Muster GmbH, Geschäftsführer: Max Mustermann, Musterstr. 123, 12345 Musterhausen

**Muster Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche**

– Vorblatt –

|  |  |
| --- | --- |
| **Angaben zum Verantwortlichen** |  |
| Name bzw. Unternehmensbezeichnung inkl. Rechtsformzusatz |  |
| ggf. vertretungsberechtigte Person des Unternehmens (z.B. GmbH-Geschäftsführer): |  |
| Anschrift: |  |
| Telefonnr.: |  |
| Faxnr.: |  |
| E-Mail-Adresse: |  |
|  |  |
| **Angaben zum Datenschutzbeauftragten (DSB):**  [falls vorhanden, sonst löschen] | [**Hinweis:** Eine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht, wenn sich mehr als 10 Mitarbeiter im Unternehmen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.] |
| Vor- und Nachname: |  |
| Anschrift: |  |
| Telefonnr.: |  |
| E-Mail-Adresse: |  |
| interner oder externer DSB? | 🞏 intern oder 🞏 extern |

– Verarbeitungstätigkeiten –

[**Hinweis:** Es sind alle Geschäftsabläufe / Prozesse zu beschreiben, mit denen personenbezogene Daten von Kunden, Mitarbeitern, Geschäftspartnern etc. verarbeitet werden. Je Prozess ist ein separates Formblatt nach dem folgenden Muster anzulegen.]

