Reinhard Zweidler

Das neue Datenschutzrecht nDSG in unserer Praxis

Hintergrund

Protection des données et évaluation

Quand 28/05/2024

GREVAL
Groupe romand d'Evaluation

Grundlagen

Art. 13 BV Schutz der Privatsphäre

[1] Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.
[2] Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

Etwas Geschichte

Das erste Bundesgesetz über den Datenschutz stammt aus dem Jahr 1992 Erst 1995 begann in der Schweiz eine signifikante Ausbreitung des Internets. Das erste Smartphone iPhone von Apple) wurde 2007 auf den Markt gebracht. Ab 2014 gab es erste Versuche mit Cloud-Diensten und Machine Learning in der Schweiz. Das Recht musste an diese **technologischen und gesellschaftlichen Veränderungen angepasst** werden.

Die **Kompatibilität des Schweizer Rechts mit dem EU-Recht**, insbesondere mit der Datenschutzgrundverordnung (DSGVO), ist das zweite grosse Anliegen des neuen Gesetzes. Das revDSG soll bewirken, dass der freie Datenverkehr mit der Europäischen Union erhalten werden kann, sodass die Schweizer Unternehmen nicht an Wettbewerbsfähigkeit einbüssen.

Das totalrevidierte Datenschutzgesetz (DSG) und die Ausführungsbestimmungen in der neuen Datenschutzverordnung (DSV) und der neuen Verordnung über Datenschutzzertifizierungen (VDSZ**) traten am 1. September 2023 in Kraft.**

Die Gleichwertigkeit zur DSGVO wurde durch das Übereinkommen 108+ gemäss Beschluss der EU-Kommission vom 15. Januar 2024 festgestellt.

Geltung des nDSG

Art. 2 Persönlicher und sachlicher Geltungsbereich

[1] Dieses Gesetz gilt für die Bearbeitung von Personendaten natürlicher Personen durch:

a. private Personen;

b. Bundesorgane.

[2] Es ist nicht anwendbar auf:

a. Personendaten, die von einer natürlichen Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden;

b. Personendaten, die von den eidgenössischen Räten und den parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden;

c. Personendaten, die bearbeitet werden durch institutionelle Begünstigte nach Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007[3], die in der Schweiz Immunität von der Gerichtsbarkeit geniessen.

Organe kantonalen Rechts unterstehen den 26 verschiedenen kantonalen Datenschutzgesetzen

Praxistipp: Immer anwendbares Recht bestimmen und In Zweifelsfällen den EDÖB oder den kantonalen Datenschutzbeauftragten konsultieren

Geltung des nDSG

Art. 2 Persönlicher und sachlicher Geltungsbereich

[1] Dieses Gesetz gilt für die Bearbeitung von Personendaten natürlicher Personen durch:

a. private Personen;

b. Bundesorgane.

[2] Es ist nicht anwendbar auf:

a. Personendaten, die von einer natürlichen Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden;

b. Personendaten, die von den eidgenössischen Räten und den parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden;

c. Personendaten, die bearbeitet werden durch institutionelle Begünstigte nach Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007[3], die in der Schweiz Immunität von der Gerichtsbarkeit geniessen.

Achtung:

Grundsätzlich findet die DSGVO der EU Anwendung:

- beim Angebot von Waren oder Dienstleistungen aus der Schweiz in der EU direkt Anwen-dung unabhängig davon, ob die Verarbeitung in der EU stattfindet
- bei Verarbeitung von Daten von EU-Niederlassungen oder EU-Bürgern
- Bei Beobachtung des Verhaltens von Personen in der EU

Organe kantonalen Rechts unterstehen den 26 verschiedenen kantonalen Datenschutzgesetzen

Praxistipp: Immer anwendbares Recht bestimmen und In Zweifelsfällen den EDÖB oder den kantonalen Datenschutzbeauftragten konsultieren

Das ist neu

1) Daten natürlicher Personen sind geschützt, jene juristischer Personen nicht mehr

- Die juristischen Personen (AG, GmbH etc.) können sich für ihren Schutz nicht mehr auf das DSG berufen. Ihnen verbleibt der Schutz durch das Firmenrecht sowie weitere bestehende Bestimmungen der Rechtsordnung (z. B. Persönlichkeitsschutz nach ZGB, UWG oder der Schutz nach Markenrecht).

