Product Service

Mehr Sicherheit.
Mehr Wert.

Gutachten
Nr. 028-713132387-000 Rev. 00

Datenschutz-Gutachten
der webbasierten Business-Software “myfactory”

Gegenstand	Datenschutz-Gutachten der webbasierten Business-Software „myfactory“
Prüfungsart	Gutachten
Grundlage	TÜV SÜD Prüfkatalog zur Qualität von Anwendungs-Software auf der Basis anerkannter Anforderungen und Standards
Prüfspezifikationen	TÜV SÜD Product Service Prüfgrundsätze, basierend auf PPP 13011:2018
Zeitraum der Gutachten-Erstellung	30. April 2018 bis 02. Juni 2018
Berichtsdatum	02. Juni 2018
Unternehmen / Auftraggeber	myfactory International GmbH
Auftrags-Nr./ Kunden-Nr.	713132387 / 73824
Straße / Postfach	Rosenheimer Straße 141 h
PLZ / Ort	81671 München
Ansprechpartner	Rainer Giersbach
TÜV-Sachverständiger	Tuan Khai Hoang
Unterauftragnehmer	Hans-Ulrich Bierhahn (Produktspezialist Datenschutz, Datensicherheit)
Ergebnis	Die Anforderungen der Prüfgrundlage sind erfüllt

Telefon: + 49 (0)89 361965 268
Telefax: + 49 (0)89 5155 2367
www.tuev-sued.de
E-Mail: swq@tuev-sued.de

TÜV SÜD Product Service GmbH
Daimlerstrasse 11
85748 Garching
Deutschland

1 Anlass, Auftrag

Entsprechend dem Auftrag und dem Prüfgegenstand geht es um ein Datenschutz-Gutachten zu „myfactory“, das eine Aussage darüber treffen soll, ob alle technischen und organisatorischen Maßnahmen getroffen wurden, um die in Deutschland geltenden Datenschutzbestimmungen zu erfüllen.

Grundlage der Begutachtung waren hauptsächlich die EU-Datenschutzgrundverordnung -DSGVO- und das Bundesdatenschutzgesetz -BDSG-.

Die Beurteilung der wirksamen Umsetzung der rechtlichen Anforderungen zur Informationssicherheit erfolgte anhand des IT-Grundschutzkompendiums des Bundesamtes für Sicherheit in der Informationstechnik -BSI-.

Das Gutachten soll und kann KEINE Zertifizierung im Sinne des Art. 42 DSGVO darstellen, sondern bewertet die Erfüllung der Datenschutz-Kriterien des TÜV SÜD Prüfkatalogs zur Qualität von Anwendungs-Software durch den Prüfgegenstand.

2 Unternehmen

Die webbasierte Business-Software „myfactory“ wird durch die myfactory International GmbH mit Sitz in München / Deutschland betrieben. Mit mehr als 24.000 Anwendern in über 4.500 Unternehmen ist sie einer der führenden Anbieter webbasierter Businesslösungen.

3 Software

Die Software „myfactory“ umfasst die Bereiche ERP, CRM, FiBu, eCommerce, Produktionsplanung und -steuerung (PPS), Mitarbeiterverwaltung und Zeiterfassung (HRM), eine Groupware-Lösung für das Business-Management, Planungs- und Auswertungswerkzeuge sowie zahlreiche Zusatzmodule. Sie kann durch Unternehmen wahlweise als Vor-Ort-Installation, in einer Private Cloud oder als SaaS-Lösung in der Cloud der myfactory International GmbH genutzt werden.

4 Prüfgegenstand

Bei dem Prüfgegenstand handelt es sich um die SaaS-Lösung von „myfactory“, die in der Cloud der myfactory International GmbH betrieben wird.

Abgrenzung:

Fragen der Funktionalität sowie der Datensicherheit, die keinen Bezug zum Datenschutz haben, werden nicht betrachtet. Software-Entwicklungsprozesse waren kein Gegenstand der Untersuchung, da das Gutachten einmalig einen konkreten gegenwärtigen Zustand widerspiegeln sollte.

