Muster-Verzeichnis Verfahren

Mittwoch, 27. November 2019

18:15

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Durchführender / Fachstelle für das Verfahren | Verfahren | Auftragsverarbeitung | Betroffene | Übertragung und Speicherung | Schutzeinstufung der Daten im Verfahren | Technische- und Organisatorische Maßnahmen | Risikobewertung | Bemerkungen |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lfd Nr. | Name | E-Mail | Telefon | Name Verfahren | Beschreibung mit Zweck  (Beschreibung der Notwendigkeit und  Verhältnismäßigkeit der Verarbeitung) | Rechtmäßigkeit | Verarbeitung besonderer  Daten nach Art. 9 DSGVO | Verarbeitung im Auftrag  Für (ich bin Auftrags-  verarbeiter) | Verarbeitung durch externen  Auftragsverarbeiter | Personengruppen | Daten =  Datenkategorien | Empfänger der Daten  (Gruppen in der Regel  keine Einzelnamen) | Empfänger im Drittland | Absicherung der Übermittlung  ins Drittland | Speicherdauer / Regelfristen für Löschung | Schutzstufe der Daten | Schutzzieleinstufung | Zugriffsberechtigte | Spezifische TOMS  für das Verfahren | Risikozahl | DSFA ja/nein | Anmerkungen zum Verfahren  (Verbesserung des Schutzes der  personenbezogenen Daten) |
|  |  |  |  | Abteilung Buchhaltung |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1 | Mustermann | muster@  Xyz.de | 0711/1234567 | Finanzbuchhaltung | Durchführung der Finanzbuchhaltung | Art. 6 Abs. 1 lit. c DSGVO,  § 257 HGB,  § 147 AO | Nein |  |  | Beschäftigte, Kunden,  Partner und Lieferanten | Reisekosten von Beschäftigten, Kundenrechnungsdaten, Daten von Partnern und Lieferanten sowie alle dazugehörigen Abrechnungsunterlagen | Mitarbeiter der  Finanzbuchhaltung | Nein |  | Nach § 147 Abs. 3 AO, zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist.  Achtung: Bei diesen Daten besteht eine Aufbewahrungspflicht! Eine Löschung vor Ablauf dieser Frist kommt nicht in Betracht! | C | 3 | Mitarbeiter der  Finanzbuchhaltung | Finanzbuchhaltung liegt auf separatem Laufwerk - ausschließlicher Zugang FiBU-Mitarbeiter | 3 | Nein | Nach Risikobewertung und Umsetzung spezifischer Maßnahmen liegt das Risiko im Akzeptanzbereich. Die Wirksamkeit wurde überprüft. Details ins der Risikobewertung zum Verfahren |
| 2 |  |  |  | Reiseplanung | Planung von Dienstreisen | Art. 6 Abs.1 lit. f DSGVO | Nein |  |  | Mitarbeiter | Stammdaten, dienstliche Kreditkarte, Reisedaten, Ausweisdaten/Reisepassdaten | Fluglinien, Eisenbahnen,  Autovermietungen,  Hotels, Buchungsplattformen,  Reisebüros, Botschaften,  Immigrationsbehörden | Bei Reisen in Drittstaaten  ggf. zur Buchung und z  ur Beantragung von Visa etc. |  | Nach§ 147 Abs. 3 AO, zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist.  Achtung: Bei diesen Daten besteht eine Aufbewahrungspflicht! Eine Löschung vor Ablauf dieser Frist kommt nicht in Betracht! | C | 3 |  |  |  |  |  |
| 3 |  |  |  | Archivierung der Daten | Optisches Archiv zur revisionssicheren Archivierung  von Auftrags- und Finanzbuchhaltungsdaten.  Geschäftsunterlagen wie Kreditorenrechnungen  oder Dokumenten werden hier manuell gescannt und archiviert. | Art. 6 Abs. 1 lit. c DSGVO,  § 257 HGB , § 147 AO | Nein |  |  | Mandanten, Lieferanten | Eingangs-, Ausgangs-, Buchungsbelege, Unterlagen von Kunden | Zugriffsberechtigte Mitarbeiter | Nein |  | Nach § 147 Abs. 3 AO, zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist. | C | 3 | Mitarbeiter der Abteilung  Buchhaltung, Controlling und Revision | Archivsystem liegt auf eigenem Server ist nicht mit dem Netz verbunden | 2 | Nein |  |
