DSGVO: „Die Bußgeldhöhen sind deutlich gestiegen“

Ab 25. Mai müssen auch Stiftungen und andere gemeinnützige Organisationen ihren Umgang mit personenbezogenen Daten gemäß der neuen Datenschutzgrundverordnung (DSGVO) dokumentieren. Wie ist das umzusetzen?

Wieland Kirch: Ein wichtiger Baustein, um der in Art. 5 Abs. 2 DSGVO normierten Rechenschaftspflicht zu genügen, ist die Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten. Damit sind zwar nicht alle von der Datenschutzgrundverordnung (DSGVO) geforderten Dokumentationspflichten erfüllt – zu dokumentieren sind auch das Betroffenenrechte-, das Datenpannen- und das Dienstleistermanagement sowie die technischen und organisatorischen Maßnahmen –, doch es ist ein wichtiger Schritt getan.

Welche Daten und Prozesse sind in dem Verarbeitungsverzeichnis zu dokumentieren?

Kirch: Das Verarbeitungsverzeichnis betrifft sämtliche Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Für jede einzelne ist eine Beschreibung anzufertigen. Als Verarbeitungstätigkeit wird im Allgemeinen ein Geschäftsprozess auf geeignetem Abstraktionsniveau verstanden. Es sollte dabei ein strenger Maßstab angelegt werden, so dass jeder neue Zweck der Verarbeitung auch eine eigene Verarbeitungstätigkeit darstellt.

Gibt es hierbei „Kann“- und „Muss“-Bestandteile?

Kirch: Pflichtbestandteile des Verarbeitungsverzeichnisses sind unter anderem der Zweck der Verarbeitung, der Betroffene, dessen personenbezogene Daten und der Datenempfänger, geordnet in Kategorien. Auch Löschfristen für die unterschiedlichen Datenkategorien müssen dokumentiert werden. Außerdem hat es durchaus Sinn, diese Pflichtbestandteile durch weitere „Kann“-Bestandteile zu erweitern, wenn sich diese einfacher verarbeitungsspezifisch abhandeln lassen. Darunter fallen Regelungen zu Betroffenenrechten, die Risikoprüfung, die Datenschutz-Folgeabschätzung oder auch die Datenminimierung.

Können Sie das genauer erklären?

Kirch: Nehmen wir als Beispiel das Prinzip der Datenminimierung, das besagt, dass nur Daten erhoben werden, die auch tatsächlich zur Zweckerfüllung benötigt werden. Wie soll man die Umsetzung dieses Prinzips dokumentieren, ohne hier nach den einzelnen Verarbeitungen zu differenzieren? Die Beachtung dieses Grundsatzes kann und sollte zudem zusätzlich in einer globalen Datenschutzrichtlinie beschrieben werden. Im Grundsatz sollte also immer so viel wie möglich vor die Klammer gezogen werden, während der Rest möglichst verarbeitungsspezifisch dokumentiert wird. Dieses Vorgehen schafft Transparenz und reduziert Redundanzen.

Welche Tools empfehlen Sie einer Stiftung für die Dokumentation ihrer Daten?
Kirch: Die geeignete Toolwahl sollte nicht unterschätzt werden, denn ein späterer ungeplanter Umstieg auf ein anderes Werkzeug kann recht aufwendig werden. Insbesondere für größere Organisationen ist eine geeignete Unterstützung für die Erstellung, Organisation, Pflege und Veröffentlichung ihrer Dokumentation wichtig. Aber auch bereits für kleinere Organisationen gibt es einige Funktionalitäten, die durchaus sinnvoll oder sogar notwendig sein können, wie zum Beispiel ein einheitlicher Index mit Verweisungstechnik auf unterschiedlichste Dokumente, Musterleitlinien, -richtlinien und -anweisungen oder die lizenzkostenfreie Bereitstellung der Dokumentation für die Belegschaft. Vieles davon kann ganz gut mit sowieso vorhandenen Mitteln, etwa Office-Produkten, abgebildet werden.

Ab wann ist mit Kontrollen zu rechnen?
Kirch: Meines Erachtens wird es vorerst wohl nur anlassbezogene Kontrollen durch die Aufsichtsbehörden geben, wenn sich z.B. Betroffene beschweren oder es zu einer Datenpannenmeldung kommt. Mittel- bis langfristig sollte auch mit anlasslosen Kontrollen gerechnet werden, wenn sich hier erst einmal der entsprechende Behördenapparat ausgebildet hat, der der erweiterten Gültigkeit der DSGVO und den höheren Bußgeldern gerecht wird.

Was droht einer Organisation, wenn sie dieser Dokumentationspflicht nicht gerecht wird?
Kirch: Die Bußgeldhöhen sind deutlich gestiegen – bis zu maximal 20 Millionen Euro und vier Prozent der weltweiten Umsatzerlöse. Denkbar sind aber auch Tätigkeitsverbote bis ein datenschutzwidriger Zustand behoben ist. Eine ausreichende Dokumentation der Datenschutzbemühungen belegt den Vorsatz der Organisation, sich datenschutzkonform zu verhalten, was im Zweifel für den Verantwortlichen ausgelegt werden wird. Sie ist im Datenpannenfall ein grundsätzlicher Nachweis dafür, dass eben möglichst kein Organisationsversagen vorliegt. Wenn nichts dokumentiert ist, liegt auf jeden Fall zumindest ein Formalmangel vor.


Foto: Schomerus & Partner mbB

Über den Autor:
Wieland Kirch ist Partner, Wirtschaftsprüfer und Steuerberater bei Schomerus, einem Beratungsunternehmen für gesellschaftliches Engagement.

Literaturtipps:

Nützliche Hinweise zum Verzeichnis von Verarbeitungstätigkeiten:

PDF von Bitkom: Das Verarbeitungsverzeichnis
Kurzpapier: Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS – GVO Beispielverzeichnis von Verarbeitungstätigkeiten
Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO

Weitere Beiträge von DIE STIFTUNG zur neuen Datenschutzgrundverordnung:

Ausgabe 05-2017, Seite 26
Richtig auf die DSGVO vorbereiten

Die Website der Bundesbeauftragten für Datenschutz und Informationsfreiheit:

www.bfdi.bund.de