# Handlungsbedarf nach Revision

**David Vasella**
Rechtsanwalt, Zürich

Das revidierte Datenschutzgesetz tritt voraussichtlich Anfang 2023 in Kraft. Bis dann müssen auch Anwaltskanzleien ihren Umgang mit Personendaten anpassen. Ein Überblick über die wichtigsten Schritte.

Das Datenschutzrecht in der Schweiz ist seit längerer Zeit in Revision.[1] Das Parlament hat das revidierte Gesetz (revDSG) am 25. September 2020 verabschiedet. Ein Vorentwurf zur revidierten Verordnung zum DSG steht zurzeit in Vernehmlassung.[2] Es wird wohl zu erheblichen Anpassungen kommen – der Vorentwurf ist gründlich missglückt. Wer sich aus Anlass der Revision mit dem DSG befasst, droht von der Komplexität des Gebiets erschlagen zu werden, auch weil der Datenschutz stärker als andere Rechtsbereiche wertungsabhängig und international geprägt ist, letzteres besonders durch die Datenschutz-Grundverordnung (DSGVO).[3] Diese Verordnung der EU gilt im gesamten EWR. Sie verschärft den Datenschutz seit dem 25. Mai 2018 erheblich. Ihr Anwendungsbereich wird oft überschätzt, aber sie kann durchaus auf Bearbeitungen durch Unternehmen mit Sitz in der Schweiz anwendbar sein, besonders in folgenden Fällen:

- Das Unternehmen hat eine Tochter, Zweigniederlassung oder andere Niederlassung im EWR-Raum (Art. 3 Abs. 1 DSGVO),
- es bietet Leistungen aktiv und gezielt auch natürlichen Personen im EWR an (Art. 3 Abs. 2 lit. a DSGVO),
- es beobachtet das Verhalten von Personen, die sich im EWR aufhalten (Art. 3 Abs. 2 lit. b DSGVO); vor allem durch Online-Tracking.

Demgegenüber genügt es nicht, Daten von Kunden oder Mitarbeitern aus dem EWR zu bearbeiten (zu beachten ist aber Art. 139 IPRG). Die folgenden Ausführungen beschränken sich deshalb auf das schweizerische Datenschutzrecht.

## 1. Verteidigungslinien

Das private Datenschutzrecht ist im Kern eine Konkretisierung des allgemeinen Persönlichkeitsrechts. Leitgedanken sind die «Bearbeitungsgrundsätze» (Art. 4 ff. DSG; Art. 6 ff. revDSG), die noch direkt persönlichkeitsnah sind und die man vereinfacht wie folgt umschreiben könnte:

- Bearbeite Daten nicht heimlich.
- Sage den Betroffenen, wozu du Daten verwendest, und halte dich daran.
- Verwende nur so viele Daten wie nötig. Falls Betroffene selbst Einstellungen vornehmen können, richte sie so ein, dass ohne Zutun des Betroffenen möglichst wenig Daten verwendet werden.
- Plane die Datenbearbeitung rechtzeitig.
- Korrigiere falsche Daten, lösche nicht mehr nötige Daten.
- Sichere Daten gegen unbefugte Zugriffe innerhalb und ausserhalb deiner Organisation.
- Tue nichts, was du als Betroffener nicht akzeptieren würdest.

Diese Grundsätze sind Kern und Ziel des Datenschutzrechts. Sie sind aber höchst wertungsoffen. Ihre Verletzung bedeutet nicht die Rechtswidrigkeit der Bearbeitung – sie kann durch Einwilligung, das Gesetz oder überwiegende Interessen gerechtfertigt sein (Art. 13 DSG, Art. 31 revDSG). Auch ist die Prüfung ihrer Einhaltung durch Betroffene, Behörden und Gerichte schwierig. Die Bearbeitungsgrundsätze tragen den Datenschutz deshalb immer weniger. Gewissermassen als zweite Verteidigungslinie sieht das Gesetz darum flankierende Massnahmen vor. In der Umsetzung sind sie aufwendig. Zu ihnen gehören z.B. die Führung eines Bearbeitungsverzeichnisses, die Durchführung einer Datenschutzfolgenabschätzung oder die Meldung schwerwiegender Datensicherheitsverletzungen an den Edöb.

