Mittelstand 4.0
Kompetenzzentrum
Planen und Bauen

Das Verzeichnis von Verarbeitungstätigkeiten

Ein Bauplan gemäß Artikel 30 DS-GVO

Mittelstand-Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Verzeichnis von Verarbeitungstätigkeiten

Betriebe, in denen personenbezogene Daten verarbeitet werden, müssen gem. Art. 30 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ein Verzeichnis von Verarbeitungstätigkeiten führen. Der Inhalt dieses Verzeichnisses ist in der Norm im Einzelnen angegeben.

Das nachfolgend wiedergegebene Muster basiert auf verschiedenen anderen Mustern, wie sie unter anderem von dem Bayerischen Landesamt für Datenschutzaufsicht veröffentlicht wurden. Es soll eine erste Orientierung bieten, um das Verzeichnis als zentrales Element des betrieblichen Datenschutzmanagements führen und einsetzen zu können. Durch eine überlegte Vorgehensweise lassen sich Effizienzgewinne im Ressourceneinsatz ebenso wie eine signifikante Senkung von Risiken erreichen.

1	Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertretwortlichen sowie ggf. seines Vertreters:	Adam und Eva GmbH In den Gärten 1 88145 Paradies Geschäftsführer: Adam Erstermann	2 Name und Kontaktdaten des betrieblichen Datenschutzbeauftragten:	Josef Zimmermann, Ges. für Datenschutz mbH In den Gärten 2 88145 Paradies Tel.: +49 1234 5678 E-Mail: dsb@paradies.de
5	Kategorien von Empfängern, denen die Daten offengelegt worden sind bzw. werden sowie Empfänger in Drittstaaten:	Steuerberater, Sozialversicherungsträger, Finanzamt, Berufsgenossenschaft, Hausbank, Hosting-Dienstleister und Software as a Service-Anbieter.	6 Übermittlung in Drittstaaten:	Übermittlungen in Drittstaaten finden ausschließlich im Rahmen der Arbeitsvorbereitung und Ausführung von Aufträgen in der Schweiz statt.

9 Name der Datenverarbeitung	10 Zwecke der Datenverarbeitung	11 Rechtsgrundlage	12 Beschreibung der Verarbeitung	13 Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DS-GVO	14 Betroffene bzw. betroffene Personengruppen	15 Personenbezogene Daten bzw. Datenkategorien	16 Empfänger bzw. Empfängerkategorien
Lohnabrechnung	Auszahlung der Löhne Abfuhr von Sozialabgaben und Steuern	Art. 6 Abs. 1 lit. c) und Art. 28 DS-GVO § 147 AO § 157 HGB $ 4 Abs. 2, 2a LStDV		ja	Mitarbeiter	Name, Vorname Geburtsdatum, -ort Bankverbindung Lohn-/Entgeltdaten Religionszugehörigkeit Sozialversicherungsdaten Steuerdaten, insbes. Berufsgenossenschaft	Steuerberater Hausbank Sozialversicherungsträger Finanzamt
Personalverwaltung	Personaladministration Personalführung Arbeitszeitverwaltung Personalbeschaffung	Art. 6 Abs. 1 lit. a), b), c) und f) sowie Art. 88 DS-GVO § 26 BDSG [3] 7 Abs. 7 ArbZeitG		nein	Mitarbeiter Auszubildene Bewerber	Name, Vorname, Anschrift(en) Zeitwirtschaftsdaten Daten zur Arbeitsleistung Leistungsbeurteilung Lebenslauf	keine

Zwar ist in Art. 30 Abs. 5 der Datenschutz-Grundverordnung eine Ausnahme von der Pflicht zum Führen eines solchen Verzeichnisses vorgesehen, diese gilt jedoch nur dann, wenn keine besonderen Kategorien personenbezogener Daten wie z.B. Gesundheitsdaten und Religionszugehörigkeit verarbeitet werden. Solche Informationen liegen dem typischen Betrieb aber regelmäßig in Form des Kirchensteuermerkmals und den Arbeitsunfähigkeitsbescheinigungen im Krankheitsfall vor.

Damit hat praktisch jeder Betrieb, der mindestens einen Beschäftigten führt – folglich auch die Ein-Mann-GmbH – ein solches Verzeichnis zu führen. Das Verzeichnis ist als internes Verzeichnis zu führen, d.h. es muss im Falle einer Kontrolle durch die zuständige Datenschutz-Aufsichtsbehörde vorgelegt werden können.

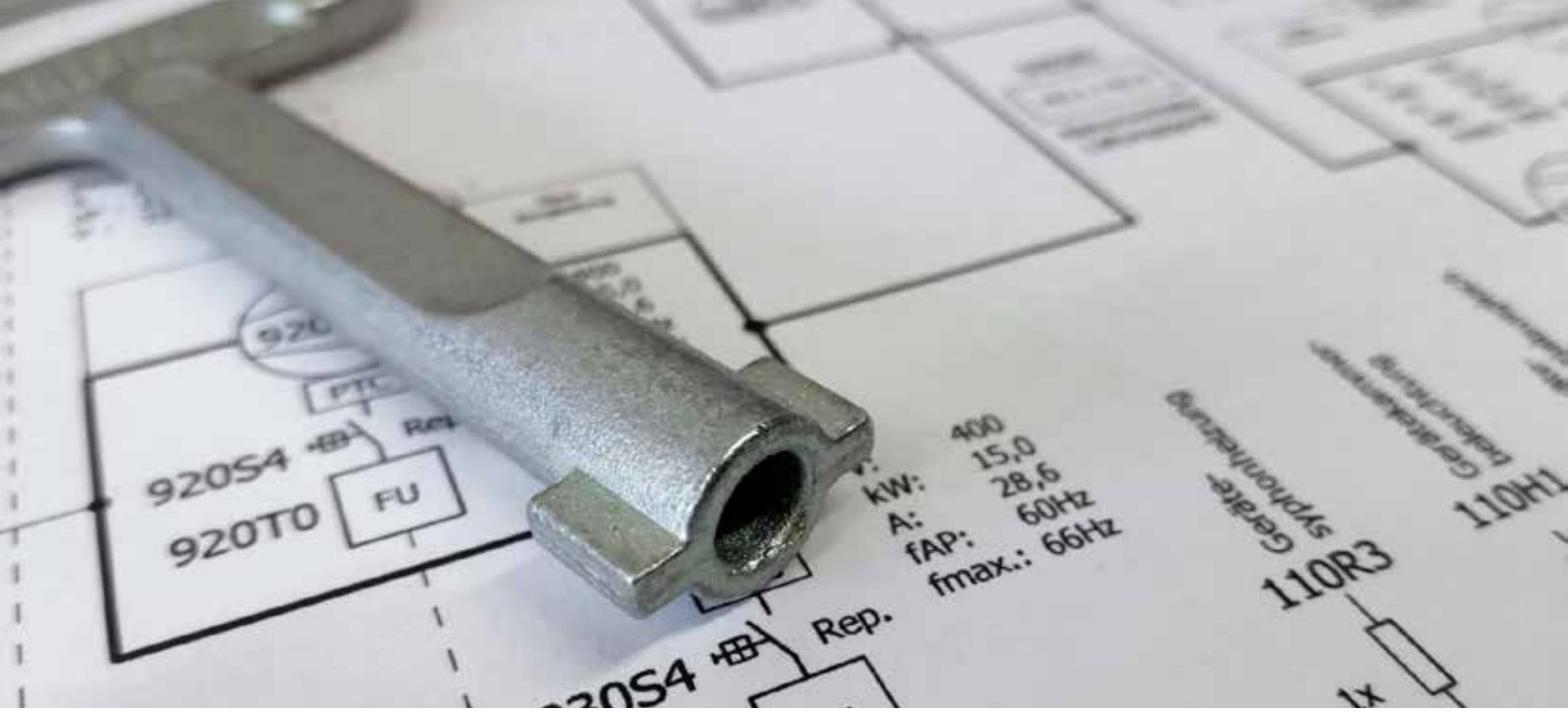
Es ist gem. Art. 30 Abs. 3 DS-GVO zulässig, das Verzeichnis in elektronischer Form, also auch z.B. als Excel-Tabelle zu führen.

3	Zweck der Verarbeitung:	Tätigkeitsgegenstand der GmbH ist die Ausführung von Maler- und Trockenbauarbeiten aller Art.	4	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten:	Kundendaten, Mitarbeiterdaten, Daten von Lieferanten und anderen Geschäftspartnern, sofern die Verarbeitung zur Erreichung der vorgenannten Zwecke erforderlich ist.
7	Regelfristen für die Löschung der Datenkategorien:	Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen vorgegeben. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht. Sofern keine spezifischen Aufbewahrungspflichten und -fristen bestimmt sind, werden sie gelöscht, sobald der Zweck ihrer Verarbeitung entfällt.	8	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen:	Die Systeme der Adam und Eva GmbH werden durch eine Vielzahl von Maßnahmen gegen unbefugten Zutritt, Zugang, Zugriff, Verlust und Zerstörung sowie gegen unzulässige Veränderung geschützt. Einzelheiten werden zur jeweiligen Verarbeitungstätigkeit beschrieben.

17	18	19	20	21	22
Drittstaatentransfer	Zugriffsberechtigte	Regelfristen für die Löschung	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen	Datenschutzfolgenabschätzung	Anmerkung
Kein Drittstaatentransfer vorgesehen	Geschäftsführung Assistenz der Geschäftsführung	10 Jahre, Art. 17 Abs. 3 lit. b) DS-GVO, § 147 Abs. 3 AO: beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist.	s. Sicherheitskonzept im Anhang	Nicht erforderlich, da kein hohes Risiko ermittelt.	
Kein Drittstaatentransfer vorgesehen	Geschäftsführung Assistenz der Geschäftsführung Bauleiter Meister	**Zeiterfassung**: unverzüglich nach Auswertung, Art. 17 Abs. 1 lit. a) DS-GVO, es sei denn: Überschreitung der werktäglichen Arbeits-zeit gem. § 3 ArbZeitG, dann 2 Jahre gem. § 16 ArbZeitG	s. Sicherheitskonzept im Anhang	Nicht erforderlich, da kein hohes Risiko ermittelt.	

Vorliegendes Template orientiert sich an einer Empfehlung des Deutschen Anwaltvereins an seine Mitglieder, die diesen unter https://anwaltverein.de/de/praxis/datenschutz zur Verfügung gestellt wird.

Ein ausführliches Template findet sich auf Seite 20/21.



