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der geprüften Datenanwendung sind ausreichende technische und organisatorische Maßnahmen ergriffen worden, um die Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten und damit die Rechte und Freiheiten der betroffenen Personen im erforderlichen Ausmaß sicherzustellen.

**Allgemeine Maßnahmen:**

* **Vertraulichkeit:**  
  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:**

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.

**7.2 Asset-spezifische Maßnahmen**

|  |  |
| --- | --- |
| Asset | Maßnahmen/Information |
| Basisdienst Client-Betrieb | MS Office-Anwendungen  Absicherung über Zugriffsberechtigungen des Dateisystems |
| Basisdienst Dateiservices | Zugriff nur für Berechtigte möglich |
| Media Standard - E-Mail Marketing (mailworx) | Zugriff nur für Berechtigte möglich |

1. **Review**

Die Kreativ GmbH als Verantwortliche veranlasst jeweils jährlich die Evaluierung und Aktualisierung des Datenverarbeitungsverzeichnisses.

1. **Beschreibung der Abkürzungen**

**10.1 Aufbewahrungsdauer**

|  |  |
| --- | --- |
| Kürzel | Beschreibung |
| 72h | 72 Stunden |
| 4w | 4 Wochen |
| 3m | 3 Monate |
| 6m | 6 Monate |
| 1y | 1 Jahr |
| 3y | 3 Jahre |
| 5y | 5 Jahre |
| 7y | Aufgrund der gesetzlichen Aufbewahrungsfristen auf jeden Fall 7 Jahre; darüberhinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen. |
| 10y | 10 Jahre |
| 30y | 30 Jahre |
| 65y | 65 Jahre |
| var | variabel nach jew. ges. Fristen |
| Wid | Widerruf der Einwilligung |
| WidSp | Widerspruch |
| Ende | bis zur Beendigung der Geschäftsbeziehungen |
| Unb | Unbegrenzt |

**10.2 Herkunft der Daten**

|  |  |
| --- | --- |
| Kürzel | Beschreibung |
| selbst | Selbstauskunft des Betroffenen |
| öff | Öffentlich verfügbare Daten |
| int | Interne Erhebung |
| ext | Von Dritten erhaltene Daten |