Quelle: Ehmann/Kranig, Erste Hilfe zur Datenschutzgrundverordnung, herausgegeben vom Bayrischen Landesamt für Datenschutzaufsicht, S. 14ff.

Muster 1: Inhalt eines Verzeichnisses von Verarbeitungstätigkeiten

Dieses Muster besteht aus einem **Vorblatt** und einer oder mehrerer **Anlagen** und (empfohlenerweise) je Anlage einer **Ergänzung zur Anlage.**

Verzeichnis von Verarbeitungstätigkeiten als Verantwortlicher gem. Art. 30 Abs. 1 DS-GVO	**Vorblatt**
Angaben zum Verantwortlichen Name und Kontaktdaten der natürlichen Person/juristischen Person/Behörde/Einrichtung etc. Name Ansprechpartner Straße Postleitzahl Ort Telefon E-Mail-Adresse Internet-Adresse	
Angaben zur Person des Datenschutzbeauftragten Anrede Titel Name, Vorname Straße Postleitzahl Ort Telefon E-Mail-Adresse	

Bezeichnung der Verarbeitungstätigkeit (Mindestinhalt)	**Anlage**
Datum der Anlegung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse	
Bezeichnung der Verarbeitungstätigkeit	
Zwecke der Verarbeitung	
Beschreibung der Kategorien betroffener Personen	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ Sonstige:
Beschreibung der Datenkategorien	☐ *(z. B.: Adressdaten, Geburtsdatum, Bankverbindung, Steuermerkmale, Lohngruppe, Arbeitszeit, bisherige Tätigkeitsbereiche, Qualifikationen etc.)* Besondere Arten personenbezogener Daten: ☐ *(z. B.: Religionszugehörigkeit, Krankmeldungen, gesundheitliche Beeinträchtigungen)*
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch werden	☐ intern Abteilung/ Funktion
	☐ extern Empfängerkategorie

Bezeichnung der Verarbeitungstätigkeit (Mindestinhalt)	Anlage
Datenübermittlung an Dritte	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt: ☐ Drittland, und zwar: (Name des Drittlandes)
Nennung der konkreten Datenempfänger	Empfängerkategorie
Fristen für die Löschung der verschiedenen Datenkategorien	
Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DS-GVO Bemerkungen: *siehe TOM-Beschreibung*	
..... Verantwortlicher	..... Datum ..... Unterschrift

Das folgende Muster stellt eine **Ergänzung der Anlage** für den Mindestinhalt dar. Um insbesondere die gesetzliche Verpflichtung erfüllen zu können, jederzeit die Zulässigkeit der eigenen Datenverarbeitung nachweisen zu können, empfiehlt es sich, auch die Daten, die in dieser Ergänzung zur Anlage angesprochen sind, auszufüllen.

Bezeichnung der Verarbeitungstätigkeit (empfohlene Ergänzung)	Ergänzung der Anlage
Rechtsgrundlage der Verarbeitung	
Dokumentation, dass Einwilligung erteilt wurde	
Dokumentation, dass Verarbeitung für Betroffenen transparent erfolgt	
Dokumentation, dass Informationspflichten eingehalten werden	
Dokumentation, dass Datenschutz durch Technik eingehalten wird	
Dokumentation des Prozesses für Auskunft, Berichtigung und Löschung	
Umsetzung Speicherbegrenzung	
Umsetzung der Sicherheit der Verarbeitung	
Auflistung aller Auftragsverarbeiter (inkl. internationaler Datentransfer mit Rechtsgrundlagen)	
Umgang mit Datenschutzverletzungen	
Darstellung der Meldepflicht an Aufsichtsbehörden	
Risikobewertung/Datenschutzfolgeabschätzung	
Dokumentation von Awareness-Maßnahmen	

Um Ihnen ein Gefühl dafür zu geben, wie so ein Verzeichnis ausgefüllt werden könnte und sollte, haben wir im Folgenden das o.g. **Muster** für ein **fiktives** produzierendes **Unternehmen** mit 50 Beschäftigten ausgefüllt.