Die dritte Verteidigungslinie des Datenschutzes liegt bei den Betroffenen: Sie haben bestimmte Rechte, etwa das Recht, Einwilligungen nicht zu erteilen oder zu widerrufen, und das Recht auf Auskunft oder auf Berichtigung von Daten. Betroffenen wird dadurch grosse Eigenverantwortung auferlegt, die wahrzunehmen zunehmend illusorisch ist. Andere Konzepte werden diskutiert, bisher aber kaum mit praktischen Folgen. Im Gegenteil: DSGVO und das schweizerische Datenschutzrecht suchen den Datenschutz zu stärken, indem sie die Kontrollrechte stärken. Statt dem Lahmen Schuhe zu geben, wäre es besser, beim Missbrauch von Daten anzusetzen und die Ressourcen der Vollzugsbehörden zu erhöhen und im Gegenzug die illusorischen, missbrauchsanfälligen Kontrollrechte zu begrenzen.

## 2. Umsetzung

Die Umsetzung des revidierten DSG ist anspruchsvoll. Es hat sich bewährt, schrittweise vorzugehen:[4]

- **Bearbeitungen und Rollen** der Beteiligten klarstellen;

# des Datenschutzgesetzes

- **Verzeichnis** der Bearbeitungen ausarbeiten;
- **Verträge** mit Partnern und Dienstleistern prüfen;
- **Datenschutzerklärung** entwerfen;
- **IT-Sicherheit** prüfen.

### 2.1 Bearbeitungen, Rollen

Zunächst muss ein Unternehmen wissen, welche Personendaten es bearbeitet. Das ist nicht immer einfach, Unternehmen denken in Wertschöpfungs-, nicht Datenbearbeitungsketten. Ausgangspunkt ist eine Klärung etwa durch einen Workshop. Leitend können folgende Fragen sein:

- Agiert das Unternehmen in einer regulierten oder exponierten Branche?
- Gehört die Auswertung von Personendaten zum Geschäftsmodell (z.B. bei Dienstleistern, die im Auftrag des Kunden Daten auswerten, die mit Endkunden des Kunden in Berührung kommen, die im Massenkundenbereich tätig sind oder deren Dienstleistung auf Machine Learning beruht)? Oder werden vor allem Daten der Kontaktpersonen von Geschäftskunden bearbeitet, z.B. in der Industrie?
- Wie ist der Datenschutz dokumentiert? Gibt es Datenschutzerklärungen in Verträgen mit Kunden, Lieferanten und Partnern?
- Wie wird mit Bewerber- und Mitarbeiterdaten umgegangen?
- Werden Daten gelöscht?

Zu entscheiden ist weiter, in welchen Rollen die beteiligten Unternehmen tätig werden, als Verantwortliche oder Auftragsbearbeiter.[5] Ein «Verantwortlicher» (Art. 5 lit. j revDSG) ist vereinfacht gesagt das Unternehmen, das entscheidet, ob und welche Personendaten wie lange bearbeitet und mit wem sie geteilt werden. Ein «Auftragsbearbeiter» (Art. 5 lit. k revDSG) hingegen besorgt eine fremde Datenbearbeitung, ohne über diese Punkte im Einzelnen zu entscheiden. Die Abgrenzung ist folgenreich, aber schwierig, und nicht jeder Dienstleister ist ein Verantwortlicher.[6]