Montageanleitung - Grundgerüst

Die nachfolgende „Montageanleitung“ gibt ausgehend von den typischen Fallkonstellationen im Handwerksbetrieb nicht abschließende Hinweise zum Zusammenbau der gesetzlichen Elemente eines Verzeichnisses von Verarbeitungstätigkeiten. Die Hinweise können jedoch eine individuelle Prüfung durch einen Fachkundigen nicht völlig ersetzen. Wer seine Situation nicht oder nicht vollständig wiederfindet, sollte unbedingt fachkundigen Rat in Anspruch nehmen.

Die nachfolgenden Eintragungen stellen lediglich Eintragungsbeispiele dar. Diese müssen jeweils durch die auf den eigenen Betrieb zutreffenden Informationen ausgetauscht werden.

Fig. 1: Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters

Die Pflicht zur Angabe eines Verantwortlichen folgt aus Art. 30 Abs. 1 Buchst. a) 1. Halbsatz DS-GVO.

Wer für eine Verarbeitung personenbezogener Daten – das sind Informationen, die einem Menschen zugeordnet werden können – verantwortlich ist, bestimmt sich nach der Regelung in Art. 4 Nr. 7 DS-GVO. Danach ist Verantwortlicher, wer über die Zwecke und Mittel solcher Verarbeitungen entscheidet. Im Normalfall entscheidet der Betrieb vertreten durch den Geschäftsleiter oder Geschäftsführer, welche Daten von welchen Personen mit welchen Mitteln verarbeitet werden. Dies geschieht z.B. in Form der Entscheidung, bestimmte Computer und Smartphones anzuschaffen und eine bestimmte Software bzw. Applikationen auf diesen Geräten zu verwenden.

Wird der Betrieb nicht als Einzelunternehmen, sondern als rechtsfähige juristische Person geführt, ist diese juristische Person als Verantwortlicher zu nennen. Zusätzlich muss angegeben werden, wer die juristische Person vertritt. Bei einer Kommanditgesellschaft ist dies der Komplementär, bei der Gesellschaft mit beschränkter Haftung der Geschäftsführer. Daraus folgt bei einer GmbH & Co. KG eine Vertretungskette, die wie folgt aussieht: Die KG wird vertreten durch die Komplementär-GmbH, die Komplementär-GmbH wird vertreten durch den Geschäftsführer.

Der Eintrag zu Fig. 1 sieht also im Falle einer GmbH & Co. KG – beispielhaft – wie folgt aus:

Adam und Eva GmbH & Co. KG
In den Gärten 1
88145 Paradies

vertreten durch die Komplementärin:
Adam und Eva Verwaltungsgesellschaft mbH, ebenda, diese vertreten durch den Geschäftsführer, Herrn Adam Erstermann

Wird der Betrieb in der Rechtsform der GmbH geführt, entfällt der Zwischenschritt über die Komplementär-GmbH und es ist lediglich die Vertretung durch den Geschäftsführer anzugeben.

Es empfiehlt sich, neben den Angaben zum Sitz des für die Datenverarbeitung verantwortlichen weitere Informationen zu dessen Erreichbarkeit aufzunehmen wie z.B. Telefonnummer und E-Mail-Adresse. Zwar folgt diese Anforderung nicht direkt aus der Verordnung, die Angabe erspart indes Aufwand bei der Kontaktaufnahme durch die Behörde.

Fig. 2: Name und Kontaktdaten des betrieblichen Datenschutzbeauftragten

Die Pflicht zur Angabe des betrieblichen Datenschutzbeauftragten und dessen Erreichbarkeit folgt aus Art. 30 Abs. 1 Buchst. a) letzter Halbsatz DS-GVO.

Nicht jeder Betrieb hat einen betrieblichen Datenschutzbeauftragten. Die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten besteht in der Regel nur für Betriebe, in denen mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten betraut sind, § 38 Abs. 1 S. 1 BDSG. Ständig mit der Verarbeitung personenbezogener Daten befasst ist insbesondere, wer permanent mit Mitarbeiter- oder Kundendaten umgeht. Das Bayerische Landesamt für Datenschutzaufsicht geht davon aus, dass Handwerker, die nur gelegentlich bei der Auftragsausführung mit Namen und Adressen von Kunden umgehen, nicht zu zählen sind.

Bei strenger Betrachtung kann jedoch auch der Handwerker auf der Baustelle mitzuzählen sein. Dies ist nach hiesiger Auffassung der Fall, wenn der Betrieb ein System einsetzt, durch das der Mitarbeiter auf der Baustelle nicht nur auf Name und Anschrift des Kunden, sondern einen weiterreichenden Zugriff auf zu verschiedenen Kunden gespeicherte Informationen hat und ggf. auch selbst kunden- und auftragsunspezifische Zusatzinformationen abrufen, aber auch hinzufügen kann.

Im typischen Handwerksbetrieb gehört eine umfangreiche oder systematische Überwachung von Personen bzw. die umfangreiche Verarbeitung besonders sensibler Daten nicht zum Tätigkeitsbild. In atypischen Konstellationen kann dies gleichwohl der Fall sein, weshalb nur in solchen Ausnahmefällen die Bestellung eines Datenschutzbeauftragten gesetzlich vorgeschrieben ist.

Die Benennung des betrieblichen Datenschutzbeauftragten ist formfrei möglich. Im Gegensatz zur alten Rechtslage ist seit dem 25.05.2018 auch eine mündliche Benennung denkbar. Allerdings ist aus Gründen der Klarheit und der Nachweisbarkeit nach wie vor eine schriftliche Bestellung ratsam.

Zum Datenschutzbeauftragten kann nur bestellt werden, wer aufgrund seines Fachwissens auf den Gebieten des Datenschutzrechts und der Datenschutzpraxis sowie seiner Fähigkeit, die in Artikel 39 DS-GVO genannten Pflichten zu erfüllen, für diese Aufgabe geeignet ist. Die oder der Datenschutzbeauftragte darf, muss aber nicht Mitarbeiter bzw. Mitarbeiterin der bestellenden Stelle sein. Die Bestellung darf in keinem Fall zu Interessenkonflikten führen, so dass Geschäftsführung und die Leitung der IT-Abteilung als zu benennende Personen nicht in Frage kommen.

Die bestellende Stelle tut gut daran, nur besonders qualifizierte Personen als Datenschutzbeauftragte zu benennen. Die Bestellung führt nämlich nicht dazu, dass der für die Datenverarbeitung Verantwortliche die ihm auferlegte Verpflichtung zur Einhaltung datenschutzrechtlicher Bestimmungen auf die oder den Datenschutzbeauftragte(n) delegieren kann.

Ist ein(e) Datenschutzbeauftragte(r) benannt, ist diese(r) an die zuständige Datenschutzaufsichtsbehörde zu melden. Die meisten Datenschutzaufsichtsbehörden halten auf ihrer Website dazu ein Meldeformular bereit. Die dort abgefragten Angaben können auch in das Feld zu Fig. 2 eingefügt werden.

Der Eintrag zu Fig. 2 sieht im Falle einer Bestellung eines externen Datenschutzbeauftragten – beispielhaft – wie folgt aus:

Datenschutzbeauftragter:
Josef Zimmermann
Gesellschaft für Datenschutz GmbH
In den Gärten 2
88145 Paradies
Telefon: +49 1234 5678
E-Mail: dsb@paradies

Über Grundsätzliches und insbesondere die Aufgaben des Datenschutzbeauftragten informiert die Datenschutzkonferenz (DSK) in ihrem Kurzpapier Nr. 12 „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“.

Impressum

Herausgeber: Mittelstand 4.0-Kompetenzzentrum Planen und Bauen / eBusiness-Kompetenzzentrum gUG (haftungsbeschränkt), Fraunhofer-Institut für Bauphysik IBP (Gesamtleitung), Fraunhofer Straße 10, 83626 Valley
Redaktion: Michael Weller (Autor), m.weller@ebusiness-kompetenzzentrum.de; Telefon: 0631-205 601 801
Gestaltung und Produktion: buildingSMART Deutschland, Wiener Platz 6, 01069 Dresden
Bildnachweis: eBusiness-Kompetenzzentrum, soweit nicht anders gekennzeichnet: pixabay.de – die nicht gekennzeichneten Fotos unterliegen der CC0 Public Domain Dedication, abrufbar unter: https://creativecommons.org/publicdomain/ ze-ro/1.0/deed.de
Online: verfügbar als PDF-Download unter: www.kompetenzzentrum-planen-und-bauen.digital - Stand: September 2018

Fig. 3: Zwecke der Verarbeitung

Die Pflicht zur Angabe der Zwecke der Verarbeitung folgt aus Art. 30 Abs. 1 Buchst. b) DS-GVO.

In dem hier vorgeschlagenen Modell erfolgt die Beschreibung der Zwecke der Verarbeitung personenbezogener Daten zweigeteilt. Zum einen dient die Datenverarbeitung in Unternehmen dem Zweck, das Unternehmensziel zu erreichen. Jede Verarbeitung von Daten, die sich diesem Ziel nicht unterordnet, ist ein unnötiger Ballast, den es zu vermeiden gilt. Zum anderen erfolgt eine Verarbeitung personenbezogener Daten untrennbar mit der Verfolgung des Unternehmensziels einhergehenden rechtlichen Anforderungen wie z.B. solchen aus dem Sozial- und Steuerrecht.

Der vorliegende Bauplan sieht vor, sich das Unternehmensziel zu vergegenwärtigen, um auf diese Weise viel leichter und sicher Klarheit darüber gewinnen zu können, ob ein einzelner Vorgang der Verarbeitung personenbezogener Daten entweder zur Erreichung dieses Ziels unverzichtbar oder untrennbar mit der Unternehmenstätigkeit aufgrund äußerer Anforderungen verbunden ist. Dazu dient der Eintrag in Fig. 3.

Soweit die Verarbeitung personenbezogener Daten sich sinnvoll in verschiedene Bereiche wie z.B. Finanzbuchhaltung, Lohnbuchhaltung, Personalverwaltung, Kundenverwaltung, Homepagebetrieb etc. unterteilen lässt, lassen sich Teil- und Sonderzwecke der in den einzelnen Bereichen vorgenommenen Verarbeitung personenbezogener Daten definieren. Die Definition dieser Teil- und Sonderzwecke wird in Fig. 10 beschrieben.

Der Eintrag zu Fig. 3 sieht danach – beispielhaft – wie folgt aus:

Tätigkeitsgegenstand der Gesellschaft ist die Ausführung von Maler- und Trockenbauarbeiten aller Art.

