Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO

(Stand 06.2017)

1. Name und Anschrift der verantwortlichen Stelle

REALTECH AG

Industriestr. 39C

69190 Walldorf

2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter

REALTECH AG
Industriestraße 39c
69190 Walldorf
Handelsregister: Registergericht Mannheim
Registernummer: HRB Nr. 351488

Umsatzsteuer-Ident-Nummer: DE 190 955 243

Vorstand: Daniele Di Croce (CEO)
Vorsitzender des Aufsichtsrats: Dr. Wolfgang Erlebach

3. Leiter der Datenverarbeitung der verantwortlichen Stelle

Sascha Mangold, Director ITO

4. Datenschutzbeauftragter

Klaus Brenner

Fa. S + R

Tannenweg 15

69190 Walldorf

Einleitung

Die REALTECH AG ist als Unternehmen nach Art. 30 der Datenschutz-Grundverordnung (DSGVO) ab dem 25.05.2018 verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Dieses ist nach Art. 30 Abs. 4 DSGVO auf Anfrage der Aufsichtsbehörde für den Datenschutz zur Verfügung zu stellen.

Aufbau und Gliederung des Verzeichnisses von Verarbeitungstätigkeiten:

Wir haben für das Verzeichnis von Verarbeitungstätigkeiten die Geschäftsprozesse in unserem Unternehmen ermittelt, mit denen wir personenbezogene Daten verarbeiten. Wir haben uns dabei am „Verarbeitungsbegriff“ i.S.d. Art. 4 Nr. 2 DSGVO orientiert. Danach ist eine „Verarbeitung“ jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Inhalt des Verzeichnisses

Nach Art. 30 Abs. 1 DSGVO hat das Verzeichnis Folgendes zu enthalten:

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
2. die Zwecke der Verarbeitung;
3. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
4. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
5. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland

oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

6. wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
7. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Die Angaben zu Ziff. 1 sind den Inhalten zu den einzelnen Verarbeitungen vorangestellt. Im Hinblick auf Ziff. 7 verweisen wir i.d.R. auf unser Datenschutzmanagementsystem, in dessen Dokumentation die betreffenden Datensicherheitsmaßnahmen aufgeführt bzw. auf diese verwiesen wird und auf die beiliegenden technisch-organisatorischen Maßnahmen bei REALTECH. Sofern es im Hinblick auf eine Verarbeitung Besonderheiten zu Datensicherheitsmaßnahmen gibt, werden wir auf diese im Verzeichnis gesondert hinweisen.

Vorangestellt werden das Öffentliche Verfahrensverzeichnis sowie die technisch-organisatorischen Maßnahmen.

Öffentliches Verfahrensverzeichnis der REALTECH AG

Das BDSG schreibt in § 4g vor, dass der Beauftragte für den Datenschutz jedermann in geeigneter Weise die folgenden Angaben entsprechend § 4e verfügbar zu machen hat:

1. Anschrift der verantwortlichen Stelle:
REALTECH AG
Handelsregister:
Registergericht Mannheim
Registernummer: HRB
Nr. 351488
Umsatzsteuer-Ident-Nummer:
DE 190 955 243

2. Vorstand:
Dipl.-Ing. (FH) Daniele Di Croce (CEO)

3. Anschrift der verantwortlichen Stelle:
Industriestraße 39c
69190 Walldorf

4. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung:
Gegenstand des Unternehmens sind: Die Entwicklung von Softwarelösungen und Dienstleister für Technologie-Consulting.
Die Datenerhebung, -verarbeitung und -nutzung erfolgt zur Ausübung der oben angegebenen Zwecke.

5. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien:
Es werden im wesentlichen personenbezogene Daten zu folgenden Personengruppen, soweit es sich um natürliche Personen handelt, erhoben, verarbeitet und genutzt, soweit diese zur Erfüllung der unter 4. genannten Zwecke erforderlich sind:
- Kundendaten:
Adressdaten, Bankdaten, Ansprechpartner, Vertragsdaten, Steuerungsdaten
- Interessentendaten:
Adressdaten, Produktinteresse
- Mitarbeiterdaten:
Adressdaten, Bankdaten, Bewerberdaten, Vertragsdaten, Daten zur Personalverwaltung und - steuerung
- Aktionärsdaten:
Adressdaten
- Daten von Aufsichtsräten:
Adressdaten, Bankdaten
- Mieterdaten:
Adressdaten, Bankdaten, Vertragsdaten
- Daten von Geschäftspartnern, Agenturen, Vermittlern und Maklern:

Adressdaten, Bankdaten, Abrechnungs- und Leistungsdaten

- Lieferantendaten:
Adressdaten, Bankdaten, Funktionsdaten
- Rechtsanwaltsdaten:
Adressdaten, Bankdaten, Funktionsdaten
- Handelsvertreterdaten:
Vertragsdaten, Bankdaten, Funktionsdaten
6. Empfänger oder Kategorien von Empfängern, denen Daten mitgeteilt werden können:

