Was bringt die Revision des Schweizer Datenschutzgesetzes mit sich, und wie hängt dies mit der DSGVO und der ePrivacy-Verordnung zusammen?

Das E-DSG und sein regulatorisches Umfeld

«Freiheit und Selbstbestimmung in der digitalen Welt hängen ganz entscheidend davon ab, dass wir die Souveränität über unsere persönlichen Daten behalten»

Heiko Maas, 2015

pwc

Inhalt

Die Revision des Schweizer Datenschutzgesetzes und sein regulatorisches Umfeld

Zusammenfassung

Der Bundesrat hat im September 2017 den Entwurf eines totalrevidierten Datenschutzgesetzes (E-DSG) präsentiert, das mehr Transparenz schaffen und die Mitbestimmungsrechte der Personen[1], über die Daten bearbeitet werden, stärken soll. Der Entwurf lehnt sich stark an die Datenschutz-Grundverordnung (DSGVO) an, die seit dem 25. Mai 2018 anwendbar ist. Eng damit verknüpft ist die ePrivacy-Verordnung, die ebenfalls von der EU verabschiedet wurde (aber noch nicht in Kraft ist) und als Lex Specialis die Privatsphäre im Internet und bei der elektronischen Kommunikation regeln soll. Diese Publikation zeigt auf, was Schweizer Unternehmen von der Revision des DSG erwarten können, inwiefern sie sich von der DSGVO unterscheidet und welche Herausforderungen die Implementierung birgt.

1 Siehe Glossar

1. Überblick über die aktuelle Situation des Datenschutzes in der Schweiz

Mit der Verbreitung digitaler Technologien in den letzten drei Jahrzehnten sind auch die Anforderungen an den Datenschutz fortlaufend gestiegen. Die im Mai 2018 in Kraft gesetzte europäische Regulierung DSGVO sowie die erwartete ePrivacy-Verordnung (die voraussichtlich 2020 in Kraft tritt) haben zum Ziel, die Persönlichkeit und die Freiheiten von Datensubjekten zu schützen. Die Kommunikations- und Vertriebskanäle entwickeln sich rasant, und die Unternehmen sind in immer grösserem Mass in der Lage, persönliche Daten zu sammeln und zu verarbeiten. Deshalb stellen die neuen Regulierungen den Schutz der Datensubjekte, über die Daten bearbeitet werden, ins Zentrum.

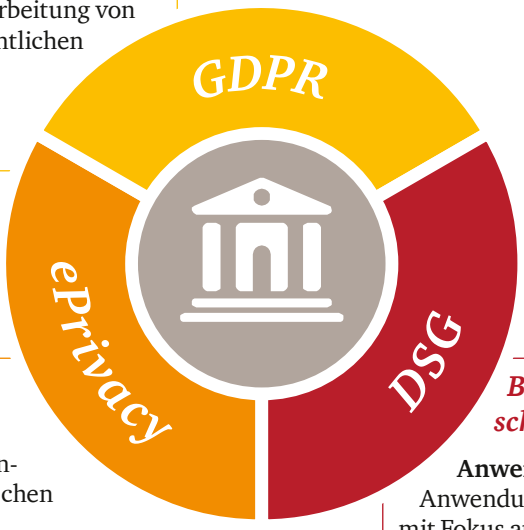
Der Bundesrat hatte bereits 2011 eine Revision des 1992 in Kraft getretenen Datenschutzgesetzes beschlossen. Nachdem die DSGVO im Jahr 2016 veröffentlicht wurde, hat der Schweizer Nationalrat entschieden, das Datenschutzgesetz unter Berücksichtigung der DSGVO zu revidieren. Betroffen davon sind alle Schweizer Unternehmen, die personenbezogene Daten bearbeiten (z.B. von Kunden oder von Mitarbeitenden). Darunter fällt jeder Umgang mit Personendaten, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten. Der Anwendungsbereich ist sehr breit, weshalb es nur wenige Unternehmen in der Schweiz geben dürfte, die von der Revision nicht betroffen sind.

