EU-DSGVO

Die Europäische Datenschutzgrundverordnung (DSGVO) und ihre Auswirkungen auf Schweizer Unternehmen

---

Inhaltsübersicht

---

1. Management Summary

1.1. Anwendbarkeit auf Schweizer Unternehmen i.B.

Die DSGVO findet ab dem 25. Mai 2018 Anwendung auf viele Schweizer Unternehmen, auch wenn die Regelung europäisches Recht darstellt. Offensichtlich ist dabei die Anwendbarkeit auf Verarbeitungen durch eine Niederlassung in der EU.

Jedoch auch ohne Niederlassung in der EU kann die DSGVO anwendbar sein, namentlich in Zusammenhang mit

(a) der Ausrichtung des Waren- oder Dienstleistungsangebots auf den europäischen (End-)Kundenmarkt
(b) der Verhaltensbeobachtung in der EU, soweit das Verhalten der betroffenen Person in der Union erfolgt.

Ersteres ist wohl auf viele Onlineshops zutreffen, die sich auf die DACH-Region ausgerichtet haben. Aber auch das Onlinetracking von Internetverhalten von potentiellen EU-Kunden könnte für viele Unternehmen die Anwendbarkeit der DSGVO eröffnen. Unklar ist bisweilen die Konsequenz eines blossen Outsourcings an ein Unternehmen in der EU. Erste Präzedenzfälle von den grösseren Aufsichtsbehörden der Unionsstaaten werden jedoch die Anwendbarkeit der DSGVO genauer festlegen müssen.

1.2. Folgen Anwendbarkeit

Die Folgen einer Unterstellung sind einschneidend. Zu denken ist zunächst die Unterstellung unter eine ausländische Aufsichtsbehörde, welcher teilweise umfassende Untersuchungskompetenz eingeräumt wird. Die Anwendbarkeit der DSGVO hat aber auch eine neue Rechenschaftspflicht und entsprechende Dokumentationspflichten zur Folge. Schliesslich ist bei Verstössen das neue DSGVO-Sanktionsregime anwendbar, welches Sanktionen von bis zu 4 % des weltweit erzielten Jahresumsatzes beinhaltet.

Anwaltskanzlei Seidenhof
Seidenhofstrasse 14
CH-6003 Luzern
www.advokatur.info

Ihre Ansprechsperson

Matthias R. Schönbächler
MLaw Rechtsanwalt

Kontaktangaben
schoenbaechler@advokatur.info
T +41 41 227 72 50
F +41 41 227 72 59

2. Einführung

Die wirtschaftliche und soziale Integration als Folge eines funktionierenden Binnenmarkts hat zu einem deutlichen Anstieg des grenzüberschreitenden Verkehrs personenbezogener Daten geführt. Diese Zunahme des unionsweiten Austauschs personenbezogener Daten zwischen öffentlichen und privaten Akteuren hat die Europäische Union zum Anlass genommen, eine griffigere und europaweite Regelung für den Datenschutz zu treffen. Im Zentrum steht dabei der Schutz der informationellen Selbstbestimmung der betroffenen Person.

> „Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht."
>
> – DSGVO-Erwägung 1, Satz 1.

Im April 2016 hat das EU-Parlament die Datenschutz-Grundverordnung (DSGVO bzw. General Data Protection Regulation (GDPR)) erlassen. Diese ersetzt damit die aus dem Jahr 1995 stammende Richtlinie 95/46/EG (Datenschutzrichtlinie) und gilt ab dem 25. Mai 2018. Anders als die Vorgängerrichtlinie entfaltet die DSGVO nach ihrem Inkrafttreten unmittelbare Wirkung in allen EU-Mitgliedstaaten. Den Mitgliedstaaten wird es daher nicht möglich sein, ausserhalb der Öffnungsklauseln den von der Verordnung festgeschriebenen Datenschutz durch nationale Regelungen abzuschwächen oder zu verstärken. Mit der Regelung zum Geltungsbereich geht jedoch zwangsweise einher, dass jeweils unterschiedliche nationale Datenschutzaufsichtsbehörden für die Durchsetzung der DSGVO auf ihrem jeweiligen Hoheitsgebiet sorgen. Neben der DSGVO werden Persönlichkeitsrechte wie die informationelle Selbstbestimmung in der sogenannten e-Privacy-Richtlinie 2009/136/EG geregelt. Die EU-Kommission hat am 10. Januar 2017 ihren offiziellen Entwurf für eine E-Privacy-Verordnung vorgelegt, welche die e-Privacy-Richtlinie (auch „Cookie-Richtlinie") ersetzen soll.