Die Begutachtung erfolgt ausschließlich anhand der zum Zeitpunkt des Gutachtens geltenden Rechtsvorschriften.

5 Maßstäbe, Anforderungen

Zusammenfassend können die Anforderungen folgendermaßen formuliert werden:

Bietet „myfactory“ die Voraussetzungen, die derzeit geltenden gesetzlichen Datenschutz-Bestimmungen in Deutschland einzuhalten und sind die internen Prozesse bei der myfactory International GmbH so beschaffen, dass sie den Datenschutz für die mit „myfactory“ verarbeiteten personenbezogenen Daten gewährleisten?

6 Prüfkonzept

Entsprechend dem Auftrag und dem Prüfgegenstand geht es um ein Datenschutz-Gutachten zu „myfactory“, das eine Aussage darüber treffen soll, ob sowohl seitens der Software-Eigenschaften als auch seitens der getroffenen technischen und organisatorischen Maßnahmen für den Betrieb der SaaS-Lösung alle Voraussetzungen gegeben sind, um die in Deutschland geltenden Datenschutzbestimmungen zu erfüllen.

Darüber hinaus sollte die Frage beantwortet werden, ob die internen Prozesse der myfactory International GmbH den Datenschutz-Anforderungen entsprechen.

Grundlage der Begutachtung waren hauptsächlich die EU-Datenschutzgrundverordnung -DSGVO- und das Bundesdatenschutzgesetz -BDSG-.

Die Beurteilung der wirksamen Umsetzung der gesetzlichen Anforderungen erfolgte anhand des IT-Grundschutzkompendiums des Bundesamtes für Sicherheit in der Informationstechnik -BSI-.

7 Durchführung

Die Prüfung für das Datenschutz-Gutachten erstreckte sich über den Zeitraum vom 30. April 2018 bis zum 02. Juni 2018. Sie umfasste Dokumentenprüfungen, Interviews und Stichproben-Tests von Software-Funktionen. Diese bezogen sich vor allem auf die Programmbereiche Adressenverwaltung, Zielgruppenverwaltung, HRM einschließlich Zeiterfassung, CRM, ERP sowie das Email-Kommunikationstool.

Die räumlichen und technischen Rahmenbedingungen für den Betrieb der SaaS-Lösung werden im Rahmen von TÜV-Zertifizierungsverfahren seit 2012 jährlich vor Ort bei der myfactory International GmbH überprüft.

8 Vorgelegte Dokumente

- Benennungsschreiben des Datenschutzbeauftragten
- Datenschutzerklärung
- Datenschutzkonzept
- Dokumentation Privacy by Design / Privacy by Default
- Dokumente von Host Europe
  - Zertifikat ISO 27001
  - Security-Konzept
  - Beschreibung der technischen und organisatorischen Maßnahmen
  - Protokoll des Audits durch myfactory
- Lösch- / Anonymisierungskonzept
- Technische und organisatorische Maßnahmen
- Vertrag über Nutzung Public Cloud
- Verpflichtungserklärung auf das Datengeheimnis
- Zusatzvereinbarung Auftragsverarbeitung

9 Gutachten

9.1 Ausgangssituation

Durch die myfactory International GmbH München / Deutschland wird die webbasierte Business-Software „myfactory“ als SaaS-Lösung in einer Public Cloud betrieben. Die Software bietet ein Komplettsystem für kleine und mittlere Unternehmen.

Eine Firma, welche „myfactory“ als SaaS-Lösung nutzen möchte, schließt dafür mit der myfactory International GmbH einen Vertrag über Auftragsverarbeitung und wird dadurch zum Kunden.

Nach Vertragsabschluss wird für den Kunden der Webzugang zu „myfactory“ freigeschaltet. Die Anzahl der möglichen Nutzer eines Kunden hängt von den jeweiligen Vertragsoptionen ab. Die Datenerhebung für „myfactory“ erfolgt mittels Dateneingabe in das System durch den Kunden.