BEISPIEL FÜR EIN AUSGEFÜLLTES MUSTER

Verzeichnis von Verarbeitungstätigkeiten als Verantwortlicher gem. Art. 30 Abs. 1 DS-GVO	**Vorblatt**
Angaben zum Verantwortlichen Name und Kontaktdaten der natürlichen Person/juristischen Person/Behörde/Einrichtung etc.	
Name	Fa. Mülltonnenproduktion GmbH & Co KG
Ansprechpartner	Max Müllmann, Geschäftsführer
Straße	Hauptstr. 1
Postleitzahl 12345	Ort Berlin
Telefon	030 – 1234567-0
E-Mail-Adresse	info@muelltonnenproduktion.de
Internet-Adresse	www.muelltonnenproduktion.de
Angaben zur Person des Datenschutzbeauftragten	
Anrede	Frau Titel
Name, Vorname	Meier Maria
Straße	Hauptstr. 1
Postleitzahl 12345	Ort Berlin
Telefon	030 – 1234567-80
E-Mail-Adresse	dsb@muelltonnenproduktion.de

Bezeichnung der Verarbeitungstätigkeit (Mindestinhalt)	**Anlage**
Datum der Anlegung: 25.05.2018	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse	Personalabteilung Huber, Klaus 030 – 1234567-70 klaus.huber@muelltonnenproduktion.de
Bezeichnung der Verarbeitungstätigkeit	Personalverwaltung
Zwecke der Verarbeitung	Durchführung des Beschäftigungsverhältnisses, Erfüllung vertraglicher und gesetzlicher Pflichten ggü. Beschäftigten
Beschreibung der Kategorien betroffener Personen	☒ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ Sonstige:
Beschreibung der Datenkategorien	☒ Adressdaten, Geburtsdatum, Bankverbindung Besondere Arten personenbezogener Daten: ☒ Religionszugehörigkeit, Krankmeldungen

Bezeichnung der Verarbeitungstätigkeit (Mindestinhalt)	Anlage
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch werden	☒ intern Personalabteilung
	☒ extern öffentliche Stellen: Sozialversicherungsträger, Finanzbehörden
Datenübermittlung an Dritte:	☒ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt: ☐ Drittland, und zwar (Name des Drittlands)
Nennung der konkreten Datenempfänger	Lohn- und Steuerbüro „Hinter-Ziehung GmbH“
Fristen für die Löschung der verschiedenen Datenkategorien	10 Jahre nach Ausscheiden der/des Beschäftigten
Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DS-GVO Bemerkungen: *siehe TOM-Beschreibung (muss einzelfallbezogen konkretisiert werden)*	
..... Verantwortlicher	..... Datum ..... Unterschrift

BEISPIEL FÜR DIE EMPFOHLENE ERGÄNZUNG DER ANLAGE FÜR DEN MINDESTINHALT

Bezeichnung der Verarbeitungstätigkeit (empfohlene Ergänzung)	Ergänzung zur Anlage
Rechtsgrundlage der Verarbeitung	Art. 88 DS-GVO und § 26 BDSG-neu
Dokumentation, dass Einwilligung erteilt wurde	–
Dokumentation, dass Verarbeitung für Betroffenen transparent erfolgt	Den Beschäftigten wird ein Hinweisblatt zum Umgang mit den sie betreffenden Daten ausgeteilt. Es handelt sich dabei um Daten, die im Rahmen der Bewerbung, zur Durchführung und dann auch zur Beendigung des Beschäftigungsverhältnisses erfasst werden. Dokumentation ist abgelegt unter: *Benennung Referenzdokumentation*

Bezeichnung der Verarbeitungstätigkeit (empfohlene Ergänzung)	Ergänzung zur Anlage
Dokumentation, dass Informationspflichten eingehalten werden	Die Beschäftigten erhalten bei Einstellung ein Informationsblatt (abgelegt unter: *Benennung Referenzdokumentation*) zu: • Name und Kontakt des Verantwortlichen (s. o.) • Kontakt der Datenschutzbeauftragten (s. o.) • Zweck und Rechtsgrundlage der Datenerhebung (s. o.) • Empfänger der Daten (Lohn- und Steuerbüro) • Speicherdauer • Rechte des Beschäftigten auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch und Datenübertragbarkeit • Beschwerderecht bei einer Aufsichtsbehörde • gesetzlich vorgeschriebene Bereitstellung der Daten • Tatsache, dass keine automatisierte Entscheidungsfindung stattfindet
Dokumentation, dass Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen eingehalten wird	Datenschutz durch Technikgestaltung wird eingehalten durch folgende Maßnahmen: • Es ist ein Ablauf festgelegt, der sicherstellt, dass bei der Herausgabe von Handys an die Mitarbeiter die GPS-Funktion regelmäßig deaktiviert ist. • Im Bereich der internen IT wird sichergestellt, dass Protokolle, die personenbezogene Daten loggen, sofort nach Erfüllung ihres Zwecks gelöscht werden. Die Daten werden in einem separaten Speicherbereich abgelegt, auf den nur Mitarbeiter der Personalabteilung zugreifen können. Dokumentation ist abgelegt unter: *Benennung Referenzdokumentation*
Dokumentation des Prozesses für Auskunft, Berichtigung und Löschung	Beschäftigte erhalten auf Anfrage Auskunft über ihre im Unternehmen verarbeiteten personenbezogenen Daten sowie folgende Informationen: • Zweck der Verarbeitung (für das Verfahren s. o.) • Kategorien der personenbezogenen Daten (s. o.) • Empfänger der Daten (Personalabteilung, Auftragsverarbeiter) • Speicherdauer • Recht auf Berichtigung und Löschung • Beschwerderecht bei einer Aufsichtsbehörde • Herkunft der Daten (sofern diese nicht direkt beim Beschäftigten erhoben wurden) Intern zuständig ist Leitung der Personalabteilung, evtl. mit Unterstützung der IT-Abteilung. Dokumentation ist abgelegt unter: *Benennung Referenzdokumentation*