Auch viele Unternehmen in der Schweiz sind von den neuen Regelungen betroffen, denn die EU wendet die DSGVO unter bestimmten Voraussetzungen weltweit an. Wichtig ist hingegen anzumerken, dass die DSGVO keine direkte Gesetzeswirkung für die Schweiz hat und das Gesetz auch nicht dem autonomen Nachvollzug unterliegt. Die Schweiz wird ihr eigenes Datenschutzrecht ebenfalls anpassen und geht dabei in eine ähnliche Richtung wie die DSGVO. Das Parlament hat die Vorlage jedoch zweigeteilt und lässt sich damit mehr Zeit mit der neuen Regulierung des Datenschutzes. Deshalb wartet der Bundesrat auch ab, mit der Europäischen Kommission Kontakt aufzunehmen, um die Umsetzungsfragen für Schweizerische Unternehmen in Bezug auf die DSGVO zu regeln.

Der Grundtenor sämtlicher Revisionen von Regelwerken mit Digitalisierungsthemen ist hingegen überwiegend gleich:

a) Mehr Transparenz
b) Mehr Verhältnismässigkeit
c) Mehr (Folge-)Bewusstsein

3. DSGVO

3.1. Überblick

Die DSGVO gilt ab dem 25. Mai 2018 auch für viele Schweizer Unternehmen, obwohl die Schweiz kein Mitgliedstaat der Union ist. Leider gibt es keine repräsentativen Umfragen, wie viele Schweizer Unternehmen schon bereit sind für das Inkrafttreten der DSGVO, doch es werden wohl nicht die Hälfte sein. Hingegen schätzen Experten, dass auch nur knapp über der Hälfte aller Unternehmen in Deutschland und Österreich bis zum 25. Mai 2018 die DSGVO umgesetzt haben werden. Dabei sind Deutschland und Österreich die ersten Mitgliedstaaten der Union, welche ihre Gesetze an die DSGVO angepasst haben.

Dies ist eine äusserst interessante Feststellung, zumal die Anwendung der DSGVO auf gewisse Datenverarbeitungen einschneidende Folgen haben kann. Zunächst bringt die Anwendbarkeit der DSGVO die Unterstellung unter die Aufsichtsbehörde des jeweiligen Mitgliedstaates der Union mit sich. In einem Untersuchungsverfahren wird dieser u.a. die Kompetenz eingeräumt, eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschliesslich eines Verbots, zu verhängen. Für ein allfälliges Verfahren gilt aufgrund der neuen Rechenschaftspflicht die Beweislastumkehr, d.h. die Beweislast liegt beim Verantwortlichen, aufgrund der eigenen Dokumentation die Einhaltung der infrage stehenden Norm zu beweisen. Kann der Verantwortliche das nicht, so droht ihm schliesslich das DSGVO-Sanktionsregime, namentlich die bereits bekannte Pönale von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs.

Bevor im Folgenden der Geltungsbereich der DSGVO umrissen wird und mit user cases zur Anwendbarkeit der DSGVO auf Schweizer Unternehmen i.B. untermalt wird, gilt es zunächst einige wenige Definitionen und Begrifflichkeiten festzuhalten. Schliesslich folgt eine kurze Zusammenfassung welche Datenschutzregeln mit der DSGVO für Schweizer Unternehmen (eher) neu sind.

3.2. Begriffe und Definitionen

Der Schutz natürlicher Personen sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung von personenbezogenen Daten, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

In Art. 4 DSGVO sind diverse Begriffsbestimmungen enthalten. Während im hiesigen DSG von einem *Bearbeiten* die Rede ist, geht man im DSGVO von einer *Verarbeitung* aus, wobei der Begriffsinhalt im Wesentlichen deckungsgleich ist. Ausserdem verwendet die DSGVO den Begriff *sensible Daten* anstelle des DSG-Begriffs *besonders schützenswerte Personendaten*. Auch die Bezeichnung der *betroffene Person* ist deckungsgleich, zumindest sobald ab der DSG-Revision nur noch natürliche Personen Datensubjekte sind, während nach heutigem Stand auch juristische Personen betroffen sein können.

