

## Risikobewertungen nach der EU Datenschutz-Grundverordnung

Im April dieses Jahres wurde ein neues Datenschutzrecht für den gesamten europäischen Rechtsraum geschaffen, die EU Datenschutz-Grundverordnung (DSGVO). Ab Mai 2018 findet dieses neue Rechtsregime unmittelbare Anwendung in allen Mitgliedstaaten der Europäischen Union und ersetzt nationales Datenschutzrecht. Datenverarbeitende Stellen in ganz Europa haben die neuen Vorschriften zu beachten.

Das neue Datenschutzrecht birgt sowohl Chancen als auch Risiken. Der Haftungsrahmen für Unternehmen bei Datenschutzverstößen oder Nichtbeachtung bestimmter Vorschriften der DSGVO wurde erheblich angehoben. Datenschutzrisiken richtig einzuschätzen und die entsprechenden Maßnahmen zu ergreifen, vermeidet aufwendige und kostenintensive Umstrukturierungen Ihrer IT-Landschaft, verringert Haftungs- und Bußgeldrisiken und sorgt so für Compliance im Datenschutz. Dafür sollten frühzeitig die richtigen Weichen gestellt werden!

Ein modernes Risikomanagement beinhaltet eine Analyse der Datenverarbeitungsprozesse Ihres Unternehmens unter Berücksichtigung der Anforderungen der DSGVO. Datenverarbeitungsprozesse, für die eine Datenschutz-Folgenabschätzung bzw. ein Privacy-Impact Assessment (PIA) nach der DSGVO zwingend vorgeschrieben ist, sollten identifiziert werden und die erforderlichen Datenschutz-Folgenabschätzungen zeitnah durchgeführt werden. Wir haben ein spezielles Konzept entwickelt, um sie dabei zu unterstützen!

### Unser Konzept

#### 1. Quick-Check Datenschutzrisiken

Im Rahmen einer datenschutzrechtlichen Ersteinschätzung, unserem Quick-Check, identifizieren und analysieren wir die Datenverarbeitungsvorgänge im Bereich des elektronischen Zahlungsverkehrs, in Ihrem Unternehmen. In einem halbtägigen Workshop in Ihrem Hause, prüfen und bewerten wir vorhandene Unterlagen und Informationen zum Datenschutz (z. B. Verfahrensverzeichnis oder Sicherheitskonzept) sowie vorhandene Unterlagen aus früher in Ihrem Hause durchgeführten PCI DSS-Audits. Auf Grundlage dieser Bestandsaufnahme zu Ihren Datenverarbeitungen und deren Risiken nehmen wir eine Risikobewertung aus technischer und juristischer Sicht nach der DSGVO vor.

Im Ergebnis können wir dann klare Aussagen dazu treffen, inwieweit Ihre Datenverarbeitungsprozesse den Anforderungen der DSGVO genügen, oder risikobehaftet sind. Insbesondere identifizieren wir Datenverarbeitungsvorgänge für die ein Privacy-Impact-Assessment (PIA) nach Art. 35 der DSGVO zwingend vorgeschrieben ist. Die Ergebnisse stellen wir Ihnen im Anschluss in Berichtsform zur Verfügung.

---

## 2. Privacy-Impact-Assessment

Soweit im Rahmen des Quick-Check Datenverarbeitungen identifiziert wurden, für die nach Art. 35 DSGVO ein PIA vorgeschrieben ist, führen wir dieses in der zweiten Stufe in Ihrem Hause durch. Dabei identifizieren wir alle für die Risikobewertung relevanten Faktoren Ihrer Datenverarbeitungsvorgänge, prüfen und analysieren diese und erstellen im Anschluss eine umfassende Risikobewertung nach der DSGVO und geben auf dieser Grundlage Empfehlungen für geeignete Organisatorische-, Datenschutz- und IT-Maßnahmen zur Beseitigung oder Minimierung der Risiken.

### Unser Angebot

Den initialen Quick-Check-Workshop inklusive Risikobewertung und Assessmentbericht (Stufe 1) bieten wir Ihnen zum Festpreis in Höhe von **6.000,00 Euro** (zzgl. Mehrwertsteuer und Reisekosten) an.

In dem Workshop klären und dokumentieren wir insbesondere folgende Punkte hinsichtlich Ihrer Systemlandschaft und der relevanten Datenverarbeitungsprozesse:

- Verarbeitung personenbezogener Daten und die Anwendbarkeit der DSGVO – unter Berücksichtigung des Audits zur Compliance-Feststellung des PCI DSS
- Mögliche Risiken für die Betroffenen
- Umfang der Datenverarbeitungen
- Entscheidungen mit Rechtswirkung für die betroffenen Personen als Folge der Datenverarbeitung
- Verarbeitung besonderer Kategorien von personenbezogenen Daten

Bei Interesse wenden sie sich bitte an:

SRC Security Research & Consulting GmbH Frau Jana Ehlers Emil-Nolde-Str. 7 53113 Bonn datenschutz@src-gmbh.de Tel: 0228 2806 0
---

### Gemeinsame Expertise

Durch bereits gemeinsam durchgeführte Risikobewertungen der Datenverarbeitungen von Zahlungsverkehrsdaten im Bereich des automatisierten elektronischen Zahlungsverkehrs konnten SRC und Scheja & Partner Rechtsanwälte und externe Datenschutzbeauftragte in der Vergangenheit bereits wertvolle gemeinsame Expertise in diesem Bereich gewinnen. Dabei profitierten die auditierten Unternehmen jeweils von dem technischen und juristischen

---

Know-how, welches durch die Zusammenarbeit in interdisziplinärer Weise in die Risikobewertung eingebracht werden konnte.

### **Scheja & Partner**

Scheja & Partner Rechtsanwälte und externe Datenschutzbeauftragte ist eine auf das Gebiet des Datenschutzrechts spezialisierte Rechtsanwaltskanzlei mit langjähriger Erfahrung in der datenschutz- und wirtschaftsrechtlichen Beratung von national und international operierenden Unternehmen und Institutionen verschiedener Branchen.

Als externe Datenschutzbeauftragte stehen Scheja & Partner in ständigem Erfahrungsaustausch mit Unternehmen, Praktikern und Aufsichtsbehörden. Wesentlicher Bestandteil der Beratung der Kanzlei sind die aktuellen Entwicklungen des Datenschutzrechts auf europäischer und nationaler Ebene und die rechtskonforme Anwendung und Umsetzung datenschutzrechtlicher Vorschriften in der Praxis.

### **SRC Security Research & Consulting GmbH**

SRC Security Research & Consulting GmbH ist ein Gemeinschaftsunternehmen der deutschen Kreditwirtschaft. Die Experten der SRC unterstützen in allen Fragen der Informationssicherheit, unabhängig davon, ob es sich um elektronischen Zahlungsverkehr, mobile und Internet-Payments, Gesundheitswesen, elektronischen Identitätsnachweis, Chipkarten oder Smartphones, digitale Signaturen, Public Key Infrastrukturen, oder technisches und organisatorisches Sicherheits-Management handelt.

Schulungen und Seminare der SRC Academy ergänzen unser Portfolio. Zu unseren Kunden zählen die Kreditwirtschaft, Finanzinstitute und Versicherungen, der Handel, der öffentliche Dienst, die Tourismusbranche und die Industrie.

SRC verfügt nicht nur über umfangreiche Erfahrung in der Bewertung von Sicherheitsmaßnahmen zum Schutz von Kartendaten aufgrund des PCI DSS-Standards, sondern auch mit der Erstellung von PIAs, speziell im Zusammenhang mit bargeldlosen Zahlungssystemen.