

• EDITORIAL



**Liebe Leserin, liebe Unternehmerin
Lieber Leser, lieber Unternehmer**

Das revidierte Datenschutzgesetz (DSG) der Schweiz, das ab dem 1. September 2023 in Kraft getreten ist, enthält strengere Strafbestimmungen für Verletzungen des Datenschutzes. Der Titelbeitrag hebt die finanziellen Konsequenzen bei Nichteinhaltung hervor.

Die Bereitschaft zur kontinuierlichen Transformation ist entscheidend, um im Wettbewerb zu bestehen. Organisationsentwicklung ist der Schlüssel zur Steigerung der Agilität, der Treiber von Innovation und einer konstruktiven Zusammenarbeit. Mehr dazu im zweiten Beitrag.

Das Schweizer Parlament plant, organisierten Insolvenzbetrug und gezielte Unternehmenszerstörung mit Gesetzesänderungen zu bekämpfen. Jedoch bleibt die Frage, ob diese Massnahmen ausreichen werden, wie der dritte Beitrag zeigt.

Der vierte Beitrag behandelt die Kapitalbeschaffung für Unternehmen und unterscheidet verschiedene Finanzierungsmethoden sowie deren Vor- und Nachteile. Ausserdem finden Sie praktische Empfehlungen für Kreditverhandlungen.

Ich hoffe, die Lektüre hilft Ihnen für Ihren Arbeitsalltag.

C. Seffinga

Carla Seffinga,
WEKA Productmanagement
Finanzen und Steuern

STRAFRECHTLICHE FOLGEN BEI NICHTEINHALTUNG DES DATENSCHUTZGESETZES

Ab dem 1. September 2023 gilt in der Schweiz das revidierte Datenschutzgesetz (DSG). Um die Wirkung des DSG zu verstärken, enthält es mehrere Strafbestimmungen für verschiedene Verletzungen des DSG. Im Gegensatz zum alten Recht sind die neuen Sanktionen im neu geltenden DSG erheblich verschärft worden. Die strafbaren Tatbestände sind in Art. 60–63 DSG festgehalten. Im anschliessenden Beitrag werden die vier strafbaren Tatbestände konkreter abgehandelt, sowie welche finanziellen Konsequenzen die Nichteinhaltung des DSG für Private und Unternehmen zur Folge hat.

• Von Lukas Lezzi

Die strafbaren Tatbestände

Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten

Art. 60 DSG bestraft die Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten. Bei der Informations- und Auskunftspflicht geht es primär um die direkten oder indirekten Beziehungen zwischen dem Verantwortlichen und den von der Datenbearbeitung betroffenen Personen.

Bei der Informationspflicht werden zwei Arten von Pflichten unterschieden, nämlich die Informationspflicht bei der Beschaffung von Daten nach Art. 19 DSG (i) sowie die Informationspflicht bei einer automatisierten Einzelfallentscheidung laut Art. 21 DSG (ii). Beide Informationspflichten zielen darauf ab, dass die betroffene Person verstehen kann, wie ihre Daten verwendet werden, um auf dieser Grundlage Entscheidungen zu treffen. Eine strafbare Handlung wird regelmässig dann anzunehmen sein, wenn man im Wissen um diese Pflichten gewisse Informationen unterschlägt oder die betroffenen Personen überhaupt nicht informiert. In aller Regel

genügt die Bereitstellung der gesetzlich geforderten Informationen auf der Webseite des Verantwortlichen, um hier ein strafbares Verhalten auszuschliessen.

Wiederum betrifft die Auskunftspflicht gemäss Art. 25 und 27 DSG die laufenden Datenverarbeitungen und ermöglicht es der betroffenen Person, über die Verarbeitung ihrer personenbezogenen Daten auf dem Laufenden zu bleiben. Bei Bedarf kann sie ihre Rechte geltend machen, um möglicherweise falsche Daten korrigieren zu lassen oder unberechtigte Datenverarbeitung zu unterbinden. Diese oben genannten Bestimmungen spielen eine wichtige Rolle im Datenschutz, da das Verständnis für die Datenerhebung und -verarbeitung die Grundlage für alle weiteren Massnahmen bildet. Somit zieht die Missachtung dieser Bestimmungen strafrechtliche Konsequenzen nach sich. Interessanterweise ist eine Verletzung von weiteren Betroffenenrechten wie etwa das Lösungsrecht oder das Recht auf Datenportabilität nicht strafbewehrt. Bei der Auskunftspflicht liegt auch nur eine strafbare Handlung vor,

wenn diese überhaupt nicht oder vor-
sätzlich falsch wahrgenommen wird.
Eine zu späte Auskunftserteilung (also
über 30 Tage ohne Kontaktaufnahme)
führt nicht zu einer Strafbarkeit.