Neu ist hingegen die Kategorisierung von Informationen in

a) Informationen, d.h. Informationen ohne jeglichen Personenbezug;
b) Personendaten, d.h. Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Ziff. 1 DSGVO);
c) Pseudonyme Daten, d.h. personenbezogenen Daten, die ohne Hinzuziehen zusätzlicher Informationen nicht mehr einer Person zugeordnet werden können (Art. 4 Ziff. 5 DSGVO); und
d) Anonyme Daten, d.h. Personenbezogenen Daten, die in einer Weise bearbeitet wurden, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann (Erw. 26 DSGVO).

Neu sind auch die Definitionen zu folgende Datenkategorien:

a) Genetische Daten (Art. 3 Ziff. 13 DSGVO) bzw. Daten zu genetischen Eigenschaften, eindeutige Informationen zur Physiologie, zur Gesundheit oder Körperproben von betroffenen Personen
b) Biometrische Daten (Art. 3 Ziff. 14 DSGVO) bzw. Daten zu körperlichen, psychischen oder verhaltenstypischen Merkmalen, die eine eindeutige Identifikation von betroffenen Personen durch technische Verfahren erlauben
c) Gesundheitsdaten (Art. 3 Ziff. 15 DSGVO) bzw. Daten, die sich auf die körperliche oder geistige Gesundheit von betroffenen Personen beziehen oder Informationen zu deren Gesundheitszustand beinhalten.

Die Konsequenz aus den neu definierten Datenkategorien ist hingegen grundsätzlich dieselbe wie nach geltendem DSG, nämlich dass Daten aus diesen Datenkategorien mit *sensiblen Daten* (Art. 9 I DSGVO) gleichgestellt werden.

Neu sind im Übrigen die Funktionen des „*Vertreters*“ (Art. 4 Ziff. 17 DSGVO). Nicht in der Union niedergelassene Verantwortliche oder Auftragsverarbeiter müssen gem. Art. 27 DSGVO einen in der Union niedergelassenen Vertreter bestellen. Umfassender ist die Funktion des allenfalls bezeichneten, internen oder externen *Datenschutzbeauftragten* des Verantwortlichen. Letztere ist insbesondere interessant, da mit den Entwurf zum neuen DSG neu die Funktion der Datenschutzberaterin oder -beraters geschaffen wird, was ab Ernennung wie im DSGVO gewisse Vorteile mit sich bringt.

3.3. Geltungsbereich DSGVO

Eine Novation ist die DSGVO in zweierlei Hinsicht. Einerseits, weil sie sich nicht darauf beschränkt „blosse“ Richtlinie zu sein, sondern nach ihrem Inkrafttreten unmittelbare Rechtswirkung in allen EU-Mitgliedstaaten entfaltet. Andererseits begnügt sie sich in Bezug auf dessen räumlichen Geltungsbereich nicht mit dem einfachen Territorialitätsprinzip, sondern knüpft an zwei separat zu betrachtenden Prinzipien an: Einerseits dem Niederlassungs- bzw. Sitzlandprinzip, andererseits am Marktortprinzip. Angeknüpft wird jedoch nicht am Unternehmen, sondern an der jeweiligen Verarbeitung.

Artikel 3 DSGVO
Räumlicher Anwendungsbereich

(1) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.

(2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

(3) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

Der Hauptanwendungsfall liegt klarerweise auf dem an das Territorialitätsprinzip angelehnten Niederlassungs- bzw. Sitzlandprinzip: Die DSGVO findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt. Dabei spielt es keine Rolle, ob die effektive Verarbeitung in der Union stattfindet oder in der Schweiz. Wenn also ein Schweizer Unternehmen eine Tochterfirma oder eine Niederlassung in einem Mitgliedstaat der Europäischen Union führt, so findet die DSGVO Anwendung auf Verarbeitungen von Personendaten in Bezug mit dessen Tätigkeit, auch wenn die Verarbeitung selbst nicht in der Union erfolgt. Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei nicht ausschlaggebend (Erwägung 22 DSGVO).

