

Wie wir mit Daten sicher und nachhaltig umgehen

Minimale Grundkenntnisse im Umgang mit Daten sind für jeden Bürger und jede Bürgerin notwendig, um bewusst und sicher im Cyberspace zu handeln. Der Beitrag zeigt, worauf zu achten ist.

Quelle: «Wie wir mit Daten sicher und nachhaltig umgehen können», Schweizerische Akademie der Technischen Wissenschaften SATW (2016)

Information wird neben Arbeitskraft, Rohstoff und Kapital als Produktionsfaktor immer wichtiger. Informationen erreichen uns heute über die verschiedensten Kanäle, vom Brief über das Radio bis zum Internet, und basieren sehr häufig auf computergespeicherten Daten. Daten werden von Menschen, immer häufiger aber bereits auch von Maschinen produziert. Die historische Mangelsituation hat sich heute zur Überflusssituation gewandelt. Aktuell verdoppelt sich der weltweite Datenbestand rund alle zwölf Monate. Mit der «Informationsüberflutung» und der dahinterstehenden «Datenexplosion» stellen sich viele Fragen: Wie werden all diese Daten verwertet? Wem sollen sie zur Verfügung stehen? Welche Auswertungen sollen erlaubt, welche verboten sein? Welche Verantwortung haben wir gegenüber der Nachwelt, damit die richtigen Daten archiviert werden und auch lesbar bleiben?

Selbstbestimmung und Demokratie brauchen kritische Auseinandersetzung

Viele Untersuchungen haben ergeben, dass den meisten Menschen eine grundlegende Ausbildung und ein genügendes Verständnis für den «Digitalen Datenraum» fehlen, obwohl sie sich tagtäglich darin bewegen. Minimale Grundkenntnisse bezüglich der Datenwelt sind für jeden Bürger und jede Bürgerin dringend notwendig, um die neuen Zusammenhänge zu erkennen, um bewusst und sicher zu handeln und die Konsequenzen ihrer Handlungen zu verstehen.

Persönliches Datenmanagement

Wir leben heute in einer Informationsgesellschaft und nutzen Computer und Handy privat und in Beruf und Schule. Da ist es zunehmend wichtig, über die dabei verwendeten Daten den Überblick zu behalten. Eigene Interessen und Kontaktpersonen können wechseln, technische Probleme und Systemwechsel mit der Zeit den Zugang zu den eigenen Daten erschweren oder blockieren; jeder kennt das. Daher ist ein persönliches Datenmanagement nötig, besonders wenn auch Dritte auf eigene oder auf gemeinsame Daten zugreifen müssen. Das Datenmanagement betrifft einerseits die Ablage der Daten und andererseits das langfristige Aufbewahren und Auffinden der Daten. Erstellen einer Liste der wichtigen Daten: Sie schafft Übersicht und hilft auch bei der Benennung von Dokumenten, Bildern, Passwörtern und Unterlagen aus der Zusammenarbeit mit

Kollegen. Gruppieren der Daten nach Aktivitäten: Datensammlungen sollen gruppiert werden. Professionell erfolgt dies mittels der konsequenten Abbildung von Aktivitäten, zum Beispiel in Projekte, und der konsequenten Zuordnung aller Daten zu jeweils einem Projekt. Backups machen: Eigene und fremde Datenträger sind anfällig für Störungen. Bei externen Speicherdiensten besteht oft nicht einmal ein formeller Vertrag zur dauerhaften Datenspeicherung. In jedem Fall sollte regelmässig eine Kopie der Daten auf einem vom aktuellen System unabhängigen Datenträger gespeichert werden; dieser Datenträger soll an einem anderen Ort, das heisst möglichst nicht im gleichen Gebäude, gelagert werden. Von Cloud-Daten können lokale Backups automatisiert gespeichert werden und umgekehrt. So bleiben auch alte Daten, die in der Cloud gelöscht werden, zugänglich. Datensammlungen für mehrere Personen: Daten, die man nicht selbst erzeugt oder für sich selbst speichert, beispielsweise Projektdaten, sollen auch in einer Liste definiert werden, die angibt, welche Datensammlungen für welche Personengruppen wichtig sind, wer darauf zugreifen darf und mit welchen Rechten (Leserecht, Schreibrecht, Recht zum Speichern oder Löschen von Daten).

Empfehlung

Ein konsequentes Datenmanagement ist notwendig, damit sich mehrere Personen in einer Datenablage zurechtfinden, aber auch keinen Schaden anrichten können. Das geeignete Speichern von Daten für ein nachhaltiges Auffinden von länger gültigen Daten (zum Beispiel in PDF) ist ein wichtiger Bestandteil des Datenmanagements.

