Datenschutz: Das neue DSG in der Schweiz im Vergleich zur DSGVO in der EU

Datenschutz? Es ist mit Sicherheit kompliziert. Politiker und Interessensvertreter nehmen sich eines Themas' an, dem ein sehr technischer Hintergrund eigen ist und bei dem ein ausgeprägter technischer Sachverstand viele juristische Probleme erleichtern würde, wenn eben das Halbwissen der Entscheider nicht wäre; das macht es kompliziert. Und in vielen Fällen wird ein neues Gesetz sehr erklärungsbedürftig, wenn es für Klarheit während dem Gesetzgebungsverfahren meist wenig Spielraum gibt, für weltfremde Kompromisse aber schon. Die Deutungshoheit obliegt dann wiederum entweder dem Gesetzgeber, zum Beispiel in Form einer Verordnung in der Schweiz oder dem Richter in Form von Urteilen, ein häufig begangener Weg in der EU. Datenschutz ist also auch und vor allem Politik. Die EU hat im Jahr 2018 mit der DSGVO einen neuen Standard gesetzt. Sie wollte mit einem ausgeprägten Schutz personenbezogener Daten vorpreschen und sich klar abgrenzen gegenüber autoritären oder sehr laschen Datenschutzregimes, wie sie in China bzw. in den USA praktiziert werden. Und irgendwann kommt dann noch die Schweiz daher, kann gegenüber den grossen internationalen Regulierungen eigentlich nur verlieren. Sie weiss, dass sie sich in das Schema der EU einbringen muss, um überhaupt eine Wirkung zu entfalten und international akzeptiert zu werden. Sie will aber eigene Akzente setzen, die gut gemeint sein mögen, den international orientierten Unternehmen und Anwendern des Datenschutzes in der Schweiz aber überwiegend Steine in den Weg legen, weil zusätzliche Vorschriften beachtet werden müssen, was das Gegenteil von Rechtssicherheit bedeutet. Datenfluss ist grenzüberschreitend, Datenverarbeitung häufig auch. Ein Unternehmen wird sich stets dafür entscheiden, mit dem strengeren Regime „compliant" zu sein, im Zweifel also mit der DSGVO.

Die DSGVO ist im Mai 2018 in Kraft getreten, das neue DSG soll es per Mitte 2022, dafür ohne Übergangsbestimmungen, die niemand braucht, denn es sind schon viele Unternehmen DSGVO-konform, mit Ausnahme jener, welche ausschliesslich den Schweizer Binnenmarkt bedienen. Das DSG (Reichweite 8,5 Mio. Einwohner) geht mit wenigen Ausnahmen bezüglich Schutzniveau weniger weit als das DSGVO (Reichweite mehr als 400 Mio.). Weil die Schweiz als Wirtschaftsraum wesentlich in die EU eingebunden ist, stellt sich die Frage nach der Sinnhaftigkeit des neuen DSG. Braucht ein kleines Land einen eigenständigen Datenschutz, der mehr bewirkt als Restwerte eines rebellischen Verhaltens? Der vorliegende Artikel versucht, Gemeinsamkeiten und Differenzen aufzuzeigen.

Konkret geht es um drei verschiedene Gesetze bzw. regulatorische Umfelder, welche für die Kommunikations- und Werbeaktivitäten in der EU und in der Schweiz eine Rolle spielen:

1. **Das DSGVO seit 2018 vs. das neue DSG ab 2022:**
   Das Regelwerk der EU ist eine direkt anwendbare Verordnung und damit gleichbedeutend wie ein Gesetz in der Schweiz (die Verordnung in der Schweiz ist ein Rechtsakt zweiten Ranges und interpretiert das Gesetz). In der DSGVO geht es im Wesentlichen um die Regelungen im Umgang mit personenbezogenen Daten. Diese werden organisatorisch und technisch im Zusammenhang mit einen Customer Management System CRM, also der Verwaltung von Kunden- und Kontaktdaten und eventuell einer Customer Data Platform CDP, also der Sammlung und Auswertung von eben diesen strukturierten Daten genutzt. Solange Anbieter und Werbetreibende sich im Bereich der anonymen oder pseudonymen Daten befinden, kommt die DSGVO nicht zur Anwendung.[1] Grundsätzlich bedarf es der Nutzung von personenbezogenen