• Öffentliche Stellen, die Daten aufgrund gesetzlicher Vorschriften (Vorliegen vorrangiger
Rechtsvorschriften) erhalten, z.B. Sozialversicherungsträger und Finanzbehörden.
• Interne Stellen, die an der Ausführung der jeweiligen Geschäftsprozesse beteiligt sind z.B. Buchhaltung, Rechnungswesen, Einkauf, Marketing, Vertrieb und EDV, REALTECH
Niederlassungen
• Externe Auftragnehmer entsprechend §11 BDSG (Verarbeitung oder Nutzung personenbezogener Daten im Auftrag)
• Externe Stellen zur Erfüllung der unter 4. genannten Zwecke

7. Regelfristen für die Löschung der Daten
Der Gesetzgeber hat vielfältige Aufbewahrungsvorschriften und –fristen erlassen. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht, wenn sie nicht mehr zur Vertragserfüllung erforderlich sind. Sofern Daten davon nicht betroffen sind, werden sie gelöscht, wenn die unter 4. genannten Zwecke wegfallen.

8. Geplante Übermittlung an Drittstaaten
Geplante Übermittlung an Drittstaaten ausschließlich von Kunden- und Projektdaten. Das Datenschutzniveau in den Drittstaaten entspricht mittels Standardvertragsklauseln dem deutschen Datenschutz.

Technische und organisatorische Maßnahmen i.S.d. § 9 BDSG und Art. 32 (1) DSGVO

der

Fa. REALTECH
Industriestraße 39c
69190 Walldorf

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- ☐ *Alarmanlage*
- ☒ *Automatisches Zugangskontrollsystem*
- ☐ *Schließsystem mit Codesperre*
- ☐ *Biometrische Zugangssperren*
- ☐ *Lichtschranken / Bewegungsmelder*
- ☒ *Schlüsselregelung (Schlüsselausgabe etc.)*
- ☐ *Protokollierung der Besucher*
- ☒ *Sorgfältige Auswahl von Wachpersonal*
- ☐ *Absicherung von Gebäudeschächten*
- ☒ *Chipkarten-/Transponder-Schließsystem*
- ☒ *Manuelles Schließsystem*
- ☒ *Videoüberwachung der Zugänge*
- ☐ *Sicherheitsschlösser*
- ☐ *Personenkontrolle beim Pförtner / Empfang*
- ☐ *Sorgfältige Auswahl von Reinigungspersonal*
- ☐ *Tragepflicht von Berechtigungsausweisen*

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☒ *Zuordnung von Benutzerrechten*
- ☒ *Passwortvergabe*
- ☒ *Authentifikation mit Benutzername / Passwort*
- ☐ *Gehäuseverriegelungen*
- ☐ *Sperren von externen Schnittstellen (USB etc.)*
- ☒ *Schlüsselregelung (Schlüsselausgabe etc.)*
- ☒ *Protokollierung der Besucher*
- ☒ *Sorgfältige Auswahl von Wachpersonal*
- ☒ *Einsatz von Intrustion-Detection-Systemen*
- ☒ *Erstellen von Benutzerprofilen*
- ☐ *Authentifikation mit biometrischen Verfahren*
- ☒ *Zuordnung von Benutzerprofilen zu IT-Systemen*
- ☒ *Einsatz von VPN-Technologie*
- ☐ *Sicherheitsschlösser*
- ☐ *Personenkontrolle beim Pförtner / Empfang*
- ☐ *Sorgfältige Auswahl von Reinigungspersonal*
- ☐ *Tragepflicht von Berechtigungsausweisen*
- ☐ *Verschlüsselung von mobilen Datenträgern*

☐ *Verschlüsselung von Smartphone-Inhalten*

☒ *Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)*

☒ *Einsatz von Anti-Viren-Software*

☒ *Verschlüsselung von Datenträgern in Laptops / Notebooks*

☒ *Einsatz einer Hardware-Firewall*

☐ *Einsatz einer Software-Firewall*

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

☒ *Erstellen eines Berechtigungskonzepts*

☒ *Verwaltung der Rechte durch Systemadministrator*

☒ *Anzahl der Administratoren auf das „Notwendigste“ reduziert*

☒ *Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel*

☒ *Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten*

☒ *Sichere Aufbewahrung von Datenträgern*

☒ *physische Löschung von Datenträgern vor Wiederverwendung*

☒ *ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)*

☒ *Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)*

☒ *Protokollierung der Vernichtung*

☐ *Verschlüsselung von Datenträgern*

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

☒ *Einrichtungen von Standleitungen bzw. VPN-Tunneln*

☒ *Weitergabe von Daten in anonymisierter oder pseudonymisierter Form*

☐ *E-Mail-Verschlüsselung*

☐ *Erstellen einer Übersicht von regelmäßigenAbruf- und Übermittlungsvorgängen*

☐ *Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen*

☐ *Beim physischen Transport: sichere Transportbehälter/-verpackungen*

☒ *Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen- findet nicht statt*

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ☒ *Protokollierung der Eingabe, Änderung und Löschung von Daten*
- ☐ *Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.*
- ☒ *Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)*
- ☒ *Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind*
- ☒ *Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts*