Schwieriger ist der Nebenanwendungsfall, namentlich das Marktortprinzips mit seinen zwei Ausprägungen. Die DSGVO findet nämlich in diesen beiden Fällen auch Anwendung auf Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter. Zunächst muss es sich um die Verarbeitung von personenbezogener Daten von betroffenen Personen handeln, die sich effektiv in der Union befinden. Zusätzlich braucht es aber noch eines der folgenden zwei Kriterien:

(a) Ausrichtung auf den (End-)Kundenmarkt

Dieses Kriterium ist erfüllt, wenn die Verarbeitung damit in Zusammenhang steht, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten. Das Anbieten von Waren oder Dienstleistungen an EU-Bürger wird dabei unabhängig davon angenommen, ob von diesen betroffenen Personen eine Zahlung zu leisten ist oder es sich um ein kostenfreies Angebot handelt. Angesichts der überwiegenden Digitalisie-

rung von unseren Waren- und/oder Dienstleistungsangeboten gibt es hier noch weitgehenden Präzisierungsbedarf. Erwägung 23 der DSGVO spricht von einer Erfassung von Unternehmen, die offensichtlich beabsichtigen, betroffenen Personen in einem Mitgliedstaat der Union Dienstleistungen anzubieten. So fällt auch beispielsweise die Zurverfügungstellung von Cloud-Services an EU-Bürger unter die DSGVO, unabhängig davon, ob dieses kostenlos erfolgt. Weiter ist die blosse Erreichbarkeit einer Website oder eines Webshops mit Waren- und/oder Dienstleistungsangeboten alleine noch kein Anbieten im Sinne der DSGVO ist. Die Erreichbarkeit kann als ein Kriterium neben vielen gesehen werden, welche sich wohl zusammenfassen lassen als Angebotsvorsatz: d.h. mit Wissen und Willen an EU-Bürger Waren oder Dienstleistungen anzubieten. Ein solcher Vorsatz kann sich bspw. in der Kundenfreundlichkeit manifestieren, indem die jeweilige Sprache angeboten wird, eine Zahlung in anderer Währung angenommen wird, Lieferbedingungen angeführt werden etc. Vertreten wird auch die Meinung, dass gezielt mit Geoblockern gearbeitet werden kann, um diese Ausrichtung zu unterbinden. Ob Geoblocker hingegen als Standard gefordert werden können, um eine Ausrichtung zu vermeiden, ist ungewiss.

(b) Verhaltensbeobachtung in der EU

Weiter ist die DSGVO anwendbar, wenn die Verarbeitung in Zusammenhang damit steht, das (Online-)Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt. Es braucht hierbei nicht erwähnt zu werden, dass bei einer Verhaltensbeobachtung das Kriterium einer späteren entgeltlichen Leistung sowieso nicht gefordert ist. Massgebend ist hier die Frage, ob die Internetaktivitäten betroffener Personen nachvollzogen werden, mit der Möglichkeit einer nachfolgenden Profilbildung. Ob effektiv die Grundlage, der für sie betreffenden Entscheidungen analysiert wird oder ob anhand dessen Entscheidungen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten vorausgesagt werden, spielt keine Rolle. So führt zum Beispiel ein Online-Tracking von EU-Bürgern und von ihrem Onlineverhalten, welches sie in der EU ausüben, stets zur Anwendbarkeit der DSGVO. Es kann hier wohl davon ausgegangen werden, dass das Online-Tracking standardmässig geografisch angepasst werden muss, um verhindern zu können unter die DSGVO zu fallen.

Unklar ist bisweilen die Konsequenz eines klassischen Outsourcings an ein Unternehmen in der EU. Mittlerweile gibt es eine starke Lehrmeinung die besagt, dass die DSGVO keine Anwendung findet auf Verarbeitungen eines schweizerischen Verantwortlichen, der einen Auftragsdatenverarbeiter in der EU beschäftigt. Zu präzisieren ist hierbei klar, dass der EU-Auftragsdatenverarbeiter selbst klar der DSGVO unterstellt ist aufgrund seiner Niederlassung. Insofern wird ein gewandter Auftragsdatenverarbeiter aus der EU in seinem Vertragsverhältnis mit einem Schweizer Unternehmen auf gewisse Standards der DSGVO beharren (vgl. Art. 28 Abs. 3 GDPR). Diese Meinung hat Vorrang zu geniessen, da auf Verarbeitungen des EU-Auftragsdatenverarbeiters die DSGVO anwendbar ist und somit kein Schutzbedarf besteht, die DSGVO

auf den Verantwortlichen anzuwenden. Ausserdem wird gemäss Marktortprinzip die DSGVO entsprechend *wegen* der EU-Ausrichtung oder der Verhaltensbeobachtung angewendet und nicht einzig aufgrund des Umstands, dass ein Schweizer Unternehmen einen EU-Auftragsdatenverarbeiter beschäftigt.

Als Konsequenz der Anwendung der DSGVO auf nicht in der EU niedergelassene Unternehmen, wurde die Funktion des *Vertreters* eingeführt. Jeder Verantwortliche oder Auftragsverarbeiter ohne Niederlassung in der Union, dessen Verarbeitungstätigkeiten sich nach Marktortprinzip auf betroffene Personen beziehen, die sich in der Union aufhalten, soll gemäss Erwägung 80 DSGVO einen Vertreter benennen müssen. Von diesem Grundsatz gibt es nur wenige Ausnahmen. Von der Pflicht befreit wird nur die gelegentliche und risikoarme Verarbeitung im Sinne dieser Erwägung.

3.4. Anwendbarkeit auf Schweizer Unternehmen i.B.

Zusammenfassend lassen sich also zum heutigen Stand folgende user-cases exemplarisch auflisten:

(a) Tochterfirma in Deutschland

→ Niederlassungs- bzw. Sitzlandprinzip Art. 3 Abs. 1 DSGVO;

(b) Niederlassung in Österreich

→ Niederlassungs- bzw. Sitzlandprinzip Art. 3 Abs. 1 DSGVO;

(c) CH-Online-Shop mit DACH-Ausrichtung

→ Marktortprinzip Art. 3 Abs. 2 lit. a DSGVO; Bsp. Toplevel-Domain .ch/.de/.at, Lieferbedingungen DACH und Preisberechnung in CHF/EUR

(d) Software as a Service (SaaS) Angebot in DACH

→ Marktortprinzip Art. 3 Abs. 2 lit. a/b DSGVO;

(e) CH-Dienstleistungsbetrieb mit Online-Tracking in Grenzregionen

→ Marktortprinzip Art. 3 Abs. 2 lit. b DSGVO;

(f) CH-Betrieb, CRM-Daten verwaltet in Deutschland

→ Keine Anwendung DSGVO

(g) CH-Online-Shop abrufbar weltweit, auf Schweiz und FL ausgerichtet

→ Keine Anwendung DSGVO;

3.5. Datenschutz – Was ist neu?

Bei all diesen Revisionen und insbesondere bei der DSGVO als grosse graue Wolke, darf zunächst nicht in Vergessenheit geraten, dass wir aus Schweizer Sicht bereits jetzt über ein hohes Datenschutzniveau verfügen. Am überwiegenden Gros der Datenschutzregulierungen – hiesigen Datenschützern bekannt als Datenschutzgrundsätze – ändert sich deshalb wenig. Die Grundsätze

i.e.S. (Art. 5 Abs. 1 DSGVO d.h. Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit) sind – mit der Einführung des noch ungeschriebenen Grundsatzes der Datenminimierung – deckungsgleich mit dem hiesigen DSG. Ausserdem sind auch *sensible Daten* (besonders schützenswerte Personendaten) in der DSGVO besonders geschützt (Art. 9 DSGVO)

