**Beispiel für ein Verarbeitungsverzeichnis Rechnungswesen und Logistik**

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, Buchhaltung |  |  |

|  |  |
| --- | --- |
| 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 |  |

Datenschutz- Folgenabschätzung: Nicht erforderlich für dieses Verfahren

Wurde durchgeführt

1. **Zweckbestimmung und Rechtsgrundlagen**

Zweckbestimmung: Verarbeitung und Übermittlung von Daten im Rahmen einer Geschäftsbeziehung mit Kunden und Lieferanten, einschließlich

automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Rechtsgrundlage(n): Art. 6 Abs. 1 lit. b, c, f DSGVO (Rechtmäßigkeit der Verarbeitung); § 132 BAO (Aufbewahrungsfristen)

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

|  |  |  |
| --- | --- | --- |
| Nr.  | Personengruppe | Anmerkung  |
| 10 | Kunden/Lieferanten | - |
| 20 | Dritte | An der Geschäftsabwicklung mitwirkende Dritte |
| 30 | Kontaktperson | Kontaktpersonen beim Kunden, Lieferanten oder Dritten |

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 | Banken zur Abwicklung des Zahlungsverkehrs | Extern  | Art. 6 Abs. 1 lit. b DSGVO |
| 2 | Rechtsvertreter im Geschäftsfall | Extern | Art. 6 Abs. 1 lit. f DSGVO |
| 3 | Wirtschaftstreuhänder für Zwecke des Auditing  | Extern | Art. 6 Abs. 1 lit. f DSGVO |
| 4 | Gerichte | Extern | Art. 6 Abs. 1 lit. f DSGVO |
| 5 | Zuständige Verwaltungs-behörden, insb. Finanzbehörden | Extern | Art. 6 Abs. 1 lit. c DSGVO |
| 6 | Vertrags- oder Geschäftspartner, die an der Lieferung oder Leistung mitwirken bzw. mitwirken soll | Extern | Art. 6 Abs. 1 lit. b DSGVO |
| 7 | Versicherungen aus Anlass des Abschlusses eines Versicherungsvertrages über die Lieferung/ Leistung oder des Eintritts des Versicherungsfalles  | Extern | Art. 6 Abs. 1 lit. b DSGVO |
| 8 | Bundesanstalt „Statistik Österreich“ für die Erstellung der gesetzlich vorgeschriebenen (amtlichen) Statistiken | Extern | Art. 6 Abs. 1 lit. c DSGVO |
| 9 | - |  |  |
| 10 | Kunden (Empfänger von Leistungen) | Extern | Art. 6 Abs. 1 lit. b DSGVO |
| 11 | Muster IT-Solution  | DL | Art. 28 DSGVO iVm AV-Vereinbarung  |

1. **Übermittlung an Empfängern in Drittländern**

Es findet keine Übermittlung in ein Drittland statt.

1. **Datenkategorien**

**10 Kunden/Lieferanten**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Datenkategorie | Bes. Kat | Straf. Rel. | Datenherkunft | Aufbew.-dauer | Empfänger |
| 10 | Name |  |  | selbst  | 7y | 1-9, 11 |
| 20 | Geschlecht |  |  | selbst | 7y | 1-9, 11 |
| 30 | Geburtsdatum  |  |  | selbst | 7y | 1-9, 11 |
| 40 | Kontaktperson beim Kunden, Lieferanten oder Dritten |  |  | selbst | 7y | 1-9, 11 |
| 50 | Anschrift |  |  | selbst | 7y | 1-9, 11 |
| 60 | Elektronische Kontaktdaten (E-Mail, Telefon, Fax, …) |  |  | selbst | 7y | 1-9, 11 |
| 70 | Firmenbuchdaten  |  |  | selbst | 7y | 1-9, 11 |
| 80 | Bankverbindungen |  |  | selbst | 7y | 1-7, 9, 11 |
| 90 | Kreditkartennummern und – unternehmen  |  |  | selbst | 7y | 1-4, 11 |
| 100 | Daten zur Bonität  |  |  | int | Ende | 1-9, 11 |
| 110 | Daten zum Zahlung- oder Leistungsverhalten des Betroffenen |  |  | int | 7y | 1-4, 6,9, 11 |
| 120 | Daten zum Kreditmanagement (z.B. Kreditlimit, Wechsellimit) |  |  | int | 7y | 1-4, 11 |
| 130 | Sperrkennzeichen (z.B. Kontaktsperre, Rechnungs-sperre, Liefersperre, Buchungssperre, Zahlungssperre) |  |  | int | 7y | 1-4, 6,9, 11 |
| 140 | Zuordnung zu einer bestimmten Kunden- und Lieferantenkategorie (einschließlich regionale Zuordnung, usw.) |  |  | int | 7y | 3, 9 , 11 |
| 150 | Kenn-Nummern für Zwecke amtlicher Statistik  |  |  | selbst | 7y | 1-9, 11 |
| 160 | Gegenstand der Lieferung oder Leistung  |  |  | int | 7y | 1-9, 11 |
| 170 | Konditionen (Lieferung, Leistung, Finanzierungs- und Zahlungsbedingen) |  |  | int | 7y | 1-9, 11 |
| 180 | Bonus-, Provisionsdaten und dgl.  |  |  | int | 7y | 1-5, 9, 11 |
| 190 | Daten zur Steuerpflicht und Steuerberechnung  |  |  | int | 7y | 2-3, 5-6, 9, 11 |
| 200 | Leistungsspezifische Aufwände und Erträge  |  |  | int | 7y | 1-6, 11 |
| 210 | Konto- und Belegdaten  |  |  | int | 7y | 1-7, 9, 11 |
| 220 | Sonderhauptbuchvorgänge (z.B. Einzelwert-berechtigung, Wechselforderung, Anzahlung, Bankgarantie) |  |  | int | 7y | 3, 5, 11 |
| 230 | Mahndaten/Klagsdaten |  |  | int | Ende | 1-5, 9, 11 |
| 240 | Bei der Leistungserbringung mitwirkende Dritte einschließlich Angaben über die Art der Mitwirkung |  |  | int | 7y | 1-9, 11 |