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- ☒ *Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)*
- ☒ *vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen*
- ☒ *schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG*
- ☒ *Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)*
- ☒ *Auftragnehmer hat Datenschutzbeauftragten bestellt*
- ☒ *Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags*
- ☒ *Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart*
- ☐ *laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten*
- ☐ *Vertragsstrafen bei Verstößen*

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- ☒ *Unterbrechungsfreie Stromversorgung (USV)*
- ☒ *Klimaanlage in Serverräumen*
- ☒ *Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen*
- ☒ *Schutzsteckdosenleisten in Serverräumen*
- ☒ *Feuer- und Rauchmeldeanlagen*
- ☒ *Feuerlöschgeräte in Serverräumen*
- ☐ *Alarmmeldung bei unberechtigten Zutritten zu Serverräumen*
- ☒ *Erstellen eines Backup- & Recoverykonzepts*
- ☒ *Testen von Datenwiederherstellung*
- ☒ *Erstellen eines Notfallplans*

☒ *Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort*

☒ *In Hochwassergebieten: Serverräume über der Wassergrenze- trifft nicht zu*

☒ *Serverräume nicht unter sanitären Anlagen*

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

☒ *physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern*

☒ *Erstellung eines Berechtigungskonzepts*

☐ *Versehen der Datensätze mit Zweckattributen/Datenfeldern*

☒ *Festlegung von Datenbankrechten*

☒ *Logische Mandantentrennung (softwareseitig)*

☐ *Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden*

☒ *Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System*

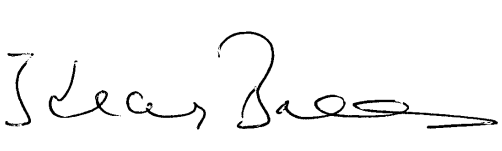
☒ *Trennung von Produktiv- und Testsystem*

30.03.17

Datum

Sascha Mangold, Director ITO
Klaus Brenner, S + R, externer DB

Verantwortlicher für die Erstellung (in Druckbuchstaben)



Unterschrift des Verantwortlichen

Verfahren (Anlagen)

Videoüberwachung

Personaldatenverarbeitung Progress- ersetzt seit 01.04.2017

Lohnbuchhaltung (DB Direct)

Finanzbuchhaltung – FiBU (SAP)- ersetzt seit 01.03.2017

Telefonanlage (Ayava analog)

E-Mail (MS Exchange online)

CRM (MS CRM online)- ersetzt seit 01.03.2017

Zutrittskontrolle (Siemens)

Projektmanagement (Profit)- ersetzt seit 01.04.2017

Softwareentwicklungstool (Jira)

Onlinespeicherplatz (MS-One Drive for Business)

Projektmanagement und Dokumentenablage (MS Sharepoint online)

SAP Business by Design- Ersatz für Progress, Profit, SAP FI und CRM ab 01.04.2017

Videoüberwachung

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Zweck der Videoüberwachung sind einerseits die Wahrnehmung des Hausrechts und der präventive Schutz vor unbefugten Zutritten zum Betriebsgelände bzw. des Bürogebäudes sowie Einbruch- und Vandalismusschutz, deshalb erfolgt eine Aufzeichnung von Videomaterial für Zwecke der Aufdeckung und Aufklärung von Straftaten.

2. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

Es werden nachfolgende Daten/Datenkategorien verarbeitet:

- optische Videoaufnahmen der Notausgänge des Unternehmens der REALTECH – eine Tonaufzeichnung erfolgt nicht

Betroffene Personengruppen

- Mieter, Mitarbeiter und Besucher der REALTECH AG

3. Empfänger oder Kategorien von Empfängern der Daten

Eine Übermittlung von Daten an Dritte erfolgt grundsätzlich nur dann, wenn der Verdacht einer Straftat vorliegt. In dem Fall kann eine Weitergabe der Daten an Strafverfolgungsbehörden erfolgen. Eine sonstige Weitergabe an Dritte erfolgt nur, wenn eine Rechtsgrundlage für die Übermittlung der Daten besteht.

4. Datenübermittlung in Drittländer

Eine Übermittlung von Daten in Drittstaaten findet grundsätzlich nicht statt.

5. Regelfristen für die Löschung der Daten

Die Videoaufnahmen werden für eine Dauer von 10 Tagen gespeichert und im Anschluss durch Neuaufnahmen automatisch überschrieben.

6. Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 BDSG)

Der Server, über den die Videoüberwachung und -aufzeichnung durchgeführt wird, befindet sich im Serverraum des Unternehmens. Insoweit wird auf die technischen und organisatorischen Maßnahmen verwiesen.