Alle Ausgaben von Daten (Bildschirmanzeigen, Ausdrucke, Exporte in Dateien) erfolgen direkt beim Kunden.

Das System „myfactory“ wird bei der HostEurope GmbH Köln in einem eigenen Rechenzentrum gehostet. Dafür wurde durch die myfactory International GmbH ein entsprechender Vertrag mit der HostEurope GmbH über Auftragsverarbeitung abgeschlossen. Das Rechenzentrum der HostEurope GmbH ist nach ISO 27001 zertifiziert.

9.2 Zulässigkeit

Die myfactory International GmbH gehört im Sinne der DSGVO und des BDSG zum nicht öffentlichen Bereich.

9.2.1 Rechtliche Einordnung

Im Rahmen des Programms „myfactory“ erfolgt durch die myfactory International GmbH keine Verarbeitung personenbezogener Daten für eigene Geschäftszwecke. Die Verarbeitung erfolgt ausschließlich im Auftrag der Kunden.

Die myfactory International GmbH erwirbt keinerlei Rechte an den mit „myfactory“ verarbeiteten personenbezogenen Daten.

Die Zwecke und Mittel der Verarbeitung mit Hilfe von „myfactory“ werden ausschließlich von den Kunden vorgegeben und in „myfactory“ entsprechend dieser Vorgaben umgesetzt. Bei der Umsetzung der Vorgaben hat die myfactory International GmbH keinerlei Entscheidungsspielräume.

9.2.2 Rechtsgrundlagen der Verarbeitung

Die myfactory International GmbH als Auftragnehmer wird für ihre Kunden mit Hilfe der Software „myfactory“ als Auftragsverarbeiter im Sinne des Art. 4 Ziff. 8 DSGVO tätig. Verantwortliche für die Verarbeitung im Sinne des Art. 4 Ziff. 7 BDSG sind die Kunden, die gegenüber der myfactory International GmbH Auftraggeber sind.

Seitens der myfactory International GmbH ist die Verarbeitung zulässig, soweit diese im Rahmen des Auftrages durch den Auftraggeber erfolgt und die weitergehenden Anforderungen aus der Auftragsverarbeitung (siehe 9.3.) erfüllt werden.

9.3 Datenschutzanforderungen aus der Auftragsverarbeitung

myfactory International GmbH als Auftragnehmer

Auf Grund der Tatsache, dass die myfactory International GmbH gegenüber den Auftraggebern ein Auftragsverarbeiter im Sinne des Art. 4 Ziff. 8 ist, obliegen ihr folgende Rechtspflichten:

- Gewährleistung hinreichender Garantien, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit der DSGVO erfolgt und der Schutz der betroffenen Personen gewährleistet wird (Art. 28 Abs. 1 DSGVO)
- Beauftragung von weiteren Auftragsverarbeitern nur mit Genehmigung der Verantwortlichen (Art. 28 Abs. 2 DSGVO)
- Verarbeitung auf der Grundlage eines Vertrages mit dem Auftraggeber, der den Festlegungen des Art. 28 Abs. 3 DSGVO entspricht.
- Verarbeitung der Daten ausschließlich entsprechend der Weisungen des Auftraggebers (Art. 29 DSGVO)
- Gewährleistung, dass alle unterstellten Personen auf das Datengeheimnis verpflichtet sind und darüber belehrt wurden, dass sie die Daten ausschließlich auf Weisung des Auftraggebers verarbeiten dürfen (Art. 29 i.V.m. Art. 32 Abs. 4 DSGVO)
- Gewährleistung technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus gemäß Art. 32 DSGVO
- Umsetzung aller Vorgaben des Auftraggebers entsprechend §11 Abs. 3 BDSG
- unverzügliche Meldung von Verletzungen des Schutzes personenbezogener Daten an den Auftraggeber
- Benennung eines Datenschutzbeauftragten (Art. 37 DSGVO i.V.m. §38 BDSG)

Die Erfüllung dieser Rechtspflichten durch die myfactory International GmbH ist gewährleistet. Die entsprechenden Maßnahmen sind schriftlich angewiesen und dokumentiert.

