Den Anforderungen der EU-Datenschutzverordnung gerecht werden

Kontrolle über das Datenuniversum

Gesetzesänderungen der EU und der Schweiz erfordern, dass personenbezogene Daten geortet und gelöscht werden können. Doch wie geht das? **Von Kaspar Geiser & Peter Schäuble**

Die neue Datenschutz-Grundverordnung der EU (General Data Protection Regulation, GDPR) fordert, dass personenbezogene Daten auf Wunsch sofort gefunden und unter gewissen Voraussetzungen gelöscht werden. Die Unternehmen müssen deshalb künftig genau wissen, wo ihre Daten liegen, wie schützenswert diese im Einzelnen sind und wie sie verarbeitet werden. Da sich im Zeitalter von SaaS, Cloud Computing und Outsourcing die Daten schnell verteilen, ist diese Kontrolle nicht leicht zu erlangen. Parallel zum GDPR revidiert die Schweiz ihr Datenschutzgesetz, der Inhalt des Vorentwurfs ist bereits bekannt. Auch dieses Gesetz nimmt Dateninhaber und -verarbeiter stärker in die Verantwortung.

Überblick verschaffen

Mit der GDPR fallen deutlich mehr Daten in den Verantwortungsbereich einer Firma als bisher. Die Verordnung erfasst auch Daten, die der Inhaber intuitiv nicht zu den eigenen Daten zählt. Es ist also unausweichlich, dass sich Unternehmen eine Übersicht über ihre Daten verschaffen und diese klassifizieren. Dabei sollten zumindest folgende Fragen geklärt werden:

- Sind die Geschäftsdaten am richtigen Ort?
- Sind sie geschützt?
- Sind alle Kopien und Speicherorte bekannt?
- Ist vollständig klar, wer Zugriff auf die Daten hat?

Daten klassifizieren

Schutzmassnahmen lassen sich einfacher ermitteln, wenn die Daten klassifiziert sind, wenn also bestimmt wird, zu welcher Datenkategorie sie gehören. Besonders sensibel und schützenswert sind insbesondere Personendaten mit Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gesundheit oder Sexualleben. Was schützenswert ist, unter-

Bild: Shutterstock/NikoNomad

scheidet sich jedoch von Unternehmen zu Unternehmen. Hat der Dateninhaber die Liste der Datenkategorien und deren Schutzbedarf erstellt, müssen alle zu schützenden Daten gefunden und einer Kategorie zugeordnet werden.

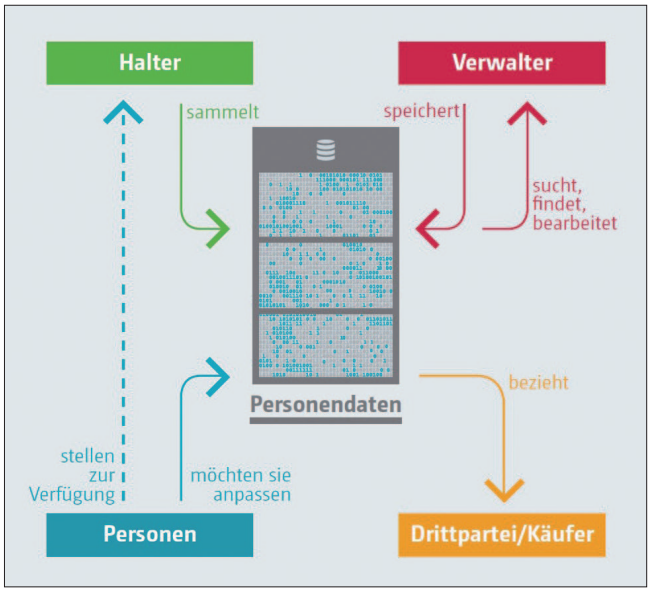
Daten finden

Die Herausforderung besteht darin, Personendaten über verschiedene Systeme hinweg zu finden. Dies macht den Einsatz eines eDiscovery-Systems nötig, das personenbezogene Daten schnell aufspürt. Dabei tauchen oft Daten auf, die keinen unmittelbaren Bezug zur Geschäftstätigkeit des Unternehmens aufweisen. Dazu gehören auch Daten, die unabsichtlich aufgrund einer falschen Systemkonfiguration gesammelt wurden. Zudem betrifft die Verordnung nicht nur Dateninhaber, sondern auch Datenverarbeiter. Dateninhaber wissen in der Regel, welche Daten sie zu welchem Zweck sammeln. Datenverarbeiter hingegen bearbeiten, speichern oder bewahren Daten, ohne sie jedoch selbst zu verwenden oder zu verändern. Beide werden auf eDiscovery angewiesen sein.