| 4 |  |  |  | Entgeltabrechnung und Lohnbuchhaltung | Berechnung der Monatsgehälter in der Personalabteilung;  Dokumentation der Erstattung von Krankengeld seitens der Krankenkassen | Art. 6 Abs. 1 lit. c DSGVO ,  § 147 AO, § 157 HGB, | Ja |  |  | Mitarbeiter | Stammdaten, Urlaubstage, Krankheitstage (ohne Befund), Monatsgehälter, Religionszugehörigkeit | Mitarbeiter der Lohnbuchhaltung  Steuerbehörden  Krankenkassen  berufsständische Versorgungswerke |  |  | Nach § 147 Abs. 3 AO, zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist.  Achtung: Bei diesen Daten besteht eine Aufbewahrungspflicht! Eine Löschung vor Ablauf dieser Frist kommt nicht in Betracht! | C | 3 |  |  |  |  |  |
| 5 |  |  |  | Allgemeine Abwicklung des Zahlungsverkehrs | Allgemeine Abwicklungen der Zahlungen über den Dienstleister XY GmbH | Art. 6 Abs. 1 lit. b DSGVO | Nein |  |  | Mitarbeiter, Kunden, Geschäftspartner | Name und Kontodaten | Mitarbeiter der Buchhaltung | Möglich |  | Zwei Jahre |  |  | Mitarbeiter der Buchhaltung und die Geschäftsführung |  |  |  |  |
| 6 |  |  |  | Controlling | Controlling zur Planung, Steuerung und Kontrolle aller Unternehmensbereiche. Das Controlling hat hier eine Kostenkontrollfunktion. | Art. 6 Abs.1 lit. f DSGVO | Nein |  |  | Mitarbeiter, Lieferanten, Kunden | Vereinzelte Daten, die im Rahmen von Abrechnungen etc. sichtbar sind. | Mitarbeiter in der Unternehmensführung | Nein |  | Keine, da keine personenbezogenen Daten verarbeitet werden |  |  | Mitarbeiter im Controlling |  |  |  |  |
|  |  |  |  | Personalabteilung |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 | Musterfrau | musterf@yzz.de | 0711/12345 | Arbeitszeiterfassung | Erfassung der Arbeitszeiten der einzelnen Mitarbeiter zur Erfüllung der Nachweispflicht nach § 7 Abs. 7 Arbeitsgesetz. | Art. 6 Abs. 1 lit. c DSGVO, § 7 Abs. 7 Arbeitsgesetz | Nein |  |  | Mitarbeiter | Name, Arbeitszeiten | Mitarbeiter der Personalabteilung | Nein |  | unverzüglich nach Auswertung des Zeitkontos, wenn keine Überschreitung der werktäglichen Arbeitszeit nach § 3 ArbZG existiert. Zu beachtende Sonderregelung: § 16 Abs. 2 ArbZG. Danach besteht eine mindestens zweijährige Aufbewahrungspflicht der Nachweise von Arbeitszeiten, die über die werktägliche Arbeitszeit hin-ausgehen. |  |  | Mitarbeiter der Personalabteilung |  |  |  |  |
| 8 |  |  |  | Recruiting/Bewerbungen | Auswertung von Bewerbungen für eine mögliche Einstellung in der Firma. | §26 BDSG | Möglich |  |  | Bewerber | Personenbezogene Bewerberdaten wie Name, Alter, E-Mail, Adresse | Personalvermittlungsagentur als Dienstleister |  |  | Löschfrist: ohne Vorliegen einer Einwilligung sechs Monate gemäß § 61 b Abs. 1 ArbGG i.V.m. § 15 AGG. Bei Vorhandensein einer Einwilligung zwei Jahre, danach entweder Löschung oder erneute Abfrage der Einwilligung.  Bei Herstellung des Kontaktes über Agenturen Speicherung der Stammdaten bis Vertragsablauf zur Prüfung von Provisionsansprüchen |  |  |  |  |  |  |  |
| 9 |  |  |  | Personalentwicklung | Zur Kommunikation und Begleitung von Veränderungsprozessen im Betrieb  (z.B. Schulungen zu Akquise, zu weitreichenden Änderungen der Gesetzeslage,  bei neuer Software etc.) sowie zur Verbesserung der abteilungsübergreifenden Zusammenarbeit werden verschiedene Coaching- und Schulungsmaßnahmen durchgeführt und dokumentiert. | Art. 6 Abs. 1 lit. f DSGVO | Nein |  |  | Mitarbeiter | Name, Position | Mitarbeiter mit Zugriff auf das Intranet |  |  | Nach Widerspruch |  |  | Mitarbeiter mit Zugriff auf das Intranet |  |  |  |  |
| 10 |  |  |  | Personalaktenführung | Personalaktenführung zur Verwaltung der Mitarbeiter der jeweiligen Abteilung. | § 26 BDSG  Art. 6 Abs.1 lit. f DSGVO | Ja |  |  | Mitarbeiter | Personaldaten, die sich in den Personalunterlagen befinden, wie etwa Schulungsurkunden, Stammdaten | Mitarbeiter der Personalabteilung |  |  | bis zum Verjährungseintritt aller absehbaren geltend zu machenden Ansprüche, § 195 BGB - also drei Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Beschäftigungsverhältnis beendet wurde. |  |  | Mitarbeiter der Personalabteilung und Geschäftsführung |  |  |  |  |