Praxistipp: Die Klagen, die den juristischen Personen für die Verletzung ihrer Rechte zur Verfügung stehen, können für beide Seiten sehr kostspielig werden

Das ist neu

2) **Genetische und biometrische Daten** sind neu ebenfalls besonders schützenswert. Folgenabschätzungen müssen durchgeführt werden, sofern ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht.

3) **Auskunftsrecht und Informationspflicht**: Bei jeder Beschaffung von Personendaten muss die betroffene Person vorgängig informiert werden. jede Person vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Sie kann – wenn nötig – auch veranlassen, dass die Daten gelöscht oder berichtigt werden.

4) Ein **Verzeichnis der Bearbeitungstätigkeiten** ist obligatorisch ausser für KMU, deren Datenbearbeitung nur ein geringes Risiko von Verletzungen der Persönlichkeit von betroffenen Personen mit sich bringt.

.

Das ist neu

5) **Rasche Meldung ist erforderlich, wenn die Datensicherheit verletzt wurde**. Sie ist an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu richten

6) **Privacy by Design** ist Datenschutz durch Technikgestaltung) für die Entwickler, den Schutz und den Respekt der Privatsphäre der Nutzerinnen und Nutzer in die Struktur der Produkte oder Dienstleistungen einzubauen, welche personenbezogene Daten sammeln werden.

7) **Privacy by Default:** Datenschutz durch Voreinstellung soll als Grundsatz sicherstellen, dass schon beim Inverkehrbringen des Produktes oder der Dienstleistung die höchste Sicherheitsstufe vorhanden ist, indem standardmässig, also ohne Eingreifen der Nutzer, alle nötigen Massnahmen für den Datenschutz und die Einschränkung der Datennutzung aktiviert sind. Sämtliche Software, Hardware sowie die Dienstleistungen so konfiguriert sein, dass die Daten geschützt sind

Geschützte Personendaten

Art. 5 Begriffe **nach nDSG**

In diesem Gesetz bedeuten:

a. *Personendaten:* alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen;

b. *betroffene Person:* natürliche Person, über die Personendaten bearbeitet werden;

Praxistipp:

Definition und Praxis dazu, was geschützte Personendaten sind, können je nach Kanton variieren,

Je nach Kontext können Adresse, Zivilstand, Beruf etc. geschützte Personendaten sein.
Um geschützte Personendaten kann es sich auch dann handeln, wenn jemand in einem Gutachten als Auskunftsperson befragt wird. Entscheidend ist der Kontext und der Schutzgrad des anwendbaren Rechts

Besonders schützenswerte Personendaten

1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,
3. genetische Daten,
4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,
5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
6. Daten über Massnahmen der sozialen Hilfe;

Informationspflicht

Der Verantwortliche ist verpflichtet, die betroffene Person über die Beschaffung ihrer Personendaten zu informieren. Diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden.

Bei jeder geplanten Datenbeschaffung oder -bearbeitung muss der Verantwortliche die betroffene Person im Vorfeld angemessen informieren. Diese Informationspflicht gilt auch, wenn die Daten nicht direkt bei der betroffenen Person beschafft werden.

Der Verantwortliche muss den betroffenen Personen die Informationen über die Beschaffung und Bearbeitung von Personendaten in knapper, transparenter, verständlicher und einfach zugänglicher Form mitteilen.

Mitgeteilt werden müssen Identität und die Kontaktdaten des Verantwortlichen, der Bearbeitungszweck und gegebenenfalls die Empfängerinnen und Empfänger, denen Personendaten bekanntgegeben werden (z. B. Auftragsbearbeiter). Wie detailliert die Informationen sein müssen, hängt von der Art der bearbeiteten Personendaten sowie von der Art und dem Umfang der Bearbeitung ab.

Die Datenschutz-Folgeabschätzung

Private und behördliche verantwortliche Datenbearbeiter müssen eine Datenschutz-Folgenabschätzung (DSFA) erstellen, wenn bei Personendatenbearbeitungen ein potenziell hohes Risiko für die Persönlichkeit oder die Grundrechte der Betroffenen erkennbar ist.

Die DSFA umschreibt die geplante Datenbearbeitung, bewertet die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen und zeigt die Massnahmen zu deren Schutz auf. Im Falle einer bereits bestehenden Datenbearbeitung prüft und weist der Verantwortliche deren wesentliche Unterschiede zur geplanten Datenbearbeitung in der DSFA aus.

