Datenschutzrevisionen und Auswirkungen auf die Softwareentwicklung

Am 25. Mai 2018 wird in der Europäischen Union die Datenschutz-Grundverordnung (EU-DSGVO, engl. General Data Protection Regulation, GDPR) in Kraft treten. Dies ist ein Fakt, der breit diskutiert wird und einiges an Aktionen auslöst.

lic. iur. Ursula Sury

Die Datenschutz-Grundverordnung ist auf alle Prozesse der Datenbearbeitung anwendbar, die sich auf personenbezogene Daten von Personen, welche sich in der EU befinden, beziehen. Sie gelangt zur Anwendung bei einer Verarbeitung im Rahmen einer EU-Niederlassung, dem Angebot von Waren und Dienstleistungen in der EU sowie bei der Verhaltensbeobachtung von Personen in der EU. Die Datenschutz-Grundverordnung gilt sowohl für ganz als auch für teilweise automatisierte Verarbeitungen personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen. Am 21. Dezember 2016 schickte der Bundesrat den Vorentwurf für das neue DSG in die Vernehmlassung, welche bis am 4. April 2017 dauert. Zu den Verordnungen zum neuen DSG ist bislang noch nichts bekannt.

Inhaltlich sind, wenn man den Vorentwurf mit dem geltenden Datenschutzgesetz der Schweiz vergleicht, einige interessante Änderungen geplant, insbesondere werden auch gewisse Grundsätze der europäischen Datenschutz-Grundverordnung übernommen.

Übersicht über wesentliche Neuerungen in der Schweiz und der EU

Automatisierte Datenbearbeitung

Da immer häufiger regelbasierte Abläufe nur noch IT-mässig erledigt werden, sieht das neue Schweizer Datenschutzgesetz vor, dass betroffene Personen bei Entscheidungen, die ausschliesslich auf automatisierten Datenbearbeitungen beruhen, über diese Situation und die rechtlichen Wirkungen informiert werden müssen und betroffenen Personen gar die Möglichkeit zu einer Stellungnahme gegeben werden muss (Art. 15 E-DSG).

Die europäische Datenschutz-Grundverordnung sieht vor, dass eine betroffene Person das Recht hat, dass sie nicht Entscheidungen unterworfen wird, welche ausschliesslich auf einer automatisierten Verarbeitung beruhen, sofern diese Entscheidungen gegenüber der betroffenen Person rechtliche Wirkungen entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (Art. 22 Abs. 1 EU-DSGVO). Diese Regel gilt nicht, wenn die Entscheidungen für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Datenbearbeiter erforderlich sind, wenn die Entscheidungen aufgrund von Rechtsschriften der Union oder der Mitgliedstaaten, denen der Datenbearbeiter unterliegt, zulässig sind (sofern diese Rechtsschriften angemessene Massnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten) oder mit ausdrücklicher Einwilligung der betroffenen Person erfolgen (Art. 22 Abs. 2 EU-DSGVO).

Datenschutz-Folgenabschätzung im IT-Projekt
Analog der Regelungen in der neuen Datenschutz-Grundverordnung der EU verlangt der Entwurf des neuen DSG eine Datenschutz-Folgenabschätzung: Besteht bei der Verarbeitung von Personendaten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen, muss vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchgeführt werden. Das heisst sämtliche möglichen Risiken müssen umschrieben und Massnahmen zur Verringerung der Risiken müssen vorgesehen werden. Geht aus der Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung tatsächlich ein hohes Risiko zur Folge hätte, sofern der Datenbearbeiter keine Massnahmen zur Eindämmung des Risikos treffen würde, muss der Datenbearbeiter die Aufsichtsbehörde darüber informieren (Art. 16 E-DSG, Art. 35 f. EU-DSGVO). Aus diesem Grund müssen Projektleiter bereits ab Beginn (und auch während ihrer Projekte) den Datenschutz stets im Blick behalten.

Meldepflicht von Datenschutzverletzungen
Auch analog der Datenschutzgrundverordnung der EU sind neu im DSG-Entwurf Datenbearbeiter verpflichtet, Verletzungen des Datenschutzes von sich aus der Aufsichtsbehörde zu melden (Art. 17 E-DSG, Art. 32 EU-DSGVO). Dies erfordert das aktive Betreiben eines Datenschutzmanagementsystems und des damit verbundenen kontinuierlichen Verbesserungssystems mit den integrierten Kontrollmassnahmen. In der Schweiz hat die Meldung von Datenschutzverletzungen unverzüglich, in der EU binnen 72 Stunden, nachdem die Verletzung bekannt wurde, zu erfolgen.

Privacy by Design und Privacy by Default
Eine weitere Analogie zur EU-Gesetzgebung ist die Pflicht, die Einhaltung des Datenschutzes in IT-Systemen möglich zu machen und bei den Default-Einstellungen die Anforderungen des Datenschutzes schon zu berücksichtigen. Wir sprechen von Privacy by Design und Privacy by Default (Art. 18 E-DSG, Art. 25 EU-DSGVO). Privacy by Design bedeutet, dass Datenschutz und Privatsphäre bereits in der Entwicklung von Technik beachtet werden sollen. Die Technik soll so angelegt werden, dass die Privatsphäre von Nutzern geschützt wird und dass Anwender die Kontrolle über die eigenen Informationen haben. Privacy by Design betrifft somit insbesondere die Architektur und Funktionalität von IT und Software. Privacy by Default bezieht sich auf die Grundeinstellungen in Produkten oder bei Dienstleistungen (z. B. Zugriffsregelungen). Produkte, welche den Grundsatz von Privacy by Default berücksichtigen, sind also standardmässig datenschutzfreundlich eingestellt. Die «Ausrede», Datenschutzeinhaltung sei wegen der IT nicht möglich, wird somit in Zukunft viel schwieriger.

Dokumentation von Datenbearbeitungen
Auch interessant ist, dass die Datenbearbeiter neu verpflichtet werden sollen, ihre Datenbearbeitung zu dokumentieren (Art. 19 lit. a E-DSG, Art. 30 EU-DSGVO). Dazu gehört z. B. auch, eine Übersicht über die Systemlandschaft zu erstellen. Auch hier verlangt das Gesetz implizit den Betrieb eines dokumentierten Datenschutzmanagement-Systems. Die Rolle der Aufsichtsbehörde wird gestärkt, so kann er auch ohne Vorankündigung Räume inspizieren, sogar vorsorgliche Massnahmen anordnen und Verwaltungsmassnahmen verfügen oder gar Datenbekanntgaben ins Ausland verbieten.

Sanktionen
Mit dem neuen Datenschutzgesetz sind Datenschutzverletzungen in der Schweiz nicht mehr Kavaliers-, sondern im wahrsten Sinne des Wortes Kapitaldelikte. Wenn die Grundsätze des Datenschutzes verletzt werden, werden Bussen bis zu 500 000 CHF ausgesprochen. Auf Antrag werden private Personen sanktioniert, welche Daten ins Ausland übermitteln oder Datenbearbeitungen auslagern, ohne dass die entsprechenden Voraussetzungen dafür gegeben sind. Auch wird bestraft, wer es unterlässt, die notwendigen Massnahmen zu treffen, um Daten gegen eine unbefugte Datenbearbeitung oder einen Verlust zu schützen, wer es unterlässt, eine Datenschutz-Folgenabschätzung vorzunehmen, wer die Grundsätze Privacy by Design und Privacy by Default nicht beachtet und wer die Datenbearbeitung nicht dokumentiert (Art. 51 E-DSG).
Im Gegensatz zur Schweiz, wo nur für private Personen eine Busse vorgesehen ist, können gemäss Datenschutz-Grundverordnung Datenschutzverletzungen mit Bussen bis zu 20 000 000 EUR oder im Fall eines Unternehmens bis zu vier Prozent seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs betragen, je nachdem, welcher der Beträge höher ist (Art. 83 EU-DSGVO). Wir sehen, Datenschutzverletzungen werden vom Kavaliersdelikt zum eigentlichen unternehmerischen Problem, ähnlich wie Wettbewerbsverletzungen. ■