**Datenschutz-Folgenabschätzung**

**System- oder Projektname:** 002-Kunden; Zielpersonen

**Zuständige Person:**

**Name** [x]

**Position** [x]

**Kontaktinformation** [x]

**System oder Projektbeschreibung und Aufgabe:**

1. **Grundlegende Informationen**

|  |  |
| --- | --- |
| **Welche personenbezogende Daten werden verarbeitet?** | Risikofaktor:Mittel |
| Vgl Verarbeitungsverzeichnis – Reiter 002 Kunden, Zielperson  |
| **Für welchen Zweck werden die personenbezogenen Daten verarbeitet?**  | Risikofaktor:Mittel |
| Zur Erfüllung des jeweiligen Kundenauftrags, sofern dieser Zielpersonen beinhaltet |
| **Welche Kategorien von betroffenen Personen sind durch die Verarbeitung erfasst?** | Risikofaktor:Mittel |
| Zielpersonen; Kunde; allenfalls Dritte |
| **Wie viele Personen sind von der Verarbeitung betroffen?**  | Risikofaktor:Niedrig |
| idR sehr wenige, weil idR nur eine Zielperson genannt wird |
| **Mit Hilfe welcher Technologie werden die Daten verarbeitet? Werden dabei auch neue Technologien genutzt?**  | Risikofaktor:Hoch/Mittel/Niedrig |
| [*bspw Datenbanken auf standalone PC (niedrig), Webportale (mittel), händisch (niedrig), cloud (hoch)*] |
| **Wurden die betroffenen Personen über die Verarbeitung informiert? Und wenn ja, welche Informationen wurden ihnen dabei gegeben?** | Risikofaktor:Hoch |
| Nein, weil dies gesetzlich ausdrücklich untersagt ist (§ 130 GewO) |
| **Werden in der Verarbeitung automatisiert Entscheidungen über die betroffene Person getroffen?**  | Risikofaktor:Hoch/Mittel/Niedrig |
| [*insbesondere auf Basis der ökonomische Situation, Gesundheit, persönliche Interessen oder Präferenzen; Zuverlässigkeit oder Verhalten; Standort oder Bewegungen*] |
| **Werden die personenbezogenen Daten mit anderen Datensätzen kombiniert oder verglichen?**  | Risikofaktor:Hoch/Mittel/Niedrig |
| [*insbesondere auf Basis der ökonomische Situation, Gesundheit, persönliche Interessen oder Präferenzen; Zuverlässigkeit oder Verhalten; Standort oder Bewegungen*] |
| **Wie werden die Daten erfasst?**  | Risikofaktor:Hoch/Mittel/Niedrig |
| [*eigene vorhandene Dateien (niedrig); von Dritten erhaltene Daten; Nachverfolgung von Daten*]  |
| **Wird sichergestellt, dass nur für den angegebenen Zweck erforderliche Daten erfasst werden?** | Risikofaktor:Hoch/Mittel/Niedrig |
| [*wenn ja, welche Maßnahmen werden dafür getroffen*] |
| **In welchem Umfang werden die Daten verarbeitet?**  | Risikofaktor:Hoch/Mittel/Niedrig |
| Nur im notwendigen Umfang |
| **Wer hat Zugriff auf die personenbezogenen Daten? Haben Auftragsnehmer Zugriff auf diese Daten und geben diese wiederum an Subauftragsnehmer weiter?** | Risikofaktor:Hoch/Mittel/Niedrig |
| [*bspw der Kunde bekommt regelmäßige Zwischen- und Endberichte, die nur mehr die angefragten Informationen – aber keine darüberhinausgehenden Daten - beinhalten*] |
| **Werden die Daten an andere Gesellschaften innerhalb der Gruppe weitergegeben oder an externe Dritte?** | Risikofaktor:Niedrig |
| Nein |
| **Werden Daten auch außerhalb der EU/EWR weitergeleitet oder haben Personen daraus Zugriff?** | Risikofaktor:Niedrig |
| Nein |
| **Wo werden die personenbezogenen Daten gespeichert?** | Risikofaktor:Hoch/Mittel/Niedrig |
| [bspw Serverstandort] |
| **Wie lange werden die personenbezogenen Daten gespeichert?** | Risikofaktor:Niedrig |
| 7 Jahre (bis Jahresende) danach |