### 2.2 Verzeichnis

Das «Bearbeitungsverzeichnis» (Art. 12 revDSG) ist ein Inventar der Bearbeitungstätigkeiten des Verantwortlichen oder Auftragsbearbeiters (wobei diese Pflicht nicht gelten soll für Unternehmen mit weniger als 250 Angestellten, deren Bearbeitungen keine hohen Risiken mit sich bringen; Art. 12 Abs. 5 revDSG i.V.m. Art. 26 E-VDSG).[7] Gesetzlich ist nicht bestimmt, wie detailliert Bearbeitungstätigkeiten zu erfassen sind. Typische Beispiele wären Kundendatenverwaltung, Finanzbuchhaltung, Dokumentenmanagement, Newsletterversand, Bewerberdaten oder Lohnabrechnung. Mitarbeiterdaten wäre dagegen zu breit. Das Verzeichnis kann elektronisch geführt werden (z.B. als Excel-Dokument) und erfasst Angaben für jede Art der Bearbeitungstätigkeit. Vorlagen sind im Internet zu finden und bei spezialisierten Kanzleien erhältlich.

### 2.3 Verträge

Wer mit Auftragsbearbeitern arbeitet, muss sie vertraglich einbinden (vgl. Art. 9 revDSG). Der Beizug ohne ausreichenden Vertrag kann strafbar sein (Art. 61 lit. b revDSG).[8] Das revDSG gibt kaum Mindestinhalte vor, die eher umfangreichen Verträge nach Vorgaben der DSGVO haben sich aber auch in der Schweiz etabliert. Unternehmen sollten prüfen, wo Auftragsbearbeiter zum Einsatz kommen und ob entsprechende Vereinbarungen bestehen. Das gilt nicht nur für Dauerdienstleistungen (z.B. Hosting), sondern auch punktuelle Unterstützung (z.B. bei einer Datenmigration).

### 2.4 Datenschutzerklärung

Das heutige DSG verlangt eine ausdrückliche Information über Datenbearbeitungen nur, wenn die Bearbeitung unerwartet wäre oder besonders schützenswerte Personendaten oder Persönlichkeitsprofile betrifft (Art. 4 Abs. 4 und Art. 14 DSG). Das revDSG ist strenger: Der Verantwortliche muss über jede Datenbeschaffung informieren, auch wenn sie auf der Hand liegt (Art. 19 revDSG). Diese Pflicht führt zu einer Fülle von Datenschutzerklärungen (DSE), die kaum gelesen werden, aber hohen Aufwand verursachen. Zu informieren ist insbesondere über die in Art. 19 Abs. 2 revDSG genannten Punkte. Das Gesetz lässt offen, wie detailliert diese Information sein muss. Weil eine Verletzung der Informationspflicht strafbar sein kann (Art. 60 Abs. 1 revDSG), werden DSE immer umfangreicher. Unternehmen sollten deshalb DSE entwerfen, z.B. eine allgemeine DSE für Kunden und Geschäftspartner, je eine für Bewerber und Mitarbeiter und Cookie-Hinweise für Websites und Apps. Die Arbeit an diesen DSE erfolgt oft parallel zur Erstellung von Bearbeitungsverzeichnissen, kann aber auch vorher oder nachher geschehen. Eine weitere

1 Eine Übersicht über den Stand der Revision auf kantonaler Ebene findet sich bei Dominika Blonski, «Entwicklungen im Datenschutzrecht», in: SJZ 2021, S. 918 ff.

2 Vgl. www.datenrecht.ch/vdsg-vernehmlassung-eroeffnet; der Text der E-VDSG findet sich z.B. unter www.datenrecht.ch/e-vdsg.

3 Verordnung (EU) 2016/679 vom 27.4.2016. Eine elektronische Fassung mit den in der Praxis wichtigen Erwägungsgründen findet sich unter www.datenrecht.ch/dsgvo-verordnung-2016-679 (alle Links am 29.8.2021 besucht).