Rechtlicher Rahmen bei Dokumenten

Der Urheber jedes Dokuments oder Bilds – es wird der Begriff «Werk» verwendet – hat vorerst das alleinige Recht an dessen Weiterverwendung und Nutzung, das so genannte Urheberrecht. Zudem hat jede Person das so genannte Recht am eigenen Bild und muss gefragt werden, bevor Fotos von ihr weitergegeben werden. Diese beiden Rechte müssen beim Umgang mit Daten immer berücksichtigt werden, namentlich bei der Veröffentlichung im Internet. Achtung: Bei einigen kostenlosen Online-Diensten wird mit der Nutzungserklärung das Nutzungsrecht an den Dienstleister übertragen.

Archivierung von Daten

Archivierung bedeutet hier die Langzeitaufbewahrung von Daten, damit diese auch nach Jahren und allfälligen Systemwechseln noch verfügbar gemacht werden können, wobei der Erhalt der Verfügbarkeit meist mit einem zusätzlichen Aufwand verbunden ist. Für die Archivierung gibt es viele Gründe, persönliche, gesetzliche und kulturelle. Ausser für Historiker sind gesetzliche und firmeninterne Gründe die wichtigsten. So müssen bestimmte Daten von Gesetzes wegen «so, wie sie sind» (authentisch, revisionsicher, integer) aufbewahrt werden. Diese Anforderung bedingt besondere technische, organisatorische und inhaltliche Massnahmen.

Technische Anforderungen an digitale Archive

Viele nehmen fälschlicherweise an, dass Speichermedien wie Festplatten oder CD-ROMs Daten dauerhaft sichern. Das stimmt nur begrenzt, denn die dauerhafte Erhaltung von digitalen Daten und die Sicherstellung ihrer Lesbarkeit sind schon nach wenigen Jahren technologisch nicht mehr gewährleistet, weil neben den Datenträgern auch entsprechende Lese-/Schreib-Stationen und Betriebssysteme einsatzfähig bleiben müssen. Daten müssen redundant, das heisst mehrfach, auf unterschiedlichen Datenträgern und an unterschiedlichen Orten gespeichert werden, um die Gefahr eines (Total-)Verlusts zu minimieren. «Stabile», das heisst neutrale, öffentlich standardisierte, möglichst einfache Dateiformate ermöglichen, dass die Inhalte auch von künftigen technologischen Systemen geöffnet und gelesen werden können. Beispiele für stabile Dateiformate sind für feste Inhalte PDF, für Bilder PNG und JPG, für veränderbare Texte und Tabellen die OpenDocument-Formate (.odt, .ods). Bei Bildern kann es sich lohnen, diese sowohl in einem Bildformat als auch als PDF abzuspeichern. Von der Datenübernahme bis zur späteren Nutzung müssen archivierte Daten geschützt gespeichert werden, das heisst, jede Bewegung der Daten muss aufgezeichnet werden und einer Person zugeordnet werden können.

Inhaltliche Anforderungen

Daten sollen möglichst strukturiert – beispielsweise in Ordnern oder in Datenbanken – abgelegt und mit Metadaten beschrieben werden. Metadaten beschreiben die Merkmale von Daten wie inhaltliche Schlüsselwörter, Erstelldatum, Grösse



In jedem Fall sollte regelmässig eine Kopie der Daten auf einem vom aktuellen System unabhängigen Datenträger gespeichert werden.

und Dateinamen. Sie erleichtern das spätere Auffinden spezifischer Inhalte. Der digitalen Archivierung stellen sich derzeit neue Herausforderungen: Dazu gehören etwa die Wiederverwendung der Daten für künftige Forschungsarbeiten, die Auswahl und Bewertung von digitalen Nachlässen und die Aufbewahrung und Vermittlung «komplexer» digitaler Objekte, die über die Struktur der klassischen Inventarisierung hinausweisen.

Internet ein Langzeitspeicher?

Digitale Langzeitarchive wandeln sich von statischen zu dynamischen Systemen, in denen die aufgenommenen Daten nicht mehr nur geordnet, verwaltet und dauerhaft gelagert, sondern auch im Internet zugänglich gemacht und aktiv bewirtschaftet werden. Zunehmend gibt es auch Internet-Archivdienste, die von Organisationen und Privaten genutzt werden können. Dass das Internet selbst vergisst, ist selten. Jedoch kann man sich nicht darauf verlassen, dass dort gespeicherte Daten später wieder zur Verfügung stehen: Dazu braucht es lokale Kopien.