Die Beschäftigten werden bei Beginn ihrer Tätigkeit für die myfactory International GmbH durch den Datenschutzbeauftragten mit den Datenschutzanforderungen vertraut gemacht und auf das Datengeheimnis verpflichtet. Alle Beschäftigten nehmen darüber hinaus an den jährlichen Datenschutzschulungen teil.

Die technischen und organisatorischen Maßnahmen sind in einem Sicherheitskonzept sowie einer vertiefenden Darstellung beschrieben, das den Auftraggebern zur Verfügung steht. Weitere Angaben zu den technischen und organisatorischen Maßnahmen sind im Abschnitt 9.4 aufgeführt.

Es ist ein Datenschutzbeauftragter benannt. Weitere Angaben dazu sind im Abschnitt 9.2 aufgeführt.

myfactory International GmbH als Auftraggeber

Mit dem Betrieb der Software im Rahmen eines Hostings hat die myfactory International GmbH die HostEurope GmbH beauftragt. Damit wird

- die myfactory International GmbH gegenüber der HostEurope GmbH zum Auftraggeber
- die HostEurope GmbH für die myfactory International GmbH ein Auftragsverarbeiter
- die HostEurope GmbH gegenüber den Auftraggebern (Kunden) der myfactory International GmbH zum Unterauftragnehmer („weiteren Auftragsverarbeiter“ im Sinne des Art. 28 Abs. 2 DSGVO)

Aus der rechtlichen Stellung der myfactory International GmbH als Auftraggeber gegenüber der HostEurope GmbH als Auftragnehmer ergeben sich für die myfactory International GmbH folgende Rechtspflichten:

- der HostEurope GmbH müssen dieselben Datenschutzpflichten auferlegt werden, die der myfactory International GmbH aus dem Vertrag mit dem Auftraggeber (Kunden) auferlegt werden (Art. 28 Abs. 4 DSGVO)
- Gewährleistung, dass die Vorgaben der Auftraggeber (Kunden) von myfactory International GmbH im vollen Umfang auch durch die HostEurope GmbH umgesetzt werden

Diese Rechtspflichten wurden und werden durch die myfactory International GmbH im vollen Umfang erfüllt.

9.4 Datenschutzbeauftragter

Entsprechend Art. 37 DSGVO i.V.m. §38 BDSG ist durch die myfactory International GmbH ein Datenschutzbeauftragter zu benennen, der die Anforderungen des Art. 37 Abs. 5 erfüllt und entsprechend der Art. 38 und 39 DSGVO tätig wird.

Es ist ein Datenschutzbeauftragter schriftlich benannt. Ein Exemplar des Benennungsschreibens ist im Besitz des Datenschutzbeauftragten, ein Exemplar im Besitz der myfactory GmbH.

Der Datenschutzbeauftragte hat das erforderliche Fachwissen in diversen Lehrgängen erworben und erhält dieses durch regelmäßige Weiterbildungsmaßnahmen. Er verfügt über langjährige Erfahrungen als Datenschutzbeauftragter.

Für die Tätigkeit als Datenschutzbeauftragten steht ihm ausreichend Arbeitszeit zur Verfügung. Er verfügt über kein eigenes Budget, bekommt die erforderlichen finanziellen und materiellen Mittel aber problemlos zur Verfügung gestellt.

Der Datenschutzbeauftragte berichtet direkt an die Geschäftsführung. Er ist gemäß Art. 38 DSGVO in die Prozesse eingebunden und nimmt seine Aufgaben entsprechend Art. 39 DSGVO wahr. Er erhält keine Anweisungen zur Ausübung dieser Tätigkeit.