|  |  |
| --- | --- |
| Datum der Anlegung: xx.yy.zzzz | Datum der letzten Änderung: xx.yy.zzz |
|  |  |
| Beschreibung der Verarbeitungstätigkeit: | z.B.: Finanzbuchhaltung |
| Zweck der Verarbeitungstätigkeit: | z.B.:  - Durchführung der Finanzbuchhaltung  - Umsetzung der gesetzlichen Vorgaben (GoBD) |
| Kategorien betroffener Personen: | 🞏 Beschäftigte  🞏 Kunden  🞏 Interessenten  🞏 Lieferanten  🞏 Anwalt  🞏 Steuerberater  🞏 Kreditoren  🞏 Debitoren  🞏 … |
| Kategorien personenbezogener Daten: | 🞏 Name  🞏 Adressdaten  🞏 Kontaktdaten  🞏 Bankverbindung  🞏 Geburtsdatum  🞏 Kfz-Kennzeichen  🞏 Interessentendaten  🞏 Beschäftigtendaten  🞏 Lieferantendaten  🞏 Kundendaten  🞏 Buchungsdaten  🞏 Daten Mahnwesen  🞏 Saldenlisten  🞏 Bilanzen  🞏 … |
| Kategorien besonderer personenbezogener Daten: | 🞏 rassische oder ethnische Herkunft  🞏 politische Ansichten  🞏 religiöse oder weltanschauliche Überzeugungen  🞏 Gewerkschaftszugehörigkeit  🞏 genetische Daten  🞏 biometrische Daten  🞏 Gesundheitsdaten  🞏 Daten zu Sexualleben / sexuelle Orientierung |
| Kategorien von Empfängern der personenbezogenen Daten: | 🞏 intern: z.B. Buchhaltung, Geschäftsführung  🞏 extern: z.B. Finanzbehörden, Sozialversicherungen, Krankenversicherungen, Zahlungsdienstleister (Hausbank) |
| Übermittlung der Daten an Dritte: | 🞏 findet nicht statt und ist auch nicht geplant  🞏 findet statt, und zwar  🞏 an: … [Name des Empfängers]  🞏 innerhalb Deutschlands  🞏 innerhalb der EU / EWR  🞏 in ein Drittland: … [Name des Landes]  🞏 an eine internationale Organisation: … [Name der Organisation]  🞏 Angabe geeigneter Garantien (bei Übermittlung an Drittland oder internationale Organisation): … |
| Fristen zur Löschung der versch. Datenkategorien: | 🞏 6 Jahre gem. Handelsrecht  🞏 8 Jahre gem. Handelsrecht  🞏 10 Jahre gem. Steuerrecht  🞏 30 Jahre gem. Sozialrecht  🞏 6 Monate für Unterlagen abgelehnter Bewerber gem. AGG  🞏 30 Jahre bei vollstreckbaren Titeln (Urteile, Vollstreckungsbescheide o.ä.)  🞏 30 Tage gem. Bundesmeldegesetz  🞏 2 Jahre wegen Gewährleistungsvorschriften  🞏 … |
| Beschreibung der technischen und organisatorischen Maßnahmen (TOM): | s. Anhang am Ende dieses Dokuments (ab S. 7) |
| **Hinweis:** Alle Angaben bis zu dieser Stelle sind **zwingend vorzunehmen** (auch die Beschreibung der technischen und organisatorischen Maßnahmen (TOM) am Ende dieses Dokuments). Die nachfolgenden Angaben können Sie dagegen **optional** erfassen. Dies kann beispielsweise sinnvoll sein, um konkrete Anfragen von Behörden oder Kunden schnell beantworten zu können. | |
| Rechtsgrundlage für die Verarbeitungstätigkeit: | 🞏 Erfüllung eines Vertrages (Erteilung eines Auftrags, Bestellung im Webshop…)  🞏 Durchführung vorvertraglicher Maßnahmen (Übersendung eines Angebots an Interessenten…)  🞏 Einwilligung (Zustimmungserklärung des Betroffenen)  🞏 Einwilligung dokumentiert  🞏 Erfüllung einer rechtlichen Verpflichtung (Aufbewahrungsfrist gem. Steuerrecht…)  🞏 Schutz lebenswichtiger Interessen (Behandlung von Schwerverletzten im Krankenhaus…)  🞏 Interessenabwägung (postalische Direktwerbung, Verhinderung von Betrug…)  🞏 … |
| Rechtsgrundlage für die Verarbeitung von besonderen personenbezogenen Daten: | 🞏 Einwilligung (Zustimmungserklärung des Betroffenen)  🞏 Einwilligung dokumentiert  🞏 aufgrund Arbeitsrecht / Sozialrecht (Daten von Beschäftigten…)  🞏 Schutz lebenswichtiger Interessen (Behandlung von Schwerverletzten im Krankenhaus…)  🞏 Mitglieder von Organisationen ohne Gewinnerzielungsabsicht (Daten von Mitgliedern gemeinnütziger Organisationen…)  🞏 vom Betroffenen offensichtlich öffentlich gemachte Daten (Daten von öffentlich zugänglichem Facebook-Profil des Betroffenen…)  🞏 Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Durchführung eines Schadensersatzprozesses…)  🞏 erhebliches öffentliches Interesse (Informationen der öffentlichen Verwaltung…)  🞏 Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin (medizinische Forschung, Qualitätskontrolle im Medizinbereich, Amtsarzt…)  🞏 öffentliches Interesse im Bereich der öffentlichen Gesundheit (Krankenversicherung…)  🞏 Archivzwecke / wissenschaftliche oder historische Forschungszwecke / statistische Zwecke (Bundesamt für Statistik, Bundesarchiv, sonstige behördliche Archive…) |
| Dokumentation allg. Informationspflicht: | 🞏 Datenschutzhinweise bei Erstkontakt übermittelt, und zwar  🞏 per E-Mail (PDF-Anhang)  🞏 per Website-Link  🞏 telefonisch  🞏 persönlich  🞏 Datenschutzhinweise bei Einholung der Einwilligung erteilt  🞏 Beschäftigte erhalten Datenschutzhinweise zusammen mit Arbeitsvertag |