Anders ist jedoch der Denkansatz bei einer jeder Datenverarbeitung: Während das heutige DSG davon ausgeht, dass jede Bearbeitung erlaubt ist, solange sie rechtmässig erfolgt bzw. gerechtfertigt werden kann, bedarf es laut der DSGVO stets einer **Rechtsgrundlage**, andernfalls sie rechtswidrig ist. Grundlage der rechtmässigen Datenverarbeitung nach Art. 6 DSGVO sind alternativ (und untereinander gleichwertig):

a) **Einwilligung** der betroffenen Person (Art. 6 Abs. 1 lit. a DSGVO)
b) Erforderlich für die **Vertragserfüllung** oder die Durchführung vorvertraglicher Massnahmen (Art. 6 Abs. 1 lit. b DSGVO)
c) Erforderlich zur Erfüllung einer **rechtlichen Verpflichtung** (Art. 6 Abs. 1 lit. c DSGVO)
d) Erforderlich zum **Schutz lebenswichtiger Interessen** der betroffenen Person oder einer anderen natürlichen Person (Art. 6 Abs. 1 lit. d DSGVO)
e) Erforderlich für die **Wahrnehmung einer Aufgabe im öffentlichen Interesse** (Art. 6 Abs. 1 lit. e DSGVO)
f) Erforderlich für die **Wahrung der berechtigten Interessen** des Verantwortlichen oder eines Dritten, sofern diese Interessen denjenigen der betroffenen Person überwiegen (Art. 6 Abs. 1 lit. f DSGVO)

Bei diesen Rechtsgrundlagen handelt es sich im Wesentlichen um die Rechtfertigungsgründe nach unserem heutigen Art. 13 DSG. Weitere Rechtsgrundlagen befinden sich im sonstigen Recht der Union (soweit in der DSGVO darauf Bezug genommen wird) sowie im Recht der jeweiligen Mitgliedstaaten, sofern dieser von der Möglichkeit einer Öffnungsklausel Gebrauch gemacht hat. Nota bene bietet die Öffnungsklausel hier keine Möglichkeit strengere Voraussetzungen zu schaffen.

Ein Paradigmenwechsel stellt hingegen die neue **Rechenschaftspflicht** („Accountability“) von Art. 5 Abs. 2 DSGVO dar: Diese besagt, dass die Einhaltung der Verarbeitungsgrundsätze durch den Verantwortlichen nachgewiesen werden muss. Folglich bedeutet dies für jeden Verarbeiter, dass die für die Einhaltung eine **Dokumentationspflicht** besteht.

Die fundamentalste Dokumentationspflicht beherbergt die DSGVO in Artikel 30, namentlich in der Pflicht zur Führung eines **Verzeichnisses von Verarbeitungstätigkeiten**. Dieses ist schriftlich oder elektronisch zu führen und auf Anfrage hin der Aufsichtsbehörde zur Verfügung zu stellen. Absätze 1 und 2 von Art. 30 DSGVO stellen dabei Pflichten jeweils für den Verantwortlichen selbst und für einen allfälligen Auftragsverarbeiter auf. Eine Ausnahme dieser

Dokumentationspflicht versteckt sich in Art. 30 Abs. 5 DSGVO. Die genannte Dokumentationspflicht entfällt bedingt für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen und kein datenschutzrechtliches Risiko besteht.

Die Erstellung und Führung eines Verzeichnisses von Verarbeitungstätigkeiten kann je nach datenschutzrechtlichen Voraussetzungen im Unternehmen eine grosse Herausforderung darstellen. Es kann aber bei sorgfältiger Erarbeitung auch die beste Voraussetzung darstellen für die Aufgleisung der DSGVO-Compliance. Die **Implementierung der DSGVO** Anforderungen kann in folgenden Schritten erfolgen.

1) Welche Anforderungen stellt die DSGVO überhaupt?

→ Gewinne eine Übersicht über die Anforderungen der DSGVO

2) Welche Datenverarbeitungen tätigt unser Unternehmen genau?

→ Dokumentiere die aktuellen Datenverarbeitungen in eurem Unternehmen

3) Dürfen diese Datenverarbeitungen nach wie vor vorgenommen werden?

→ Erstelle eine Anforderungs- und Gap-Analyse

4) Was muss konkret vorgekehrt werden?

→ Complianceplanung: Ausarbeitung von Datenschutzrichtlinien, Verarbeitungsprozessdefinitionen, Datenschutzerklärung, Einwilligungsprotokollierung, Auslandsübermittlungsregeln, Datenschutzrechtlicher Verträge und sonstiger Korrespondenz

5) Wer kann diese Vorkehrungen treffen?

→ Projektplanung: Organisiere intern den Datenschutz

6) Wie kann ich die DSGVO nachhaltig gewährleisten?