Fig. 4: Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten

Die Pflicht zur Angabe von Kategorien betroffener Personen und Kategorien personenbezogener Daten folgt aus Art. 30 Abs. 1 Buchst. c) DS-GVO.

Wie bereits zu Fig. 3 erfolgt auch im Hinblick auf die Kategorien betroffener Personen und die Kategorien personenbezogener Daten die Aufforderung an den Ersteller des Verzeichnisses von Verarbeitungstätigkeiten, sich zunächst eine grundlegende Klarheit in Bezug auf alle in der Datenverarbeitung des für diese Verantwortlichen vorkommenden Informationen und die Möglichkeit ihrer Zuordnung zu einem Menschen Klarheit zu verschaffen.

Unterteilt man hiernach die Datenverarbeitungsvorgänge in sinnvolle Einheiten, stellt man fest, dass nicht überall der gesamte Datenbestand verarbeitet wird. Die Unterscheidung und ihre Darstellung im Verzeichnis von Verarbeitungstätigkeiten wird in Fig. 14 und Fig. 15 beschrieben.

Der Eintrag zu Fig. 4 kann danach – beispielhaft – wie folgt aussehen:

Kundendaten, Mitarbeiterdaten, Lieferantendaten sowie Daten von anderen Geschäftspartnern, sofern deren Verarbeitung der vorbeschriebenen Zwecke erforderlich ist. Details werden zur jeweiligen Verarbeitungstätigkeit beschrieben.

Diese recht allgemeine Beschreibung ermöglicht eine Bestandsaufnahme aller vorkommenden Kategorien von personenbezogenen Daten und den betroffenen Personen. Bereits hier kann man leicht feststellen, ob Personen oder Daten vorkommen, die für die Erreichung des Unternehmensziels keine Relevanz aufweisen. Auf eine

solche lediglich wünschenswerte – nice to have – Verarbeitung muss verzichtet und die Prozesse auf das Notwendige – must have – beschränkt werden.

Fig. 5: Kategorien von Empfängern, denen die Daten offengelegt worden sind bzw. werden sowie Empfänger in Drittstaaten

Die Pflicht zur Angabe der Kategorien von Empfängern einschließlich solcher in Drittländern folgt aus Art. 30 Abs. 1 Buchst. d) DS-GVO.

Wie zu Fig. 3 und Fig. 4 bereits geschildert, geht es an dieser Stelle darum, einen Gesamtüberblick über die Empfänger personenbezogener Daten zu erhalten. Im typischen kleinen, mittelständischen Handwerksbetrieb sind in der Regel die Zuständigkeiten für die Behandlung personenbezogener Daten auf wenige Personen im Büro verteilt und keine selbstständigen Organisationseinheiten wie z.B. Personalabteilungen vorhanden. Zudem ist die vorhandene IT-Infrastruktur in der Regel überschaubar. Interne Empfänger sind daher regelmäßig nicht vorhanden.

Gleichwohl finden personenbezogene Daten den Weg zu Empfängern außerhalb des Unternehmens. Typischerweise sind gegenüber dem Finanzamt und den Sozialversicherungsträgern Meldungen abzugeben. Löhne und Gehälter werden unbar ausgezahlt, so dass die Hausbank auch die Kontoinformationen der Mitarbeiter erhält. Die Information über die Bankverbindung von Kunden erhält die Hausbank dann, wenn die Kunden ihre Rechnungen auf das Konto des Unternehmens begleichen. Mitarbeiterinformationen und Kundeninformationen erhält in vielen Fällen aber auch der Steuerberater, der die Buchhaltung für den Betrieb übernimmt. Nicht vergessen werden darf der Hosting-Dienstleister, bei dem die Homepage des Betriebes zu Hause ist. Dieser hat Kenntnis von den Nutzern, die die Homepage besuchen.

Für den Fall, dass Werkzeuge wie z.B. Aufgaben-Management-Tools in der Cloud genutzt werden (Software as a Service), muss geschaut werden, ob in der Anwendung, die nicht auf dem eigenen Gerät, sondern im Internet ausgeführt wird, z.B. Namen und sonstige zu einem Menschen gehörende Informationen eingetragen sind.

Der Eintrag zu Fig. 5 sieht danach – beispielhaft – wie folgt aus:

Finanzamt, Sozialversicherungsträger, Zahlungsdienstleister, Steuerberater, Hosting-Dienstleister, Software as a Service-Anbieter.

Fig. 6: Übermittlung in Drittstaaten

Die Pflicht zur Angabe einer Übermittlung in Drittstaaten folgt aus Art. 30 Abs. 1 Buchst. e) DS-GVO.

Wie zu den vorherigen Fig. 3 bis Fig. 5 ausgeführt, geht es an dieser Stelle um einen generellen Überblick über die Verarbeitungstätigkeiten. Ein Drittlandsbezug liegt vor, wenn personenbezogene Daten in einen Staat außerhalb des räumlichen Anwendungsbereichs der Datenschutz-Grundverordnung, weitergeleitet werden.

Dies kommt etwa in Betracht durch die Nutzung von Services US-amerikanischer Anbieter oder in den Grenzregionen z.B. zur Schweiz, wenn dort ansässige Dienstleister beauftragt werden. Hierbei ist dann auch besonderes Augenmerk darauf zu richten, dass der zwingend erforderliche Vertrag zur Verarbeitung personenbezogener Daten im Auftrag durch den Dienstleister im Drittstaat die nach der Datenschutzgrundverordnung notwendigen Garantien für den Schutz und die Sicherheit der Daten beinhaltet.

Es kann aber auch bei Tätigkeiten im normalen Geschäftsbetrieb in Nicht-EU-Staaten zur einer Datenübermittlung in diese Länder kommen, wenn zum Beispiel Mitarbeiter für eine Tätigkeit in diesen Staaten angemeldet oder für diese Zimmer oder Fahrzeuge vor Ort reserviert werden.

Der Eintrag zu Fig. 6 könnte demnach – beispielhaft – wie folgt aussehen:

Datenübermittlungen in Drittstaaten finden ausschließlich im Rahmen der Arbeitsvorbereitung und Ausführung von Aufträgen in der Schweiz statt.

Bei der Inanspruchnahme beliebter Cloud-Speicher wie z.B. Dropbox, G-Drive etc. muss darauf geachtet werden, die Datenübermittlung an diese Dienstleister mit Sitz in den USA auf eine geeignete vertragliche Grundlage zu stellen. Dieser Vertrag zur Verarbeitung von personenbezogenen Daten im Auftrag, der erforderlich ist, selbst wenn nur Dokumente aus der Textverarbeitung, die aber einen Rückschluss auf den Ersteller oder den Adressaten zulassen, dort abgelegt werden, muss sicherstellen können, dass der Beauftragte die europäischen Datenschutzstandards einhält. Das lässt sich nur vermeiden, indem keine personenbezogenen Daten übermittelt werden. Technisch kann man das durch eine Verschlüsselung der Dokumente vor ihrer Übermittlung zur Ablage in der Cloud realisieren.

Fig. 7: Regelfristen für die Löschung von Datenkategorien

Die Pflicht zur Angabe von Löschfristen nach Datenkategorien folgt aus Art. 30 Abs. 1 Buchst. f) DS-GVO.

Wie bei den vorangegangenen Fig. 1 bis Fig. 6, so geht es auch hier um einen grundlegenden Überblick. Aufbewahrungsfristen können je nach konkreter Ausgestaltung des Verarbeitungsvorganges von höchstens ein bis zwei Tagen wie etwa bei Videoüberwachung oder wenigen Tagen bei den unvermeidlichen Log-Files zur Website bis hin zu zehn Jahren im Handels- und Steuerrecht reichen.

Vor diesem Hintergrund darf die Anforderung in Art. 30 Abs. 1 Buchst. f) DS-GVO, wonach diese Angaben „wenn möglich" zu machen sind, nicht dahin verstanden werden, dass diese Angabe optional ist. Vielmehr bedeutet dies, dass eine konkrete Zahl nur dann genannt werden muss, wenn nur diese zutrifft. Im Übrigen muss eine allgemeine Angabe zu den Löschfristen erfolgen.

An dieser Stelle des Verzeichnisses von Verarbeitungstätigkeiten genügt daher eine allgemein gehaltene Information, die an geeigneter Stelle konkretisiert wird.

Der Eintrag zu Fig. 7 könnte daher – beispielhaft – wie folgt aussehen:

Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und-fristen vorgegeben. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht. Sofern Daten keinen spezifischen Aufbewahrungspflichten und-fristen unterliegen werden sie gelöscht, sobald der Zweck ihrer Verarbeitung entfällt. Detailliertere Angaben finden sich bei der Beschreibung der jeweiligen Verarbeitungstätigkeit.

Fig. 8: Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Die Pflicht zur allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen folgt aus Art. 30 Abs. 1 Buchst. g) i.V. mit Art. 32 Abs. 1 DS-GVO.

Schließlich ist auch diese Angabe im Hinblick auf einen allgemeinen Überblick wie bereits in Fig. 1 bis Fig. 7 ausgeführt. Wie zu Fig. 7 bereits erläutert, darf auch hier die gesetzliche Formulierung, dass diese Angabe nur „wenn möglich" zu machen ist, nicht dahin verstanden werden, dass diese lediglich optional zu machen wäre. Sie ist vielmehr verpflichtend.

Eine Angabe ist aber nur möglich, wenn tatsächlich technische und organisatorische Maßnahmen ergriffen und eingeführt wurden. Diese Maßnahmen sollen aber nicht so detailliert beschrieben werden, dass sie dem Betrachter des Verzeichnisses die potenziellen Angriffspunkte in der IT-Sicherheit offenbaren.

Der Eintrag zu Fig. 8 könnte folglich – beispielhaft – wie folgt aussehen:

Die Systeme der Adam und Eva GmbH & Co. KG werden durch eine Vielzahl von Maßnahmen gegen unbefugten Zutritt, Zugang, Zugriff, Verlust und Zerstörung sowie gegen unzulässige Veränderung geschützt. Einzelheiten werden zur jeweiligen Verarbeitungstätigkeit beschrieben.

Damit sind die in das Verzeichnis von Verarbeitungstätigkeiten aufzunehmenden allgemeinen Beschreibungen des IT-Einsatzes im Betrieb vollständig. Im Anschluss gilt es, diesen allgemeinen Überblick sinnvoll in verschiedene Bereiche des IT-Einsatzes zu unterteilen. Als Differenzierungskriterium eignet sich eine Betrachtung der Sinneinheiten von Verarbeitungsvorgängen.