Verstösse gegen die Mitwirkungspflicht
werden ebenfalls gemäss Art. 60 DSGVO
strafrechtlich verfolgt. Die Mitwirkungs-
pflicht bezieht sich auf Untersuchun-
gen des Eidgenössischen Datenschutz-
und Öffentlichkeitsbeauftragten (EDÖB),
wenn der Verdacht besteht, dass eine
Datenverarbeitung gegen das DSGVO ver-
stösst (gemäss Art. 49 ff. DSGVO). Grund-
sätzlich sind alle Personen zur Mitwir-
kung verpflichtet. Berufsgeheimnisse
oder Zeugnisverweigerungsrechte, wie
etwa das Recht, sich selbst nicht belas-
ten zu müssen, können dem aber ent-
gegenstehen. Eine strafbare Handlung
liegt dementsprechend nur dann vor,
wenn man Unterlagen nicht herausgibt
oder Auskünfte verweigert, ohne dass
man sich auf einen der vorgenannten
Gründe berufen kann.

Verletzung von Sorgfaltspflichten

Art. 61 DSGVO statuiert eine Strafbarkeit
für die Verletzung einiger, ausgewählter
Pflichten des DSGVO:

- Für den Transfer von Personendaten
in einen Staat ohne angemessenen
Datenschutz gemäss Anhang 1 Da-
tenschutzverordnung (DSV), ohne
dass Massnahmen gemäss Art. 16
Abs. 2 DSGVO getroffen wurden oder
ohne dass eine Ausnahme gemäss
Art. 17 DSGVO vorliegt.
- Für Übertragung der Datenbearbei-
tung an einen Auftragsbearbeiter im
Sinne von Art. 9 DSGVO ohne die Ver-
einbarung, die Daten nur so zu bear-
beiten, wie der Verantwortliche das
darf, oder wenn die Daten aufgrund
einer Geheimhaltungsvorschrift nicht
hätten an einen Auftragsbearbeiter
übertragen werden sollen. Zudem ist
es strafbar, wenn der Verantwortliche
die Einhaltung der Datensicherheit
durch den Auftragsbearbeiter nicht



überprüfen kann. Die Überprüfung
kann regelmässig durch ein Audit-
Recht oder die Zurverfügungstellung
von Audit-Berichten (z. B. ISAE-Ber-
richt) erfüllt werden.

- Für die Nichteinhaltung der Mindest-
vorschriften der Datensicherheit ge-
mäss Art. 8 Abs. 3 DSGVO i. V. m. Art. 3
DSV: Dieser Tatbestand ist allerdings
in der Praxis wohl sehr schwierig
nachzuweisen, weil Art. 1 DSV aus-
drücklich sagt, dass auch die Daten-
sicherheitsmassnahmen abhängig
vom Risiko der entsprechenden Da-
tenbearbeitung ausgestaltet werden
müssen und auch Kostenüberlegun-
gen in diese Abwägung miteinfließen
dürfen. Eine strafrechtliche Relevanz
dürfen somit wohl nur Fälle haben
die keinerlei Datensicherheitsmass-
nahmen im Bereich Vertraulichkeit,
Verfügbarkeit und Datenintegrität ge-
troffen haben.

Berufliche Schweigepflicht

Das «kleine» Berufsgeheimnis des DSGVO
schützt geheime Personendaten vor
ungerechtfertigter Offenlegung. Damit
eine strafbare Handlung vorliegen kann,
müssen die Personendaten nicht öf-
fentlich bekannt sein, und es muss ein
schutzwürdiges Interesse an ihrer Ge-
heimhaltung bestehen.

Die berufliche Schweigepflicht im Sinne
von Art. 62 DSGVO hat die gleiche Funktion
wie das Berufsgeheimnis nach Art. 321
des Strafgesetzbuchs (StGB), ist aber
weniger weitgreifend. Zum Beispiel
sehen die Prozessordnungen häufig
Befreiungen von der Zeugnispflicht für
Personen vor, die dem Berufsgeheim-
nis unterliegen; diese Befreiungen gel-
ten grundsätzlich nicht für Personen,
die der Schweigepflicht nach dem DSGVO
unterliegen. Der Kreis der Personen,
die der Schweigepflicht unterliegen, ist
dafür viel weiter als jener nach Art. 321
StGB. Jede Person, die folgenden Tat-
bestand erfüllt, unterliegt potenziell der
Schweigepflicht: Es handelt sich um
eine Person, die bei der Ausübung ih-
res Berufs, der die Kenntnis von Daten
erfordert, Kenntnis von ebensolchen
erlangt hat. Hier fallen insbesondere
Personen in Betracht, welche anderen
Berufsgeheimnissen des StGB oder des
Nebenstrafrechts unterstehen, solche,
die diesem Geheimnis aber nicht un-
terstehen, wie beispielsweise Personal
in HR-Abteilungen. Ansonsten sind die
Begriffe «Geheimnis» und «Offenba-
ren» im gleichen Sinne wie in Art. 321
StGB auszulegen. Auch der Begriff der
Hilfspersonen, die der Schweigepflicht
unterliegen (Art. 62 Abs. 2 DSGVO),
ist ähnlich wie in Art. 321 StGB. Die
Fachperson kann durch die Einwilli-
gung der betroffenen Person von ihrer
Schweigepflicht entbunden werden,
aber auch aufgrund einer gesetzlichen
Bestimmung (z. B. Zeugnispflicht in ei-
nem Verfahren oder Meldepflicht wie in
Art. 314d des Zivilgesetzbuchs).

Eine Verletzung eines Berufsgeheimnis-
ses des StGB oder des Nebenstrafrechts,
also z. B. des Arzt- oder Bankkunden-
geheimnisses, geht einer Verletzung
von Art. 62 DSGVO vor, wenn es sich bei
den Berufsgeheimnis-geschützten Da-
ten auch um Personendaten gehandelt
hat. Im Fokus des Art. 62 DSGVO bleiben
somit insbesondere Personen, die kei-
nem Berufsgeheimnis unterstehen, wie

z. B. HR-Mitarbeitende oder Naturheiler und Naturheilerinnen. Aber auch der betriebliche Datenschutzberater kann sich bei einer vorsätzlichen Offenlegung von geheimen Personendaten strafbar machen.

Wer macht sich strafbar?

In erster Linie erfolgt die Bestrafung von natürlichen Personen. Eine Hilfsperson, im StGB auch Gehilfe genannt, wird nicht bestraft, da es sich bei den DSGVO-Verstössen lediglich um Übertretungen handelt. Auf die Einführung einer direkten Bestrafung von Unternehmen wird im Gegensatz zur Europäischen Datenschutz-Grundverordnung im DSGVO verzichtet. Die Mehrheit der strafbaren Verhaltensweisen betrifft den Verantwortlichen der Datenbearbeitung. Auftragsbearbeiter können sich insbesondere bei der Verletzung der Datensicherheit strafbar machen.

Bei Verstössen innerhalb von geschäftlichen Betrieben hat die Strafverfolgungsbehörde die Möglichkeit, von der Verfolgung dieser Individuen abzusehen und stattdessen den geschäftlichen Betrieb zu bestrafen, sofern die vorgesehene Geldbusse von CHF 50000.– nicht überschritten wird und die erforderlichen Untersuchungen für die Bestrafung einer Einzelperson unverhältnismässig wären. Anzumerken ist, dass der Art. 64 Abs. 2 DSGVO, wonach bei Bussen bis CHF 50000.– statt der natürlichen Person der Geschäftsbetrieb gebüsst werden kann, der natürlichen Person wenig Entlastung bringen dürfte. Die Regelung setzt voraus, dass sich die verantwortliche Person nur mit unverhältnismässigem Aufwand ermitteln lässt.