Ein hohes Risiko kann sich aus der Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung ergeben. Das Gesetz nennt beispielsweise die umfangreiche Bearbeitung besonders schützenswerter Personendaten und die systematische, umfangreiche Überwachung öffentlicher Bereiche.

Resultiert aus der DSFA, dass ein hohes Restrisiko für die Persönlichkeit oder die Grundrechte der Betroffenen bestehen bleibt, so muss eine Stellungnahme des EDÖB eingeholt werden.

Strafbestimmungen

Art. 60 Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten

[1] Mit Busse bis zu 250 000 Franken werden private Personen auf Antrag bestraft:

a. die ihre Pflichten nach den Artikeln 19, 21 und 25–27 verletzen, indem sie vorsätzlich eine falsche oder unvollständige Auskunft erteilen;

b. die es vorsätzlich unterlassen:

1. die betroffene Person nach den Artikeln 19 Absatz 1 und 21 Absatz 1 zu informieren, oder

2. ihr die Angaben nach Artikel 19 Absatz 2 zu liefern.

[2] Mit Busse bis zu 250 000 Franken werden private Personen bestraft, die unter Verstoss gegen Artikel 49 Absatz 3 dem EDÖB im Rahmen einer Untersuchung vorsätzlich falsche Auskünfte erteilen oder vorsätzlich die Mitwirkung verweigern.

Strafen in der EU bei Anwendung der DSGVO sind höher

GDPR Enforcement Tracker

tracked by CMS law·tax·future

The CMS.Law GDPR Enforcement Tracker is an overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete, which is why we appreciate any indication of further GDPR fines and penalties. *Please note that we do not list any fines imposed under national / non-European laws (with the exception of fines under the UK GDPR), under non-data protection laws (e.g. competition laws / electronic communication laws) and under "old" pre-GDPR-laws. We have, however, included a limited number of essential ePrivacy fines under national member state laws.*

New features: "ETid" and "Direct URL"!
We have assigned a unique and permanent ID to each fine in our database, which makes it possible to precisely address fines, e.g. in publications. Once an "ETid" has been assigned to a fine, it remains the same, even if the fine is overturned or amended by courts at a later date, or if we add fines that were issued chronologically before. The "Direct URL" (click "+" or on a specific ETid to view details of a fine) can be used to share fines online, e.g. on Twitter or other media.

Show 100 entries Search: audit

ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
ETid-1009	IRELAND	2021-12-09	110,000	Limerick City and County Council	Art. 13 GDPR, Art. 12 GPDR, Art. 15 GDPR	Insufficient fulfilment of data subjects rights	link link
ETid-829	ITALY	2021-07-22	400,000	Atac s.p.a.	Art. 5 GDPR, Art. 6 GDPR, Art. 30 GDPR, Art. 32 GDPR	Non-compliance with general data processing principles	link link
ETid-827	ITALY	2021-07-22	800,000	Roma Capitale	Art. 5 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 25 GDPR, Art. 28 GDPR, Art. 32 GDPR	Non-compliance with general data processing principles	link link
ETid-826	ITALY	2021-07-22	200,000	Regione Lombardia	Art. 5 (1) a), c) GDPR, Art. 6 (1) c), e) GDPR, Art. 6 (2) GDPR, Art. 6 (3) b) GDPR	Non-compliance with general data processing principles	link link
ETid-791	GERMANY	2020	65,000	Company	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link link
ETid-569	HUNGARY	2020-12-10	22,200	Budapesti Műszaki és Gazdaságtudományi Egyetem (Budapest University of Technology and Economics)	Art. 5 (1) a), b), c) GDPR, Art. 6 (1) GDPR, Art. 9 (2) GDPR, Art. 12 GDPR, Art. 13 GDPR	Insufficient legal basis for data processing	link
ETid-381	POLAND	2020-07-15	22,300	Office for geodesy and cartography	Art. 31 GDPR, Art. 58 GDPR	Insufficient cooperation with supervisory authority	link
ETid-272	BELGIUM	2020-04-28	50,000	Proximus SA	Art. 31 GDPR, Art. 58 GDPR, Art. 37 GDPR	Insufficient involvement of data protection officer	link
ETid-51	FRANCE	2019-06-13	20,000	Employer UNIONTRAD COMPANY	Art. 5 (1) c) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 32 GDPR	Insufficient legal basis for data processing	link

Höchste Busse in der EU bis jetzt:

Stadtverwaltung Rom
€ 800’000

wg. Nichteinhalten grundlegender Datenverarbeitungsprinzipien

Das nDSG in der Praxis

Worauf muss ich als Projektleiterin/Projektleiter achten?