**20 Dritte (An der Geschäftsabwicklung mitwirkende Dritte)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Datenkategorie | Bes. Kat | Straf. Rel. | Daten-herkunft | Aufbew.-dauer | Empfänger |
| 10 | Name |  |  | selbst | 7y | 1-11 |
| 20 | Geschlecht |  |  | selbst | 7y | 1-11 |
| 30 | Geburtsdatum  |  |  | selbst | 7y | 1-11 |
| 40 | Kontaktperson beim Kunden, Lieferanten oder Dritten |  |  | selbst | 7y | 1-11 |
| 50 | Anschrift |  |  | selbst | 7y | 1-11 |
| 60 | Elektronische Kontaktdaten (E-Mail, Telefon, Fax, …) |  |  | selbst | 7y | 1-11 |
| 70 | Firmenbuchdaten  |  |  | selbst | 7y | 1-11 |
| 80 | Bankverbindung  |  |  | selbst | 7y | 1-7, 11 |
| 90 | Kreditkartennummern und –unternehmen  |  |  | selbst | 7y | 1-4, 6, 11 |
| 100 | Daten zur Bonität  |  |  | int | Ende | 3, 11 |
| 110 | Daten zum Zahlungs- oder Leistungsverhalten des Betroffenen |  |  | int | 7y | 1-4, 6, 10-11 |
| 120 | Daten zum Kreditmanagement (z.B. Kreditlimit, Wechsellimit) |  |  | int | 7y | 1-4, 11 |
| 130 | Sperrkennzeichen (z.B. Kontaktsperre, Rechnungs-sperre, Liefersperre, Buchungssperre, Zahlungssperre) |  |  | int | 7y | 1-4, 6, 9, 11 |
| 140 | Zuordnung zu einer bestimmten Kunden- und Lieferantenkategorie (einschließlich regionale Zuordnung, usw.) |  |  | int | 7y | 3, 9-11 |
| 150 | Kenn-Nummern für Zwecke amtlicher Statistik  |  |  | selbst | 7y | 1-11 |
| 160 | Gegenstand der Lieferung oder Leistung  |  |  | int | 7y | 1-11 |
| 170 | Konditionen (Lieferung, Leistung, Finanzierungs- und Zahlungsbedingen) |  |  | int | 7y | 1-11 |
| 180 | Bonus-, Provisionsdaten und dgl.  |  |  | int | 7y | 1-5, 9, 11 |
| 190 | Daten zur Steuerpflicht und Steuerberechnung  |  |  | int | 7y | 2-3, 5-6, 11 |
| 200 | Leistungsspezifische Aufwände und Erträge  |  |  | int | 7y | 1-6, 11 |
| 210 | Konto- und Belegdaten  |  |  | int | 7y | 1-7, 11 |
| 220 | Sonderhauptbuchvorgänge (z.B. Einzelwert-berichtigung, Wechselforderung, Anzahlung, Bankgarantie  |  |  | int | 7y | 3, 5, 11 |
| 230 | Mahndaten/Klagsdaten  |  |  | int | Ende | 1-5, 11 |

**30 Kontaktpersonen (Kontaktpersonen beim Kunden, Lieferanten oder Dritten)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Datenkategorie | Bes. Kat | Straf. Rel. | Datenherkunft | Aufbew.-dauer | Empfänger |
| 10 | Name |  |  | selbst  | 7y | 1-11 |
| 20 | Funktionstitel, Unternehmens-funktion  |  |  | selbst | 7y | 1-11 |
| 30 | Geschlecht |  |  | selbst | 7y | 1-11 |
| 40 | Zugehöriger Kunde, Lieferant oder Dritter |  |  | selbst | 7y | 1-11 |
| 50 | Zusätzliche Daten zur Adressierung (zu Handen…) |  |  | selbst | 7y | 1-11 |
| 60 | Elektronische Kontaktdaten (E-Mail, Telefon, Fax, …) |  |  | selbst | 7y | 1-11 |
| 70 | Umfang der Vertretungsbefugnis  |  |  | selbst | 7y | 1-11 |
| 80 | Vom Betroffenen bearbeitete Geschäftsfälle  |  |  | selbst | 7y | 1-11 |

1. **Technisch-organisatorische Maßnahmen**

**7.1 Allgemeine sicherheitsrelevante Informationen**

**Zertifizierungen:** Zertifizierung des IT-Betreibers nach ISO/IEC 27001:2013

**Betroffene Assets:** Basisdienst Client-Betrieb / Basisdienst Dateiservices / SAP
Finanzbuchhaltung

**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-AnwendungenAbsicherung über Zugriffsberechtigungen des Dateisystems; ; Zugriff nur für Berechtigte möglich |
| Basisdienst Dateiservices | Absicherung über Zugriffsberechtigungen des Mail- und Dateisystems; ; Zugriff nur für Berechtigte möglich |
| SAP Finanzbuchhaltung | Absicherung über Zugriffsberechtigungen der Buchhaltungsanwendungen; 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 |