Die Strafbestimmungen

Die Verletzung einer strafrechtlichen Bestimmung des DSGVO ist eine Übertretung und kann mit einer Geldbusse von bis zu CHF 250000.– auf Antrag bestraft werden.

Hervorzuheben ist aber, dass alle Delikte im DSGVO nur bei (eventual-)vorsätzlicher Begehung strafbar sind im Gegensatz zu den Verletzungen der diversen Berufsgeheimnisse in der Schweiz, die auch fahrlässig begangen werden können. Das heisst für die Praxis: Sofern mit Personendaten gewissenhaft umgegangen wird und eine rudimentäre Datenschutz-Governance vorhanden ist, ist das Risiko für die einzelnen Personen, sich bei einer Datenbearbeitung strafbar zu machen, sehr gering.

Strafbestimmungen ausserhalb des DSGVO

Abschliessend sei anzumerken, dass neben den Regelungen des DSGVO auch ausserhalb dieses Gesetzes strafrechtliche Vorschriften bestehen, die insbesondere darauf abzielen, den Datenschutz zu stärken. Hierbei sind insbesondere die Art. 179^{novies} und Art. 179^{decies} StGB zu erwähnen. Ersterer befasst sich mit der widerrechtlichen Erlangung von sensiblen personenbezogenen Daten, die nicht öffentlich verfügbar sind. Diese Bestimmung bezieht sowohl die physische Beschaffung (etwa das Entwenden einer Akte) als auch die digitale Erlangung ein. Art. 179^{decies} des StGB ahndet jene, die die Identität einer anderen Person missbräuchlich verwenden, indem sie sich als diese Person ausgeben, entweder um ihr Schaden zuzufügen oder sich Vorteile zu verschaffen.

Fazit

Bei Nichtbeachtung des DSGVO können finanzielle Konsequenzen von bis zu CHF 250000.– für natürliche Personen entstehen. Die Zeit wird allerdings zeigen müssen, ob hier tatsächlich viele Strafanträge gestellt werden, welche dann auch zu Verurteilungen führen. Sofern eine Datenschutz-Governance in einem Unternehmen besteht und die einzelnen Personen, welche die Datenbearbeitungen durchführen, sich nicht vorsätzlich über die internen Regeln

hinwegsetzen, wie z. B. nicht erlaubte Speicherorte verwenden, besteht nur ein sehr geringes Risiko einer Strafbarkeit. Für einen betrieblichen Datenschutzberater besteht auch kein strafrechtliches Risiko, wenn sich Mitarbeitende in seinem Unternehmen nicht an das DSGVO und die internen Regeln halten. Es ist aber sicher empfehlenswert für den Datenschutzberater, allfällige Missstände zu dokumentieren und ggf. der Geschäftsleitung oder dem obersten Leitungsorgan zur Kenntnis zu bringen.

Für Mitglieder der Geschäftsleitung oder des obersten Leitungsorgans besteht das Risiko einer Strafbarkeit, wenn sie sich überhaupt nicht um den Datenschutz in ihrem Unternehmen kümmern oder wenn sie bewusst nach Meldung vom Datenschutzberater beispielsweise das DSGVO verletzen.

TIPP



- Das neue DSGVO bringt hohe Bussen mit sich, die aber nur für die Verletzung von einzelnen Pflichten und nicht generell bei jeglicher Verletzung des DSGVO ausgesprochen werden können.
- Alle neuen Strafbestimmungen sind Übertretungen.
- Im Fokus stehen die natürlichen Personen. Unternehmen können aber in Ausnahmefällen auch gebüsst werden.
- Das Risiko, sich strafbar zu machen, ist für den Einzelnen gering, weil nur vorsätzliches Handeln strafbar ist.
- Eine gute interne Datenschutz-Governance und Schulung der Mitarbeitenden vermindert das Risiko einer Strafbarkeit aufgrund eventualvorsätzlichen Handelns enorm.



AUTOR

RA Dr. iur. Lukas Lezzi ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz- und Finanzmarktrecht.