**Fragebogen zur DSGVO-Umsetzung**

|  |
| --- |
| Verantwortliche(r): **Klicken Sie hier, um Text einzugeben.**  Datum: **5. November 2019** |

1. **Auf Basis welcher Rechtsgrundlagen verarbeiten Sie personenbezogene Daten?***(Mehrfachnennungen möglich)*

Art. 6 Abs. 1 Bst. a DSGVO – Einwilligung

Wenn ja, übermitteln Sie uns ein Muster der von Ihnen verwendeten Einwilligungserklärung!

Art. 6 Abs. 1 Bst. b DSGVO – Erfüllung eines Vertrages

Wenn ja, nennen Sie die Vertragsarten, die in Ihrem Unternehmen als Rechtsgrundlage in Frage kommen (z. B. Arbeitsvertrag, Mietvertrag): **Klicken Sie hier, um Text einzugeben.**

Art. 6 Abs. 1 Bst. c DSGVO – Erfüllung einer rechtlichen Verpflichtung

Nennen Sie die rechtlichen Verpflichtungen, auf die Sie sich bei der Datenverarbeitung stützen: **Klicken Sie hier, um Text einzugeben.**

Art. 6 Abs. 1 Bst. f DSGVO – Berechtigte Interessen

Begründen Sie, worin diese Interessen konkret bestehen und welche Datenverarbeitungen Sie damit rechtfertigen: **Klicken Sie hier, um Text einzugeben.**

Andere Rechtsgrundlage (z. B. Art. 9 Abs. 2 DSGVO)

**Klicken Sie hier, um Text einzugeben.**

1. **Wie wird die Informationspflicht nach Art. 13 DSGVO in Ihrem Unternehmen umgesetzt?**

Beschreiben Sie die Umsetzung und übermitteln Sie die von Ihnen verwendeten Informationsblätter einschliesslich der Datenschutzerklärung auf Ihrer Internetseite oder führen Sie hier die entsprechenden Weblinks auf:

**Klicken Sie hier, um Text einzugeben.**

1. **Ist in Ihrem Unternehmen ein dokumentierter Prozess vorhanden, wie mit den Rechten der betroffenen Personen nach Art. 12 bis 22 DSGVO umgegangen wird?**

Ja. Beschreiben Sie diesen Prozess in Stichworten:

**Klicken Sie hier, um Text einzugeben.**

Nein. Grund: **Klicken Sie hier, um Text einzugeben.**

1. **Stellen Sie sicher, dass bei der Änderung oder Neuentwicklung von Produkten oder Dienstleistungen Datenschutzanforderungen gemäss Art. 25 DSGVO von Anfang an mitberücksichtigt werden?**

Ja. Beschreiben Sie dieses Verfahren in Stichworten:

**Klicken Sie hier, um Text einzugeben.**

Nein. Grund: **Klicken Sie hier, um Text einzugeben.**

1. **Werden in Ihrem Unternehmen Datenverarbeitungen an Auftragsverarbeiter ausgelagert?**

Ja. Nennen Sie die Kategorien der eingesetzten Auftragsverarbeiter (z. B. IT-Dienstleister, Buchhaltungsbüro): **Klicken Sie hier, um Text einzugeben.**

Senden Sie uns exemplarisch eine Kopie eines Auftragsverarbeitungsvertrages zu!

Nein.

1. **Haben Sie für Ihr Unternehmen ein vollständiges Verarbeitungsverzeichnis nach Art. 30 DSGVO erstellt?**

Ja. Übermitteln Sie uns eine Kopie Ihres Verarbeitungsverzeichnisses!

Nein. Grund: **Klicken Sie hier, um Text einzugeben.**

1. **Wie stellen Sie sicher, dass geeignete technische und organisatorische Massnahmen zur Sicherstellung insbesondere der Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit der Daten nach Art. 32 DSGVO (Sicherheit der Verarbeitung) getroffen werden?***(Mehrfachnennungen möglich)*

Sie orientieren sich an anerkannten Standards oder Normen, wie beispielsweise an der ISO/IEC 27000-Normenreihe.

Nennen Sie die konkreten Standards bzw. Normen: **Klicken Sie hier, um Text einzugeben.**

Sie können Zertifizierungen im Bereich der Daten- oder Informationssicherheit im weitesten Sinn nachweisen.

Nennen Sie die Zertifizierung: **Klicken Sie hier, um Text einzugeben.**

Sie werden durch externe Dienstleister bei der Planung und Umsetzung von technischen und organisatorischen Massnahmen unterstützt.