Montageanleitung - Feineinstellung

Nachdem in einem Grundgerüst der Rahmen, innerhalb dessen die Verarbeitung personenbezogener Daten im Betrieb abläuft, umrissen wurde, ist eine Feineinstellung der Datenverarbeitung vorzunehmen. Hierzu werden die Datenverarbeitungsvorgänge detaillierter betrachtet und in sinngebende Einheiten unterteilt. Zu jeder Sinneinheit werden dann die Einzelkriterien der Datenverarbeitung aufgenommen, so dass im Ergebnis die Rechtmäßigkeit jeder einzelnen Behandlung eines personenbezogenen Datums anhand des Verzeichnisses von Verarbeitungstätigkeiten nachgewiesen werden kann. Aufgrund der Regelung in Art. 5 DS-GVO trifft den für die Datenverarbeitung Verantwortlichen eine Rechenschaftspflicht, der auf diese Weise nachgekommen werden kann.

Fig. 9: Name der Datenverarbeitung

In der Spalte zu Fig. 9 werden die in sinnvolle Einheiten unterschiedenen Datenverarbeitungsvorgänge mit einem sinnfälligen Namen versehen. Für kleine und mittlere Handwerksbetriebe bietet das Muster des Bayerischen Landesamtes für Datenschutzaufsicht eine gute Orientierung. In diesem ist vorgeschlagen, folgende Sinneinheiten zu bilden:

- Lohnabrechnung
- Personalverwaltung
- Betrieb der Firmenwebsite
- Kundenverwaltung

Diese Bezeichnungen für Verarbeitungstätigkeiten stellen lediglich Vorschläge dar. Denkbar sind weitere, gesondert zu benennende Verarbeitungstätigkeiten, wenn zum Beispiel besondere Anwendungen in der Cloud – also über das Internet – eingesetzt werden, wie es z.B. zum Aufgabenmanagement recht häufig der Fall ist. Ein solches Werkzeug dient als Brücke zwischen der Personalverwaltung und der Kundenverwaltung und will daher nicht so recht entweder in die eine, noch in die andere Verarbeitungstätigkeit passen. Aufgrund dessen bietet sich an, solche Anwendungen gesondert auszuweisen:

- Aufgabenmanagement

Ferner ist hier eine vor allem bei in abgelegenen Bereichen gelegenen Betrieben verbreitete Videoüberwachung als Einbruchs- und Diebstahlschutz außerhalb der Bürozeiten nicht berücksichtigt. Diese Verarbeitungstätigkeit, bei der ja Personen, die in den Aufnahmebereich der Kamera geraten, erfasst werden, ist bei Vorhandensein also ebenfalls zu ergänzen:

- Videoüberwachung

Im Falle der Videoüberwachung gelten weitere Anforderungen an deren Rechtmäßigkeit, die aus den Transparenzpflichten der Datenschutz-Grundverordnung fließen. Die prominenteste Pflicht dürfte diejenige zur Ausschilderung der Videoüberwachung mit dem bekannten Piktogramm sein:

Zeichen nach DIN 33450

Fig. 10: Zwecke der Datenverarbeitung

Die Spalte zu Fig. 10 dient der Konkretisierung der allgemeinen Angaben in Fig. 3. Das bedeutet, die recht grobe Beschreibung der Hauptzwecke der Verarbeitung personenbezogener Daten wird nun auf die gebildeten Sinneinheiten der Verarbeitungstätigkeit heruntergebrochen. Anders ausgedrückt: die zur Erreichung des in Fig. 3 definierten Hauptzwecks notwendigen Zwischen- und Hilfszwecke sind hier anzugeben.

Die Zwecke lassen sich in Bezug auf die in Fig. 9 vorgenommene Unterscheidung wie folgt definieren:

- Lohnabrechnung
  - Auszahlung der Löhne und Gehälter
  - Abfuhr von Sozialabgaben und Steuern
- Personalverwaltung
  - Personaladministration
  - Personalführung
  - Arbeitszeitverwaltung
  - Personalbeschaffung
- Betrieb der Firmenwebsite
  - Außendarstellung
- Kundenverwaltung
  - Bearbeitung von Aufträgen
  - Rechnungstellung
  - Postalische Werbung
- Aufgabenmanagement
  - Ressourcenplanung und -einsatz
  - Fortschrittskontrolle
- Videoüberwachung
  - Einbruchs- und Diebstahlschutz
  - Erfassung und Aufklärung von Straftaten

Die oben definierten Zwecke stellen lediglich typische Ziele der jeweiligen Verarbeitungstätigkeit dar. Die Aufzählung ist daher weder in dieser Form zwingend, noch abschließend. Werden von den hier aufgeführten abweichende oder weitere Zwecke verfolgt, so sind diese in das Verzeichnis von Verarbeitungstätigkeiten aufzunehmen, nicht zutreffende sind zu entfernen.

Bei der Definition der Zwecke empfiehlt sich, verschiedene Zwischen- und Teilziele nach Möglichkeit in einem Oberbegriff zusammenzufassen. Anderenfalls droht die erforderliche Übersichtlichkeit des Verzeichnisses von Verarbeitungstätigkeiten verloren zu gehen. Damit kann es seinen Zweck, die Rechtmäßigkeit der Verarbeitungstätigkeiten übersichtlich zu plausibilisieren nicht mehr erfüllen.

Allerdings sollte man sich auch davor hüten, zumindest auch verfolgte Zwecke an dieser Stelle zu verschweigen. Das Verzeichnis dient zunächst der Selbstkontrolle und sollte dabei helfen, die Vorgänge ausfindig zu machen, an denen Ressourcen verschwendet werden. Das gelingt selbstverständlich nur, wenn alle Zwecke offengelegt werden und man sich selbstkritisch fragt, ob man dieses Ziel tatsächlich verfolgen möchte und falls man dies bejaht, es auf die gewählte Weise überhaupt erreicht werden kann.

Fig. 11: Rechtsgrundlage

Da das Verzeichnis von Verarbeitungstätigkeiten der Erfüllung der Rechenschaftspflicht dient, sollten an dieser Stelle auch die Rechtsgrundlagen der jeweiligen Datenverarbeitung angegeben werden. Dies stellt erfahrungsgemäß für den zur Erstellung des Verzeichnisses Verpflichteten schon deshalb eine Herausforderung dar, weil er als nicht Rechtskundiger kaum in der Lage ist, diese auch nur aufzufinden, sofern diese sich nicht geradezu aufdrängen.

Die wichtigsten Rechtsgrundlagen einer Verarbeitung personenbezogener Daten im kleinen, mittelständischen Handwerksbetrieb zu den einzelnen, hier behandelten Verarbeitungstätigkeiten lauten:

- Lohnabrechnung
  - Art. 6 Abs. 1 Buchst. c) DS-GVO
  - Art. 28 DS-GVO
  - § 147 AO
  - § 157 HGB
  - § 4 Abs. 2, 2a LStDV
- Personalverwaltung
  - Art. 6 Abs. 1 Buchst. a), b), c) und f) DS-GVO
  - Art. 88 DS-GVO
  - § 26 BDSG
  - § 7 Abs. 7 ArbZeitG
- Betrieb der Firmenwebsite
  - Art. 6 Abs. 1 Buchst. f) DS-GVO
  - Art. 28 DS-GVO
  - § 14 TMG
  - § 15 TMG
- Kundenverwaltung
  - Art. 6 Abs. 1 Buchst. b) und c) DS-GVO
  - § 257 HGB
  - § 147 AO
- Aufgabenmanagement
  - Art. 6 Abs. 1 Buchst. b), c) und f) DS-GVO
  - Art. 28 DS-GVO

- Art. 88 DS-GVO
- § 26 BDSG

► Videoüberwachung
- § 4 Abs. 1 Nr. 2 und 3, Abs. 3 BDSG

Diese Aufzählung ist lediglich beispielhaft. Das bedeutet, dass bei der Erstellung eines auf eine konkrete Situation zutreffenden Verzeichnisses von Verarbeitungstätigkeiten andere oder weitere Rechtsgrundlagen anzugeben sind.

Fig. 12: Beschreibung der Verarbeitung

An dieser Stelle können allgemeine Angaben zum eingesetzten System, insbesondere der jeweils verwendeten Software gemacht werden.

Fig. 13: Verarbeitung besonderer Arten personenbezogener Daten i.S. von Art. 9 Abs. 1 DS-GVO

Besondere Arten personenbezogener Daten im Sinne von Art. 9 Abs. 1 DS-GVO kommen im typischen kleinen, mittelständischen Handwerksbetrieb in Form von Informationen zur religiösen oder weltanschaulichen Überzeugung in Form des Kirchensteuermerkmals, ggf. einer Gewerkschaftszugehörigkeit sowie von Informationen zur sexuellen Orientierung über die Angabe zum Familienstand und ggf. von Kinderfreibeträgen sowie zur Gesundheit im Falle der Einreichung von ärztlichen Bescheinigungen über eine Arbeitsunfähigkeit vor.

Der Eintrag in der betreffenden Zeile zu den hier vorgeschlagenen Verarbeitungstätigkeiten lautet also immer „Ja“, wenn innerhalb der beschriebenen Tätigkeit solche Informationen verwendet werden. Typischerweise ist dies bei der Lohnabrechnung und bei der Personalverwaltung der Fall. Es kann auch im Rahmen des Aufgabenmanagements der Fall sein, wenn z.B. Aufgaben von erkrankten Mitarbeitern über die betreffende Verarbeitungstätigkeit umverteilt werden und die Gründe offen liegen.

Gewöhnlicherweise fallen solche besonderen Arten personenbezogener Daten in Verarbeitungstätigkeiten im Zusammenhang mit der Firmenwebsite, der Kundenverwaltung und der Videoüberwachung nicht an. In diesen Fällen ist das Wort „Nein“ in der betreffenden Zeile einzutragen.