Was die neuen Gesetze zum Schutz der Personendaten für Schweizer Unternehmen konkret bedeuten, welche Massnahmen zu ergreifen sind und was es bei der bevorstehenden Entwicklung zu beachten gilt, wird in den folgenden Kapiteln dargestellt. Dieses Dokument fokussiert in erster Linie auf das E-DSG und darauf, welche Abhängigkeiten zur DSGVO bestehen.

DSGVO

Anwendungsbereich:
EU-Verordnung mit Fokus auf den allgemeinen Datenschutz im Zusammenhang mit der Verarbeitung von Personendaten im privaten und im öffentlichen Sektor

Status: Ratifiziert und in Kraft
In Kraft ab/seit: 25. Mai 2018



ePrivacy

Anwendungsbereich:
EU-Verordnung mit Fokus auf den Datenschutz im Internet und in der elektronischen Kommunikation

Status: Entwurf in Ratifizierung beim EU-Parlament und beim Europarat
In Kraft ab/seit: 2020 (voraussichtlich)

Bundesgesetz über den Datenschutz (DSG)

Anwendungsbereich:
Anwendungsbereich: Schweizer Bundesgesetz mit Fokus auf den allgemeinen Datenschutz im Zusammenhang mit der Verarbeitung von Personendaten im privaten und im öffentlichen Sektor

Status: Entwurf in Ratifizierung bei der Schweizer Bundesversammlung
In Kraft ab/seit: 2019 (voraussichtlich)