4 Ein Umsetzungsleitfaden kann beim Autor des vorliegenden Beitrags bezogen werden.

5 Vgl. David Vasella, «Auftragsbearbeitung im Privatbereich», in: Digma 3/2019, S. 110 ff.

6 Illustrativ sind die Ausführungen des Bayrischen Landesamts für Datenschutz, abrufbar unter www.lda.bayern.de/media/veroeffentlichungen/FAQ_Abgrenzung_Auftragsverarbeitung.pdf AbgrenzungAuftragsverarbeitung.pdf.

7 Der E-VDSG will nun zusätzlich zu den Bearbeitungsverzeichnissen bei bestimmten riskanten Bearbeitungen auch noch ein Bearbeitungsreglement vorschreiben (Art. 4). Eine gesetzliche Grundlage für eine solche Pflicht fehlt aber.

8 Eine gesetzgeberische Fehlleistung, denn ein vertragsloser Auftragsbearbeiter ist ein Verantwortlicher, was einer Bekanntgabe durch den Auftraggeber entgegenstehen kann, für sich genommen aber nicht strafwürdig ist.

Frage ist, wo und wie die DSE zur Verfügung gestellt werden. Es dürfte ausreichend sein, wenn der Verantwortliche bspw. in den AGB oder einer Offerte auf die DSE im Internet verweist. In vielen Fällen sollte es genügen, die DSE überhaupt nur im Internet zur Verfügung zu stellen.

### 2.5 Weitere Aufgaben

Der Verantwortliche muss ein Bewusstsein haben, welche Risiken sich aus seiner Bearbeitung für Betroffene ergeben können, und gegebenenfalls erforderliche Massnahmen treffen. Bringt eine Bearbeitung voraussichtlich «hohe Risiken» mit sich, verlangt das revDSG eine Datenschutz-Folgenabschätzung (DSFA, Art. 22 revDSG). Das betrifft etwa die Bearbeitung besonders schützenswerter Personendaten (Art. 5 lit. c revDSG)[9] in grösserem Umfang (Art. 22 Abs. 2 lit. a revDSG) oder ein «Profiling mit hohem Risiko» (Art. 5 lit. g revDSG).[10] Ergibt eine DSFA, dass die Risiken trotz Abhilfemassnahmen hoch sind, muss der Edöb informiert werden (Art. 23 revDSG). Letzteres kann der Verantwortliche abwenden, indem er einen Datenschutzberater bestellt (Art. 10 revDSG).

Eine weitere Neuerung betrifft Verletzungen der Datensicherheit. Anders als heute müssen sie dem Edöb gemeldet werden, wenn sie voraussichtlich zu hohen Risiken führen (Art. 24 Abs. 1 revDSG). Unter Umständen müssen auch betroffene Personen informiert werden. Auftragsbearbeiter müssen ihrerseits den Verantwortlichen informieren. Diese Meldepflichten können einen definierten internen Prozess verlangen.

### 2.6 Betroffenenrechte

Das Datenschutzrecht will dem Betroffenen Kontrolle über die Bearbeitung «seiner» Personendaten ermöglichen. Betroffene können vom Verantwortlichen bspw. jederzeit Auskunft verlangen, ob und welche Daten er bearbeitet, zusammen mit einer Kopie der Daten (Art. 8 DSG; Art. 25 Abs. 2 revDSG). Wer vorsätzlich eine falsche oder unvollständige Auskunft gibt, macht sich strafbar (Art. 60 Abs. 1 lit. a revDSG). Wie heute haben Betroffene das Recht, unrichtige Personendaten berichtigen zu lassen (Art. 6 Abs. 5 und 32 revDSG) und der Bearbeitung zu widersprechen (Art. 30 Abs. 2 lit. b revDSG). Dann ist die weitere Bearbeitung nur zulässig, soweit sich der Verantwortliche auf einen Rechtfertigungsgrund berufen kann (Art. 31 Abs. 1 revDSG). Neu ist das Recht auf «Datenportabilität» (Art. 28 revDSG). Betroffene können die Herausgabe bestimmter Daten in gängigen elektronischen Formaten verlangen.[11]

Bei Verantwortlichen mit vielen Begehren drängt es sich auf, Prozesse und Musterkorrespondenz vorzusehen. Das ist aber keine Rechtspflicht.