|  |  |  |  | Auftragsabwicklung |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 11 | Hardseller | hardseller@  Xyz.de | 0711/6235272 | Anlegung von Aufträgen | Erfassung der Daten für Anlegung des Auftrags | Art. 6 Abs. 1 S. 1 lit.b DSGVO | Nein |  |  | Kunde | Kundenstammdaten, Auftragsdaten | Mitarbeiter im Vertrieb | Möglich |  | 10 Jahre mit Ablauf des Kalenderjahres, in dem der Auftrag beendet wurde |  |  |  |  |  |  |  |
|  |  |  |  | Marketing und Vertrieb |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 12 | Marketer | marketer@  Xyz.de | 0711/342623 | Tracking-Maßnahmen | Speicherung der IP-Adresse, der besuchten Unterseiten und der Verweildauer durch die Tracking Software beim Besuch der Webseite. Darüber hinaus Einsatz des Analysetool „Google Analytics“ zur Optimierung des Webauftritts. | Art. 6 Abs. 1 S. 1 lit. a DSGVO |  |  |  | Webseitenbesucher | IP-Adresse der Webseitenbesucher  Bewegungen und Clicks der Besucher auf der Webseite  Browser-Fingerprints | Dienstleister XY | Ja | Privacy-Shield | bei bloßem Besuch der Internetseite maximal sieben Tage. |  |  |  |  |  |  |  |
| 13 |  |  |  | Newsletter | Versand von Newslettern und Kundenrundbriefen | Art. 6 Abs. 1 S. 1 lit. a DSGVO, § 7 III UWG |  |  |  | Newsletter-Abonnenten; Kunden | E-Mail-Adresse, ggf. Name | Dienstleister XY | Möglich | Privacy-Shield | Grundsätzlich bei nicht mit einer Befristung versehenen Einwilligungen unbeschränkt bzw. unmittelbar nach Widerruf der Einwilligung oder nach Widerspruch. |  |  |  |  |  |  |  |
|  |  |  |  | Sonstige Verfahren |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 14 |  |  |  | Wartung der Software | Softwarewartung zur Behebung von Fehlern, zur Verbesserung der Performance oder anderer Attribute und Anpassungen an Veränderungen. | Art. 6 Abs. 1 S. 1 lit. f DSGVO |  |  |  | Mitarbeiterdaten, Kundendaten, Lieferantendaten | Alle personenbezogenen Daten, die in der Software sichtbar sind. | Mitarbeiter von XY GmbH als IT-Dienstleister | Nein |  | Es findet keine Speicherung statt, nur Kenntnisnahme |  |  |  |  |  |  |  |
| 15 |  |  |  | IT-Infrastruktur/Netzwerkadministration/IT-Sicherheit | Betreuung und Administration der IT-Infrastruktur | Art. 6 Abs. 1 S. 1 lit. b und f DSGVO |  |  |  | Kunde, Geschäftspartner und Mitarbeiter | Jede Art von Daten | Mitarbeiter IT |  |  | Es findet keine Speicherung statt, nur Kenntnisnahme |  |  |  |  |  |  |  |
| 16 |  |  |  | Audits | Interne Audits für die kontinuierliche Überwachung von Prozessen zur Erfüllung von gesetzlichen Standards oder Richtlinien im Unternehmen. | Art. 6 Abs. 1 S. 1 lit. f DSGVO |  |  |  | Kunde, Geschäftspartner und Mitarbeiter | Jede Art von Daten | Auditoren, Abteilungsleiter, GF |  |  | Es findet keine Speicherung statt, nur Kenntnisnahme |  |  |  |  |  |  |  |
| 17 |  |  |  | E-Mail-System: Outlook | Bereitstellung, Verarbeitung und Archivierung von der E-Mail Kommunikation zur Datensicherung und effizienten Prozessgestaltung. | Art. 6 Abs. 1 S. 1 lit. f DSGVO |  |  |  | Mitarbeiter und Dritte (IT-Dienstleister etc.) | Name, E-Mail, ggf. Anschrift , Kontaktdaten, Nutzungsdaten | Mitarbeiter der IT-Abteilung, mit Zugriffsberechtigung, E-Mail-Empfänger |  |  | unverzüglich nach Zweckerfüllung, bzw. § 147 Abs. 3 AO, zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist. |  |  |  |  |  |  |  |