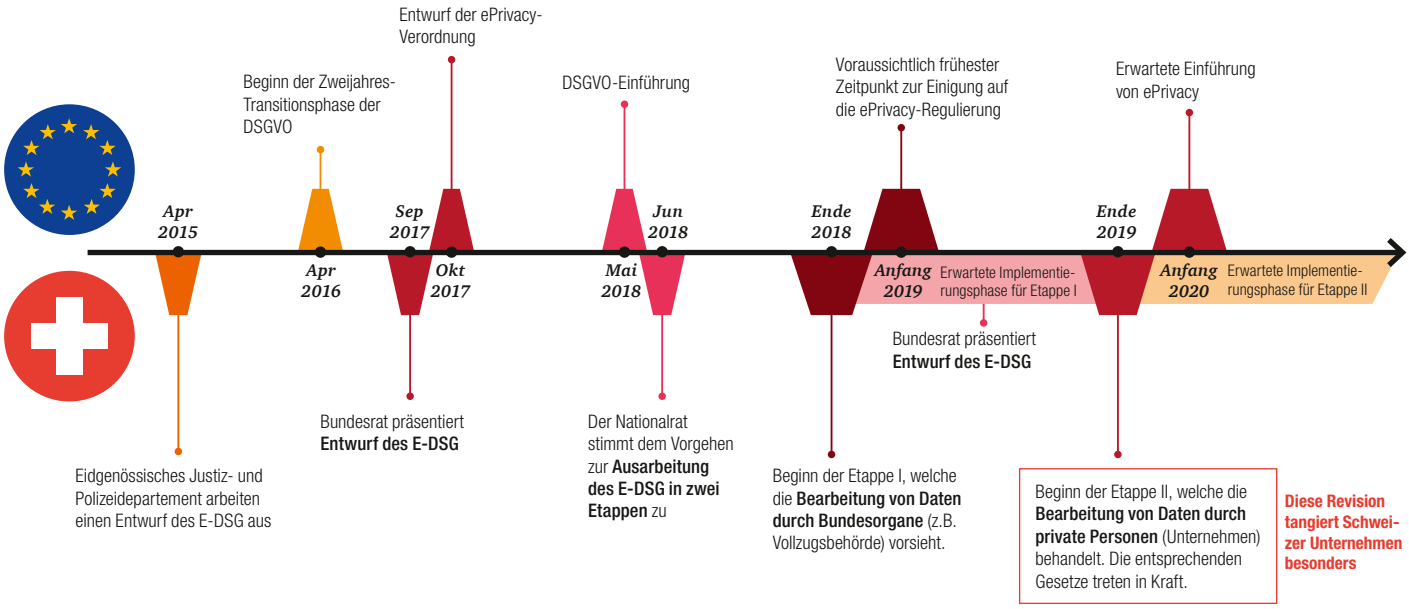
2. Die Revision des Schweizer DSG

Das revidierte Datenschutzgesetz soll das bestehende Schweizer Datenschutzgesetz (DSG) ersetzen. Es soll dem technologischen Fortschritt Rechnung tragen und den Schutz persönlicher Daten von natürlichen Personen[2] stärken. Die Revision wird sich inhaltlich an die DSGVO anlehnen.

2.1 Der Zeitplan der Totalrevision

Ursprünglich war beabsichtigt, mit der Totalrevision des DSG in einem einzigen Schritt sowohl den Verpflichtungen aus dem Schengen-Vertragswerk nachzukommen als auch die Anforderungen der DSGVO zu erfüllen. Streng genommen muss die Schweiz allerdings nur diejenigen datenschutzrechtlichen Bestimmungen übernehmen, die aus den Schengen-Verträgen resultieren. Damit sie jedoch als ein Drittstaat mit einem dem EU-Level vergleichbaren Datenschutzniveau anerkannt wird, sollen die relevanten Punkte dennoch auch an das europäische Recht angepasst werden. Andernfalls besteht das Risiko, dass der Austausch von Daten zwischen der Schweiz und der EU durch Auflagen erschwert wird.

Mittlerweile wurde entschieden, die Totalrevision in zwei Etappen aufzuteilen. So könne die Umsetzung von EU-Recht, die aufgrund der Schengen-Verträge binnen einer bestimmten Frist vollzogen werden muss (Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts), vorab beraten werden. Anschliessend könne die Totalrevision des Datenschutzgesetzes «ohne Zeitdruck» angegangen werden. Für Schweizer Unternehmen ist entsprechend insbesondere die zweite Etappe relevant. Sie soll voraussichtlich bis Ende 2020 abgeschlossen werden.



2.2 Das E-DSG und worin es sich vom aktuellen DSG unterscheidet

Die vorliegenden Ausführungen basieren auf dem im September 2017 präsentierten Entwurf des Datenschutzgesetzes (E-DSG). Das E-DSG stärkt viele bestehende Rechte von betroffenen Personen, führt diverse neue Anforderungen ein und schränkt in einigen wenigen Fällen existierende Artikel ein. Der neue Entwurf unterscheidet sich in den folgenden Kernpunkten von der bisherigen Gesetzgebung (DSG):

Schutzobjekt: natürliche Personen

Während das DSG aus dem Jahr 1992 den Schutz von Daten sowohl natürlicher als auch juristischer Personen regelte, beschränkt sich das E-DSG auf Daten natürlicher Personen.

Sanktionen

Im Gegensatz zum DSG definiert der Entwurf für den neuen Gesetzestext klare Sanktionen. So können Individuen, die das E-DSG vorsätzlich verletzen, mit einem Bussgeld von bis zu CHF 250'000 bestraft werden.

2 Siehe Glossar

Besonders schützenswerte Personendaten

Das E-DSG erweitert die Auflistung von Daten, die unter diese Kategorie fallen. So werden genetische sowie biometrische Daten (z.B. Fingerabdruck), die eine natürliche Person eindeutig identifizieren, neu ebenfalls berücksichtigt.

Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen

Datenverarbeitern werden erhöhte Sorgfaltspflichten auferlegt, die zudem genauer definiert sind. So müssen Datenverantwortliche und -verarbeiter bereits bei der Planung der Datenbearbeitung das Risiko einer Persönlichkeitsverletzung durch angemessene Massnahmen verringern. Zudem sind sie verpflichtet, durch Voreinstellungen zu gewährleisten, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.

