

lige Rechte auf Schadenersatz o.Ä. erloschen sind.

Aber wenn kein Hinderungsgrund besteht, wären die Daten eigentlich zu löschen. Allerdings ist es eben auf Grund der Speichermethoden wie Magnetbändern oder nicht mehr modifizierbaren optischen Datenträgern wie beschreibbaren DVDs praktisch unmöglich, gezielt Daten aus einem einzelnen Backup-Datensatz zu löschen.

Recht auf Berichtigung

Ähnlich problematisch ist das Recht auf Berichtigung von personenbezogenen Daten in Backup-Archiven. Ein Modifizieren von Daten in Backup-Archiven ist technisch ähnlich unmöglich wie das gezielte Löschen der Daten. Auch widerspricht das Modifizieren von Daten in Archiven dem Sinn der Archivierung, bei der es ja um die unveränderte Speicherung geht. Es ist da auch eine rechtliche Vorgabe, dass man die Daten unverändert wiederherstellen können muss. Auch darauf geht die DSGVO nicht ein.

Technische Lösungsvorschläge



Gibt es technische Möglichkeiten, die Vorgaben der DSGVO dennoch umzusetzen, ohne dass die skizzierten Probleme schlagend werden? Nun, hier kann uns die Kryptographie zu Hilfe kommen. Werden personenbezogene Daten verschlüsselt, so sind sie nur mehr für den Besitzer des kryptographischen Schlüssels wiederherstellbar. Gerade im Bereich des Backups kommt der Verschlüsselung eine wichtige Rolle zu. Da Backups außer Haus gelagert werden sollen, mitunter sogar bei externen Firmen, gehört es zum Stand der Technik, die Daten auf den Backup-Speichermedien zu verschlüsseln, sodass sie selbst in frem-

den Händen sicher sind und nicht gelesen werden können. Hier werden jedoch im Regelfall alle Daten mit demselben Schlüssel verschlüsselt. Dies muss jedoch nicht sein.

Denkbar wäre eine Lösung, bei der man die auf jeweils eine Person bezogenen Daten mit jeweils einem eigenen Schlüssel für das Backup oder Archiv verschlüsselt. Um bestimmte personenbezogene Daten in Backups oder Archiven zu löschen würde es dann genügen, die jeweiligen zugehörigen Schlüssel zu löschen. Ohne Schlüssel gibt es keine Möglichkeit mehr, die Daten zu entschlüsseln und dadurch auch faktisch keine personenbezogenen Daten mehr. Allerdings müssen nunmehr die Schlüssel besonders gut gegen Löschen gesichert werden, da ohne sie keine Restaurierung möglich ist. Würden die Schlüssel ebenfalls einem Backup unterworfen werden, würde das die personenbezogenen Daten erst wieder wiederherstellbar machen. Da aber die Schlüssel relativ geringe Datenmengen darstellen, wäre eine entsprechend sichere Speicherung ohne Verwendung von Backup- oder Archivierungssystemen denkbar.

Zwar klingt eine solche technische Lösung verführerisch, jedoch muss man bedenken, dass die derzeitigen Backup- und Archivierungssysteme eine solche Vorgehensweise nicht bieten, sondern diese Methodik erst schrittweise eingeführt werden muss. Daher löst dieser Vorschlag das unmittelbare Problem nicht.

Juristischer Lösungsansatz



Es eine Modifikation bzw. Erweiterung der DSGVO als einzig gangbarer Weg. Man müsste die DSGVO entsprechend erweitern, sodass der Spezialfall der „eingefrorenen“

Daten in Backups und Archiven explizit geregelt wird, ohne dass dadurch die Rechte der Betroffenen eingeschränkt werden. Es bedarf einer Definition dieser Datenklasse dahingehend, dass klar gestellt wird, dass diese Daten in ihrer Verarbeitung eingeschränkt sind und nur mehr gespeichert werden. Die Rechte hinsichtlich dieser Daten sind dann entsprechend zu modifizieren, sodass sie mit den technischen Gegebenheiten kompatibel sind. Auskunftsrechte müssten darauf beschränkt werden, dass die Betroffenen lediglich erfahren, dass die Daten noch in Backups oder Archiven vorliegen, aber nicht mehr verarbeitet werden und daher auch keine Informationen über den Inhalt der Daten gegeben werden können. Löschen- und Modifikationsrechte müssten für „eingefrorene“ Daten ausgesetzt werden.

Um der betroffenen Person dennoch maximalen Schutz ihrer Daten zu gewährleisten, sollte eine Verständigungspflicht des Verantwortlichen hinzugefügt werden für den Fall, dass die personenbezogenen Daten aus dem Backup oder Archiv wieder ins System eingespielt und damit verarbeitbar gemacht werden. Dadurch wäre gewährleistet, dass die Person ihre Rechte an den nunmehr verarbeitbaren Daten wieder in vollem Umfang ausüben kann.

Die **Digital Society** wird diesbezüglich einen konkreten textuellen Vorschlag für eine Änderung der DSGVO ausarbeiten und an die EU-Kommission übermitteln.

Weitere Beiträge zum Thema Datenschutz-Grundverordnung finden sich unter

<http://digsociety.at/dsgvo/>



Dipl. Ing. Roland Giersig

Roland Giersig ist Physiker, studiert Rechtswissenschaften, ist Sicherheitsexperte und Inhaber der Firma SafeSec. Er ist Experte auf dem Gebiet Safety & Security, sowie im Bereich der Grundrechte und Datenschutz. Seine Anliegen sind besonders die Transparenz der öffentlichen Verwaltung und die Einhaltung der Grundrechte im digitalen Raum.

Digital Talk: Meinungsbeeinflussung, Fake News & Hate Speech

Mittwoch 2018-12-12 18:00-21:00

Digital Society · Graben 17/10 · 1010 Wien



Als die Druckerpresse erfunden wurde, wurde sie recht bald dazu verwendet Stimmung für bestimmte Anliegen zu machen. Mit der Wahrheit nahm man es damals wie heute nicht so genau. Das führte zur Einführung der Impressumspflicht. Heute befinden wir uns durch die digitale Transformation in einer ähnlichen Situation. Jeder hat sozusagen eine moderne Druckerpresse zu Hause und kann theoretisch Millionen von Menschen erreichen. Wie können die Phänomene der neuen digitalen Medien in den Griff bekommen werden und positiv für die Entwicklung unserer Demokratie genutzt werden?