Fig. 14: Betroffene bzw. betroffene Personengruppen

Die Angaben in Fig. 14 stellen eine Aufteilung der in Fig. 4 allgemein definierten Gruppe von betroffenen Personen dar, indem nun nach einzelnen Verarbeitungstätigkeiten differenziert dargelegt wird, welche Personen in einer Tätigkeit vorkommen. Typischerweise lassen sich folgende Unterscheidungen treffen:

► Lohnabrechnung
- Mitarbeiter

► Personalverwaltung
- Mitarbeiter
- Auszubildende
- Bewerber

► Betrieb der Firmenwebsite
- Website-Besucher

► Kundenverwaltung
- Kunden

► Aufgabenmanagement
- Mitarbeiter
- Auszubildende
- Kunden

► Videoüberwachung
- Mitarbeiter
- Besucher
- Eindringlinge

Fig. 15: Personenbezogene Daten/Datenkategorien

Die in Fig. 15 einzustellenden Angaben stellen eine weitere Ausdifferenzierung der Verarbeitung von Daten der zu Fig. 14 angegebenen Betroffenen dahingehend dar, dass hier nun aufgezeichnet wird, welche Einzelinformationen zu ihnen in der betreffenden Verarbeitungstätigkeit vorkommen. Im typischen kleinen, mittelständischen Handwerksbetrieb finden sich folgende Einzelangaben zu den hier vorgeschlagenen Verarbeitungstätigkeiten:

- Lohnabrechnung
  - Name, Vorname
  - Geburtsdatum und -ort
  - Bankverbindung
  - Lohn-/Entgeltdaten
  - (ggf.) Religionszugehörigkeit
  - Sozialversicherungsdaten
  - Steuerdaten, insbes. Steuerklasse, Freibeträge
  - Berufsgenossenschaftsangaben
- Personalverwaltung
  - Name, Vorname
  - Anschrift(en)
  - Zeitwirtschaftsdaten
  - Daten zur Arbeitsleistung
  - Leistungsbeurteilung
  - Lebenslauf
  - Bewerbungsunterlagen
- Betrieb der Firmenwebsite
  - IP-Adresse(n)
- Kundenverwaltung
  - Name, Vorname
  - Anschrift(en)
  - Kontaktinformation, insbes. Telefonnummer, E-Mail-Adresse
  - Information zum Auftrag
  - (ggf.) Bankverbindung
- Aufgabenmanagement
  - Name, Vorname
  - Anschrift(en)
  - Information zum Auftrag
  - Arbeitsfortschritt
- Videoüberwachung
  - Äußere Erscheinung, Bild der Betroffenen

Auch insoweit gilt, dass die hier vorgestellte Aufzählung keineswegs Allgemeingültigkeit beansprucht, sondern lediglich einen Anhaltspunkt dafür liefern soll, welche Einzelangaben zu betroffenen Personen im Regelfall in typischen betrieblichen Situationen vorkommen. Die Aufzählung ist zu berichtigen oder zu ergänzen, soweit die tatsächlichen Gegebenheiten in dem Betrieb, für den das Verzeichnis von Verarbeitungstätigkeiten konkret erstellt wird, abweichen.

Fig. 16: Empfänger/Empfängerkategorien

Die Eintragungen in der Spalte Fig. 16 dienen der Konkretisierung und Zuordnung der allgemein gehaltenen Angaben in Fig. 5 zu den einzelnen Verarbeitungstätigkeiten. Insoweit zeigen sich in kleinen, mittelständischen Handwerksbetrieben die folgenden typischen Konstellationen nach hier vorgeschlagenen Verarbeitungstätigkeiten:

- Lohnabrechnung
  - Steuerberater
  - Hausbank (Zahlbeträge und -empfänger)
  - Sozialversicherungsträger
- Personalverwaltung
  - keine
- Betrieb der Firmenwebsite
  - Hosting-Dienstleister
- Kundenverwaltung
  - keine
- Aufgabenmanagement
  - Software as a Service-Anbieter
- Videoüberwachung
  - (ggf.) Strafverfolgungsbehörde

Der Aufzählung liegt die Annahme zugrunde, dass in dem betreffenden Betrieb die Personalverwaltung durch eine Bürokraft miterledigt wird und die Kundendatenbank nicht bei einem externen Dienstleister gespeichert wird. Da die typischen IT-Werkzeuge für ein Aufgabenmanagement heute sog. Cloud-Lösungen darstellen, die unter dem Fachbegriff „Software as a Service“ beschrieben und verstanden werden können, ist hier eine entsprechende Angabe gemacht worden.

Selbstverständlich ist auch die Auflistung der potenziellen Empfänger hier nur beispielhaft erfolgt und bei der Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten für einen konkreten Betrieb muss die tatsächliche Situation erfasst werden. Weicht diese von dem Beispiel ab, sind die Angaben anzupassen bzw. entsprechend zu ergänzen.

Fig. 17: Drittstaatentransfer

Bei den Eintragungen in die Spalte Fig. 17 handelt es sich um die Konkretisierung der allgemeinen Angaben in Fig. 6. Im kleinen, mittelständischen Handwerksbetrieb kommen Drittstaatentransfers in der Regel nur in den Fällen vor, in denen Aufträge in solchen Ländern ausgeführt werden oder in denen IT-Dienstleistungen von Anbietern in Drittstaaten in Anspruch genommen werden. Hier ergibt sich in der Praxis kein einheitliches Bild, da die eingesetzten IT-Werkzeuge und der räumliche Tätigkeitsbereich der Betriebe naturgemäß je nach Sitz, Branche und Unternehmensphilosophie stark divergiert.

Findet ein Drittstaatentransfer personenbezogener Daten nicht statt, das heißt: alle personenbezogenen Daten werden ausschließlich auf Systemen verarbeitet, die sich physikalisch im räumlichen Geltungsbereich der Datenschutz-Grundverordnung befinden, kann in der entsprechenden Zeile zur jeweiligen hier vorgeschlagenen Verarbeitungstätigkeit das Wort „Nein“ eingetragen werden.

Findet demgegenüber ein solcher Drittstaatentransfer statt, sollte der Drittstaat, in den eine Übermittlung erfolgt, angegeben werden. Werden z.B. unverschlüsselte Dokumente, die etwa Namen von Mitarbeitern oder Kunden enthalten im Google-Drive gespeichert, findet ein Transfer dieser Daten in die USA und damit außerhalb des räumlichen Geltungsbereichs der Datenschutz-Grundverordnung statt. Daher muss die Angabe zu der betreffenden Verarbeitungstätigkeit entweder „Ja“, besser aber „USA“ lauten.

Zwei weitere typische Beispiele für einen oftmals nicht bewussten Drittstaatentransfer lassen sich im Bereich der Firmenhomepage und des Aufgabenmanagements antreffen:

Ein gutes Online-Marketing setzt auf multimediale Inhalte und eine niederschwellige Erreichbarkeit.

Dazu werden auf Firmenwebsites bisweilen Videos, die über YouTube verfügbar sind, eingebunden. In diesen Fällen muss – weil technisch unvermeidbar – die IP-Adresse des Nutzers an den YouTube-Server in die USA übermittelt werden, damit das Video auf dem Bildschirm des Nutzers angezeigt werden kann. Dies gilt auch für Anfahrtskizzen oder Schrifttypen, die z.B. aus einer Adobe- oder Google-Datenbank beim Aufruf der Firmenwebsite nachgeladen werden. In diesen Fällen ist der Drittstaatentransfer in dem Verzeichnis von Verarbeitungstätigkeiten auszuweisen.

Ein Drittstaatentransfer kann auch bei einem Einsatz eines Cloud-basierten Aufgabenmanagement-Werkzeuges vorliegen, wenn etwa die Angebote US-amerikanischer Anbieter wie z.B. „Asana“, „smartsheet“ oder „Trello“ verwendet werden. Bei der Verwendung von Microsoft Planner kommt es auf die Buchung der sog. „Euro-Cloud“ zum Office 365-Paket an. Eine Speicherung in Deutschland, allerdings auf den Servern eines US-amerikanischen Unternehmens bietet etwa „MeisterTask“. Ebenfalls mit einem Rechenzentrum in Deutschland, aber auch der Option zur lokalen Installation steht „allegra“ der Stuttgarter Steinbeis GmbH & Co. KG zur Verfügung.

Bei der Einschaltung von Dienstleistern in Drittstaaten ist auf Besonderheiten, insbesondere das Vorliegen ausreichender datenschutzrechtlicher Garantien zu achten. Hierzu müssen ggf. besondere Verträge wie etwa die EU-Standardvertragsklauseln abgeschlossen werden.

Im Datenverkehr mit den USA ist derzeit der so genannte EU-US-Privacy Shield in Kraft, der Datenübermittlungen auf eine rechtliche Grundlage stellt. Allerdings ist dieser Rechtsakt unter Juristen und Datenschützern umstritten, so dass hier die weitere Entwicklung stets im Auge zu behalten ist.

Fig. 18: Zugriffsberechtigte

Zum Nachweis der Rechtmäßigkeit der Datenverarbeitung gehört es, Unberechtigte von einem Zugriff auf personenbezogene Daten auszuschließen. Folglich gilt es festzulegen, wer im Rahmen bestimmter Verarbeitungstätigkeiten Zugriff auf bestimmte Daten, die einem Menschen zugeordnet werden können, nehmen können soll. Betrachtet werden hierbei die innerhalb des Betriebes arbeitenden Personen mit Ausnahme der betroffenen Personen selbst, da man als Betroffener ohne-

hin Kenntnis von den zu schützenden Informationen hat. Insoweit lassen sich im kleinen, mittelständischen Handwerksbetrieb in der Regel folgende Konstellationen antreffen:

- Lohnabrechnung
  - Geschäftsführung
  - Assistenz der Geschäftsführung
- Personalverwaltung
  - Geschäftsführung
  - Assistenz der Geschäftsführung
  - Bauleiter bzw. Meister
- Betrieb der Firmenwebsite
  - Geschäftsführung
  - Assistenz der Geschäftsführung
- Kundenverwaltung
  - Geschäftsführung
  - Assistenz der Geschäftsführung
  - Kundendienst
  - Bauleiter bzw. Meister
- Aufgabenmanagement
  - Geschäftsführung
  - Assistenz der Geschäftsführung
  - Bauleiter bzw. Meister
  - Mitarbeiter
- Videoüberwachung
  - Geschäftsführung
  - Assistenz der Geschäftsführung

Wie bereits zu den vorherigen Fig. 9 bis Fig. 16 ausgeführt, kann auch diese Aufzählung nur beispielhaft wiedergeben, wie Zugriffsberechtigungen vergeben werden. Insbesondere bei der Stellenbezeichnung ergeben sich regionale Unterschiede. Ferner unterscheiden sich die Formen interner Organisation stark in Abhängigkeit von der Betriebsgröße, so dass für die Lohnabrechnung in größeren Betrieben nicht die Assistenz der Geschäftsleitung als „Stabsstelle“, sondern ein(e) eigens mit diesen Aufgaben betraute(r) Mitarbeiter(in) vorhanden ist. Dies trifft bisweilen auch auf das Aufgabenmanagement zu. Selbstverständlich ist auch hier die Aufzählung anzupassen und ggf. zu ergänzen, wenn das Verzeichnis von Verarbeitungstätigkeiten für den konkreten Betrieb erstellt wird, so dass die tatsächlichen Gegebenheiten abgebildet werden.