| 18 |  |  |  | Internetzugang | Gewährleistung von Internetzugang. | Art. 6 Abs. 1 S. lit. f |  |  |  | Mitarbeiter | Browserverläufe, Name, ggf. E-Mail | Mitarbeiter der IT-Abteilung |  |  | bis zum Verjährungseintritt aller absehbaren Ansprüche - sieben Monate gemäß §§ 4, 5 KSchG, beginnend mit dem Ausspruch einer evtl. Kündigung. |  |  |  |  |  |  |  |
| 19 |  |  |  | Nutzerverwaltung und Zugriffsberechtigung IT | Verwaltung von Nutzern und Zugriffsberechtigungen im Active Directory-Verzeichnisdienst | Art. 6 Abs. 1 S. lit. f |  |  |  | Mitarbeiter | Name, Nutzerkennung, berufliche Position, E-Mail-Adresse | Mitarbeiter der IT-Abteilung  Vorgesetzte |  |  | unverzüglich nach Ausscheiden des Mitarbeiters |  |  | Mitarbeiter der IT-Abteilung |  |  |  |  |
| 20 |  |  |  | Persönliches Coaching | Individuelle Beratung einer Person in persönlichen Gesprächen. Notizen und Empfehlungen werden während des Gesprächs in schriftlicher Form notiert |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 21 |  |  |  | Online-Coaching | Persönliches Coaching im Rahmen von Online- oder Telefonmeetings. Aufzeichnung des Coachings als Video und Dokumentation des Gesprächs in Notizen. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 22 |  |  |  | Patientenbehandlung | Behandlung des Patienten zur Vorsorge / bei akuten Problemen. Dokumentation der Behandlung in der Patientenakte (Papier / digital). |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 23 |  |  |  | Kundenverwaltung | Verwaltung und Organisation der Kunden- und Interessentendaten in einer Datenbank / Programm. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 24 |  |  |  | Schulungen / Training | Durchführung von Schulungen / Trainings mit Qualifizierungstest zum Abschluss. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 25 |  |  |  | Webseite | Betrieb einer Webseite / Blog für Marketing, Werbung und Außenauftritt. Erfassung personenbezogener Daten in Logfiles auf Server und ggf. im CMS. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 26 |  |  |  | Webseitenanalyse | Zur Erfassung der Besucherstatistik und daraus folgend die Optimierung der Webseite werden die Zugriffe auf die Webseite analysiert. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 27 |  |  |  | Kontaktformular | Kontaktanfrage über die Webseite für Interessenten und Kunden zur Beantwortung einer spezifischen Anfrage / Frage. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 28 |  |  |  | Kommentarfunktion im Blog | Seitenbesucher können Kommentare abgeben, um eine Diskussion oder Kommunikation am Blog aufzubauen. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 29 |  |  |  | Mitgliederbereich / Login-Bereich | Den Besuchern der Webseite / den Kunden wird ein Mitgliederbereich angeboten, um  - an Diskussionen teilzunehmen  - Beiträge zu verfassen  - auf bezahlte digitale Ware zugreifen zu können |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 30 |  |  |  | Veröffentlichung von persönlichen Informationen Dritter | In Blogbeiträgen werden Interviews und / oder Bilder von Dritten veröffentlicht. Es werden dabei fachliche Informationen zum Blog publiziert. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 31 |  |  |  | Affiliate Marketing | Monetarisierung der Webseite, um durch Produktempfehlungen oder Produktverlinkungen eine Provision durch Käufe von Webseitenbesuchern zu erhalten. Käufe werden durch Gesetze Cookies bei Käufern dienen dazu, die tatsächliche Provision dem Affiliate Partner zuzuordnen. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 32 |  |  |  | Onlineshop | Verkauf von Waren und Dienstleistungen über einen eigenen / oder über einen Dritten Onlineshop. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 33 |  |  |  | Firewalladministration | Zum sicheren Betrieb des Unternehmensnetzwerks wird als Gateway zum Internet eine Firewall betrieben. Es werden regelmäßig Logfiles protokolliert und ausgewertet, um sicherheitskritische Events zu identifizieren. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 34 |  |  |  | IT Serviceprozesse | Es werden IT-Vorfälle und Änderungswünsche im Incident- und Changemanagement-Tool von Kunden / Mitarbeitern erfasst. Die IT-Mitarbeiter können anhand der Tickets die Fälle klassifizieren und bearbeiten. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 35 |  |  |  | PC-User Management | Jeder PC-User im Unternehmen / beim Kunden erhält einen eigenen PC / Laptop und eine eigene Benutzerkennung mit Passwort, sowie eine E-mail Adresse. Die Verwaltung der User wird auf Anweisung des Kunden umgesetzt |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 36 |  |  |  | Administration von Applikationen mit personenbezogenen Inhalten | Zur Konfiguration, Wartung und Durchführung von Updates an zentralen IT-Systemen mit personenbezogenen Daten (z.B. HR-Software, CRM-Software...) müssen die Administratoren Zugriff auf das System erhalten. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 37 |  |  |  | Mitgliederverwaltung | Übersicht und Verwaltung der Mitglieder mit ihren persönlichen Daten in einer Excel Liste, Access Datenbank, externen Anwendung... |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 38 |  |  |  | Terminanmeldung | Anmeldung einzelner Mitglieder für vereinsinterne Veranstaltungen. Eigenständige Anmeldung der Teilnehmer per Telefon / Mail über ein Onlineportal. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 39 |  |  |  | Jubiläum | Ehrung langjähriger Mitglieder nach 10, 20, .... jähriger Mitgliedschaft oder bei runden Geburtstagen. Auswertung der Jubiläen jährlich in Excel Tabellen. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 40 |  |  |  | Übermittlung der Mitgliedsdaten an den übergeordneten Verband | Meldung der persönlichen Daten der Mitglieder beim Eintritt in den Verein an den übergeordneten Verein. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 41 |  |  |  | Beendigung des Beschäftigungsverhältnisses |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 42 |  |  |  | Mahnwesen |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 43 |  |  |  | Lieferantenmanagement |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Hinweis: Das Musterverzeichnis dient als Hilfestellung. So können Sie das Verzeichnis aufbauen.

**Barth Datenschutz empfiehlt:**

Kleinstunternehmen und kleine Vereine mit weniger als 10 Verfahren können diese Tabelle verwenden, anpassen und als Verzeichnis führen. Die Risikobewertung und Schutzeinstufung kann auch im zweiten Schritt erfolgen (Stichwort kontinuierliche Verbesserung). Wenn Sie das Verzeichnis nicht in OneNote führen wollen, können Sie die Tabelle auch in Excel kopieren.

**Unternehmen mit mehr als 10 Verfahren (ist der Regelfall) empfehle ich folgende Vorgehensweise:**

* 1. Erfassen der Verfahren mit Hilfe der Word-Vorlage "Erfassen Verfahren"
  2. Zusammentragen der ausgefüllten Bögen hier in der Dokumentenbibliothek (eigener Ordner ist vorhanden)
  3. Nutzen Sie diese Liste um die Ergebnisse aus den Bögen zusammenfassen - Die Spalten, die Sie nicht ausfüllen können, weil nicht erfasst durch die Mitarbeiter lassen Sie einfach leer (aber nicht die Spalten löschen)
  4. Die Daten aus der Liste tragen Sie in die DSGVO-APP (Online-Verfahrensverzeichnis ADD-On) ein. Diese Liste selbst belassen Sie in OneNote.

**Hinweis: Im Ad-On sind zahlreiche Standardverfahren bereits vorhanden und müssen nur noch minimal angepasst werden. Spezielle Branchenvorlagen kann Barth Datenschutz für Ärzte, Apotheken, Dienstleistungsunternehmen, Fitnessclubs, Vereine, Kanzleien, Industrie und Handwerk zur Verfügung stellen.**