1. **Rechtliche Beurteilung**

**Schwellwertanalyse**

|  |  |
| --- | --- |
| **Vorfrage: Ist die Datenanwendung in der Black oder White List gelistet? Ist eine Datenschutzfolgenabschätzung jedenfalls erforderlich oder kann sie entfallen?** | Black List: Datenschutzfolgenabschätzung ist jedenfalls durchzuführenWhite List: Keine Datenschutzfolgenabschätzung erforderlich, sondern lediglich zu dokumentieren, dass ein inhaltsgleicher Fall vorliegt. |
| Black und white lists noch nicht verfügbar |
| **Liegt eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche vor?** | In diesem Fall ist jedenfalls eine Datenschutzfolgenabschätzung durchzuführen (Art 35 Abs 3 lit c DSGVO). |
| nein |
| **Liegt eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art 9 DSGVO, von Daten von Kindern oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art 10 DSGVO vor?** | In diesem Fall ist jedenfalls eine Datenschutzfolgenabschätzung durchzuführen (Art 35 Abs 3 lit a DSGVO). |
| Ja – weil Aufträge auch strafrechtlich relevante Daten und/oder Gesundheitsdaten umfassen können |
| **Welcher Natur ist die Verarbeitung? Wie groß ist ihr Geltungsbereich und in welchem Kontext (zu sonstigen Verarbeitungen) steht sie? Welche Absicht bzw welcher Zweck wird verfolgt?** | Sofern die Art der Verarbeitung an sich, der Umfang der Daten, Übermittlungen oder Zwecke, die Umstände oder der Zweck der Verarbeitung selbst zu einem Risiko führen, ist eine Datenschutzfolgenabschätzung durchzuführen. |
| Es werden Daten lediglich im Rahmen des Auftrags des Kunden verarbeitet. Vor Annahme eines Auftrags wird geprüft, ob der Kunde ein berechtigtes Interesse an dieser Information hat (zB: zu prüfen, ob die Ehefrau des Kunden eine sexuelle Beziehung hat, ist ein Auftrag, der angenommen wird; ob die Nachbarin eine sexuelle Beziehung hat, ist ein Auftrag, der nicht angenommen wird) |

**Rechtliche Risikobewertung**

|  |  |
| --- | --- |
| **Erfolgt die Verarbeitung zu festgelegten, eindeutigen und legitimen Zwecken?** | Der Zweck und Umfang der Verarbeitungstätigkeit muss im Vorfeld klar abgegrenzt und definiert sein. |
| Ja |
| **Liegt ein Rechtfertigungsgrund des Art 6 DSGVO vor?** | Es ist zu prüfen und zu beschreiben, auf welcher Rechtsgrundlage die Daten verarbeitet werden. |
| Ja – berechtigte Interessen des Kunden |
| **Soweit sensible Daten verarbeitet werden, wurden Teile dieser Daten bereits von der betroffenen Person veröffentlicht oder sind sie allgemein öffentlich zugänglich?**  |  |
| Oftmals ja, im Einzelfall auch nein |
| **Werden nur die für den konkreten Zweck notwendigen Daten verarbeitet oder gibt es gelindere Mittel? Können statt personenbezogenen Daten auch anonyme Daten verwendet werden?** | Die Datenverarbeitung darf - auch mit Blick auf Privacy by default - nur solche Daten enthalten, deren Verarbeitung für den Zweck angemessen und erheblich ist. |
| Nur die für den konkreten Zweck notwendigen Daten werden verarbeitet |
| **Werden die Daten nur solange (personenbezogen) aufbewahrt, als dies zur Erreichung des Zwecks absolut erforderlich ist?** | Nach dem Ende gesetzlicher Aufbewahrungspflichten ist eine strenge Prüfung der Aufbewahrungsdauer abzubilden. |
| Zur Aufbewahrungsdauer siehe oben; danach werden die Daten gelöscht bzw anonymisiert |
| **Haben nur die Personen Zugriff auf personenbezogene Daten, die diese tatsächlich im Rahmen der Zweckerfüllung benötigen?** | Auch innerhalb des Unternehmens ist zu gewährleisten, dass der Datenzugriff auf das notwendige Ausmaß beschränkt ist. |
| Zu den Zugriffsberechtigen siehe oben; sonst hat niemand Zugriff |
| **Wurde der Betroffene ausreichend informiert?** | Die nach Art 13 und 14 DSGVO erforderlichen Informationen müssen den Betroffenen rechtzeitig und vollständig zur Verfügung stehen. |
| Nein, zumal dies gesetzlich ausdrücklich untersagt ist (§ 130 GewO) |
| **Kann der Betroffene jederzeit Auskunft über seine Daten sowie eine maschinenlesbare Kopie erhalten?** | Die nach Art 15 und 20 DSGVO zustehenden Rechte müssen auch technisch innerhalb der Frist umsetzbar sein. |
| Ja, aber er bekommt nur eine Leermeldung, wie gesetzlich vorgesehen (§ 130 GewO) |
| **Kann der Betroffene seine Daten berichtigen, löschen und deren Verarbeitung einschränken lassen?** | Die nach Art 16, 17, 18, 19 und 21 DSGVO zustehenden Rechte müssen auch technisch innerhalb der Frist umsetzbar sein. |
| Nen |
| **Welche Empfänger bekommen auf Basis welcher Rechtsgrundlage welche Daten? Sind die notwendigen vertraglichen Verpflichtungen eingehalten?** | Neben Übermittlungsempfängern, die Daten zu eigenen Zwecken auf Basis einer gesonderten Rechtsgrundlage verarbeiten, sind insbesondere auch Auftragsverarbeiter und die zugrundeliegenden Verträge nach Art 28 DSGVO darzustellen. |
| Ausschließlich der Kunde [und foglende Auftragsverarbeiter][sofern zutreffend: *mit allen Auftragsverarbeitern ist eine DSGVO-konformer Auftragsverarbeitungsvertrag abgeschlossen worden]* |
| **Erfolgt eine Übermittlung an Empfänger außerhalb des EWR? Werden nachweisbare, geeignete Garantien eingehalten?** | Sofern kein Angemessenheitsbeschluss der EU-Kommission vorliegt, müssen geeignete Garantien getroffen und nachgewiesen werden (zB Standarddatenschutzklauseln). |
| Nein |

1. **Technische Risikobewertung**

Siehe Verarbeitungsverzeichnis – Reiter Datensicherheit. Diese Maßnahmen erachten wir als ausreichend.

1. **Maßnahmen zur Risikobegrenzung**

|  |  |  |  |
| --- | --- | --- | --- |
| **Festgestelltes Risiko** | **Wahrscheinlichkeit eines Risikoeintritts, Auswirkung und Folgen für betroffene Personen**  | **Maßnahmen zur Risikobegrenzung**  | **Risikoeffekt (Hoch/mittel/****niedrig)**  |
| Daten werden anderen Personen bekannt | Geringe Wahrscheinlichkeit, weil angemessene Datensicherheitsmaßnahmen getroffen wurden; Auswirkungen könnten für den Betroffenen unangenehm sein, gerade die sensiblen Daten werden oft aber ohnehin einem beschränkten Kreis an Personen bekannt sein.  | (i) Angemessene Datensicherheits-maßnahmen(ii) Geheimhaltungs-erklärungen(iii) regelmäßige Mitarbeiterschulungen | gering |
| Zielperson erkennt, dass Überwachung stattfindet | Geringe Wahrscheinlichkeit, weil angemessene Datensicherheitsmaßnahmen getroffen wurden. idR Folgenlos, weil Zielperson dann das Verhalten anpasst  | Nicht erforderlich | gering |

1. **Implementierung**

|  |
| --- |
| **Wer ist für die Implementierung der getroffenen Maßnahmen zuständig?**  |
| [*Name, Position, Kontaktadresse*] |
| **Getroffene Maßnahme** | **Datum der Fertigstellung**  |
| (i) Angemessene Datensicherheits-maßnahmen(ii) Geheimhaltungserklärungen(iii) regelmäßige Mitarbeiterschulungen |  |