7. Zugriffsberechtigte Personen

Zugriffsrechte werden ausschließlich über Administratoren vergeben.
Zur Administration der Hard- und Software bestehen ferner Zugriffsrechte für die Systemadministratoren. Dies sind die FM Mitarbeiter.

Personaldatenverarbeitung Progress-

wird ab 01.04.2017 als reines Archivsystem genutzt, die Daten migriert in SAP by Design und dort findet die produktive Arbeit statt!

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Die Verarbeitung von Daten von Beschäftigten erfolgt im Bereich der Personalabteilung HR. Zweck der Verarbeitung ist Begründung, Durchführung, Ausgestaltung und Beendigung von Beschäftigungsverhältnissen.

Daten von Bewerbern werden für Zwecke der Auswahl von potentiellen Beschäftigten erhoben, verarbeitet und genutzt. Sobald ein Beschäftigungsverhältnis begründet worden ist (z.B. durch Aufnahme der Arbeitstätigkeit) werden die Beschäftigtendaten verwendet, um die Pflichten des Arbeitgebers („verantwortliche Stelle“) gegenüber den Beschäftigten erfüllen zu können. Gleiches gilt für etwaige Rechtspflichten gegenüber staatlichen Stellen – z.B. im Bereich der Sozialabgaben.

Im Unternehmen wird eine betriebliche Altersversorgung angeboten. Um diese Zwecke erfüllen zu können, ist eine Verarbeitung von Daten von ausgeschiedenen Beschäftigten im Rahmen der Erforderlichkeit geboten.

2. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

Es werden nachfolgende Daten/Datenkategorien verarbeitet:

- Daten zur Person
    - Name, Anschrift, Geburtsdatum, Telefonnummer
    - Angaben zur Religionszugehörigkeit
    - Angaben zum Familienstand / Angaben zu Kindern
    - Bankverbindung
- Angaben zur beruflichen Qualifikation und Schulausbildung
- Angaben zu Lohnpfändungen
- Angaben zur beruflichen Weiterbildung
- Urlaubszeiten
- Informationen im Zusammenhang mit dem betrieblichen Eingliederungsmanagement (BEM); diese werden jedoch gesondert geführt.

Betroffene Personengruppen:

- Beschäftigte des Unternehmens
- Bewerber
- ehemalige Beschäftigte
- ggf. Dritte

3. Empfänger oder Kategorien von Empfängern der Daten

Die Daten werden intern im Unternehmen an Beschäftigte mit Personalverantwortung weitergegeben, wenn und soweit dies für betriebliche Belange zwingend erforderlich ist.

Eine Weitergabe von Beschäftigtendaten findet ferner an staatliche Stellen statt, soweit gesetzliche Übermittlungsverpflichtungen bestehen.

Eine Weitergabe an nichtöffentliche Stellen findet grundsätzlich nur dann statt, wenn hierfür eine Rechtsgrundlage besteht.

Im Übrigen fiindet eine Weitergabe von Beschäftigtendaten nur statt, wenn der betroffene Beschäftigte eine schriftliche Einwilligung erteilt hat.

4. Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer findet nicht statt.

5. Regelfristen für die Löschung der Daten

Personaldaten werden für die Dauer des Beschäftigungsverhältnisses gespeichert und werden spätestens 10 Jahre nach Beendigung des Beschäftigungsverhältnisses gelöscht-Skills und Ausbildungsdaten sofort. Ausgenommen hiervon sind die Daten, für die andere gesetzliche Aufbewahrungspflichten bestehen.

Daten über eine Abmahnung werden für maximal 36 Monate gespeichert.

Sofern der Beschäftigte ein Angebot der betrieblichen Altersversorgung in Anspruch nimmt, werden die Beschäftigtendaten auch über das Ende des Beschäftigungsverhältnisses verarbeitet und genutzt, soweit dies für die Erbringung der betrieblichen Altersversorgung erforderlich ist.

6. Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 BDSG)

Die Personaldaten werden auf dedizierten virtuellen Servern im Serverraum verarbeitet. Insoweit gelten die allgemeinen technischen und organisatorischen Maßnahmen, auf die insoweit verwiesen wird.

Im Hinblick auf die Zugriffskontrolle wird Sorge dafür getragen, dass ausschließlich Mitarbeiter der Personalabteilung Zugriffsrechte erhalten. Es gibt zudem nur ein kleines Administratorenteam, das für die Vergabe von Rechten zuständig ist. Mitarbeiter außerhalb der Personalabteilung erhalten nur dann Zugriffsrechte, wenn dies von der Geschäftsleitung in Textform genehmigt wurde.

7. Zugriffsberechtigte Personen

Mitarbeiter der Personalabteilung als Administratoren, die Geschäftsführung.