Datenschutz-Folgenabschätzung

Datenverantwortliche oder -verarbeiter sind gemäss dem E-DSG verpflichtet, eine Datenschutz-Folgenabschätzung vorzunehmen, wenn die vorgesehene Datenbearbeitung zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt. Dabei müssen sowohl Risiken als auch geeignete Massnahmen umschrieben werden.

Meldung von Verletzungen des Datenschutzes

Datenverantwortliche haben dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) im Falle einer Datenschutzverletzung so rasch wie möglich Meldung zu erstatten, wenn ein grosses Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht. Sofern erforderlich, sind auch die betroffenen Personen zu informieren.

2.3 Wie unterscheidet sich das E-DSG von der DSGVO?

Das E-DSG orientiert sich stark an der DSGVO, die im Mai 2018 in Kraft getreten ist. Dies ist in wirtschaftlicher Hinsicht essenziell, da ein Datenaustausch mit Unternehmen und Staatsorganen aus Ländern, die nicht über einen vergleichbaren Schutz von Personendaten verfügen, nur unter erschwerten Bedingungen durchgeführt werden kann.

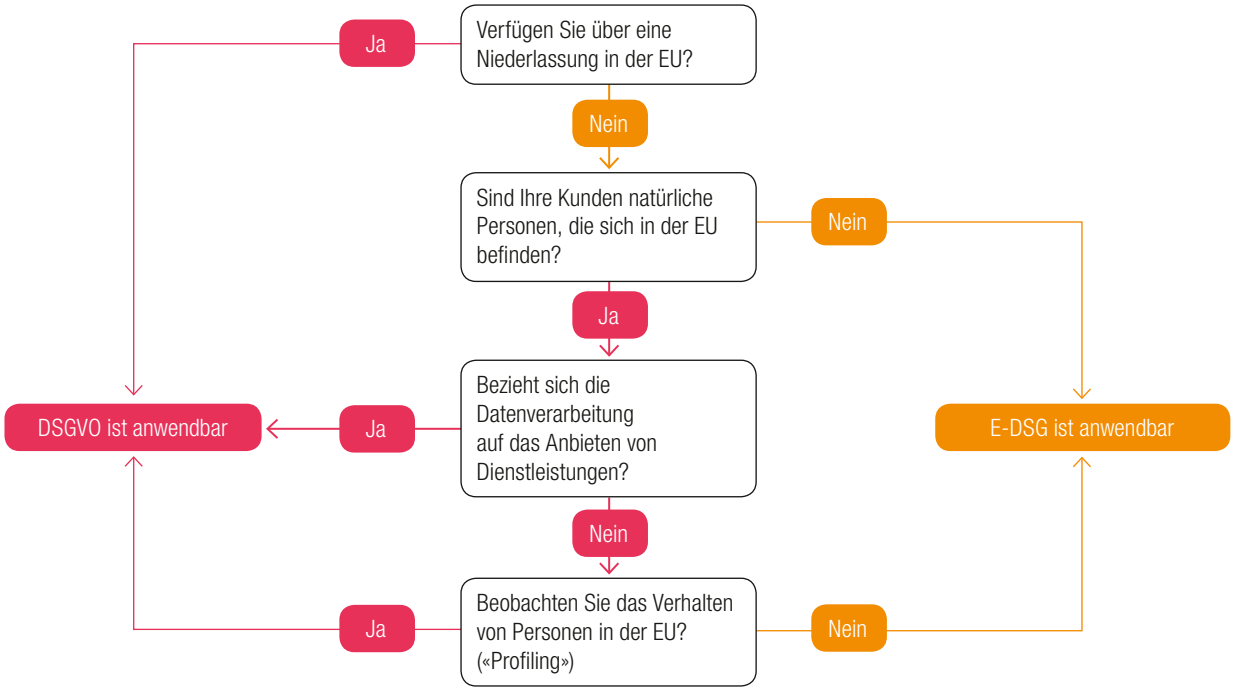
Obwohl das E-DSG inhaltlich an die DSGVO angelehnt ist, gibt es doch Unterschiede. Die wichtigsten sind nachstehend aufgeführt:

Hauptkriterien		**DSGVO**	**E-DSG**
Kategorien	**Spezifizierung**		
Allgemeine Vorschriften	**Geografische Reichweite**	Einheiten in der EU und/oder Einheiten, die Daten von natürlichen Personen innerhalb der EU bearbeiten	Einheiten, die in der Schweiz ansässig sind
	Bussgelder	Bis zu EUR 20 Millionen oder 4% des Umsatzes (der höhere der beiden Beträge definiert die Maximalstrafe)	Bis zu CHF 250'000 (Einzelpersonen)
Grundsätze der Bearbeitung von persönlichen Daten		Die Verarbeitung von Personendaten ist grundsätzlich verboten, es sei denn, es besteht eine rechtliche Grundlage	Die Bearbeitung von Personendaten ist grundsätzlich erlaubt, es sei denn, die Persönlichkeit einer betroffenen Person wird verletzt
		Die folgenden Bearbeitungsprinzipien sollen für alle persönlichen Daten, die verarbeitet werden, berücksichtigt werden: 1. Zweckbindung 2. Datenminimierung 3. Richtigkeit 4. Speicherbegrenzung 5. Integrität und Vertraulichkeit 6. Rechenschaftspflicht	Die folgenden Bearbeitungsprinzipien sollen für alle persönlichen Daten, die verarbeitet werden, berücksichtigt werden: 1. Zweckbindung 2. Datenminimierung 3. Richtigkeit 4. Speicherbegrenzung 5. Integrität und Vertraulichkeit
Verzeichnis von Verarbeitungstätigkeiten		Führung eines Dateninventars bei DSGVO und E-DSG	
Datenschutz-verletzung	**Fristen**	Innerhalb von 72 Stunden	«so rasch wie möglich»
	Empfänger	Aufsichtsbehörde und unter bestimmten Bedingungen die betroffenen Personen	Schweizer Aufsichtsbehörde und auf deren Anfrage die betroffenen Personen
Datenschutzrechte		Ein Datensubjekt hat das Recht auf Übertragbarkeit der persönlichen Daten	Es besteht kein Recht auf Übertragbarkeit
		1. Recht auf Berichtigung ungenauer personenbezogener Daten 2. Recht auf Auskunft 3. Recht auf Einschränkung der Verarbeitung 4. Recht auf Vergessenwerden – Löschung 5. Widerspruchsrecht 6. Recht, die Einwilligung zu widerrufen 7. Recht, nicht Gegenstand einer ausschliesslich automatisierten Verarbeitung zu sein	Nur Auskunftsrecht (die restlichen Rechte sind nicht explizit im E-DSG ausformuliert, sind aber durch das Schweizer Rechtssystem anderweitig geregelt und durchsetzbar

3. Was die Revision für Schweizer Unternehmen bedeutet

3.1 Entscheidungsbaum – wo befindet sich Ihr Unternehmen?

Für ein Schweizer Unternehmen gelten, je nach seinen spezifischen Marktaktivitäten, entweder ausschliesslich die Vorschriften des E-DSG, oder es gelangen sowohl das E-DSG als auch die DSGVO zur Anwendung. Die nachfolgende Grafik gibt Ihnen einen Überblick, welche Regelwerke für Ihr Unternehmen relevant sind.



3.2 Herausforderungen bei der Implementierung des neuen Datenschutzgesetzes

PwC begleitete über mehrere Jahre zahlreiche Unternehmen in der Schweiz und der EU bei der Analyse, der Konzeptdefinierung und der Implementierung der Anforderungen der DSGVO. Parallel führte PwC bei diversen Finanzdienstleistungsunternehmen eine Benchmarking-Analyse durch, um Markteinblicke in die Design- und Umsetzungsfortschritte bei der Implementierung der DSGVO zu erhalten.