| Dokumentation Prozess Auskunftsanfragen: | Betroffene Personen erhalten auf Anfrage Auskunft über die im Unternehmen verarbeiteten personenbezogenen Daten sowie folgende Informationen:  - Zwecke der Verarbeitung  - Kategorien personenbezogener Daten  - Empfänger oder Kategorien von Empfängern  - geplante Speicherdauer (falls möglich) oder Kriterien für Festlegung der Speicherdauer der personenbezogenen Daten  - Recht auf Berichtigung, Löschung, Widerspruch, Einschränkung der Verarbeitung und Beschwerde bei zuständiger Aufsichtsbehörde  - Herkunft der Daten (soweit diese nicht direkt bei der betroffenen Person erhoben wurden)  - ggf. Infos über Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und ggf. aussagekräftige Infos über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person  Ein entsprechender Prozess ist installiert und dokumentiert, es existiert eine Vorlage für ein entsprechendes Auskunftsschreiben. |
| Umsetzung Grundsatz Speicherbegrenzung: | Die Daten der betroffenen Personen werden nur so lange gespeichert, wie dies zur Erfüllung des Zwecks des jeweiligen Datenverarbeitungsvorgangs erforderlich ist und soweit der Löschung keine gesetzlichen Aufbewahrungsfristen entgegenstehen. |
| Auftragsverarbeiter (AV): | 🞏 es werden keine AV eingesetzt  🞏 im Rahmen dieser Verarbeitungstätigkeit werden folgende AV eingesetzt:  - Dienstleister A (AV-Vertrag besteht)  - Dienstleister B (AV-Vertrag besteht)  - Dienstleister C (kein AV-Vertrag erforderlich, da keine Weisungsgebundenheit aufgrund des Berufsrechts von C)  … |
| Konkrete Maßnahmen zur Sicherheit dieser Verarbeitungstätigkeit: | 🞏 TOMs (s. Anhang)  🞏 zusätzlich werden bei dieser Verarbeitungstätigkeit folgende Maßnahmen umgesetzt:  - Original-Papierakten in Safe  - Backup-Datenträger in Safe  - Kommunikation ausschließlich über zertifizierte und verschlüsselte E-Mails (s. Vereinbarung vom …)  - Datenzugriff über gesondertes Berechtigungskonzept  … |
| Dokumentation Prozess Datenpannen: | Der Prozess für die Reaktion auf etwaige Datenschutzverletzungen ist installiert und dokumentiert, insbesondere kennen alle beteiligten Personen im Unternehmen die gesetzlich vorgesehenen Reaktionsfristen.  Es existiert eine Vorlage für ein entsprechendes Info-Schreiben an die Aufsichtsbehörde bzw. an die Betroffenen.  In jedem Fall werden die Geschäftsführung und der System-Administrator [**optional:** „sowie der Datenschutzbeauftragte“] so schnell wie möglich nach Erkennen der Datenschutzverletzung über diese informiert. Sodann werden alle wesentlichen Informationen über die Datenschutzverletzung gesammelt und analysiert. Anschließend werden die erforderlichen Informationen für eine evtl. Benachrichtigung der Aufsichtsbehörde bzw. der betroffenen Personen zusammengestellt. Besteht ein konkretes Risiko für Betroffene, dann wird die zuständige Aufsichtsbehörde unverzüglich, aber spätestens binnen 72 Std. informiert. Bei einem voraussichtlich hohen Risiko werden die von der Datenschutzverletzung betroffenen Personen unverzüglich darüber informiert. |
| Datenschutz-Folgenabschätzung (DSFA): | 🞏 keine DSFA erforderlich, da Verarbeitungstätigkeit auf „Whitelist“ der Aufsichtsbehörden  🞏 keine DSFA erforderlich aus sonstigen Gründen: … [z.B. „kein hohes Risiko“ etc.]  🞏 DSFA erforderlich, da Verarbeitungstätigkeit auf „Blacklist“ der Aufsichtsbehörden  🞏 DSFA erforderlich wegen  🞏 Verwendung neuer Technologien  🞏 voraussichtlich hohem Risiko durch Art, Umfang, Umstand oder Zweck der Verarbeitung  🞏 DSFA dokumentiert |
| Dokumentation Sensibilisierung / Unterrichtung der Beschäftigten: | Alle Beschäftigten erhalten zu Beginn ihrer Tätigkeit im Unternehmen zusammen mit ihrem Arbeitsvertrag ein Info-Blatt zum Datenschutz. Außerdem müssen sie eine Verpflichtungserklärung zur Vertraulichkeit unterzeichnen.  Für alle Beschäftigten erfolgt eine Unterweisung bzgl. der Grundlagen des Datenschutzes durch eine entsprechende Arbeitsanweisung [**alternativ:** „durch den Datenschutzbeauftragten“, „durch einen externen Referenten“, „mittels Software“, „mittels E-Learning“, „mittels allen Beschäftigten zur Verfügung stehender Fachliteratur“ etc.].  Es finden regelmäßig (mind. 2x jährlich) Meetings mit allen Beschäftigten statt, in denen u.a. auch Infos bzgl. des Datenschutzes erfolgen. Die Teilnahme der Beschäftigten an diesen Meetings wird durch ihre Unterschrift unter dem Meeting-Protokoll dokumentiert. |