Lohnbuchhaltung (DB Direct)

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Die Verarbeitung von Daten im Bereich der Lohnabrechnung erfolgt durch Einbindung eines externen Lohnbuchhaltungsdienstleisters (SD Workx, 63303 Dreeich, Im Gevierth 13c). Mit dem Dienstleister wurde ein Auftragsdatenverarbeitungsvertrag geschlossen.

Zur Durchführung der Lohnabrechnung werden an den Lohnbuchhaltungsdienstleister Daten über die Beschäftigten, deren Lohneingruppierung, Konfession, Angaben zur Krankenversicherung, Arbeitszeiten und ggf. weitere für die Lohnabrechnung unerlässlichen Daten verschlüsselt weitergegeben.

Der Lohnbuchhaltungsdienstleister führt die Lohnabrechnung durch und bereitet die Überweisung von Gehaltszahlungen vor. Die Überweisung selbst erfolgt durch unser Unternehmen. Gleiches gilt für zu zahlende Sozialabgaben. Auch hier wird eine Berechnung durch Lohnbuchhaltungsdienstleister durchgeführt und die Überweisungen vorbereitet. Die Auszahlung der Sozialabgaben erfolgt dann wiederum selbst durch unser Unternehmen und zwar im Vieraugenprinzip, weshalb der Leiter der FiBu Einsicht in die fertigen Daten hat.

2. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

Es werden nachfolgende Daten/Datenkategorien verarbeitet:

- Daten zur Person
    - Name, Anschrift, Geburtsdatum
    - Angaben zur Religionszugehörigkeit
    - Angaben zum Familienstand / Angaben zu Kindern
    - Bankverbindung
- Angaben zu Lohnpfändungen

Betroffene Personengruppen:

- Beschäftigte des Unternehmens

3. Empfänger oder Kategorien von Empfängern der Daten

Empfänger der Daten ist der Lohnbuchhaltungsdienstleister. Darüber hinaus erhalten auch Mitarbeiter mit Personalverantwortung unter Berücksichtigung des „Need-to-know“-Prinzips ggf. Kenntnis von Bruttolohnberechnungen.

Einen Teil der Daten wird zudem im Rahmen der gesetzlichen Pflichten an Sozialversicherungsträger bzw. Krankenkassen weitergegeben.

Im Falle von Lohnpfändungen werden ggf. Daten an den bzw. die Gläubiger im Rahmen der gesetzlichen Vorgaben weitergegeben.

4. Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer findet nicht statt.

5. Regelfristen für die Löschung der Daten

Lohnbuchhaltungsdaten werden als buchhaltungsrelevante Daten für 10 Jahre aufbewahrt und im Anschluss gelöscht, soweit diese nicht im Zusammenhang mit Verfahren bei der Finanzverwaltung oder vor den Finanzgerichten erforderlich sind.

6. Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 BDSG)

Die Lohnbuchhaltungsdaten werden auf dedizierten virtuellen Servern im Serverraum verarbeitet. Insoweit gelten die allgemeinen technischen und organisatorischen Maßnahmen, auf die insoweit verwiesen wird.

Der Lohnbuchhaltungsdienstleister verarbeitet die Daten auf einem dedizierten Server in einem Rechenzentrum in Deutschland. Der gesamte Rechenzentrumsbetrieb ist nach ISO 27001 und PCI-DSS zertifiziert. Das Statement of Applicability (SOA) ist vor der Beauftragung des Dienstleisters in Augenschein genommen und geprüft worden. Gleiches gilt für die Kontrolle des Auftragsdatenverarbeiters nach § 11 Abs. 2 BDSG.

Im Übrigen werden die Lohnbuchhaltungsdaten wie Personaldaten behandelt. Insoweit gelten die dortigen Ausführungen entsprechend.

7. Zugriffsberechtigte Personen

Mitarbeiter der Personalabteilung als Administratoren, Mitarbeiter des Lohnbuchhaltungsdienstleisters, Leiter FiBu

Finanzbuchhaltung – FiBU (SAP)-

wird ab 01.03.2017 als reines Archivsystem genutzt, die Daten migriert in SAP by Design und dort findet die produktive Arbeit statt!

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Die Finanzbuchhaltung (FiBu) dient der Erfassung und Dokumentation aller finanzwirksamen Vorgänge im Unternehmen. Erfasst werden alle Umsätze sowie das Anlagevermögen im Unternehmen.

Die FiBu dient weiter dem Zweck der Steuer- und Abgabenerfassung und -zahlung an die Finanzverwaltung sowie ggf. weitere öffentlichen Stellen, an die Steuern, Gebühren oder sonstige Abgaben zu zahlen sind.

2. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

Es werden nachfolgende Daten/Datenkategorien verarbeitet:

- Namen, Anschrift, Bankverbindungen, Umsatzsteuer-Identifikationsnummer von Debitoren und Kreditoren
- Umsätze inkl. Rechnungsnummern, Verwendungszwecke und sonstige Angaben, die im Zusammenhang mit Finanztransaktionen anfallen
- Angaben zu Anlagevermögen

Betroffene Personengruppen:

- Debitoren, Kreditoren

3. Empfänger oder Kategorien von Empfängern der Daten

Daten der FiBu werden – soweit gesetzlich erforderlich – an die Finanzverwaltung weitergegeben. Eine Weitergabe der Daten erfolgt auch an Steuerberater und Wirtschaftsprüfer.