9.5 Datenschutz-Schulung der Beschäftigten

Alle Beschäftigten wurden zu Beginn ihrer Tätigkeit durch den Datenschutzbeauftragten mit den Datenschutz-Vorschriften vertraut gemacht. Darüber hinaus finden für alle Beschäftigten jährliche Datenschutz-Schulungen statt, die schriftlich nachgewiesen werden.

9.6 Weitere Anforderungen

Für die Auftraggeber der myfactory International GmbH können sich unter Umständen weitergehende Datenschutz-Anforderungen ergeben (z.B. in Bezug auf besondere Kategorien personenbezogene Daten gemäß Art. 9 DSGVO i.V.m. §22 BDSG).

Das Programm „myfactory“ bietet alle Voraussetzungen, um solche Anforderungen zu erfüllen.

Darüber hinaus verfügt die myfactory International GmbH über alle technischen und organisatorischen Voraussetzungen, um durch Anpassungen, Zusatzmodule oder andere kundenspezifische Lösungen Aufträge zur Erfüllung eventueller weitergehenden datenschutzrechtlicher Pflichten zu erfüllen.

9.7 Datenschutz-Dokumente

Aus den Datenschutzbestimmungen, die für die Auftragsdatenverarbeitung durch die myfactory International GmbH gelten, ergibt sich die Verpflichtung zum Führen der nachfolgend aufgeführten Datenschutz-Dokumente:

Dokument	Rechtsgrundlage	Status
Datenschutz- und Informationssicherheitskonzept	Art. 32 DSGVO	vorhanden
Nachweis der Verpflichtung auf das Datengeheimnis	Art. 29 i.V.m. Art. 32 Abs. 4 DSGVO	vorhanden
Verträge über die Auftragsverarbeitung durch die myfactory International GmbH	Art. 28 Abs. 3 DSGVO	vorhanden
Vertrag über Auftragsdatenverarbeitung durch die HostEurope GmbH	Art. 28 Abs. 3 DSGVO	vorhanden
Lösch- / Anonymisierungs-Pseudonymisierungskonzept	Art. 32 Abs. 1 Buchst. a	vorhanden
Dokumentation der technischen und organisatorischen Maßnahmen	Art. 32 DSGVO	vorhanden
Nachweis der datenschutzgerechten Technikgestaltung	Art. 25 DSGVO	vorhanden

9.8 Datenschutzgerechte Technikgestaltung

Die Realisierung der Forderung des Art. 25 DSGVO zur datenschutzgerechten Technikgestaltung setzt bei „mydactory“ vor allem folgende Softwareeigenschaften voraus:

9.8.1 Die Software muss die Gewährleistung der Rechte betroffener Personen unterstützen / ermöglichen

a) Es müssen Recherchen nach allen in ihr gespeicherten Daten einer Person möglich sein.

Über die Schaltfläche „Auskunft / Export“ im Register „Datenschutz“ in den Stammdaten der Adressen und Ansprechpartner können alle gespeicherten personenbezogenen Daten als Report ausgegeben werden. Es ist ein Export in eine Datei im Excel- oder CSV-Format möglich.

b) Die Daten einer Person müssen sich löschen lassen

Die Löschung oder Anonymisierung von Personen oder Personengruppen ist nach diversen Kriterien möglich und im Lösch- und Anonymisierungskonzept beschrieben.

c) Die Verarbeitung der Daten einer Person muss sich einschränken lassen

Über die Kennzeichnung „Inaktiv“ kann der Datensatz einer Person verborgen werden, ist aber immer noch aufrufbar und änderbar. Über das Berechtigungssystem kann die Bearbeitung solcher inaktiven Datensätze begrenzt werden:

d) Die Kundendaten müssen sich manuell verändern (berichtigen, ergänzen) lassen. In Abhängigkeit von den mit den Daten verbundenen Risiken sollte bei Bedarf eine Protokollierung erfolgen, wer, wann, was geändert hat.

Eine Änderung oder Ergänzung personenbezogener Daten ist jederzeit möglich. Im „Historie“-Register werden alle Änderungen von Stammdaten und deren früheren Inhalte gespeichert. Beim Anonymisieren werden diese Historie-Daten unwiederbringlich gelöscht.

e) Die Daten einer Person müssen sich in ein verbreitetes Format exportieren lassen (Datenübertragbarkeit)

Über die Schaltfläche „Auskunft / Export“ im Register „Datenschutz“ in den Stammdaten der Adressen und Ansprechpartner können alle gespeicherten personenbezogenen Daten in eine Datei im Excel- oder CSV-Format exportiert werden.

9.8.2 Die Software muss die Forderungen „privacy by default“ und „privacy by design“ erfüllen

a) Es muss mit der Software möglich sein, ein hohes Niveau der Vertraulichkeit und Integrität zu gewährleisten (z.B. durch ein zuverlässiges Authentifizierungsverfahren, verschlüsselte Speicherung von Passwörtern usw.)

Die Authentifizierung erfolgt per Benutzername und Kennwort, optional auch per 2-Faktor-Authentifizierung über eine Authenticator-App. Diese Einstellung kann unternehmensweit erlaubt, verboten oder benutzerindividuell eingestellt werden.

Die Kennwörter werden als salted Hashwert in der Datenbank abgespeichert, eine Rückchiffrierung ist nicht möglich. Wurde das Kennwort vergessen, wird stets ein neues Kennwort generiert und der Benutzer nach der Anmeldung aufgefordert, dieses zu ändern.

b) Die Standard-Einstellungen nach der Installation bzw. nach dem Neuanlegen eines Nutzers müssen das höchste Datenschutz-Niveau haben.

Neu eingerichtete Nutzer haben standardmäßig die wenigsten Rechte. Das Übertragen weiterer Rechte muss explizit erfolgen. Das Konzept der Rechtevergabe ist dokumentiert.

c) Fehlbedienungen dürfen nicht zu einer Verletzung des Datenschutzes führen.

Diese Anforderung ist noch nicht durchgehend erfüllt. Eine vorbildliche Umsetzung erfolgt zum Beispiel bei der Anonymisierung. Hier erfolgen mehrere Sicherheitsabfragen, deren Voreinstellungen den Aufruf der Anonymisierungsfunktion sofort abbrechen. Ein versehentliches Drücken der Enter-Taste würde also sofort zum Abbruch der Funktion führen.
Im Gegensatz dazu ist z.B. bei der Löschfunktion in den Stammdaten die Voreinstellung der Sicherheitsabfrage „OK“. Das heißt, dass ein versehentlicher Tastenanschlag ohne weitere Warnung zur Löschung des betreffenden Datensatzes führt.

d) Es müssen so weit wie möglich Plausibilitätsprüfungen getätigter Eingaben durchgeführt werden. Erkannte Fehler muss das System dem Nutzer so erläutern, dass er geeignete Hinweise zur Fehlerbeseitigung erhält.

Im Test wurden logisch fehlerhafte Eingaben, fehlende Pflichteingaben, doppelte Vergaben z.B. von Kundennummern usw. vom System erkannt und in einem Fehlerhinweis an den Benutzer erläutert.

9.8.3 Die Software muss Löschungen nach Ablauf der Speicherfrist erlauben

Diese Funktion ist in „myfactory“ komfortabel und genau festlegbar integriert. Im Lösch- und Anonymisierungskonzept sind die entsprechenden Funktionen und Prozesse dokumentiert.

9.8.4 Wenn mit der Software personenbezogene Daten auf Basis einer Einwilligung erhoben werden, muss die Software die Möglichkeit bieten, die Einwilligungen so zu speichern, dass sie später als Nachweis der erteilten Einwilligung dienen können. Es muss möglich sein, den Widerruf von Einwilligungen zu verarbeiten.