[1] Daten also, welche einer Person nicht zugeordnet werden können. Ein Beispiel dafür aus aktuellem Anlass: Man hätte die Diskussion um die Datenbeschaffenheit und -bearbeitung in der Swiss-Covid App eigentlich mit einem Satz beenden können: Die Daten sind zu keinem Zeitpunkt personenbezogen, also anonym; man kann nie Rückschlüsse auf einzelne Personen ziehen. Damit ist das Thema erledigt. Der Rest hat nur noch mit Vertrauen in den Anbieter, den Staat zu tun und ob dieser es sich leisten will, durch die Hintertür doch noch eine Verbindung zwischen der anmeldenden Person und dem Prozess des Tracing zu erstellen. Wer die Anwendungen aus den Häusern Facebook, Amazon oder Google nutzt, ist

Copyright Mayoris 2021

Daten zu Werbezwecken gemäss dieser Verordnung einer expliziten und freiwilligen Einwilligung und ein jederzeitiges Widerspruchsrecht für den Nutzer. Und es gibt ein Verbot, diese Zusage mit der Leistung aus einem Vertrag zu koppeln. Dem Nutzer muss mitgeteilt werden, wofür seine Daten verwendet werden. Das Profiling steht im Zentrum, also die Fähigkeit oder der Vorgang, dass ein „Computer" automatisch ein Persönlichkeitsprofil erstellt. So können Segmente von Nutzern und Kunden aufgrund deren Verhaltensmuster erstellt werden, die es dem Unternehmen ermöglichen, zielgerichteter und relevanter Werbung zu schalten oder zu versenden; das konkrete Targeting über digitale Kanäle.
Das neue DSG verlangt auch weiterhin keine explizite Einwilligung für das Profiling (vgl. den Ausnahmefall des Profiling „mit hohem Risiko"). Es braucht lediglich eine Datenschutzerklärung DSE, in der geschrieben steht, zu welchem Zweck der Anwender mit personen-bezogenen Daten umgehen will (Zweckbindung, z.B. personalisierte Werbung für Marketing-zwecke). Diese DSE darf aber nicht beliebige Schweinereien beinhalten, sondern der Nutzungszweck muss „verhältnismässig" und nicht „ungewöhnlich" sein, was in Zukunft durch Gerichte zu interpretieren ist. Die Erklärung muss dem Nutzer in der Schweiz lediglich auf der Firmenwebseite oder in aktiver Kommunikation mit dem Nutzer wie E-Mail oder auf einer App zur Kenntnis gebracht werden. Es gilt das Opt-Out Prinzip. Im Zusammenhang mit AGB oder mit dem Ausfüllen eines Formulars gilt die Berechtigung als eingeholt, wenn AGB bzw. Formular als eigentliche Annahmeobjekte akzeptiert werden. In der EU muss die Erklärung explizit akzeptiert werden. Und dieses Häklein muss zum Nutzer oder Kunden auf einer Datenplattform abgelegt werden, für die Übersicht über die zukünftige Verwendung bis zum Widerruf und für die Informationspflicht dem Berechtigten gegenüber. Informations- und Auskunftspflichten über die eigeholte „Permission" und damit die rechtmässige Nutzung von personenbezogenen Daten werden im neuen DSG ähnlich streng wie in der DSGVO sein. Ein „confirmed Opt-In" für die Nutzung von E-Mail-Adressen (d.h. einfache Bestätigung einer Anmeldung, vgl. weiter unten) lässt sich schwer beweisen. Was macht jetzt ein international tätiges Unternehmen in der Schweiz? Es erstellt eine DSGVO-konforme DSE inkl. positivem Opt-In und Widerspruchsrecht für personalisierte Werbung und wendet sie für alle Nutzer an, zumal nicht einwandfrei geklärt werden kann, ob ein bestimmter Nutzer aus der Schweiz oder der EU kommt. Das DSG ist damit diesbezüglich irrelevant. Auch die Auftragsdatenbearbeitung, also die Übertragung und Bearbeitung von personen-bezogenen Daten an bestimmte Dienstleister muss in einem Vertrag geregelt werden. Für den Beizug von Unterauftragsbearbeitern, was in einigen Fällen für Dienstleister im „near-" oder „off-shoring" Bereich zutrifft, braucht es neu eine Genehmigung. Der Bundesrat legt „unsichere" Drittländer fest. Ähnlich wie in der EU, wo im Urteil „Schrems II" das Privacy Shield Abkommen mit den USA gekippt wurde, gelten die Vereinigten Staaten dabei nicht als sicherer Drittstaat.