Ansonsten erfolgt eine Weitergabe der Daten, wenn und soweit eine Rechtsgrundlage für die Datenübermittlung vorliegt.

4. Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer findet nicht statt.

5. Regelfristen für die Löschung der Daten

Buchhaltungsdaten werden für eine Dauer von 10 Jahren aufbewahrt.

6. Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 BDSG)

Die FiBu werden auf IT-Systemen im Serverraum verarbeitet. Insoweit gelten die allgemeinen technischen und organisatorischen Maßnahmen, auf die insoweit verwiesen wird.

7. Zugriffsberechtigte Personen

Mitarbeiter der FiBu als Administratoren, Mitarbeiter der Finanzverwaltung im Falle von Betriebsprüfungen, Steuerberater (anlassbezogen), Wirtschaftsprüfer (anlassbezogen)

Telefonanlage (Ayava analog)

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Erbringung von Telekommunikationsdienstleistungen für eigene (interne) Zwecke

2. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

Es werden nachfolgende Daten/Datenkategorien verarbeitet:

- Nebenstelle
- ggf. Name
- Verkehrsdaten (i.S.d. § 96 TKG)

Betroffene Personengruppen:

- Beschäftigte
- Kunden / Interessenten
- Vertragspartner
- sonstige Dritte

3. Empfänger oder Kategorien von Empfängern der Daten

Die Verkehrsdaten werden grundsätzlich nicht weitergegeben, sondern nur anlassbezogen für die Beseitigung von Störungen bzw. für Abrechnungsprüfungen genutzt. ADV wurde mit der Hersteller-(Wartungs-)firma geschloßen.

4. Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer findet nicht statt.

5. Regelfristen für die Löschung der Daten

Verkehrsdaten werden maximal für 6 Monate gespeichert. Aggregierte Daten können darüber hinaus gespeichert und genutzt werden, sofern sichergestellt ist, dass aus den Daten kein Personenbezug mehr herzuleiten ist.

6. Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 BDSG)

Die Telefonanlage befindet sich im Serverraum. Insoweit gelten die allgemeinen technischen und organisatorischen Maßnahmen, auf die insoweit verwiesen wird.

7. Zugriffsberechtigte Personen

Telefonanlagen-Administratoren, IT

E-Mail (MS Exchange online)

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Elektronische Kommunikation per E-Mail

2. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

Es werden nachfolgende Daten/Datenkategorien verarbeitet:

- „Bestandsdaten“ – Name
- E-Mail-Adresse
- ggf. weitere Headerdaten
- „Inhaltsdaten“ (Inhalte von E-Mails – „Body“)

Betroffene Personengruppen:

- Beschäftigte
- Kunden / Interessenten
- Vertragspartner
- sonstige Dritte

3. Empfänger oder Kategorien von Empfängern der Daten

Mitarbeiter, Vorgesetzte, Kunden, Vertragspartner, sonstige Dritte

4. Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer findet dann statt, wenn sich der jeweilige Kommunikationspartner in einem Drittstaat befindet.

Darüber hinaus kann bei einer Kommunikation per E-Mail über das Internet grundsätzlich nicht ausgeschlossen werden, dass E-Mails über Kommunikationssysteme in Drittstaaten geroutet werden.

5. Regelfristen für die Löschung der Daten

Für E-Mails gelten, soweit diese als Geschäftsbriefe zu qualifizieren sind, Aufbewahrungspflichten nach dem HGB. Die Aufbewahrungspflicht bezieht sich auf einen Zeitraum von 6 Jahren.

Nach Ablauf dieser Frist werden die entsprechenden Daten routinemäßig gelöscht, wenn sie nicht mehr zur Durchführung oder Beendigung von Verträgen erforderlich sind.

Kurzfristigere Löschungen werden in besonderen Bereichen (z.B. Bewerberdaten) vorgenommen.

6. Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 BDSG)

Der lokale E-Mail-Server befindet sich im Serverraum. Zusätzlich gibt es ein E-Mail Archivierungsprogramm auf einem Server im Serverraum. Insoweit gelten die allgemeinen technischen und organisatorischen Maßnahmen, auf die insoweit verwiesen wird.

Der online Exchange Server befindet sich in einer Cloud von MS auf europäischem Boden, ein ADV wurde abgeschlossen.

7. Zugriffsberechtigte Personen

E-Mail-Account-Inhaber -beschränkt auf ihren Account, Administratoren, IT

CRM (MS CRM online)

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Die Software wird für Zwecke der Adressverwaltung, Kundenpflege, Marketing, Durchführung von Kundenanschreiben/-informationen etc. verwendet.

2. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

Es werden nachfolgende Daten/Datenkategorien verarbeitet:

- Name
- Titel
- Vorname
- Privatadresse
- Telefon
- Fax
- Telefon (privat)
- Mobiltelefon
- Internetadresse
- E-Mail
- Position
- Geburtsdatum
- Firma
- Firmenanschrift
- Mitarbeiteranzahl
- Branche
- Kundennummer
- Kundenart
- Telefon (Firma)
- Fax (Firma)
- Kontakthistorie

Betroffene Personengruppen:

- Beschäftigte
- Kunden
- Vertragspartner
- Dritte

3. Empfänger oder Kategorien von Empfängern der Daten

- Beschäftigte aus anderen Abteilungen
- Dienstleister für den Versand von Informationen an Personen, deren Daten im CRM-System gespeichert sind
- ggf. Dritte

4. Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer findet grundsätzlich nicht statt.

5. Regelfristen für die Löschung der Daten

Die Datensätze werden für die Dauer des jeweiligen Vertragsverhältnisses bzw. rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnis gespeichert. Eine Verwendung der Daten kann ferner auf Basis einer Einwilligung des Betroffenen oder – bei Vorliegen der gesetzlichen Voraussetzungen – auf Basis einer Interessenabwägung (z.B. nach § 28 Abs. 1 Nr. 2 BDSG) erfolgen.
Eine Löschung erfolgt grundsätzlich nicht automatisch. Im Unternehmen wird der Datenbestand im CRM regelmäßig gesichtet. Nicht mehr für die Zwecke des Verfahrens erforderliche Daten werden dann manuell gelöscht.

6. Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 BDSG)

Das CRM-System wird auf einem europäischen Server in der MS Cloud betrieben. Ein ADV ist abgeschlossen.

7. Zugriffsberechtigte Personen

Beschäftigte, Marketing als Administratoren, IT

Zutrittskontrolle (Siemens)

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Die Software wird für Zwecke der geordneten und dokumentierten Zutrittskontrolle mittels eine Chipkarte verwendet.

2. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

Es werden nachfolgende Daten/Datenkategorien verarbeitet:

- Name, Vorname
- Personalnummer u. Kostenstelle bei eigenen MA
- Firma

Betroffene Personengruppen:

- Beschäftigte
- Kunden, Mieter
- Vertragspartner
- Dritte

3. Empfänger oder Kategorien von Empfängern der Daten

Die Verkehrsdaten werden grundsätzlich nicht weitergegeben, sondern nur anlassbezogen für die Beseitigung von Störungen bzw. für Straftatenprüfungen genutzt. ADV wurde mit der Hersteller-(Wartungs-)firma geschloßen.

4. Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer findet grundsätzlich nicht statt.

5. Regelfristen für die Löschung der Daten

Verkehrsdaten werden maximal für 8 Wochen gespeichert und dann automatisch überschrieben. Aggregierte Daten können darüber hinaus gespeichert und genutzt werden, sofern sichergestellt ist, dass aus den Daten kein Personenbezug mehr herzuleiten ist.

6. Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 BDSG)

Die Zutrittsanlage befindet sich im Serverraum. Insoweit gelten die allgemeinen technischen und organisatorischen Maßnahmen, auf die insoweit verwiesen wird.

7. Zugriffsberechtigte Personen

FM als Administratoren, IT

Projektmanagement (Profit)-

wird ab 01.04.2017 als reines Archivsystem genutzt, die Daten migriert in SAP by Design und dort findet die produktive Arbeit statt!

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Die Software wird für Zwecke des Projektmanagements sowie zu deren Aufwandsverrechnung -Dauer, Reisekosten- und zur Mitarbeiterverwaltung verwendet.

2. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

Es werden nachfolgende Daten/Datenkategorien verarbeitet:

- Name, Vorname
- Geburtsdatum
- Personalnummer u. Kostenstelle bei eigenen MA
- Firma

Betroffene Personengruppen:

- Beschäftigte
- Freelancer
- Kunden
- Vertragspartner
- Dritte

3. Empfänger oder Kategorien von Empfängern der Daten

Die Projektdaten werden grundsätzlich nicht weitergegeben, sondern nur anlassbezogen für Prüfungen genutzt. ADV wurde mit der Hersteller-(Wartungs-)firma Information Desire GmbH geschloßen.

4. Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer findet grundsätzlich nicht statt.

5. Regelfristen für die Löschung der Daten

Projektdaten werden für 5 Jahre gespeichert zur Finanzprüfung, Rechnungsdaten nach 10 Jahren.

6. Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 BDSG)

Die PROfitsoftware läuft auf einem Server im Serverraum. Insoweit gelten die allgemeinen technischen und organisatorischen Maßnahmen, auf die insoweit verwiesen wird.