**Anhang zum Verarbeitungsverzeichnis – TOM**

[**Hinweis:** Die nachfolgend exemplarisch angeführten Maßnahmen in der rechten Tabellenspalte sind an die Bedingungen im eigenen Unternehmen anzupassen. Nicht vorhandene Maßnahmen sind daher zu löschen, fehlende ggf. zu ergänzen, bestehende Maßnahmen können – falls erforderlich – auch mit Anmerkungen versehen werden.]

**1. Gewährleistung der Vertraulichkeit**

[**Hinweis:** Es soll durch geeignete Maßnahmen sichergestellt werden, dass personenbezogene Daten nur einem bestimmten Empfängerkreis zugänglich sind, wie z.B. Verpflichtungserklärungen zur Vertraulichkeit seitens der Mitarbeiter, Verschlüsselung, Passwortregeln, Kontrollmaßnahmen, Zertifizierung o.ä.]

|  |  |
| --- | --- |
| Zutrittskontrolle:  (Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.) | - Alarmanlage  - mechanische Fenstersicherungen  - Absicherung von Gebäudeschächten  - Schließsystem mit Codesperre (PIN-Code, Fingerabdruck etc.)  - manuelles Schließsystem  - Schließsystem mit Sicherheitsschlössern  - Videoüberwachung  - Bewegungsmelder  - Schlüsselregelung Beschäftigte  - Personenkontrolle am Empfang  - Tragepflicht von Berechtigungsausweisen (Besucher, Wartungsdienst…)  - Verschließen der Türen bei Abwesenheit  … |
| Zugangskontrolle:  (Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.) | - Erstellen von Benutzerprofilen mit unterschiedlichen Berechtigungen  - Pflicht zur Passwortnutzung  - Authentifikation durch biometrische Verfahren (Fingerabdruck, Irisscan…)  - Authentifikation durch Benutzername und Passwort  - Verriegelungen an Rechnergehäusen  - Einsatz von VPN-Technologie bei Zugriff von außen auf die internen Systeme  - Sperren von externen Schnittstellen (USB, CD-Rom…)  - Einsatz von Intrusion-Detection-Systemen  - Begrenzung der Fehlversuche bei Anmeldung am System  … |
| Zugriffskontrolle:  (Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.) | - Nutzer-Berechtigungskonzept  - Verwaltung der Nutzerrechte durch Systemadministrator  - Anzahl der Administratoren auf das Notwendigste reduziert  - Verwenden einer Passwortrichtlinie  - Protokollierung von Zugriffen auf Anwendungen  - physische Löschung von Datenträgern vor Wiederverwendung  - ordnungsgemäße Vernichtung von Datenträgern  - Einsatz von Aktenvernichtern  - Inanspruchnahme von Dienstleistern zur Aktenvernichtung (inkl. Protokollierung der Vernichtung)  - Aufbewahrung von Datenträgern in abschließbaren Schränken  - Aufbewahrung von Aktenordnern in abschließbaren Schränken  … |
| Trennungsgebot:  (Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.) | - physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern  - logische Mandantentrennung  - Datensätze mit Zweckattributen/Datenfeldern  - Trennung der Zuordnungsdaten und der eigentlichen Daten auf einem getrennten System bei Pseudonymisierung  - Festlegung von Datenbankrechten durch Vorgaben im Berechtigungskonzept  - Trennung von Produktiv- und Testsystem  … |
| Auftragskontrolle:  (Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.) | - sorgfältige Auswahl des Auftragnehmers (Überprüfung des Dienstleisters)  - vorherige Prüfung und Dokumentation der beim Auftragnehmer existierenden TOMs  - schriftliche Vereinbarung mit dem Auftragnehmer  - Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit  - Datenschutzbeauftragter beim Auftragnehmer  - Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags  - vertraglich festgelegte Kontrollrechte gegenüber dem Auftragnehmer  - regelmäßige Überprüfung des Auftragnehmers und seiner Tätigkeiten  - vertraglich festgelegte Vertragsstrafen bei Verstößen  … |
| Pseudonymisierung: | - Nutzung von pseudonymisierten Daten bei Datenübermittlung an externe Dienstleister  … |
| Verschlüsselung: | - Datenträgerverschlüsselung unter Windows 10 mittels Bitlocker  - Nutzung von hardwareseitig verschlüsselten USB-Festplatten  … |
| Zertifizierung (z.B. ISO): | … |

**2. Gewährleistung der Integrität**

[**Hinweis:** Es soll durch geeignete Maßnahmen sichergestellt werden, dass die Korrektheit von personenbezogenen Daten und die korrekte Funktionsweise von Systemen gewährleistet wird, etwa durch Zugriffsbeschränkungen, Fehleranalyse o.ä.]

|  |  |
| --- | --- |
| Eingabekontrolle:  (Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.) | - Protokollierung der Eingabe, Änderung und Löschung von Daten im System  - individuelle Benutzernamen für Nutzer  - sichere Aufbewahrung von Papierunterlagen, von denen Daten ins EDV-System übernommen wurden  - Nachvollziehbarkeit durch Berechtigungskonzept  … |
| Weitergabekontrolle:  (Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.) | - Nutzung von Standleitungen bzw. VPN-Tunneln  - Weitergabe von Daten in anonymisierter oder pseudonymisierter Form (wenn möglich)  - verschlüsselte E-Mail-Übertragung (SSL/TLS)  - Verschlüsselung E-Mail-Inhalte (Software-Zertifikat)  - vertraglich vereinbarte Rechte und Pflichten in Bezug auf die Datenweitergabe  - festgelegte Löschfristen  - sichere Transportverpackungen  - sorgfältige Auswahl von Transportpersonal bzw. -dienstleistern  - Nutzung von mobilen Datenträgern mit Verschlüsselungsfunktion  - Regelungen zum sicheren Transport von Datenträgern  … |