Nur scheinbar anonyme Daten

Auch die Gesetzgebung in der Schweiz beschäftigt sich mit dem Aspekt «Profiling». Als Profiling gilt jede Auswertung von Daten, die das Ziel hat, wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, etwa betreffend der Arbeitsleistung oder der Gesundheit. Bei dem Vorgehen reichert ein Programm ursprünglich anonymisierte Daten mit externen Informationen an und macht so den Rückschluss auf eine Person möglich. Dadurch macht Profiling den Datenbestand, für den ein Unternehmen zuständig ist, wesentlich grösser.

Solche Informationen können sich in den verschiedensten Orten einnisten. Applikationsdaten, Anhänge von E-Mails, aber auch Metadaten von Dateien enthalten oft besonders schützenswerte Personendaten. Erfahrungen aus eDiscovery-Projekten zeigen, dass sich heikle Daten auch in Legacy-Applikationen, in Löschordnern, in lokalen E-Mail-Archiven oder in überschriebenen Dokumenten verstecken können.



Datenbewegungen: Die Verantwortung liegt bei den Dateninhabern (Halter) und den Datenbearbeitern (Verwalter)

Zentrale Massnahmen

Ein eDiscovery-System allein bringt noch keine Garantie, dass die Datenschutzpflichten erfüllt werden. Im Betrieb sind die folgenden Massnahmen zentral:

- Jede Änderung in den Datensammlungen automatisch im Suchindex nachführen.
- Konzeptsuche nutzen.
- In der Suchanfrage und in den Datensammlungen Abweichungen bei der Namensschreibweise berücksichtigen.
- Digitalisierte Dokumente mit OCR in maschinenlesbaren Text umwandeln.
- Benutzer dürfen nur Informationen finden, für die sie die Zugriffsrechte besitzen.
- Daten zentralisieren: Die eigenen Daten sollten auf möglichst wenige Standorte und Services verteilt sein. So verkleinert sich der Kreis der Personen und Systeme mit Zugang zu sensitiven Informationen.

Daten löschen

Mit den Daten wird täglich gearbeitet: Sie werden bearbeitet, weitergegeben oder gelöscht. Beim Löschen verschwinden die Daten aber nicht vollständig. Sie sind zwar in den jeweiligen Anwendungen nicht mehr sichtbar, doch weiterhin vorhanden. Bei einem Export der Daten kann es passieren, dass auch vermeintlich gelöschte Einträge an Drittsysteme übertragen werden: Wenn diese den Status «nicht sichtbar» ignorieren, werden die Daten wieder sichtbar.

Noch schwieriger wird es, wenn unstrukturierte Daten etwa in Textdokumenten vorkommen. Wird ein solches Dokument gelöscht, so ist es aus Betriebssystemsicht in vielen Fällen nach wie vor find- und lesbar. Technisch ist also Löschen beinahe nicht möglich. Wollen sich Dateninhaber schützen, braucht es deshalb vertragliche Vereinbarungen mit dem Datenbearbeiter.

Fazit: Wettbewerbsvorteil

Um die Bestimmungen zu erfüllen, müssen Dateninhaber die Übersicht über ihre Daten haben und ihre Infrastruktur den neuen Anforderungen anpassen. Denn Anfragen zu personenbezogenen Daten werden bestimmt eintreffen. Nur mit der richtigen Vorbereitung können Dateninhaber dann auch schnell reagieren.

In der Praxis werden Unternehmen wohl eine Programmierschnittstelle einführen, die eine automatisierte Erfüllung der Auskunftspflicht ermöglicht. Gut umgesetzt, kann der Umgang mit Personendaten sogar zu einem USP von Unternehmen werden. ■

Kaspar Geiser ist Geschäftsleiter des Hosting-Anbieters aspectra:
www.aspectra.ch
Peter Schäuble ist Gründer und Geschäftsführer von Eurospider:
www.eurospider.com