7. Zugriffsberechtigte Personen

Projektoffice als Administratoren, IT

Softwareentwicklungstool (Jira)

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Die Software wird für Zwecke der Entwicklung von Softwareprodukten eingesetzt. Dort unterstützt es das Anforderungsmanagement, die Statusverfolgung und später den Fehlerbehebungsprozess.

2. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

Es werden nachfolgende Daten/Datenkategorien verarbeitet:

- Name, Vorname
- Mailadresse
- Telefonnummer

Betroffene Personengruppen:

- Beschäftigte

3. Empfänger oder Kategorien von Empfängern der Daten

Die Daten werden grundsätzlich nicht weitergegeben, sondern nur projektbezogen im Projektteam genutzt. ADV wurde mit der Hersteller-(Wartungs-)firma Atlassian, Sydney, Australien, geschloßen.

4. Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer findet grundsätzlich nicht statt.

5. Regelfristen für die Löschung der Daten

Die Daten werden mit Projektende gelöscht, sofern keine gesetzlichen anderen Fristen vorliegen.

6. Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 BDSG)

Die Jirasoftware läuft auf einem Server im Serverraum. Insoweit gelten die allgemeinen technischen und organisatorischen Maßnahmen, auf die insoweit verwiesen wird.

7. Zugriffsberechtigte Personen

Administratoren, IT, Projektmitarbeiter

Onlinespeicherplatz (MS-One Drive for Business)

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Lokal auf dem PC gespeicherte Dokumente werden in die Cloud synchronisiert und können dann für Dritte freigeschaltet werden.

2. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

Es werden nachfolgende Daten/Datenkategorien verarbeitet:

- „Bestandsdaten“ – Name
- E-Mail-Adresse
- gesch. Telefonnummer

Betroffene Personengruppen:

- Mitarbeiter

3. Empfänger oder Kategorien von Empfängern der Daten

Mitarbeiter, Vorgesetzte

4. Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer findet grundsätzlich nicht statt.

5. Regelfristen für die Löschung der Daten

Die Daten werden mit Projektende gelöscht, sofern keine gesetzlichen anderen Fristen vorliegen.

6. Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 BDSG)

Die One-Drive-software läuft auf einem Server im Serverraum. Insoweit gelten die allgemeinen technischen und organisatorischen Maßnahmen, auf die insoweit verwiesen wird.

Darüberhinaus wird One-Drive auf einem europäischen Server in der MS Cloud betrieben. Ein ADV ist abgeschlossen.

7. Zugriffsberechtigte Personen

Mitarbeiter -beschränkt auf ihren Account, Administratoren IT

Projektmanagement und Dokumentenablage (MS Sharepoint online)

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Cloudbasierter Dienst von MS für operatives Projektmanagement und interne Dokumentenablage zur Teamnutzung.

2. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

Es werden nachfolgende Daten/Datenkategorien verarbeitet:

- „Bestandsdaten“ – Name
- E-Mail-Adresse
- gesch. Telefonnummer

Betroffene Personengruppen:

- Mitarbeiter

3. Empfänger oder Kategorien von Empfängern der Daten

Mitarbeiter, Vorgesetzte

4. Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer findet grundsätzlich nicht statt.

5. Regelfristen für die Löschung der Daten

Die Daten werden mit Projektende anlaßbezogen gelöscht, sofern keine gesetzlichen anderen Fristen vorliegen.

6. Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 BDSG)

Sharepoint wird auf einem europäischen Server in der MS Cloud betrieben. Ein ADV ist abgeschlossen.

7. Zugriffsberechtigte Personen

Mitarbeiter -beschränkt auf öffentlichen Bereich für MA-Informationen, MA projektbezogen gemäß Freigabe durch Projektleiter, Administratoren IT

SAP Business by Design

Diese Software wird in der Cloud genutzt, die Daten werden nur in Deutschland verarbeitet. Es ersetzt vier andere, bisherige Systeme, nämlich CRM – sofort zum 01.03.2017-, SAP FI- sofort zum 01.03.2017-, Profit und Progress zum 01.04.2017.

Die genaue Definition bitte den vier Vorsystemen entnehmen- diese werden deshalb im Verfahrensverzeichnis nicht gelöscht, sondern bei Migration und Ersatz/Wegfall des Systems entsprechend gekennzeichnet!

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Ersatz der bisherigen verstreuten Toollandschaft durch ein zentrales ERP-System

- Projektmanagement
- CRM- Kundendaten, Salespipeline
- Mitarbeiterverwaltung
- Urlaubs- und Krankheitsverwaltung MA
- Projektbezogene Zeiterfassung
- Reisekosten
- HR-Mitarbeiterstammdaten

2. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

3. Empfänger oder Kategorien von Empfängern der Daten

4. Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer findet grundsätzlich nicht statt.

5. Regelfristen für die Löschung der Daten

6. Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 BDSG)

SAP Business by Design wird auf einem europäischen Server in der Cloud betrieben. Ein ADV ist abgeschlossen.

7. Zugriffsberechtigte Personen

s. Rollen- und Zugriffskonzept