Empfehlung

Verwaltungs- und Geschäftsdaten müssen professionell gespeichert und für digitale Archive zum Beispiel mit Metadaten aufbereitet werden. Die Daten müssen rund alle fünf Jahre kopiert werden, damit sie lesbar bleiben. Ausserdem sollen für «nachnutzende» Generationen die Datenprozesse akribisch dokumentiert werden.

Privatsphäre ist nicht Privatsache

Informationen entstehen immer in einem Kontext. Mit der Digitalisierung und Vernetzung werden persönliche Daten leicht aus dem Kontext gerissen. Wenn Sie beispielsweise über eine Krankheit im Internet googeln, weiss der Suchma-

schinenbetreiber vermeintlich bald einiges über Sie. Vielleicht haben Sie aber nicht nach Ihrem eigenen Gebrechen gesucht, sondern nach der Krankheit eines Nachbarn. Informationen ohne Kontext können also leicht missinterpretiert werden. Im Grunde geht es im obigen Beispiel um die Privatsphäre und das Grundrecht auf «informationelle Selbstbestimmung». Sie sollen prinzipiell selber bestimmen können, wer über Sie was weiss. Klar braucht soziale Interaktion persönliche Daten, sonst bleibt Kommunikation oberflächlich. Klar braucht ein Lieferant Ihre Adresse, um Ihnen bestellte Ware zustellen zu können. Klar braucht der Staat persönliche Daten, damit er seine gesetzlichen Aufgaben erfüllen kann. Jedoch ist es europäische Philosophie, dass niemand «alles» über Sie wissen darf - es sei denn, dass Sie dem zustimmen.

Demokratie und Marktwirtschaft brauchen Privatsphäre

Das Gegenteil von Selbstbestimmung ist Fremdbestimmung. Doch damit funktionieren weder unsere Gesellschaft noch der Staat noch die Marktwirtschaft. Die Marktwirtschaft als System ist auf selbstbestimmt handelnde, mündige Konsumentinnen und Konsumenten angewiesen, die auch Manipulationsversuche erkennen können, damit der Wettbewerb wirklich zum Tragen kommen kann. Deshalb sollten wir einer Entwicklung, in der die Privatsphäre zu verschwinden droht, nicht tatenlos zuschauen.

Privatsphäre durch Eigenverantwortung: Selbst-datenschutz

Gratisangebote und Bequemlichkeit verlocken leicht zur Preisgabe von Teilen der Privatsphäre. Kurzfristiger Nutzen einer kostenlosen App, der Sie auf Ihrem Smartphone alle Zugriffsrechte

einräumen, kann langfristige Folgen haben. Sind die dabei freigegebenen Daten wirklich so «harmlos», dass Sie diese mit der App teilen und die Kontrolle darüber verlieren wollen?

Privatsphäre durch Technik: Anwendung eines Systemdatenschutzes

Moderne Computeranwendungen, auch viele Apps, unterstützen oft den Schutz der Privatsphäre der Benutzer, aber häufig erst nach sorgfältiger Einstellung ihrer Benutzungsparameter. Daher Vorsicht bei Neuinstallationen; nachträgliche Einstellungsveränderungen sind oft schwierig und unsicher.

Privatsphäre durch Recht

In allen Industrieländern gibt es Datenschutzgesetze für den Persönlichkeitsschutz in Informationssystemen bis hin zu Auskunfts- und Berichtigungsrechten für die einzelnen Betroffenen. Aber diese Gesetze sind national ausgerichtet, sodass im globalen Cyberspace Regulierungslücken verbleiben, die straffrei ausgenützt werden können. Daher sind Anstrengungen im Verbund, zum Beispiel auf europäischer Ebene, notwendig, um Recht durchsetzen zu können.

Empfehlung

Selbstbestimmt handelnde, mündige Bürgerinnen und Bürger beziehungsweise Konsumentinnen und Konsumenten brauchen Privatsphäre. Für den Selbstdatenschutz ist jeder selbst verantwortlich. Dabei empfiehlt es sich, dem Prinzip der Datensparsamkeit zu folgen, das heisst, nur Daten bekannt zu geben, die wirklich von der Gegenpartei gebraucht werden. Der Staat soll mit Anforderungen für den Systemdatenschutz sowie im Datenschutzrecht den Rahmen für eine sichere Privatsphäre schaffen. ■