### 2.7 Ausland

Personendaten dürfen nur ins Ausland gelangen, wenn der Empfängerstaat ein angemessenes Schutzniveau hat (Art. 6 Abs. 1 DSG; Art. 16 Abs. 1 revDSG). Fehlt ein solcher Schutz (wie z.B. in den USA, in China oder in Indien), muss der Exporteur i.d.R. Ersatzmassnahmen treffen, z.B. mit dem Exporteur einen entsprechenden Vertrag schliessen (Art. 6 Abs. 2 lit. a DSG; Art. 16 Abs. 2 lit. d revDSG). Dazu werden meist Standarddatenschutzklauseln der EU verwendet, die für die Schweiz akzeptiert sind. Eine Schweizer Firma, die zum Beispiel einem US-amerikanischen Software-as-a-Service-Anbieter Daten anvertraut, muss sicherstellen, dass er in seinen AGB auf die Standardvertragsklauseln verweist.

Exporteure müssen zudem vor jeder Übermittlung prüfen, ob das lokale ausländische Recht den Behörden überschiessende Zugriffsrechte gewährt, denn dann bewirken die Standardvertragsklauseln keinen angemessenen Schutz.[12] Ausser in grösseren Unternehmen haben sich solche Prüfungen bisher nicht durchgesetzt. Künftig werden wohl standardisierte Risikoeinschätzungen für einzelne Länder öffentlich verfügbar sein.

## 3. Risiken

Das Datenschutzrecht verlässt sich nicht auf Grundsätze und flankierende Massnahmen. Auch die Durchsetzung wird verbessert. Bspw. erhält der Edöb die Kompetenz, verbindliche Verfügungen zu erlassen (Art. 51 revDSG). Die Strafbarkeitsrisiken steigen an. Bussen stellen heute eine Ausnahme dar. Neu werden bei Verstössen viel höhere Bussen angedroht, sofern sie mit Vorsatz erfolgen und der Betroffene Strafantrag stellt (Art. 60 ff. revDSG). Bspw. drohen bis zu 250 000 Franken Busse, wenn jemand vorsätzlich Datensicherheitsmassnahmen unterlässt, die Informationspflicht verletzt, eine unvollständige oder unrichtige Auskunft erteilt, Personendaten unbefugterweise an Empfänger im Ausland übermittelt, einen Auftragsbearbeiter einsetzt, ohne ihn korrekt einzubinden, oder geheime, aufgrund des Berufs anvertraute Personendaten unbefugt an Dritte bekanntgibt. Die Busse trifft primär die für die Verletzung verantwortlichen Personen – wer die bussenbedrohte Handlung veranlasst und die Verletzung will oder in Kauf nimmt, ist daher im Risiko, auch wenn er nicht zur Geschäftsleitung zählt.[13]

Neben Rechts- steigen auch Reputationsrisiken. Umso wichtiger wird es, die Bearbeitungsgrundsätze einzuhalten, Bearbeitungen besser zu erklären und zu unterlassen, was zwar erlaubt ist, aber ein ungutes Gefühl hinterlässt.

9 Bspw. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Gesundheitsdaten, Daten über die Intimsphäre oder die Zugehörigkeit zu einer bestimmten Rasse oder Ethnie oder Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen oder über Sozialhilfemassnahmen.

10 Dazu www.datenrecht.ch/ueberlegungen-zum-profiling-mit-hohem-risiko.

11 Dazu Lena Götzinger / David Vasella, «Datenportabilität und ihre Umsetzung», in: SZW 1/2021, S. 40 ff.

12 Der Edöb hat sich hierzu geäussert, vgl. www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html#-2053327153.

13 Vgl. David Rosenthal / Seraina Gubler, «Die Strafbestimmungen des neuen DSG», in: SZW 1/2021, S. 52 ff.