Fig. 19: Regelfristen für die Löschung

Die Eintragungen in die Spalte zu Fig. 19 dienen der Konkretisierung der Angaben im Feld zu Fig. 7 und konkretisieren die dort recht allgemeinen Angaben zur jeweils definierten einzelnen Verarbeitungstätigkeit. Typischerweise sind bei den hier vorgeschlagenen einzelnen Verarbeitungstätigkeiten folgende Regelfristen für die Löschung einzuhalten:

- Lohnabrechnung
  - 10 Jahre (Art. 17 Abs. 3 Buchst. b) DS-GVO; § 147 Abs. 3 AO: beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist)
- Personalverwaltung
  - Zeiterfassung: unverzüglich nach Auswertung (Art. 17 Abs. 1 Buchst. a) DS-GVO), es sei denn: Überschreitung der werktäglichen Arbeitszeit gem. § 3 ArbZeitG, dann Sonderregel in § 16 Abs. 2 ArbZeitG: 2 Jahre
  - Beschäftigte: in der Regel 3 Jahre nach Ausscheiden aus dem Betrieb, Art. 17 Abs. 3 Buchst. e) DS-GVO zum Verjährungseintritt aller absehbar geltend zu machenden Ansprüche gem. § 195 BGB, also beginnend mit dem Ende des Kalenderjahres, in dem das Beschäftigungsverhältnis endete
  - Zugriffsberechtigungen: unverzüglich nach Ausscheiden des Mitarbeiters (Art. 17 Abs. 1 Buchst. a) DS-GVO)
  - Internetzugang: zum Verjährungsende aller absehbaren Ansprüche 7 Monate gem. §§ 4, 5 KSchG, beginnend mit dem Ausspruch der Kündigung
  - Abgelehnte Bewerber: 6 Monate nach Abschluss des Bewerbungsverfahrens (§ 61b ArbGG i.V. mit § 15 AGG)
- Betrieb der Firmenwebsite
  - 7 Tage bei bloßem Websitebesuch, § 15 TMG
- Kundenverwaltung
  - 10 Jahre (Art. 17 Abs. 3 Buchst. b) DS-GVO, § 147 Abs. 3 AO, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist)
    ACHTUNG AUFBEWAHRUNGSPFLICHT und GoBD!
- Aufgabenmanagement
  - Unverzüglich nach Erledigung der Aufgabe, soweit die Arbeit abgenommen wird (Art. 17 Abs. 1 Buchst. a) DS-GVO)
- Videoüberwachung
  - Unverzüglich nach Sichtung, maximal 2 Tage nach dem Aufzeichnungszeitpunkt

Wie bereits zuvor dargestellt, werden die hier genannten Regelfristen lediglich beispielhaft für eine typische

Konstellation im kleinen, mittelständischen Handwerksbetrieb vorgestellt. Bei der Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten für einen konkreten Betrieb muss daher für alle diese Fristen ihre Einschlägigkeit erneut überprüft und die Anwendbarkeit von abweichenden Sonderbestimmungen festgestellt werden. Darüber hinaus kommen je nach Art der tatsächlichen Verarbeitungstätigkeiten weitere zu beachtende Regelfristen in Betracht.

Darüber hinaus kann es vorkommen, dass abweichend von dem hier unterstellten lediglich unterstützenden Einsatz einer Aufgabenmanagement-Software mittels dieses IT-Werkzeugs leistungs- und abrechnungsrelevante Informationen erzeugt und gespeichert werden, die dann denselben Löschfristen unterliegen wie zur Kundenverwaltung bzw. zur Personalverwaltung angegeben.

Werden Löschfristen nicht beachtet, liegt eine rechtswidrige Verarbeitung personenbezogener Daten vor, die eine Geldbuße nach sich ziehen kann.

Fig. 20: Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Die Angaben in der Spalte zu Fig. 20 dienen der Konkretisierung der allgemeinen Angaben im Feld zu Fig. 8 und deren Zuweisung zu einer definierten einzelnen Verarbeitungstätigkeit.

Technische und organisatorische Maßnahmen in dem hier gemeinten Sinne sind solche, die die Rechtmäßigkeit des Umgangs mit personenbezogenen Daten sicherstellen sollen und können. Das heißt die gemäß Art. 32 DS-GVO zu ergreifenden Maßnahmen müssen Integrität (Richtigkeit) und Vertraulichkeit der Datenverarbeitung gewährleisten können.

In der Praxis bietet es sich bei einer überschaubaren IT-Infrastruktur – das heißt, in Betrieben mit recht wenigen Geräten und wenigen Software-Anwendungen – an, die technischen und organisatorischen Maßnahmen den tatsächlichen Gegebenheiten entsprechend einheitlich zu definieren.

Dazu kann man eine Anlage zum Verzeichnis der Verarbeitungstätigkeiten entwerfen, auf die hier verwiesen werden kann. Übergreifend lassen sich in dieser Anlage die nachfolgend aufgeführten Punkte zu technischen und Organisatorischen Maßnahmen in elf Schritten definieren. Dabei kann Berücksichtigung finden, dass einige der aufgeführten einzelnen Maßnahmen in der eingesetzten Software, insbesondere in Fachanwendungen bereits in den Grundeinstellungen angelegt sind. Hier hilft es, das Anwenderhandbuch zu Rate zu ziehen und softwareseitige Sicherheitsmaßnahmen einfach abzuschreiben.

Die nachfolgende Übersicht kann auch als Checkliste zur Selbstkontrolle verwendet werden:

- **Zugangskontrolle** (= alle Maßnahmen, die verhindern sollen und können, dass Unbefugte Zugang zu Anlagen erhalten, mittels derer personenbezogene Daten verarbeitet werden)
  - Alarmanlage
  - Chipkarten-/Transponder-Schließsystem
  - Abschließbarer Serverschrank
  - Sorgfältige Auswahl des Reinigungspersonals
  - Sicherheitsschlösser
- **Datenträgerkontrolle** (= alle Maßnahmen, die verhindern sollen und können, das Unbefugte Datenträger lesen, kopieren, verändern oder löschen können)
  - Sichere Aufbewahrung von Datenträgern
  - Einrichtung von Standleitungen
  - Einrichtung von VPN-Tunneln
  - Weitergabe von Daten in pseudonymisierter Form

- Weitergabe von Daten in anonymisierter Form
- Verschlüsselung von Datenträgern
- Vernichtung von Datenträgern nach DIN 32757
- Einsatz von Aktenvernichtern bzw. Dienstleistern mit Datenschutz-Gütesiegel
- Protokollierung der Vernichtung

- **Speicherkontrolle** (= alle Maßnahmen, die verhindern sollen und können, dass Unbefugte von gespeicherten personenbezogenen Daten Kenntnis nehmen sowie diese eingeben, verändern oder löschen können)
  - Festlegung von Berechtigungen in IT-Systemen
  - Differenzierte Berechtigungen für lesen, löschen und ändern
  - Differenzierte Berechtigungen für Daten
  - Anwendungen und Betriebssystem(e)
  - Verwaltung der Rechte durch Systemadministrator(en)
  - Anzahl der Systemadministratoren auf das Notwendigste reduziert
  - Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
  - Protokollierung von Zugriffen auf Anwendungen
- **Benutzerkontrolle** (= alle Maßnahmen, die verhindern sollen und können, dass Unbefugte die IT-Systeme des Betriebes von außen, d.h. durch Remote-Control, benutzen können)
  - Festlegung zugangsberechtigter Mitarbeiter
  - Erstellen von Benutzerprofilen
  - Passwortvergabe
  - Anmeldung an Systemen mit Benutzername und Passwort
  - Regelmäßige Kontrolle von Berechtigungen
  - Sperrung von Berechtigungen ausscheidender Mitarbeiter
  - Zuordnung von Benutzerprofilen zu IT-Systemen
  - Einsatz von Verschlüsselungstechnologie
  - Einsatz von Anti-Viren-Software
- **Zugriffskontrolle** (= alle Maßnahmen, die gewährleisten sollen und können, dass die zur Benutzung eines IT-Systems Berechtigten dies nur im Rahmen der ihnen explizit zugewiesenen Zugangsberechtigung tun können)
  - Festlegung von Berechtigungen in IT-Systemen
  - Differenzierte Berechtigungen für lesen, löschen und ändern
  - Differenzierte Berechtigungen für Daten
  - Anwendungen und Betriebssystem(e)
  - Verwaltung der Rechte durch Systemadministratoren
  - Reduzierung der Zahl der Systemadministratoren auf das Notwendigste
  - Passwortrichtlinie inkl. Passwortlänge und Passwortwechsel
  - Protokollierung von Zugriffen auf Anwendungen
- **Übertragungskontrolle** (= alle Maßnahmen, die gewährleisten sollen und können, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten übermittelt oder sonst zur Verfügung gestellt wurden)
  - Einrichtung von Standleitungen
  - Einsatz von Verschlüsselungstechnologien
  - Erstellen einer Übersicht regelmäßig durchzuführender Abruf- und Übermittlungsvorgänge
  - Dokumentation der Empfänger von Daten
  - Dokumentation der zeitlichen Dauer der Überlassung
  - Dokumentation vereinbarter Löschfristen
- **Transportkontrolle** (=alle Maßnahmen, die gewährleisten sollen und können, dass bei der Übermittlung und dem Transport personenbezogener Daten die Vertraulichkeit und die Richtigkeit der Daten nicht verletzt wird)
  - Einrichtung von Standleitungen
  - Einsatz von Verschlüsselungstechnologien
- **Wiederherstellbarkeit** (= alle Maßnahmen, die gewährleisten sollen und können, dass IT-Systeme und Daten im Störungsfall wiederhergestellt werden können)
  - Erstellen eines Backup- und Recovery-Konzepts
  - Festplattenspiegelung ggf. nach Vereinbarung mit Dienstleister(n)
  - Testen der Wiederherstellung von Systemen und Daten
  - Erstellen eines Notfallplans
- **Zuverlässigkeit** (= alle Maßnahmen, die gewährleisten sollen und können, dass alle Funktionen der IT-Systeme zur Verfügung stehen und Störungen gemeldet werden)
  - Unabhängig voneinander laufende Systeme
  - Automatisierte Meldung von Fehlfunktionen
  - Anti-Viren-Software
- **Datenintegrität** (= alle Maßnahmen, die gewährleisten sollen und können, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können)
  - Erstellen eines Backup- und Recovery-Konzepts
- **Verfügbarkeitskontrolle** (= alle Maßnahmen, die gewährleisten können und sollen, dass personenbe-

zogene Daten gegen Zerstörung und gegen Verlust geschützt sind)

- Geräte zur Überwachung von Temperatur und Feuchtigkeit im Serverraum
- Feuer- und Rauchmeldeanlage(n)
- Feuerlöscheinrichtung im Serverraum
- Aufbewahrung bzw. Durchführung der Datensicherung an einem sicheren, ausgelagerten Ort
- Alarmierung bei unberechtigtem Zutritt zum Serverraum
- Erstellen eines Notfallplans

Die hier aufgeführten Maßnahmen sind wie alle anderen Eintragungen lediglich Beispiele und erheben keinen Anspruch auf Vollständigkeit. Bei der Erstellung der Dokumentation der technischen und organisatorischen Maßnahmen für einen konkreten Betrieb sind diejenigen Maßnahmen anzugeben, die tatsächlich vorhanden sind.