Unter den Adressdaten gibt es in „myfactory“ neue Felder, welche die Zustimmung dokumentieren. Dies läuft zwar unter dem Punkt „Newsletter“ kann aber allgemein verwendet werden.

Neben der Information „Newsletteranmeldung: Ja/ Nein/ Noch nicht erfasst“ stehen hier ein Datums-Feld, eine Referenz zu einem Kontakteintrag oder Dokument sowie ein freies Eingabefeld zur Verfügung. Die Referenz zu einem Dokument könnte z. B. ein eingescannter Brief in der myfactory-Dokumentendatenbank sein.

9.8.5 Für den Versand von Newslettern muss die Software (über die Anforderung gemäß Punkt 9.8.4 hinaus) in der Lage sein

- **ein Double-Opt-In-Verfahren zu realisieren**
- **bei Benutzung von Trackern zu jedem Tracker eine gesonderte Einwilligung einzuholen**
- **in Abhängigkeit von den Einwilligungen in Tracker unterschiedliche Newsletter zu versenden**
- **Blacklists für Adressen von Empfängern zu verwalten, die Werbung widersprochen haben.**

Im Bereich eCommerce wird eine Newsletter-Registrierung angeboten. Dabei kommt das Double-Opt-In-Verfahren zum Einsatz. Der Interessent erhält eine E-Mail mit einem Bestätigungslink. Diese E-Mail kann als Kontakt (mit dem gesamten Wortlaut) automatisch eingetragen werden.

Klickt der Interessent auf den Link, kann eine zweite E-Mail als Bestätigung geschickt werden, Auch diese E-Mail, die z.B. die erforderlichen Informationen nach Art. 13 DSGVO enthalten könnte, kann mit dem gesamten Wortlaut als Kontakt automatisch gespeichert werden. Somit ist über die Kontakte der Adresse eine lückenlose Historie der Registrierung bzw. Anmeldung gegeben. Das gleiche Verfahren kann z. B. auch bei Shop-Registrierungen eingesetzt werden. Das Referenzfeld im Adressdatensatz „Kontakt“ wird dabei automatisch befüllt.

Zusätzlich gibt es noch die Möglichkeit im „Datenschutz“-Register den Erhebungsgrund manuell einzutragen und einen selbstdefinierten Aufbewahrungsgrund zu hinterlegen.

Eine Nutzung von Trackern in Newslettern ist nicht vorgesehen.

10 Zusammenfassung

Es wurden die Voraussetzungen für die Gewährleistung des Datenschutzes bei Nutzung der SaaS-Lösung von „myfactory“ geprüft, die in der Cloud der myfactory International GmbH betrieben wird. Dabei wurden die Datenschutz-Anforderungen der Europäischen Datenschutzgrundverordnung – DSGVO – sowie des Bundesdatenschutzgesetzes – BDSG -zugrunde gelegt. Die Beurteilung der wirksamen Umsetzung der rechtlichen Anforderungen zur Informationssicherheit erfolgte anhand des IT-Grundschutzkompendiums des Bundesamtes für Sicherheit in der Informationstechnik -BSI-.

Das Ergebnis Datenschutz-Prüfung der Cloud-Lösung von „myfactory“ lautet wie folgt:

Die Software „myfactory“ bietet alle technischen und organisatorischen Voraussetzungen für die Einhaltung des Datenschutzes gemäß DSGVO und BDSG.

Die internen Prozesse des Betreibers myfactory International GmbH sind datenschutzkonform.

Verbesserungsbedarf gibt es vor allem in Bezug auf eine durchgängige Gestaltung von Sicherheitsabfragen entsprechend der Anforderungen der Privacy by design. Die festgestellten vereinzelten Unzulänglichkeiten sind aber minimal und beeinträchtigen die Rechtskonformität von „myfactory“ nicht.

Garching, den 04.06.2018

TÜV SÜD Product Service GmbH

Software-Qualität und Escrow Services

Prüfer: …….. Review des Berichts ……..…..

Hans-Ulrich Bierhahn Tuan Khai Hoang