→ Festhalten an Prozessabläufen, Schulung des Personals, Awareness in der Geschäftsführung und Aufnahme des Datenschutzes als Stabsfunktion

Was zwar bereits mit dem Grundsatz der Datensicherheit im Datenschutzrecht verankert ist, wurde mit der DSGVO – sowie künftig auch mit dem neuen DSG – als eigenständiger Datenschutzprozess auf Gesetzesstufe festgehalten. Die Rede ist von der **Datenschutzfolgeabschätzung** (Privacy Impact Assessment). Laut Art. 35 DSGVO ist eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen, wenn eine Form der Verarbeitung, voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Diese ist vom Verantwortlichen vorab durchzuführen unter Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde.

Weiter und ebenfalls beim Grundsatz der Datensicherheit anzusiedeln, sind die neuen Grundsätze des Privacy by design und Privacy by default (Art. 25 DSGVO). Nach **Privacy by design**, müssen technische und organisatorische Massnahmen zur Einhaltung der Datenschutzgrundsätze schon bei der Planung bzw. Systemgestaltung vorgekehrt werden. Mit **Privacy by default** wurde die Pflicht zur datenschutzfreundlichen Voreinstellung eingeführt.

Schliesslich wurde in Art. 33 DSGVO die Meldepflicht von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde eingeführt. Sogenannte **Data Breaches** hat der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde zu melden. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. Einzige Ausnahme von dieser Meldepflicht ist die begründete Annahme, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Mittlerweile dürfte allseits bekannt sein, dass im Falle von groben Verstössen gegen die DSGVO nebst einem Klage- oder Beschwerdeverfahren auch exorbitante Geldbussen drohen können. Die **Höchstsanktion** wurde medial überall bekanntgegeben. Sie ist denn auch eine Novation: Bei Verstössen gegen gewisse Bestimmungen werden nach Art. 83 DSGVO Geldbussen von bis zu EUR 20‘000‘000.00 verhängt oder im Fall eines Unternehmens von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs. Bei geringeren Datenschutzverletzungen beträgt sie bis zu EUR 10‘000‘000.00 oder im Fall eines Unternehmens bis zu 2 %. Jahresumsatzes. Je nach Unternehmenstätigkeit könnte jedoch die blosse Tatsache mehr Angst bereiten, dass in einem Untersuchungsverfahren eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschliesslich eines Verbots, ausgesprochen werden könnte.

4. Ausblick

Das Datum der Inkraftsetzung ist in aller Munde, doch **was wird erwartet?** Die Erwartungshaltung der Datenschutzaufsichtsbehörden wird sich – vorbehaltlich groben Verstössen – wohl zunächst darauf beschränken, ob die Inkraftsetzung der DSGVO beim einzelnen Verarbeiter angekommen ist. Unter Verweis auf die vorgenannte mögliche Compliance-Projektierung, wird erwartet werden können, dass per Stichtag folgende Fragen beantwortet werden können:

1) Welche Anforderungen stellt die DSGVO überhaupt?

2) Welche Datenverarbeitungen tätigt unser Unternehmen genau?

3) Dürfen diese Datenverarbeitungen nach wie vor vorgenommen werden?

4) Ansatzweise Complianceplanung: Was muss konkret vorgekehrt werden?

Diese Anforderungen lassen sich meines Erachtens in folgende drei Grundpfeiler gliedern:

(a) Awareness der DSGVO

Verständnis der Datenschutzgrundsätze, Rechte der betroffenen Personen, Dokumentations- und Mitwirkungspflichten, aber auch Unterstellung unter Aufsichtsbehörden und Sanktionsregime.

(b) Datenmapping: Minimum Dokumentation nach Art. 30 DSGVO

Übersicht über eigene Datenverarbeitungsprozesse und verarbeiteter Datenkategorien, Risikogehalt von den Verarbeitungen und Selbstanalyse

(c) Ernsthafte und richtig dokumentierte Bemühungen mit Risikofokus

Ansätze eines Mappings und einer Complianceplanung, ein minimales Datenverzeichnis sowie Evaluation allfälliger Missstände