Es muss gewährleistet sein, dass die ergriffenen bzw. noch zu ergreifenden Maßnahmen unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der von der Datenverarbeitung im Betrieb betroffenen Personen ein angemessenes Schutzniveau herstellen, Art. 32 Abs. 1 DS-GVO.

Der Geschäftsführer muss ferner sicherstellen, dass die ihm unterstellten Personen, die mit personenbezogenen Daten umgehen, diese nur auf rechtmäßige Weise behandeln. Hierzu sind die Mitarbeiter, aber auch die Auszubildenden, Leiharbeiter und Praktikanten sowie ggf. auch Aushilfen auf die Einhaltung des Datenschutzes zu verpflichten. Aus Gründen der Nachweisbarkeit empfehlen Datenschutz-Aufsichtsbehörden, die Verpflichtung schriftlich vorzunehmen. Hierzu hält z.B. das Bayerische Landesamt für Datenschutzaufsicht ein Musterformular zur Verfügung.

Das Musterformular ist auf Seite 19 dieses Handbuchs wiedergegeben.

Fig. 21: Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO ist immer dann erforderlich, wenn von einer bestimmten Verarbeitungstätigkeit personenbezogene Daten betreffend ein hohes Risiko für die Rechte und Freiheiten der von der betreffenden Verarbeitungstätigkeit betroffenen Personen ausgeht. Dies ist die Ausnahme und nicht die Regel.

Im Rahmen der Ermittlung der Risikoschwelle sind folgende Aspekte zu berücksichtigen:

- Scoring, Profiling, Evaluation, z.B. die Einschätzung der Kreditwürdigkeit und das auf Verhaltensweisen eines Menschen basierende Schalten von Werbemaßnahmen
- Automatisierte Einzelfallentscheidungen
- Systematische Überwachung
- Verarbeitung sensitiver Daten
- Nach der Zahl der Betroffenen, der Datenmenge und Datenkategorien sowie der Dauer der Verarbeitung eine als umfangreich einzustufende Datenverarbeitung
- Zusammenführen oder Abgleichen von Datenbeständen, wenn von Seiten der Betroffenen damit nicht zu rechnen ist
- Verarbeitung von Daten besonders schutzbedürftiger Personen
- Neuartigkeit von Verarbeitungsvorgängen
- Verwendung neuer Technologien wie z.B. Fingerabdrucksensoren, Gesichtserkennung etc.

- Übermittlung von personenbezogenen Daten an Empfänger außerhalb des räumlichen Geltungsbereichs der Datenschutz-Grundverordnung
- Verarbeitungen, bei denen betroffenen Personen erschwert wird, ihre Rechte auszuüben oder eine Leistung in Anspruch zu nehmen wie z.B. die Beurteilung der Kreditwürdigkeit durch eine Bank vor Vergabe eines Darlehens

Die Datenschutz-Folgenabschätzung ist nach dem Wortlaut der Regelung nur für künftige Verarbeitungen erforderlich. Also ist sie bei Verarbeitungen, mit denen vor dem 25. Mai 2018 begonnen wurde, nicht zwingend.

Sie ist aber durchzuführen, wenn durch eine neue Verarbeitungstätigkeit mindestens zwei der oben genannten Kriterien erfüllt werden. Daher sind Unternehmen bei der Einführung neuer digitaler Werkzeuge verpflichtet, den oben genannten Kriterienkatalog mit den tatsächlichen Vorgängen abzugleichen. Das Ergebnis ist auch dann zu dokumentieren, wenn eine Datenschutz-Folgenabschätzung nicht erforderlich ist. Ist eine Datenschutz-Folgenabschätzung nicht erforderlich, kann in der betreffenden Zeile des Verzeichnisses von Verarbeitungstätigkeiten „nicht erforderlich, da kein hohes Risiko ermittelt“ vermerkt werden.

Fig. 22: Anmerkung

Dieses Feld dient der Möglichkeit, Besonderheiten zu einer einzelnen Verarbeitungstätigkeit zu erfassen.

Weitere allgemeine Anforderungen an Handwerksbetriebe

Neben dem Führen des Verzeichnisses von Verarbeitungstätigkeiten gem. Art. 30 DS-GVO treffen Handwerksbetriebe als für die Datenverarbeitung Verantwortliche gem. Art. 4 Nr. 7 DS-GVO weitere Pflichten, den nachzukommen ist. Die Pflichterfüllung sollte ebenso wie die betreffenden Verarbeitungstätigkeiten selbst dokumentiert werden. Nur dadurch ist gewährleistet, dass Betriebe der recht weitreichenden Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO nachkommen können.

Hierzu gehören unter anderem die Handlungen im Zusammenhang mit der Geltendmachung der Rechte der von der Datenverarbeitung Betroffenen, also von Mitarbeitern, Kunden, Lieferanten etc. Diese können nämlich nach den §§ 15 ff. DS-GVO

- Auskunft verlangen über
  - die Verarbeitungszwecke
  - Kategorien personenbezogener Daten, die verarbeitet werden
  - die Empfänger oder Kategorien von Empfängern, denen gegenüber die Daten offengelegt wurden und noch werden
  - die geplante Dauer der Speicherung
  - das Bestehen eines Rechts auf Berichtigung
  - das Bestehen eines Rechts auf Löschung
  - die Herkunft personenbezogener Daten
  - das Bestehen einer automatisierten Entscheidungsfindung einschließlich eines Profiling und inklusive einer Aufklärung über die involvierte Logik sowie die Tragweite der automatisierten Entscheidungsfindung
- Berichtigung sie betreffender personenbezogener Daten verlangen
- Löschung sie betreffender personenbezogener Daten verlangen
- Einschränkung der Verarbeitung verlangen und
- Bereitstellung zur Übertragung verlangen

Muster für eine schriftliche Verpflichtung auf den Datenschutz

VERPFLICHTUNG ZUR EINHALTUNG DER DATENSCHUTZRECHTLICHEN ANFORDERUNGEN NACH DER DATENSCHUTZ-GRUNDVERORDUNG

Frau/Herr

wurde darauf verpflichtet, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlaubt oder eine Verarbeitung der betreffenden Daten vorgeschrieben ist. Die Grundsätze der Datenschutz-Grundverordnung für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

a) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;

c) dem Zweck angemessen und erheblich sowie auf das für Zwecke der Verarbeitung notwendige Maß beschränkt sein – Grundsatz der Datenminimierung;

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen – Grundsatz der Integrität und Vertraulichkeit.

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe bestraft werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch – zivilrechtliche – Schadensersatzansprüche können sich ergeben, soweit der Verpflichtete schuldhaft gegen die hier niedergelegten Grundsätze handelt. Die sich aus dem Arbeits- oder Dienstverhältnis sowie ggf. aus gesonderten Vereinbarungen ergebenden Vertraulichkeits- und Verschwiegenheitsverpflichtungen werden durch diese Verpflichtungserklärung nicht berührt.

Die hier niedergelegten Verpflichtungen gelten auch dann fort, wenn das Arbeits- oder Dienstverhältnis beendet wurde.

Mir sind die hier aufgezeigten Verpflichtungen bekannt. Ich werde sie einhalten. Eine Ausfertigung dieser Verpflichtungserklärung habe ich erhalten:

_____, den _____._____._____

Ort, Datum

_____ _____

Verpflichteter Dienstherr/Arbeitgeber

Muster eines einfachen Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DS-GVO
(Alle Angaben sind lediglich als Eintragungsbeispiel zu verstehen - weiße Ziffern auf rotem Grund beziehen sich auf die Ausfüllhinweise

1	Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters:	Adam und Eva GmbH In den Gärten 1 88145 Paradies Geschäftsführer: Adam Erstermann	2	Name und Kontaktdaten des betrieblichen Datenschutzbeauftragten:	Josef Zimmermann, Ges. für Datenschutz mbH In den Gärten 2 88145 Paradies Tel.: +49 1234 5678 E-Mail: dsb@paradies.de
5	Kategorien von Empfängern, denen die Daten offengelegt worden sind bzw. werden sowie Empfänger in Drittstaaten:	Steuerberater, Sozialversicherungsträger, Finanzamt, Berufsgenossenschaft, Hausbank, Hosting-Dienstleister und Software as a Service-Anbieter.	6	Übermittlung in Drittstaaten:	Übermittlungen in Drittstaaten finden ausschließlich im Rahmen der Arbeitsvorbereitung und Ausführung von Aufträgen in der Schweiz statt.