**3. Gewährleistung der Verfügbarkeit**

[**Hinweis:** Es soll durch geeignete Maßnahmen sichergestellt werden, dass EDV-Systeme die an sie gestellten Anforderungen zuverlässig erfüllen. Dazu gehören Infrastrukturmaßnahmen, System-Wartung, Datensicherung o.ä.]

|  |  |
| --- | --- |
| Verfügbarkeitskontrolle:  (Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.) | - unterbrechungsfreie Stromversorgung (USV), zumindest für Server  - Alarmanlage im Serverraum  - Klimaanlage in Serverräumen  - Überwachung von Temperatur und Feuchtigkeit in Serverräumen  - Schutzsteckdosenleisten für EDV-Geräte  - Feuer- bzw. Rauchmeldeanlagen  - Feuerlöschgeräte an mehreren, entsprechend gekennzeichneten Stellen im Gebäude  - Datensicherungs-Konzept  - regelmäßiges Testen der Funktionsweise der Datensicherung  - Notfallkonzept  - Aufbewahrung von Datensicherung an sicherem, ausgelagertem Ort  - Serverräume nicht unterhalb von sanitären Anlagen gelegen  - keine Wasserleitungen in Serverräumen bzw. über den Server-Rechnern  - Serverräume nicht in Hochwasser gefährdeten Kellerräumen  … |

**4. Gewährleistung der Belastbarkeit der Systeme**

[**Hinweis:** Durch geeignete Maßnahmen soll die Belastbarkeit der EDV-Systeme sichergestellt werden, so dass diese etwaige Software-Mängel, eine erhöhte Anzahl von Anfragen, Viren und sonstige Malware, Hackerangriffe etc. abwehren können. Entsprechende Maßnahmen sind etwa die Nutzung von Firewalls, Virenscannern, Intrusion-Detection-Systemen o.ä.]

|  |  |
| --- | --- |
| Belastbarkeit der IT-Systeme: | - Antiviren-Software  - Hardware-Firewall  - Software-Firewall  - Intrusion-Detection-System  - sorgfältige Auswahl des externen IT-Dienstleisters  … |

**5. Wiederherstellung der Verfügbarkeit**

[**Hinweis:** Es soll durch geeignete Maßnahmen sichergestellt werden, dass nach einem Systemfehler oder -ausfall die Funktionsfähigkeit der Systeme so schnell wie möglich wiederhergestellt werden kann. Geeignete Maßnahmen wären hierfür zuständige Systembetreuer, ausreichende Hard- und Software o.ä.]

|  |  |
| --- | --- |
| Wiederherstellbarkeit von IT-Systemen: | - sorgfältig ausgewählter interner System-Administrator  - Vorhaltung von Ersatz-Hardware / Server  - Vorhaltung von Ersatz-Hardware / Arbeitsplätze  - sorgfältig ausgewählter IT-Dienstleister  … |

**6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM**

[**Hinweis:** Es soll durch geeignete Maßnahmen sichergestellt werden, dass der Stand der Informations-Sicherheit regelmäßig geprüft, aktualisiert und dies auch dokumentiert wird.]

|  |  |
| --- | --- |
| Informations-Sicherheits-Management-System (ISMS): | - regelmäßige Prüfung der TOM (mind. 2x jährlich) durch Geschäftsführer und System-Administrator [falls vorhanden] zusammen mit Datenschutzbeauftragten [falls vorhanden]  - Einsatz einer ISMS-Software  - elektronisches Datenschutz-Handbuch mit Vorgaben zu regelmäßigen Prüfintervallen (ggf. eingebunden in vorhandenes Dokumenten-Management-System)  … |

**Wichtiger Hinweis:** Bei diesem Muster handelt es sich um eine Orientierungs- und Arbeitshilfe zur DSGVO. Für die Bearbeitung und den Inhalt der von Ihnen ausgefüllten Vorlage können wir keine Verantwortung übernehmen. Falls Sie Fragen zur Bearbeitung der Vorlage haben, wenden Sie sich bitte an einen Rechtsanwalt oder eine entsprechend berechtigte Person.