Andere Methoden oder getroffene Massnahmen. Beschreiben Sie diese in Stichworten:

**Klicken Sie hier, um Text einzugeben.**

**Folgende Aussagen zur Datensicherheit treffen für Ihr Unternehmen zu:**

1. Datensicherheitsrichtlinien sind vorhanden und von der Geschäftsleitung freigegeben.

Ja  Nein  nicht anwendbar

1. Anlagenwerte, wie z. B. Hardware (Notebooks, Server, Mobiltelefone usw.) sowie Software als auch andere technischer Infrastruktur, werden inventarisiert sowie deren zulässiger Gebrauch ist geregelt.

Ja  Nein  nicht anwendbar

1. Für die Nutzung von mobilen Geräten (Notebooks, Mobiltelefone usw.) existieren spezifische Richtlinien.

Ja  Nein  nicht anwendbar

1. Die Verantwortlichkeiten und Rollen im Zusammenhang mit der Datensicherheit sind im Unternehmen klar geregelt und dokumentiert.

Ja  Nein  nicht anwendbar

1. Ein Rollen- und Berechtigungskonzept ist etabliert.

Ja  Nein  nicht anwendbar

1. Kryptographische Verfahren zum Schutz personenbezogener Daten sind implementiert und das Schlüsselmanagement ist geregelt als auch dokumentiert.

Ja  Nein  nicht anwendbar

1. Ein Lösch- sowie Backupkonzept ist etabliert.

Ja  Nein  nicht anwendbar

1. Es ist ein Schwachstellenmanagement implementiert.

Ja  Nein  nicht anwendbar

1. Systemereignisse werden protokolliert und überwacht.

Ja  Nein  nicht anwendbar

1. Die Vertraulichkeit und Integrität der Daten, die innerhalb des Unternehmens oder im Austausch mit einer externen Stelle übertragen oder zum Abruf bereitgestellt werden, sind gewahrt und entsprechende Richtlinien sind vorhanden.

Ja  Nein  nicht anwendbar

1. Es finden regelmässig Informationssicherheitsüberprüfungen statt.

Ja  Nein  nicht anwendbar

Wenn ja, zuletzt am: **Klicken Sie hier, um Text einzugeben.**

1. Die Mitarbeitenden werden regelmässig geschult und sensibilisiert.

Ja  Nein  nicht anwendbar

1. **Wie viele Datenschutzverletzungen nach Art. 33 und 34 DSGVO sind bei Ihnen seit Geltung der DSGVO (20. Juli 2018) bekannt geworden?**

Anzahl: **Klicken Sie hier, um Text einzugeben.**

Keine

1. **Gibt es einen (dokumentierten) Prozess, um Datenschutzverletzungen innerhalb 72 Stunden bei der Datenschutzstelle zu melden?**

Ja.

Nein. Grund: **Klicken Sie hier, um Text einzugeben.**

1. **Ist ein Datenschutzbeauftragter benannt und der Datenschutzstelle gemeldet?**

Ja. Meldedatum: **Klicken Sie hier, um Text einzugeben.**

Art der Meldung:  Onlineformular  Brief  E-Mail  Anders: **Klicken Sie hier, um Text einzugeben.**

Nein. Grund: **Klicken Sie hier, um Text einzugeben.**

1. **Welche Aufgaben hat Ihr Datenschutzbeauftragter?** *(Mehrfachnennungen möglich)*

Beratung der Geschäftsführung

Beratung der Fachabteilungen

Sensibilisierung der Mitarbeiter

Durchführung interner Audits/Kontrollen

Beantwortung/Klärung von Datenschutzbeschwerden

Beantwortung von Anfragen zu Betroffenenrechten

Aufgabenplanung der Fachabteilungen

Durchführung der Meldung von Datenschutzverletzungen (Art. 33 und 34 DSGVO)

Beratung in Bezug auf Datenschutz-Folgenabschätzungen (Art. 35 DSGVO)

Sonstige: **Klicken Sie hier, um Text einzugeben.**

Wir haben keinen Datenschutzbeauftragten.

1. **Sind, falls Sie einen Datenschutzbeauftragten benannt haben, die Prüfberichte der letzten (zwei) Audits des Datenschutzbeauftragten vorhanden und besitzen diese eine einheitliche Prüfmethodik?**

Ja. Übermitteln Sie Kopien der Prüfberichte!

Nein. Grund: **Klicken Sie hier, um Text einzugeben.**

1. **Gibt es ein Konzept im Unternehmen, wer bezogen auf den Datenschutz wofür zuständig ist (z. B. Schulung der Mitarbeiter, Meldung von Datenschutzverletzungen)?**

Ja. Übermitteln Sie uns eine Kopie des Konzepts (sofern vorhanden) oder beschreiben dieses in Stichworten: **Klicken Sie hier, um Text einzugeben.**

Nein. Grund: **Klicken Sie hier, um Text einzugeben.**

1. **Stellen Sie sicher, dass Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen erkannt und für diese eine Datenschutz-Folgenabschätzung durchgeführt wird?**

Ja.

Nein. Grund: **Klicken Sie hier, um Text einzugeben.**

**>> ENDE Fragebogen**