Bezeichnung der Verarbeitungstätigkeit (empfohlene Ergänzung)	Ergänzung zur Anlage
Umsetzung Speicherbegrenzung	Die Daten der Beschäftigten werden nur so lange gespeichert, wie es zur Erfüllung der Verarbeitungstätigkeit erforderlich ist. Die geltenden handels- und steuerrechtlichen Aufbewahrungspflichten für Personaldaten werden eingehalten. Bei Einstellung werden Bewerbungsunterlagen, die für die Durchführung des Beschäftigungsverhältnisses nicht mehr erforderlich sind (z. B. Bewerbungsanschreiben, Zeugnisse) unwiderruflich gelöscht bzw. der Person zurückgegeben Dokumentation ist abgelegt unter: *Benennung Referenzdokumentation*
Umsetzung der Sicherheit der Verarbeitung	Umsetzung der Sicherheit erfolgt u. a. durch: • Personalakten befinden sich in einem verschlossenen Schrank in der Personalabteilung. Die Schlüssel haben nur Mitarbeiter aus der Personalabteilung. • Versand von ausschließlich verschlüsselten E-Mails zur Kommunikation • Trennung des Laufwerks der Personalabteilung vom übrigen Unternehmensnetzwerk • Zugriff auf Personalakten über gesondertes Berechtigungskonzept – statt Klarnamen der Beschäftigten werden Personal-Kennziffern zur Pseudonymisierung verwendet Dokumentation ist abgelegt unter: *Benennung Referenzdokumentation*
Auflistung aller Auftragsverarbeiter (inkl. internationaler Datentransfer mit Rechtsgrundlagen)	Folgende Auftragsverarbeiter werden hier eingesetzt: • Lohn- und Steuerbüro „Hinter-Ziehung GmbH“ Vertrag mit Auftragsverarbeiter ist abgelegt unter: *Benennung Referenzdokumentation*
Umgang mit Datenschutzverletzungen	Bei Datenschutzverletzungen tritt zunächst die interne Meldekette in Kraft: • Information an Leitung der Personalabteilung, Geschäftsleitung und Datenschutzbeauftragte • Je nach Schwere der Verletzung des Schutzes personenbezogener Daten erfolgt ggf. Meldung an die Aufsichtsbehörde.

Bezeichnung der Verarbeitungstätigkeit (empfohlene Ergänzung)	Ergänzung zur Anlage
Darstellung der Meldepflicht an Aufsichtsbehörde	Bei Verletzung des Schutzes personenbezogener Daten startet die interne Meldekette: • Information an Leitung der Personalabteilung, Geschäftsführung, Datenschutzbeauftrage • Zusammenstellen der erforderlichen Informationen und Einschätzung, ob eine Meldung an die Aufsichtsbehörde erforderlich ist • Kommunikation an Aufsichtsbehörde geschieht unverzüglich und möglichst binnen 72 Stunden. Sofern 72 Stunden nicht einzuhalten sind, ist der Meldung eine Begründung für die Verzögerung beizufügen. • Die Meldung an die Aufsichtsbehörde erfolgt in Form eines in Abstimmung mit der Geschäftsführung, der Personalleitung und Datenschutzbeauftragten ausgefüllten Meldebogens inkl. aller erforderlichen Informationen gemäß Art. 33 DS-GVO. Vorlage des Meldebogens ist abgelegt unter: *Benennung Meldebogen*
Risikobewertung/Datenschutz-Folgenabschätzung	Keine Datenschutz-Folgenabschätzung erforderlich, da weder Verwendung neuer Technologien noch Art, Umstand oder Zweck der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Beschäftigten zur Folge hat.
Dokumentation von Sensibilisierungsmaßnahmen	Innerbetriebliche Sensibilisierungsmaßnahmen zum Datenschutz und zur entsprechenden Sensibilisierung erfolgen durch regelmäßige Aushänge zum Thema durch die Datenschutzbeauftragte, Beschäftigtenschulungen und thematische Newsletter. Die Sensibilisierungsmaßnahmen sind abgelegt unter: *Benennung Referenzdokumentation*