2. **ePrivacy Richtline (2009) und ihre Neuauflage vs. Fernmeldegesetz FMG Art. 45c lit. b in der Schweiz (2006)**
   Hier geht es um die berühmten Cookies, „first party" und „third party", neuartiges Teufelszeug aus dem digitalen Zeitalter (😊), Code-Snippets bzw. Textbausteine, welche dem Nutzer im Browser gesetzt werden und es dem Anbieter ermöglichen, diesen zu verfolgen und die Informationen daraus für eigene Werbezwecke nutzbar zu machen; ohne Einwilligung und nur im anonymisierten Bereich, nota bene. Diese Cookies sind die technische Grundlage für eine

angesichts der Intransparenz der Anbieter schon gar nicht legitimiert, sich über die Swiss-Covid App kritisch zu äussern. Das fahrlässige Verhalten den eigenen Daten gegenüber in den sozialen Kanälen wiegt um ein Vielfaches schwerer als alle Bedenken gegen die App.

Copyright Mayoris 2021

milliardenschwere Targeting-Industrie, seit dem Aufkommen der Browser, welche das Zugangsfenster zu Inhalten der Anbieter sind. Mächtige Datenbanken erlauben dank genauer Verhaltensanalyse ein sehr detailliertes Targeting für die Zwecke des Programmatic Advertising.
In den letzten Jahren haben sich aus diesen Rechtsgrundlagen sowohl in der EU als auch in der Schweiz die sogenannten Cookie-Banners auf Webseiten entwickelt, welche grundsätzlich lästig sind und „oben rechts" weggeklickt werden, ohne dass die verlinkte Datenschutzerklärung gelesen wird, welche über die Verwendung von Cookies Auskunft geben würde. Es geht primär um die Third Party Cookies, welche von Drittanbietern auf der eigenen Webseite eines Unternehmens eingebunden werden können (Tracking, Google, Facebook, Webanalyse, usw.). Diese werden von den Browsern zunehmend blockiert und in den nächsten 2-3 Jahren – so von einigen Anbietern bereits angekündigt - gänzlich abgeschafft. Dadurch werden die First Party Cookies relevanter, welche vom Anbieter selbst im Zusammenhang mit der Webseite und geplanten Werbemassnahmen eingebunden werden. Im Einzelnen sind das:

- Notwendige Cookies: Diese werden benötigt, damit eine Webseite und die Seitennavigation überhaupt technisch funktionstüchtig sind. Sie sind notwendig und werden nie Gegenstand einer Einwilligung.
- Präferenz- oder funktionale Cookies: Hier geht es um Voreinstellungen wie z.B. Sprache oder die Region, in welcher ein Nutzer sich befindet.
- Statistische Cookies: Hier geht es um Seitenabrufe, Verweildauer, Besucherfluss, SEO-Ranking; Diese werden anonym gesammelt, um das Ökosystem einer Webseite grundsätzlich zu verbessern.
- Werbe- oder Marketing-Cookies: Das sind die Nutzer-Cookies, welche anonym verwendet werden, um die Nutzer aufgrund der Webbesuche für die zukünftige Werbeansprache zu targeten.

Die ePrivacy-Richtlinie in der EU steht seit Jahren vor einer Neuauflage und irrlichtert durch die Institutionen. Die verschiedenen Interessen bringen in regelmässigen Abständen neue Versionen aufs Parkett und schiessen diese mit jeder neuen EU-Ratspräsidentschaft, also sechs Monate später, regelmässig ab. Das Spiel geht mit ungewissem Ausgang weiter. Inhaltlich würde es um die Regelung und das Einwilligungsverfahren zu den verschiedenen Cookies gehen.

Die Gerichte haben sich deshalb ermächtigt gesehen, in dieser Sackgasse für mehr Rechtssicherheit zu sorgen: Im Jahr 2019 hat der EuGH, im Jahr 2020 dann präzisierend der Bundesgerichtshof BGH in Deutschland mit Vorabklärung durch den EuGH entschieden, dass undifferenzierte Cookie Banner nicht mehr rechtmässig sind. Als Folge davon sind viele Unternehmen dazu übergegangen, detaillierte Cookie-Übersichten anzubieten, welche es dem Nutzer erlauben einzelne Cookie-Kategorien anzuwählen und zuzulassen. Allerdings verfolgen die Anbieter die Hoffnung, dass der Nutzer weiterhin den prominenten Button „Alle Cookies zulassen" ohne grossen Aufhebens akzeptiert. Faktisch hat dies aber bereits zu einem massiven Einbruch der Marketing-Cookies geführt, der Basis also für das bisher eher ungezügelte Targeting von Nutzern quer durch das Internet. Und was geschieht in der Schweiz? Auch hier löst nicht das DSG dieses Thema, sondern Art. 45c lit. b des Fernmeldegesetzes. Aus der Interpretation dieses Artikels wird sich am generellen Akzept des Cookies-Banners auch in Zukunft nichts ändern, Targeting wird demzufolge in der Schweiz einfacher bleiben als in der EU. Es werden keine detaillierten Cookie-Übersichten verlangt.

Copyright Mayoris 2021

3. **Wettbewerbsrecht in der EU vs. das Gesetz über den unlauteren Wettbewerb UWG Art. 3 Abs. 1, lit. o in der Schweiz**
   Diese Gesetze regeln im Speziellen die Einwilligung für den Versand von E-Mails und Newsletter mit werblichem Inhalt an eine grössere Empfängerliste. Ein Gericht in Österreich hat diese Zahl willkürlich einmal mit 70 bezeichnet. Bis zur DSGVO waren die Anforderungen an die Opt-Ins innerhalb der EU sehr unterschiedlich geregelt. Während Deutschland das Double-Opt-In schon seit Jahren kennt, sind die anderen EU-Staaten erst mit der Revision des Datenschutzes nachgezogen und haben – nicht kraft Buchstaben im Gesetz, sondern über die Erfordernisse der Datenminimierung und der Beweispflicht dem Nutzer gegenüber - faktisch das Double-Opt-in zur Pflicht gemacht. In der Schweiz ist nach wie vor das Confirmed Opt-In (also ohne zweites Bestätigungsmail) ausreichend. Man darf sich aber fragen, wie ein Unternehmen unter dem neuen DSG der Informationspflicht ohne Double Opt-In nachkommen will. Faktisch ist das nämlich nicht möglich. Allerdings sagt Art. 3 Abs.1 lit. o auch, dass Massenwerbung an Kunden ohne deren Einwilligung aber mit Hinweis auf die Ablehnungsmöglichkeit zulässig ist. Dieser Artikel und damit die Zulässigkeit des Massenversandes an bestehende und nachweisbare Kunden ohne Opt-In gilt weiterhin.

Hier eine tabellarische Übersicht über die rechtlichen Anforderungen bezüglich der Nutzung von personenbezogenen Daten und von Cookie-Kategorien mit den entsprechenden (revidierten) Gesetzen in der EU und in der Schweiz (inkl. Vorschriften für E-Mail und Call Centers):

Gegenstand	DSGVO 2018	Rev.DSG 2022	RL ePrivacy 2009	FMG Art. 45c lit. b	UWG Art. 3 Abs. 1 lit. o-w
Rechtsraum	EU Direkt anwendbar	CH Verordnung folgt	EU Umsetzung in Ländern	CH Direkt anwendbar	CH Direkt anwendbar
Wirkung ausserhalb Rechtsgebiet (extraterritorial)	X	X	X		X
Sanktionen/Bussgelder Richtet sich an:	Bis Euro 10 Mio. od. 2% vom globalen Umsatz Unternehmen	Bis CHF 250K persönlich			
Datenschutzerklärung für personenbezogene Daten (insbesondere Profiling)	Opt-in	Info, Kenntnis			
Datenschutzbeauftragter	obligatorisch	freiwillig			
Notwendige Cookies anonym + personenbezogen	Info	Info	Info	Info	
Präferenz Cookies anonym + personenbezogen			Opt-In**	Info	
Statistische Cookies anonym + personenbezogen			Opt-In**	Info	
Marketing Cookies anonym und personenbezogen, 3rd party			Opt-In**	Info	
Werbe-Mailings postalisch	Opt-In	Info			
Call Center-Anrufe: Pflicht zur Anzeige einer im Telefonverzeichnis registrierten Rufnummer					Opt-out: Kein Eintrag im Tel-Verzeichnis ausreichend***
E-Mail, Newsletter: ergibt sich nicht aus Datenschutz, sondern aus Wettbewerbsrecht	Double-Opt-in aufgrund der Beweispflicht				confirmed Opt-In*
Definiert Gültigkeit einer Einwilligung	X	X	Vgl. DSGVO		X

*ähnlich wie bei der DSGVO kann es sein, dass sich aus den Anforderungen an die Informationspflichten bei einem Unternehmen das Double-Opt-in faktisch von selbst ergibt, weil mit confirmed Opt-in der Beweis nicht erbracht werden kann.

Copyright Mayoris 2021

**ergibt sich nicht aus der aktuellen Richtlinie, sondern aus Richterrecht im Jahr 2020; wird in der Neuauflage der ePrivacy-Richtlinie aber vermutlich übernommen.
*** Bei Geschäftsbeziehung ist Telefonmarketing ohne Opt-out möglich; viele Mobil-Nummern sind im Telefonverzeichnis nicht eingetragen, was dem Opt-out gleichgestellt ist.

Aufgrund der veränderten Anforderungen an Cookie-Einwilligungen und für die systematische Befolgung von Opt-in Kriterien beim E-Mail Versand sind grössere Unternehmen dazu übergegangen, ein sogenanntes „Trust-Centers“ nach aussen, bzw. eine „Customer Management Platform“ zwecks interner Datenverwaltung für die Nutzer ihrer Webseite und für alle Kunden einzurichten. Cookie-Kategorien werden definiert, der Verwendungszweck erklärt, Cookie-Anbieter aufgelistet. Der Nutzer kann einzelne Cookie-Kategorien akzeptieren oder nach wie vor die gesamten Cookies mit einem Klick akzeptieren („alle akzeptieren“), was im Sinne des intuitiven Benutzerverhaltens nach wie vor im Vordergrund stehen und von vielen Konsumenten gewählt wird, ohne zu überlegen. Technisch werden die Daten auf einer Customer Data Plattform gespeichert, was dem Anbieter ermöglicht, Cookie-Permissions und E-Mail Opt-Ins über die digitalen Kanäle zu verknüpfen und das Profiling je nach Auswahl des Nutzers über alle Kanäle zu gestalten. Das ist mit der DSGVO und dem neuen DSG sehr ratsam und für ein personalisiertes Marketing im Sinne der Marketing Automation ein nicht zu unterschätzender Wettbewerbsvorteil. Wer systematisch alle Permissions der Nutzer und Kunden über möglichst viele digitale Kanäle einholt, ist nicht nur „compliant“ mit dem Gesetz, sondern kann in Zukunft die Möglichkeiten einer umfassenden Datenbasis viel besser nutzen als Unternehmen, welche diesem Thema nicht die notwendige Aufmerksamkeit schenken. Gutes Consent Management zahlt sich aus. Zur Erinnerung: Die DSGVO wurde ursprünglich gegen die grossen Datenkraken (auch GAFA genannt: Google, Apple, Facebook, Amazon) aus den USA geplant, um ihnen den ungezügelten und unkontrollierten Umgang mit personenbezogenen Daten zu entziehen. Diese haben alle Hebel in Bewegung gesetzt, um den Datenschutz in der EU zu respektieren, denn ihr Geschäftsmodell besteht aus dem intelligenten und personalisierten Umgang mit (kostenlosen) Konsumenten-Daten. Dagegen tun sich viele kleineren Unternehmen schwer, die teilweise unklaren und in der Umsetzung kostspieligen Vorschriften der DSGVO zu befolgen.

Bild: Ausschnitt aus einer Consent-Abfrage, in welchem die Cookies einzeln als Basis eines umfassenden Consent Managements verwaltet werden.

Copyright Mayoris 2021

Fazit:

Was macht demnach ein Unternehmen, das internationale Märkte bedient? Es hält sich strikt an die DSGVO, ignoriert das DSG weitgehend oder erfüllt es längst, weil die DSGVO bereits in Kraft ist und in den meisten Fällen strenger ist. Der Blick auf die Sanktionen bestätigt die Bedeutung der DSGVO, denn dort geht es um Bussgelder in der Höhe von 10 Mio. Euro oder bis 2% des globalen Jahresumsatzes. Die Schweiz kennt kein Bussgeld für Unternehmen, sondern im neuen DSG nur persönliche Sanktionen bzw. Bussen an die Adresse von Manager bis CHF 250'000. Mit dem Umfang der Sanktionen aus der DSGVO ist die Risikoabwägung für den CEO in Bezug auf die Einhaltung des Datenschutzes zugunsten der Gesetzestreue eindeutiger geworden. Compliance lohnt sich aber nicht nur aus rechtlichen Gründen, denn ein möglicher Reputationsschaden als Folge eines schweren Verstosses gegen den Datenschutz mag sich noch viel gravierender auswirken als ein Rechtsverstoss. Oder sind wir im Umgang mit personenbezogenen Daten schon so liederlich geworden, dass ein Shitstorm von heute keinen negativen Einfluss auf den Geschäftsgang von morgen haben wird? Die Volksseele ist bei der Verletzung von moralischen Standards mit erhöhtem Schutzbedarf wie Menschenrechte oder Gesundheit doch noch sensibler als bei der Verletzung des Datenschutzes, leider.

Der Schweiz ist mit dem neuen DSG jedenfalls kein grosser Wurf gelungen; schon gar nicht mit einem eigenständigen Gesetz vier Jahre nach dem Inkrafttreten der DSGVO. Wir können uns zwar versichern, dass wir nicht in allen Fällen den Anforderungen der DSGVO erlegen sind und unseren eigenen Weg gehen. In der Umsetzung kann dies aber bei internationalen Unternehmen nur für Unverständnis sorgen. Im Vordergrund sollte nicht der Widerstand gegen die grosse Staaten-gemeinschaft stehen, sondern einheitliche Vorschriften, Rechtssicherheit und die Basis für neue Geschäftsmodelle, welche sich aus den Chancen des Datenschutzes ergeben. Diesen möglichen Wettbewerbsvorsprung aus einer strengen Regulierung haben wir längst verspielt. Investieren sollten Unternehmen trotzdem und langfristig in den Aufbau eines umfassenden Datenumfeldes, ein unschätzbares Asset. Das braucht viel Zeit und Geld. Befolgen Sie die DSGVO und andere Vorschriften in der EU, und gut ist; das neue DSG ist aus der internationalen Perspektive im Wesentlichen eine unnötige Randnotiz.

Copyright Mayoris 2021