Fallen in meinem Projekt überhaupt Personendaten an?

Du kannst in Deinem Projekt it Personendatensammlungen zu tun haben, wenn Du zum Beispiel

- Umfragen durchführst
- Stellungnahmen auswertest
- Anträge verwaltest
- Newsletter betreibst
- Zugriffe auf eine Projekt-Website auswertest

Also immer dann, wenn personenbezogene Daten verarbeitet werden. «Verarbeitet» beginnt im Sinne der DSGVO bereits mit der Speicherung. Und auch physische strukturierte Ablagen gelten als «Verarbeitung». In diesen Fällen musst Du die folgenden Themen beachten.

Zustimmung der Betroffenen einholen

Vor dem Erfassen der Daten müssen die betroffenen Personen ihre Einwilligung geben, und sie müssen über den Zweck der Erhebung, die Rechtsgrundlage, ihre Rechte und die Kontaktmöglichkeiten informiert werden.

Im Verarbeitungsverzeichnis erfassen lassen

Erstelle ein Verarbeitungsverzeichnis ausser die Datenbearbeitung bringt nur ein geringes Risiko von Verletzungen der Persönlichkeit von betroffenen Personen mit sich.

Das nDSG in der Praxis

Bei hohen Risiken weitere Massnahmen treffen
Wenn die Bearbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat, dann musst Du vorgängig eine «Datenschutz-Folgeabschätzung» vornehmen. Das ist etwa dann der Fall, wenn Du in Deinem Projekt neue Technologien verwendest oder mit besonders heiklen Personendaten zu tun hast, weil Du beispielsweise eine Erhebung im Gesundheitswesen durchführst oder Interviews zu politischen Einschätzungen führst.
In diesem Fall musst du eine Risikobewertung vornehmen und geeignete Massnahmen treffen, um den Schutz der personenbezogenen Daten sicherzustellen.

Sofort melden, wenn etwas schiefgelaufen ist
Wenn es zu einer Panne bei personenbezogenen Daten kommt, musst Du uns das sofort melden (datenschutz@ebp.ch), damit wir unverzüglich die Aufsichtsbehörden informieren können («möglichst binnen 72 Stunden»). In schweren Fällen müssen auch die betroffenen Personen informiert werden.
Beispiele für solche Datenpannen sind:

- Diebstahl der Login-Daten in einem Online-Shop, in einer Kollaborations-Plattform oder ähnlich
- Sammlung von Personendaten wird an falschen Empfängerkreis versendet
- Verlust eines Datenträgers, der eine Sammlung von Personendaten enthält

Und:

In allen Berichten, denen Personendaten zugrundeliegen, wenigstens im Anhang detailliert ausführen: Protection by default, Protetion by device, Zustimmunbgserklärungen und Löschunge der Daten ,

ZUSAMMENFASSUNG: Was muss ich tun?

1. Klären: Erhebe oder verarbeite ich Personendaten? Sind diese allenfalls besonders geschützt?
2. Klären: Welches Datenschutzrecht kommt zur Anwendung?
3. Klären: Besteht für diese Datenerhebung und -verarbeitung eine gesetzliche Grundlage?
   - *Wenn ja:* Betroffene Personen informieren (Datenschutzerklärung abgeben, auch wenn die Daten bei Dritten beschafft werden)
   - *Wenn nicht:* Zustimmung einholen (sicherheitshalber schriftlich unterzeichnet)
4. Datenverarbeitung im Verzeichnis eintragen
5. Bei hohen Risiken => Datenschutzfolgeabschätzung
6. Daten vor Zugriff Dritter sichern (auch innerhalb des Büros oder der Verwaltungseinheit)
7. Personendaten baldmöglichst anonymisieren oder pseudonymisieren
8. Pannen inkl. Cyberangriffe sofort melden (an zuständigen Datenschutzbeauftragten innert 72 h)
9. Personendaten gehen nie als Rohdaten an den Auftraggeber
10. Daten löschen, sobald sie nicht mehr gebraucht werden (Achtung: Aufbewahrungspflicht in der Regel 10 Jahre)
11. In den Evaluationsberichten: Erklärung, wie mit Personendaten umgegangen wurde.

Fragen? Diskussion

Wer weiss jetzt, was wann und für wen gilt?