Datenschutz: Viel Neues

Dieter Zoubek

Soziale Netzwerke und internationale Internet-Handelsunternehmen waren in Sachen Datenschutz sehr häufig in den Medien vertreten. Es ging häufig um den Verdacht, dass mit den Daten von Bürgern nicht sehr achtsam umgegangen wird.

Die gute Nachricht ist, dass am 25. Mai neue, sehr bürgerfreundliche Regelungen in Kraft treten. Es darf als Quantensprung gesehen werden, dass die Datenschutzgrundverordnung (DSGVO) EU-weit einheitlich gilt.

Da die meisten großen Unternehmen Niederlassungen in der EU haben, unterliegen sie voll den neuen Regeln. Betroffen sind aber nicht nur internationale Firmen, sondern auch alle österreichischen Unternehmen, etwa Handwerker, Physiotherapeuten, bis hin zum Heurigenbetreiber. Vereine sind ausnahmslos exakt gleich betroffen wie Unternehmen.

Die wichtigsten Aspekte für Bürger:

- Grundloses Speichern von Daten und Verarbeiten von Personendaten ist verboten. Erlaubt ist es nur mehr, wenn ein Rechtsgrund (z.B. Zustimmung oder Vertrag) vorhanden ist.
- Recht auf Vergessen. Auf Wunsch eines Bürgers müssen Daten vom speichernden Unternehmen vollständig gelöscht werden.
- Recht auf Auskunft. Alle Bürgerinnen und Bürger haben Anspruch darauf vom speichernden unternehmen oder Verein zu erfahren, welche Daten über sie gespeichert werden. Im Normalfall muss die Auskunft gratis erfolgen, es gibt aber auch Ausnahmen.
- Recht auf Richtigstellung. „Fehlerhafte Daten“ müssen auf Wunsch richtig gestellt werden.
- „Datenportabilität“, bedeutet, dass Unternehmen, zum Beispiel soziale Netzwerke, aber auch Vereine, es erleichtern müssen, dass man von einem Anbieter zu einem anderen wechselt und seine Daten „mitnimmt“.

Rechte für Bürger bedeutet im Gegenzug Pflichten für Unternehmer und Vereine. Es kann auch sein, dass Abläufe geändert oder völlig neu organisiert werden müssen. Die Erfüllung der DSGVO ist daher primär eine organisatorische Angelegenheit und sicher nicht nur eine schnell erledigbare Pflichtübung.

Grundprinzipien

Die Behandlung von personenbezogenen Daten (Daten natürlicher Personen) ist mehreren Grundregeln unterworfen:

- Verarbeitung (=Speichern) ausschließlich mit konkretem Grund
- Sowenig Daten wie nötig (für den besagten Grund) speichern
- Daten so kurz wie möglich speichern – schon beim Speichern muss klar sein, wann die Daten gelöscht werden.

Bei Vereinen geht es primär um Mitgliederdaten. Wenn ein Verein nur Daten verarbeitet (=speichert), die für die Mitgliederverwaltung erforderlich sind (zum Beispiel Name, Anschrift, Kontaktdaten, Eintritts-/Austrittsdatum, Mitgliederklasse, Zahlungsdaten) braucht es dafür vom Mitglied keinerlei gesonderte Genehmigung. Wenn mehr Daten gehalten werden sollen, als für die Mitgliederverwaltung erforderlich, ist es sinnvoll, dafür Zustimmungen einzuholen.

Wesentlich ist, dass bei jedem Mitglied eine Information mitgeführt wird, wann der betreffende Datensatz gelöscht oder pseudonymisiert wird. Ewiges Speichern ist verboten!

Sinnvoll wäre etwa, einen Event zu setzen, dass die Daten nach Ende der Mitgliedschaft bzw. nach Erfüllung aller Forderungen (offener Mitgliedsbeträge) pseudonymisiert werden. Bei einer Datenschutzanfrage eines Mitgliedes, muss Löschungszeitpunkt oder Event mit beauskunftet werden.

Für Vereinsvorstände und Freiwillige (bei Projekten) wird es sinnvoll sein, separate Prozesse mit anderen Löschkriterien als bei den Mitgliedern zu definieren.

Es ist immer ein „Verzeichnis von Verarbeitungstätigkeiten“ zu führen. Dessen Vorlage kann ggf. von der Datenschutzbehörde verlangt werden. Hier ist zu verzeichnen in welchen Situationen wann warum welche Daten wie lange gespeichert werden. Nach der betreffenden Frist MÜSSEN Daten gelöscht oder pseudonymisiert werden.

Bürger haben das Recht auf vollständige Auskunft welche Daten über sie gespeichert sind; weiters auf Richtigstellung, auf Löschung sowie auf Datenportabiliät (Datenmitnahme beim Wechsel von Vertragsverhältnissen zu anderen Dienstleistern).

Sensible Daten

Achtung: Wenn ein Verein personenbezogener Daten, „aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung“ dann wird alles viel komplizierter.

Dass man derartige Daten besitzt, kann auch bei Vereinen viel leichter passieren als man vielleicht annimmt: Herkunft einer Person (Migrant?), Religionsbekenntnis, Sozialversicherungsnummer, Fingerabdrücke (Login!), Familienstand fallen alles schon in die Kategorie sensibler Daten.

Bei Vereinen die Angestellte haben – soll es geben – verarbeitet man natürlich jedenfalls Sozialversicherungsnummer und Krankenstandsinfos.

Dann braucht es eine Datenschutz-Folgenabschätzung, manchmal auch einen besonders ausgebildeten Datenschutzbeauftragten.

Fristen und Strafen

Alle Pflichten (Auskunft, Richtigstellung, Löschung, …) müssen jeweils nach vier Wochen kostenlos erfüllt werden. Bei Nichtbefolgung drohen Strafen (bis 20 Millionen Euro), die „wirksam, verhältnismäßig und abschreckend“ sein müssen.

Zum Autor

Sollten noch Fragen offen geblieben sein, stehe ich gerne per E-Mail für Ihre Fragen zur Verfügung.

Dipl.Ing. Dieter Zoubek,
Geprüfter Datenschutzexperte,
dieter.zoubek@gmx.at

Links

- DSGVO (Datenschutzbehörde)
  https://www.dsb.gv.at/datenschutz-grundverordnung
- Checkliste (WKO)
  https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Checkliste.html
- Online Ratgeber (WKO)
  https://dsgvo.wkoratgeber.at/
  DSVGO (Wikipedia)
  https://www.dsb.gv.at/datenschutz-grundverordnung