DIE NEUE DATENSCHUTZGRUNDVERORDNUNG

Um die **Fragmentierung des Datenschutzrechts** in Europa aufzuheben und um **personenbezogene Daten unter einen noch effektiveren Schutz** zu stellen, hat die EU die neue Datenschutzgrundverordnung (DSGVO) erlassen.

Besonderheit der DSGVO: "**Öffnungsklauseln**" für die nationalen Gesetzgeber

Der durch die Verordnung vorgegebene Schutz darf nicht unterschritten werden, jedoch können in einzelnen Bereichen ergänzende und konkretisierende nationale Regelungen getroffen werden. Diese Umsetzungsfreiräume hat der deutsche Gesetzgeber durch das **neue Bundesdatenschutzgesetz (BDSG)** im Juli 2017 genutzt.

DIE WICHTIGSTEN ÄNDERUNGEN FÜR STIFTUNGEN

- ✓ **Privilegien entfallen**

  Derzeit im BDSG bestehende, die **Spendenwerbung privilegierende Vorschriften** entfallen. Die DSGVO hingegen stellt den "risikobasierten Ansatz" als maßgebliche Zulässigkeitserwägung dar. Danach ist bei der rechtlichen Einschätzung der Zulässigkeit von Werbung auf die "berechtigten Erwartungen" des jeweiligen Betroffenen abzustellen. Diese Wertungsfrage alleine stellt Rechtsanwender vor immense Unsicherheiten.

- ✓ **Höhere Anforderungen an die IT**

  Seitens der IT sind insbesondere **spezielle IT-Sicherheitsanforderungen** einzuhalten. Datenschutz muss außerdem schon bei der Planung neuer Verarbeitungsvorgänge durch die **Vornahme datenschutzrechtlicher Grundeinstellungen und bei der Entwicklung neuer Geräte durch datenschutzfreundliche Konzeption** berücksichtigt werden ("**privacy by default" und "privacy by design**").

- ✓ **Einführung von besonderen Prüfungen im Vorfeld**

  Die DSGVO führt die sog. **Datenschutz-Folgenabschätzung (DSFA)** ein. Im Grundsatz ist diese vergleichbar mit der Vorabkontrolle nach bisher gültigem Datenschutzrecht. Derzeit ist zu erwarten, dass der DSFA im Unterschied zur Vorabkontrolle durch die rechtliche Ausgestaltung ein größerer Anwendungsbereich zukommt. Eine **DSFA** ist immer dann vorzunehmen, wenn „(…) eine Form der **Verarbeitung**, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung **voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge** (hat)“. Die Idee dahinter ist schnell ersichtlich: Verantwortliche sollen für die Rechte der Betroffenen sensibilisiert bleiben und die relevanten Prozesse und Vorgänge ständig überprüfen. Mögliche Risiken bei bestimmten Datenverarbeitungen sollen dadurch bewusster behandelt und **datenschutzrechtlich möglicherweise problematische Prozesse von vornherein besser evaluiert** werden.

- ✓ **Höhere Voraussetzungen für Einwilligungen**

  Die Grundverordnung legt einen restriktiven Ansatz im Umgang mit personenbezogenen Daten fest. Dies führt dazu, dass **an eine Einwilligung hohe Voraussetzungen** geknüpft werden. Unter anderem müssen Einwilligungsklauseln vereinbar mit AGB-Recht sein. Das heißt, sie dürfen z.B. nicht überraschend oder missbräuchlich sein. Daneben sind sog. Pauschaleinwilligungen unwirksam. Die Einwilligung muss sich also auf einen konkreten Fall beziehen und zudem freiwillig gegeben werden.

- ✓ **Gesteigerte Dokumentationspflichten**

  Der Verantwortliche, also die natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung entscheidet, hat die **Einwilligung nachweisbar zu dokumentieren**. Daneben müssen dem Einwilligenden alle Informationen gegeben werden, die mit Art, Umfang und Reichweite der Einwilligung zu tun haben. Betroffene sind außerdem umfangreicher als bislang über Ihre Rechte zu informieren und Angaben über die Speicherdauer müssen zur Verfügung gestellt werden.

- ✓ **Mehr Transparenz und Information**

  Hinzu treten eine Vielzahl von **Transparenz- und Informationspflichten**. Besonders ins Gewicht fällt dabei die Verpflichtung, Mitglieder, Beschäftigte und Spender deutlich umfassender als bisher über die Verarbeitung ihrer personenbezogenen Daten und die Möglichkeiten zur Ausübung ihrer Rechte zu informieren.

- ✓ **Interne Datenschutz-Management-Systeme werden unabdingbar**

  Neben der Erforderlichkeit, Einwilligungen sorgsam zu dokumentieren, werden außerdem die **internen Organisationspflichten,** die durch Art. 5 DSGVO geschaffen werden, gravierende Auswirkungen haben. Selbst kleine Organisationen müssen danach nicht nur die neuen Pflichten einhalten, sondern auch umfassend **dokumentieren, dass diese Pflichten eingehalten werden**. Im Kern müssen damit **Datenschutz-Management-Systeme** geschaffen werden, die in der Lage sind, jeden datenschutzrechtlich relevanten Vorgang umfassend zu dokumentieren und datenschutzrechtliche Compliance nachzuweisen **(sog. Rechenschaftspflicht)**, z.B. die **Verarbeitung personenbezogener Daten, die Zweckbindung und geeignete technische und organisatorische Maßnahmen**.

Daneben gibt es eine Vielzahl weiterer Bereiche, in denen nunmehr zügiges aber überlegtes Handeln gefragt ist.

Ab 25. Mai 2018 ist Compliance erforderlich.

FOLGEN BEI NICHTEINHALTUNG

- Ansprüche auf zivilrechtlichen Schadensersatz
- strafrechtliche Verfolgung
- Bußgelder im Ernstfall **bis zu 20 Mio. Euro oder auch 4% des gesamten weltweit erzielten Jahresumsatzes**