4. Kapitel. Grundsätze für die Verarbeitung personenbezogener Daten

1. Verbot mit Erlaubnisvorbehalt

Im Datenschutzrecht gilt das sog. Prinzip des „Verbots mit Erlaubnisvorbehalt". Das bedeutet, dass niemand mit personenbezogenen Daten von anderen umgehen, d.h. Daten erheben, speichern oder weitergeben darf, wenn er nicht über eine ausdrückliche Einwilligung (siehe Definition 6) der betroffenen Person verfügt oder aber sich auf eine Rechtsgrundlage berufen kann, die ihm erlaubt oder sogar anordnet, mit den Daten umzugehen. Wenn man danach Daten verarbeiten darf, muss sichergestellt sein, dass dabei insbesondere die Zweckbindung, Richtigkeit und Erforderlichkeit beachtet werden und nicht zuletzt darüber Rechenschaft abgelegt werden kann. Die Bedeutung dieser Grundsätze wird im Folgenden näher erklärt.

DEFINITION 6:

Einwilligung ist jede freiwillig, für einen bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

2. Rechtmäßigkeit

Die Verarbeitung personenbezogener Daten ist nach Art. 6 Abs. 1 DS-GVO nur rechtmäßig, wenn die betroffene Person eine Einwilligung erteilt hat, die Verarbeitung für die Erfüllung eines Vertrages oder einer rechtlichen Verpflichtung erforderlich ist oder, was in der Praxis die größte Bedeutung haben wird, die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen der betroffenen Person überwiegen.

Wichtig ist, dass jeder, der mit personenbezogenen Daten umgehen möchte, vorher prüft, ob er eine Rechtsgrundlage hat, auf die er sich berufen kann. Eine Verarbeitung ohne Rechtsgrundlage ist unzulässig und kann zu hohen Bußgeldern führen.

a) Einwilligung

Eine Einwilligung (und damit die Möglichkeit auf dieser Basis Daten zu verarbeiten) ist nur dann wirksam, wenn

- sie freiwillig (d.h. ohne Zwang oder Druck – schwierig z.B. im Arbeitsverhältnis) abgegeben wird,
- sie für einen bestimmten Fall abgegeben wird (d.h. Einwilligung zur Datenverarbeitung zu allen heute und in Zukunft relevanten Zwecken wäre unbestimmt und ungültig),
- die betroffene Person klar und verständlich informiert wurde (wer die Einwilligung haben möchte, muss klar und deutlich sagen, für welchen konkreten Zweck die Daten verarbeitet werden sollen),
- die betroffene Person darüber informiert wurde, dass sie die Einwilligung jederzeit widerrufen kann (ohne dass sie einen Grund angeben muss) und
- die Einwilligung schließlich durch eine eindeutig bestätigende Handlung erfolgt ist (z.B. schriftliche Erklärung, Ankreuzen einer Erklärung im Internet [sog. opt-in]; Achtung: Das „Stehenlassen" eines bereits vorangehakten Kästchens im Internet [sog. opt-out] reicht nicht).

Einwilligungen sind im Interesse des Datenschutzes sicher die beste Variante, da der, der sie haben möchte, die betroffene Person klar und deutlich informieren muss, keinen Druck ausüben darf und die betroffene Person deshalb im besten Fall gut informiert und völlig freiwillig der Datenverarbeitung zustimmt. Wegen des jederzeitigen Rechts auf Widerruf und des Aufwands, das Vorliegen der konkreten Einwilligung nachweisen zu können, versuchen viele, ihre Verarbeitung eher auf eine andere Rechtsgrundlage zu stützen.

b) Vertragserfüllung

Personenbezogene Daten, die zur Erfüllung eines Vertrages notwendig sind, dürfen verarbeitet werden. Wenn jemand ein Auto kauft, darf der Käufer z.B. Namen, Kontaktdaten und Bankverbindung des Verkäufers erhalten. Und der Verkäufer wiederum darf natürlich Name, Anschrift – und bei Ratenkauf auch (die z.B. über die Schufa eingeholte) Bonität – des Käufers erheben und verarbeiten.