Per Stichtag der Inkraftsetzung kann wohl keine vollständige Compliance erwartet werden. Klar sein dürfte auch, dass die DSGVO vor dem 25. Mai 2018 keine Vorwirkung zeitigt. Als Anekdote hierzu lässt eine Verfügung des Landesbeauftragten für den Datenschutz von Baden-Württemberg vom 25. November 2016 anführen, welche vom Verwaltungsgericht Karlsruhe aufgehoben wurde. Sie richtete sich gegen eine Auskunftei, deren Speicher- und Löschfristen den Anforderungen der DSGVO vermeintlich nicht entsprechen würde und verfügte, dass Informationen für Bonitätsauskünfte, die nach dem 24. Mai 2018 gespeichert würden, innert drei Jahren zu löschen seien. Richtigerweise wurde anerkannt, dass eine gesetzliche Grundlage dazu fehlt und eine DSGVO-Verfehlung am 25. Mai 2018 nicht vorhergesagt werden kann.

Einige starke Aufsichtsbehörden, insbesondere in Deutschland und Frankreich, haben Vorbildfunktion eingenommen. Fortlaufend werden Merkblätter, Weisungen und Informationsschreiben publiziert, welche einerseits den Verantwortlichen, aber insbesondere auch den Aufsichtsbehörden als Arbeitshilfen dienen sollen. Nicht nur sind eine Grosszahl von Unternehmen nicht bereit für die DSGVO – auch eine grosse Zahl an Aufsichtsbehörden und Datenschutzbeauftragen werden erste Präzedenzfälle und Praxisentscheide der grösseren Aufsichtsbehörden abwarten.

Unklar ist wie bereits ausgeführt, ob bei einem klassischen Outsourcing an Auftragsverarbeiter in der EU die DSGVO zur Anwendung kommt. Dies ist frappant, zumal dies eine nicht unwesentliche ökonomische Tragweite hat. Bis zu einem ersten massgebenden Entscheid bleibt diese Antwort jedoch offen.

Insgesamt weist die DSGVO über vierzig Öffnungsklauseln auf, welche den Mitgliedstaaten die Möglichkeit einräumen, eigenes Datenschutzrecht einfliessen zu lassen. Bisweilen haben einzig Deutschland und Österreich entsprechende Anpassungsgesetzgebungen eingeführt. Wie sehr durch diese Öffnungsklauseln die Europaweite Einheitlichkeit gebrochen wird ist noch nicht absehbar.

Das Ziel sollte sein, weder eine Alibi-Compliance durchzuführen, noch die Aufforderungen von Aufsichtsbehörden zur Einhaltung der DSGVO abzuwarten. DSGVO-Compliance kann nicht in einer einmaligen und einseitigen Due Diligence erfolgen, sondern soll ein nachhaltiger und von der Geschäftsleitung getragener Prozess sein. Zu bedenken ist jedoch: Wer einmal auf den Radar der Aufsichtsbehörden gelangt, wird dort wohl für die nahe Zukunft bleiben.

5. Take-Aways

- Die DSGVO ersetzt die Datenschutz-Richtlinie 95/46/EG und hat direkte Gesetzeswirkung in der EU

- Sie findet auch Anwendung auf viele Schweizer Unternehmen, nämlich bei Verarbeitungen

  1. durch eine Niederlassung in der EU

  2. ohne Niederlassung in der EU, aber in Zusammenhang mit
     (a) der Ausrichtung auf den europäischen (End-)Kundenmarkt; oder
     (b) der Verhaltensbeobachtung in der EU von Verhalten in der EU

- Die Folgen einer Unterstellung sind einschneidend:

  1. Unterstellung Aufsichtsbehörde
  2. Kompetenzen im Untersuchungsverfahren
  3. Folge neuer Rechenschaftspflicht
  4. DSGVO-Sanktionsregime: bis zu 4 % weltweit erzielten Jahresumsatzes

- Was wird erwartet am 25. Mai 2018?

  (a) Awareness DSGVO
  (b) Datenmapping: Minimum Dokumentation nach Art. 30 DSGVO
  (c) Ernsthafte und richtig dokumentierte Bemühungen mit Risikofokus

Gerne beraten wir Sie, ob die DSGVO auf Ihr Unternehmen Anwendung findet und wie Sie ihr Unternehmen datenschutzrechtlich für die DSGVO aufrüsten.

Matthias R. Schönbächler
MLaw Rechtsanwalt