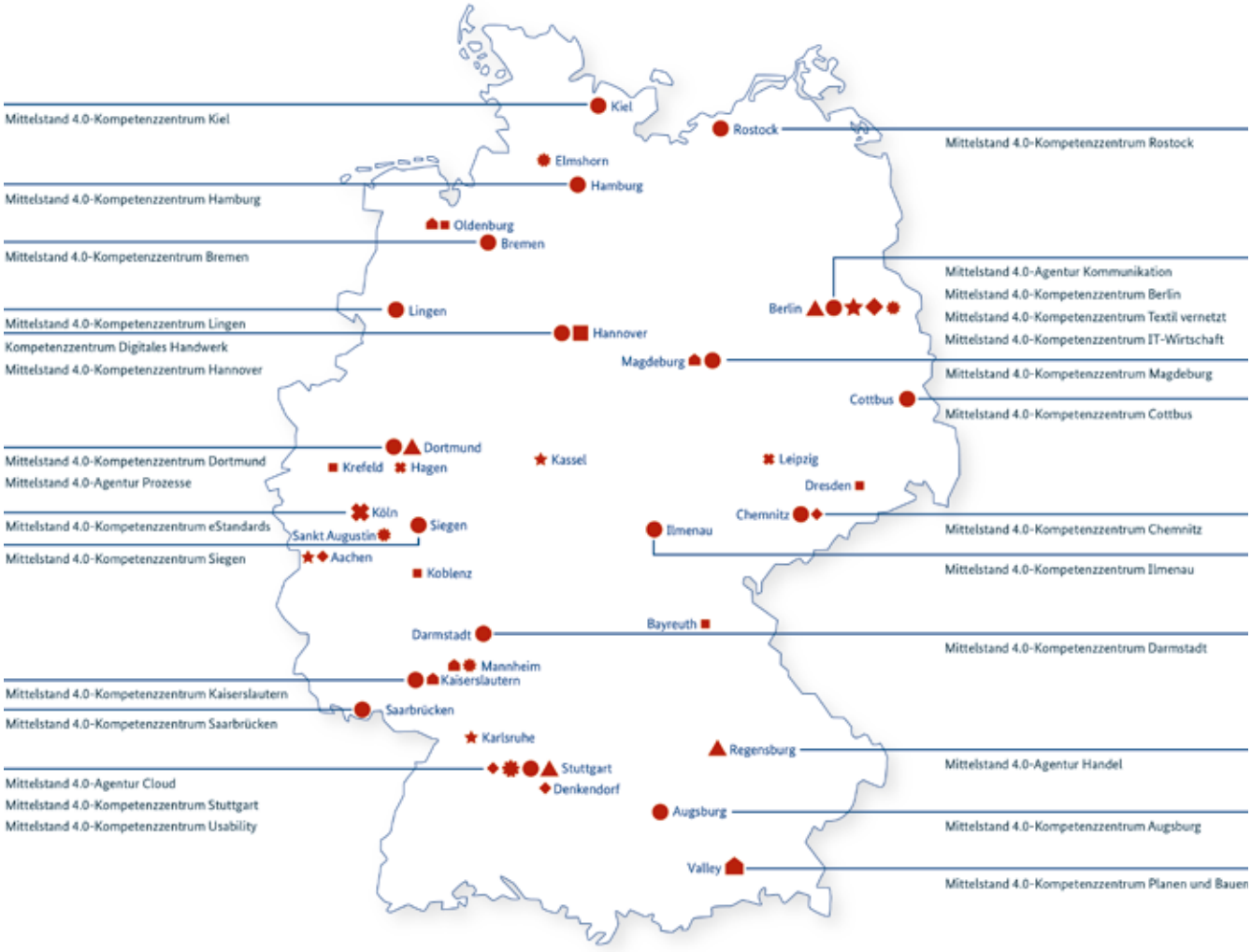
9 Name der Datenverarbeitung	10 Zwecke der Datenverarbeitung	11 Rechtsgrundlage	12 Beschreibung der Verarbeitung	13 Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DS-GVO	14 Betroffene bzw. betroffene Personengruppen	15 Personenbezogene Daten bzw. Datenkategorien	16 Empfänger bzw. Empfängerkategorien
Lohnabrechnung	Auszahlung der Löhne Abfuhr von Sozialabgaben und Steuern	Art. 6 Abs. 1 lit. c) und Art. 28 DS-GVO § 147 AO § 157 HGB § 4 Abs. 2, 2a LStDV		ja	Mitarbeiter	Name, Vorname, Geburtsdatum, -ort, Bankverbindung, Lohn-/Entgeltdaten, Religionszugehörigkeit, Sozialversicherungsdaten, Steuerdaten, insbes. Berufsgenossenschaft	Steuerberater, Hausbank, Sozialversicherungsträger, Finanzamt
Personalverwaltung	Personaladministration Personalführung Arbeitszeitverwaltung Personalbeschaffung	Art. 6 Abs. 1 lit. a), b), c) und f) sowie Art. 88 DS-GVO § 26 BDSG [3] 7 Abs. 7 ArbZeitG		nein	Mitarbeiter Auszubildene Bewerber	Name, Vorname, Anschrift(en) Zeitwirtschaftsdaten Daten zur Arbeitsleistung Leistungsbeurteilung Lebenslauf Bewerbungsunterlagen	keine
Betrieb der Firmenwebsite	Außendartellung	Art. 6 Abs. 1 lit. f) und Art. 28 DS-GVO §§ 14, 15 TMG		nein	Website-Besucher	IP-Adresse	Hosting-Dienstleister
Kundenverwaltung	Bearbeitung von Aufträgen Rechnungsstellung Postalische Werbung	Art. 6 Abs. 1 lit. b) und c) DS-GVO § 257 HGB § 147 AO		nein	Kunden	Name, Vorname, Anschrift(en), Kontaktinformationen insb. Telefonnummer(n), E-Mail Adresse, Auftragsinformationen ggf. Bankverbindung	keine
Aufgabenmanagement	Ressourcenplanung Ressourceneinsatz- Fortschrittskontrolle	Art. 6 Abs. 1 lit. b), c) und f), Art. 28, Art. 88 DS-GVO § 26 DS-GVO		nein	Mitarbeiter Kunden	Name, Vorname Anschrift(en) Antragsinformationen Arbeitsfortschritt	Software as a Service-Anbieter
Videoüberwachung	Einbruchsschutz- Diebstahlschutz Aufklärung von Straftaten	§ 4 Abs. 1 Nr. 2 und 3, Abs. 3 BDSG		nein	Mitarbeiter Besucher Eindringlinge	Äußere Erscheinung der Betroffenen	ggf. Strafverfolgungsbehörde

im Handbuch „Das Verzeichnis von Verarbeitungstätigkeiten - Ein Bauplan gemäß Artikel 30 DS-GVO“)

3	Zweck der Verarbeitung:	Tätigkeitsgegenstand der GmbH ist die Ausführung von Maler- und Trockenbauarbeiten aller Art.	4	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten:	Kundendaten, Mitarbeiterdaten, Daten von Lieferanten und anderen Geschäftspartnern, sofern die Verarbeitung zur Erreichung der vorgenannten Zwecke erforderlich ist.
7	Regelfristen für die Löschung der Datenkategorien:	Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen vorgegeben. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht. Sofern keine spezifischen Aufbewahrungspflichten und -fristen bestimmt sind, werden sie gelöscht, sobald der Zweck ihrer Verarbeitung entfällt.	8	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen:	Die Systeme der Adam und Eva GmbH werden durch eine Vielzahl von Maßnahmen gegen unbefugten Zutritt, Zugang, Zugriff, Verlust und Zerstörung sowie gegen unzulässige Veränderung geschützt. Einzelheiten werden zur jeweiligen Verarbeitungstätigkeit beschrieben.

17 Drittstaatentransfer	18 Zugriffsberechtigte	19 Regelfristen für die Löschung	20 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen	21 Datenschutzfolgenabschätzung	22 Anmerkung
Kein Drittstaatentransfer vorgesehen	Geschäftsführung Assistenz der Geschäftsführung	10 Jahre, Art. 17 Abs. 3 lit. b) DS-GVO, § 147 Abs. 3 AO: beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist.	s. Sicherheitskonzept im Anhang	Nicht erforderlich, da kein hohes Risiko ermittelt	
Kein Drittstaatentransfer vorgesehen	Geschäftsführung Assistenz der Geschäftsführung Bauleiter Meister	**Zeiterfassung**: unverzüglich nach Auswertung, Art. 17 Abs. 1 lit. a) DS-GVO, es sei denn: Überschreitung der werktäglichen Arbeits-zeit gem. § 3 ArbZeitG, dann 2 Jahre gem. § 16 ArbZeitG **Beschäftigte** i.d.R. 3 Jahre nach Ausscheiden aus dem Betrieb Art. 17 Abs. 3 lit. e) DS-GVO ab dem Ende des Kalenderjahres, in dem das Beschäftigungsverhältnis endete. **Zugriffsberechtigungen:** unverzüglich nach Ausscheiden des Mitarbeiters Art. 17 Abs. 3 lit. a) DS-GVO. **Internetzugang**: Verjährungsende aller absehbaren Ansprüche: 7 Monate gem. §§ 4, 5 KSchG ab Ausspruch der Kündigung **Abgelehnte Bewerber:** 6 Monate nach Abschluss des Bewerbungsverfahrens, § 61b ArbGG i.V. mit § 15 AGG	s. Sicherheitskonzept im Anhang	Nicht erforderlich, da kein hohes Risiko ermittelt	
Kein Drittstaatentransfer vorgesehen	Geschäftsführung Assistenz der Geschäftsführung	7 Tage bei bloßem Website-Besuch	s. Sicherheitskonzept im Anhang	Nicht erforderlich, da kein hohes Risiko ermittelt	
Kein Drittstaatentransfer vorgesehen	Geschäftsführung Assistenz der Geschäftsführung Kundendienst Bauleiter Meister	10 Jahre, Art. 17 Abs. 3 lit. b) DS-GVO, § 147 Abs. 3 AO, beginnend mit dem Ende des Kalnderjahres, in dem das Dokument entstanden ist - AUFBEWAHRUNGSPFLICHT!-GoBD-Archiv!	s. Sicherheitskonzept im Anhang	Nicht erforderlich, da kein hohes Risiko ermittelt	
Kein Drittstaatentransfer vorgesehen	Geschäftsführung Assistenz der Geschäftsführung Mitarbeiter	Unverzüglich nach Erledigung der Aufgabe, Art. 17 Abs. 1 lit. a) DS-GVO	s. Sicherheitskonzept im Anhang	Nicht erforderlich, da kein hohes Risiko ermittelt	
Kein Drittstaatentransfer vorgesehen	Geschäftsführung Assistenz der Geschäftsführung	Unverzüglich nach Sichtung, max. 2 Tage nach Aufzeichnungszeitpunkt	s. Sicherheitskonzept im Anhang	Nicht erforderlich, da kein hohes Risiko ermittelt	

Mittelstand 4.0
Kompetenzzentrum Planen und Bauen



Über Mittelstand Digital

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalsierung. Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Weitere Informationen finden Sie unter www.mittelstand-digital.de

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages