Datenschutz CH und EU: Was wird wirklich neu?

Wir haben schon seit 26 Jahren ein Datenschutzgesetz!

Die Schweiz hat schon seit 26 Jahren ein Datenschutzgesetz und zwei ergänzende Verordnungen für Tätigkeiten von Privaten und Bundesorganen. Darin sind die wichtigsten Datenschutzanforderungen verbindlich geregelt. Wer Daten einer Person bearbeitet, muss:

- eine gesetzliche Grundlage oder eine Einwilligung haben (Warum)
- mit den Daten verhältnismässig umgehen (Minimum beim «Wer macht Was»: Zugriffe, Aufbewahrung und Archivierung regeln, etc.)
- sicherstellen, dass die bearbeiteten Daten inhaltlich richtig sind
- die Sicherheit, insbesondere die Informatiksicherheit, gewährleisten

Der Eidgenössische Datenschutzbeauftragte hat dabei den Auftrag, die Umsetzung des Datenschutzes mittels Empfehlungen, Informationen und Kontrollen durchzusetzen.

Analoges regeln die Kantone für Behörden von Kanton und Gemeinden. Die Kantonalen Datenschutzbeauftragten sind hier für die Unterstützung und Kontrolle der Umsetzung zuständig.

Auch in der EU gibt es seit 23 Jahren eine Datenschutzrichtlinie. Diese verpflichtet die einzelnen Länder der Union ihre Landesgesetze gemäss der Richtlinie auszugestalten. Je nach Land der EU ist die Datenschutzaufsicht unterschiedlich ausgestaltet.

Ein sorgfältig handelnder Verwaltungsrat und CEO müsste folglich:

- ein Überblick über die in der Unternehmung bearbeiteten Daten haben,
- die Datenschutzkonformität bei der Bearbeitung in allen Dimensionen prüfen,
- die Risiken (auch Legalrisks) bei der Bearbeitung managen.

Stand der Datenschutzmaturität in den Unternehmen

Die meisten Unternehmen haben sich bis in den letzten Jahren, trotz bestehendem Gesetz, kaum um den Datenschutz gekümmert. Dazu gibt es insbesondere folgende Gründe:

- Datenschutz beschäftigt sich mit der Bearbeitung von Informationen über Personen. Diese sind heute mehrheitlich digital gehalten, verarbeitet, transportiert etc. Dadurch wird das Thema aus Sicht des Managements der IT klassischen Unterstützungsprozessen zugeordnet.
- Digitales, also Virtuelles und nicht Sichtbares, entzieht sich immer noch unserem menschlichen Wertesystem. Wir könnten uns die Bedeutung in der Dimension der Persönlichkeitsverletzung oder der Geldwerte von Digitalem kaum vorstellen!
- Die Digitalisierung und somit die Möglichkeiten, aber auch Pflicht, mit und aus (auch personenbezogenen) Informationen (Big Data, IoT etc.) Werte zu schaffen, ist eher neu.
- Die Unternehmensgrenzen werden immer offener und kaum eine Unternehmung kann noch ohne Outsourcingverhältnisse leben. Dies ist nur schon an der intuitiven Verwendung von Apps durch Mitarbeitende ersichtlich.
- Und nicht zuletzt: Datenschutzverletzungen ziehen bis anhin kaum Strafen mit sich.

Wann kommen welche Gesetze und wie sind diese anwendbar?

Die EU setzt am 25. Mai 2018 die Datenschutzgrundverordnung (DSGVO oder auf Englisch GDPR) in Kraft. Diese Verordnung ist für die einzelnen Länder der Union direkt anwendbar. Eine gewisse

Gestaltungsfreiheit besteht aufgrund von Öffnungsklauseln, die eine Konkretisierung, Ergänzung oder Modifikation zulassen, aber niemals einen Widerspruch.

Die Schweiz hat ihr Datenschutzgesetz ebenfalls überarbeitet. Es liegt ein Entwurf vor, der eventuell in zwei Etappen im Jahre 2019 in Kraft treten wird, so der Bundesrat.

Welche Änderungen der Entwurf noch erfahren wird, ist offen. Sicher wird aber das Schweizer Gesetz sowohl vom Wording als auch vom Inhalt her nahe an der DSGVO sein.

Eine Herausforderung für Schweizer Unternehmer ist, dass die EU betreffend der Anwendbarkeit ihrer DSGVO vom Marktortprinzip und Personenprinzip ausgeht, d.h. wer Daten einer Person, die dauernden Wohnsitz in der EU hat, bearbeitet (Angebot von Waren oder Dienstleistungen in der EU; allgemeine Übernahme von Datenbearbeitungen von Personen aus der EU), unterliegt den Regelungen der DSGVO. Natürlich liegt hier der Teufel im Detail und entsprechen muss im Einzelfall abgeklärt werden.

Wenn aber auch nur für einzelne Personengruppen die DSGVO anwendbar ist, muss aus Gründen der Praktikabilität das ganze Managementsystem entsprechend aufgebaut werden.

Die wichtigsten Neuerungen im Überblick

Folgende Punkte sind sowohl für die Schweiz als auch für die EU zu beachten:

- Wer den Datenschutz verletzt, wird sanktioniert. Dies können sehr hohe persönliche Geldstrafen (CH; VR und C-Level) oder Verwaltungsstrafen für Unternehmen (EU) sein.
- Der betroffenen Person muss klar sein, was mit ihren Daten warum gemacht wird. Dies bedeutet, dass die Einverständniserklärungen genügend klar sind.
- Bezüglich Kindern sieht die EU vor, dass eine Einverständniserklärung der Erziehungsberechtigten vorliegen muss, was zur Folge hat, dass Unternehmen das Alter ihrer User kennen und ggf. eine zusätzliche Sicherheitsstufe vorsehen müssen.
- Die Transparenz für die betroffene Person impliziert, dass über den ganzen Lifecycle der Datenbearbeitung Klarheit herrscht, d.h. wie mit den Personendaten umgegangen wird etc. Dazu gehört auch die Information über Outsourcingverhältnisse, weil damit für die Betroffenen erhöhte Risiken verbunden sind.
- Beim Outsourcing ist abzuklären und zu kontrollieren, dass die Bearbeitungen nur im Rahmen des gesetzlich zulässigen erfolgen.
- Zur Umsetzung des Datenschutzes gehört, dass man dokumentiert, welche Datenbearbeitungen warum erfolgen (Gesetz oder informierte Einwilligung).
- Die IT und die Organisation muss im täglichen Betrieb und im Rahmen von Projekten den Datenschutz zwingend abbilden: Privacy by Design und Privacy by Default. Auch dies muss nachgewiesen werden.
- Im Betrieb - aber vor allem im Rahmen von Projekten - muss immer abgeklärt werden, welchen Einfluss dies auf Personendaten haben könnte: Privacy Impact Assessment.
- Datenschutzverletzungen müssen (mindestens ab einer gewissen Schwere) der Datenschutzaufsicht gemeldet werden.

Kurz gesagt, Unternehmensverantwortliche tragen das Risiko grober Sanktionen, wenn sie den Datenschutz nicht nachweisbar umsetzen. Das Abfassen von allgemeinen Datenschutzerklärungen genügt nicht. Diese müssen konkretisiert und dann im Unternehmen umgesetzt werden.

Zusammenfassung

- Der Datenschutz wird nicht grundsätzlich neu geregelt, es wird vor allem deren nachweisbare Einhaltung mittels harter Sanktionen eingefordert.
- An die Einwilligungen durch die Betroffenen und damit die Transparenz in die Datenbearbeitung (Homepage) werden erhöhte Anforderungen gestellt.
- Datenschutzverletzungen müssen der Datenschutzaufsicht gemeldet werden.

Ursula Sury ist selbständige Rechtsanwältin in Luzern, Zug und Zürich (CH) und Vizedirektorin an der Hochschule Luzern - Informatik. Sie ist zudem Dozentin für Informatikrecht an verschiedenen Nachdiplomstudien. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig.