



*Vielen Dank, dass Sie unseren Artikel heruntergeladen haben.
Wir wünschen Ihnen viel Vergnügen beim Lesen!*

Datenschutz

Das neue DSG in der Schweiz im Vergleich mit der DSGVO in der EU

Der vorliegende Artikel beschreibt die Gemeinsamkeiten und Unterschiede zwischen dem neuen Datenschutzgesetz in der Schweiz (ab September 2023) und der DSGVO der Europäischen Union (seit Mai 2018), bezieht sich dabei auch verwandte Gesetze wie das Gesetz über den unlauteren Wettbewerb (für E-Mail Opt-Ins) und das Fernmeldegesetz (für die Einwilligung zu Cookies; in der EU ePrivacy).

Der Inhalt beschränkt sich aber auf die Regelung dieser Einwilligungspflichten für Marketing-Kommunikation, beschreibt also nicht alle Änderungen, welche durch das DSG verursacht werden. Allerdings hält der Autor nicht mit Kritik am DSG zurück, das sich zwar mit grosser zeitlicher Verzögerung an die DSGVO anlehnt, aber doch – wie in der Schweiz üblich – anders sein will, was für die internationale Wirkung des Datenschutzes und die angestrebte Rechtssicherheit für Unternehmen wenig sinnvoll ist.



Gliederung

Einleitung

1. DSGVO seit 2018 vs. das neue DSG ab September 2023
2. ePrivacy Richtlinie (2009) und ihre Neuauflage vs. Fernmeldegesetz FMG Art. 45c lit. b in der Schweiz (2006)
3. Wettbewerbsrecht in der EU vs. das Gesetz über den unlauteren Wettbewerb UWG Art. 3 Abs. 1, lit. o in der Schweiz
4. Tabelle mit Rechtlichen Anforderungen
5. Annex: Trust Center, Customer Management Plattform, Consent Management
6. Fazit



Einleitung

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 die Lösung einiger juristischer Probleme erleichtern würde; wenn eben das Halbwissen der Entscheider nicht wäre. Und in einigen Passagen 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 dem Richter in Form von Urteilen, ein häufig begangener Weg in der EU und der Schweiz. Datenschutz ist also auch und vor allem Politik.

DSGVO seit 2018 in Kraft

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 im September 2023, 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 kundzutun? 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. DSGVO seit 2018 vs. das neue DSG ab September 2023

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 einem 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, weil diese Daten nicht einer Person zugeordnet werden können.

Der Datenschutz reguliert die Nutzung personenbezogener Daten.

Grundsätzlich bedarf für die Nutzung von personenbezogenen Daten zu Werbezwecken gemäss dieser Verordnung einer expliziten und freiwilligen Einwilligung und eines jederzeitigen Widerspruchsrechts 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 hier 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 personenbezogenen Daten umgehen will (Zweckbindung, z.B. personalisierte Werbung für Marketingzwecke). 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 für Tracking und Profiling explizit angefordert werden.

Dieses Häklein muss zum Nutzer oder Kunden auf einer Datenplattform abgelegt werden, für die zentrale Übersicht über die zukünftige Verwendung bis zum Widerruf und für die Informationspflicht dem Berechtigten gegenüber. Informations- und Auskunftspflichten über die eingeholte „Permission“ und damit die rechtmässige Nutzung von personenbezogenen Daten sind im neuen DSG ähnlich streng wie in der DSGVO. Ein „confirmed opt-In“ für die Nutzung von E-Mail-Adressen (d.h. einfache Bestätigung einer Anmeldung ohne doppelte Bestätigung, vgl. weiter unten) lässt sich schwer beweisen.

Was macht jetzt ein international tätiges Unternehmen in der Schweiz mit der DSG?

Es erstellt eine DSGVO-konforme DSE inkl. positivem Double-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 personenbezogenen 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.

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; bisher ohne explizite Einwilligung und nur im anonymisierten Bereich, nota bene. Diese Cookies sind die technische Grundlage für eine milliarden schwere 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.



2. ePrivacy Richtlinie (2009) und ihre Neuauflage vs. Fernmeldegesetz FMG Art. 45c lit. b in der Schweiz (2006)

Neue Regeln für die Verwendung von Cookies

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 1-2 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 irrt durch die Institutionen (Stand Ende 2022). 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



Gerichte springen in die Bresche und regeln bei Cookies, was der Gesetzgeber versäumt hat

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 die meisten 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 Zulassung von 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.



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.

Double-Opt-In oder Confirmed Opt-In

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 Informations- bzw. der Beweispflicht ohne Double Opt-In nachkommen kann. 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.





4. Tabelle mit Rechtlichen Anforderungen

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	n DSG 2023	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	Bis Euro 10/20 Mio. od. 2/4% vom globalen Umsatz Unternehmen	Bis CHF 250K persönlich			
Richtet sich an:					
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 + personenbezogen			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.

**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.



5. Annex: Trust Center, Customer Management Plattform, Consent Management

Trust Center und Customer Management Plattform

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 Plattform“ 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 steht und von vielen Konsumenten ohne zu überlegen gewählt wird.

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.





Consent Management

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.

Diese Webseite verwendet Cookies

Wir verwenden Cookies, um Inhalte und Anzeigen zu personalisieren, Funktionen für soziale Medien anbieten zu können und die Zugriffe auf unsere Website zu analysieren. Außerdem geben wir Informationen zu Ihrer Verwendung unserer Website an unsere Partner für soziale Medien, Werbung und Analysen weiter. Unsere Partner führen diese Informationen möglicherweise mit weiteren Daten zusammen, die Sie ihnen bereitgestellt haben oder die sie im Rahmen Ihrer Nutzung der Dienste gesammelt haben.

ALLE COOKIES ZULASSEN

Auswahl erlauben **Nur notwendige Cookies verwenden**

☒ Notwendig ☐ Präferenzen ☐ Statistiken ☐ Marketing [Details ausblenden](#)

Cookie-Erklärung **Über Cookies**

Marketing-Cookies werden verwendet, um Besuchern auf Webseiten zu folgen. Die Absicht ist, Anzeigen zu zeigen, die relevant und ansprechend für den einzelnen Benutzer sind und daher wertvoller für Publisher und werbetreibende Drittparteien sind.

Name	Anbieter	Zweck	Ablauf	Typ
__hssc	Hubspot Inc	Erfasst statistische Daten zu Website-Besuchen des Benutzers, wie z. B. die Anzahl der Besuche	1 Tag	HTTP

Die Cookie-Erklärung wurde das letzte Mal am 24.11.20 von [Cookiebot](#) aktualisiert

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



6. Fazit

Was macht demnach ein Unternehmen, das internationale Märkte bedient?

Es hält sich strikt an die DSGVO, ignoriert bei den oben genannten Anforderungen 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 10/20 Mio. Euro oder bis 2/4% des globalen Jahresumsatzes (DSGVO Art. 83; je nach Verstoss).

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 direkter 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.

Das DSG ist fünf Jahre nach der DSGVO kein grosser Wurf

Der Schweiz ist mit dem neuen DSG jedenfalls kein grosser Wurf gelungen; schon gar nicht mit einem eigenständigen Gesetz fünf 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 Staatengemeinschaft 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.

Vielen Dank, dass Sie unseren Artikel heruntergeladen haben.

Hat dieser Artikel Ihr Interesse geweckt?

Nehmen Sie Kontakt mit uns auf.

Weitere Themen finden Sie auf unserer [Website](#).

Ihr Ansprechpartner informiert Sie gerne:

Urs Thüring
CEO | Partner



+41 41 783 87 19



urs.thuering@mayoris.com



Rotkreuz und Zürich