Wir haben folgende Bereiche beobachtet, in denen die Marktakteure Fortschritte im Zusammenhang mit der DSGVO zu verzeichnen haben:

1. **Management der persönlichen Daten und Bildung eines Verzeichnisses von Verarbeitungstätigkeiten**

   Die Herausforderung beim Management der persönlichen Daten besteht darin:

   a) ein Verzeichnis von Verarbeitungstätigkeiten zu bilden und

   b) das Verzeichnis in die Geschäftstätigkeit zu integrieren und aktuell zu halten.

   Je nach Geschäftsmodell und Diversität der Datenlandschaft bestehen nach wie vor folgende Herausforderungen, um das Verzeichnis von Verarbeitungstätigkeiten zu definieren:

   1. Persönliche Datenattribute/Kategorien zu identifizieren und ihren Zweck sowie die rechtlichen Grundlagen festzulegen, um eine Taxonomie persönlicher Daten zu bilden. Zusätzlich steht im Zentrum der Taxonomie, das «Business As Usual – BAU» aufrechtzuerhalten, indem Prozesse und Kontrollen implementiert werden. Sie sollen sicherstellen, dass bei jeglicher Änderung in der Verarbeitung persönlicher Daten innerhalb der Geschäftstätigkeit die Taxonomie reflektiert wird.

2. Verzeichnisse aktuell zu halten, sodass Änderungen im System in den Verarbeitungsverzeichnissen reflektiert werden.
3. Personendaten, die an Dritte transferiert werden, zu identifizieren und in der Taxonomie zu reflektieren. Auch dabei sind die Aufrechterhaltung und die Integration des BAU eine zentrale Herausforderung für Finanzdienstleister.

2. Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen

Datenschutz durch Technikgestaltung bezieht sich auf organisatorische und technische Massnahmen, die implementiert werden, um den Grundsätzen der Regulierung zu entsprechen. Dabei ist es essenziell, die Rechte betroffener Personen vor Beginn und während der Bearbeitung personenbezogener Daten zu schützen. Datenschutz durch datenschutzfreundliche Voreinstellungen besagt, dass als Standardeinstellung nur diejenigen persönlichen Daten gesammelt und verarbeitet werden dürfen, die für einen bestimmten Zweck der Verarbeitung erforderlich sind. Neue Produkte oder Änderungen an bestehenden Produkten bedürfen einer Risikobewertung. Aber auch bei vorhandenen Daten und Prozessen muss Klarheit herrschen, welche Daten zu welchem Zweck verwendet werden.

Für die Überprüfung, ob der Grundsatz der Datenminimierung eingehalten wird, wird antizipiert, einen Benchmark aus der Industrie zu verwenden. Zurzeit gibt es keinen einheitlichen Benchmarking-Service. Hier wird aus der Erfahrung mit der DSGVO auf externe Berater und Service-Provider verwiesen, die bereits Erfahrung in der Industrie haben und solche Benchmarks qualitativ zur Verfügung stellen können.

Eine weitere Herausforderung sind, wie sich bei der DSGVO gezeigt hat, das Design und die Implementierung von Konzepten, Policen und Kontrollen, die die Aktualisierung von Sicherheitsstandards und -plänen im Sinne einer kontinuierlichen Einhaltung der DSGVO-Grundsätze gewährleisten. Diese Herausforderung ist beim E-DSG ebenfalls zu erwarten.

Besonders bei der Definition der Anforderungen und bei der Ausführung des E-DSG ist darauf zu achten, dass bei den zu implementierenden Massnahmen ein konkreter «Audit-Trail» vorgewiesen wird, um die kontinuierliche Einhaltung der Regulierung sicherzustellen.

Gerade das Thema Cybersicherheit spielt eine immer wichtigere und ergänzende Rolle im Datenschutz. Die technischen und organisatorischen Massnahmen zum Schutz der Daten und die damit einhergehende Compliance mit den Datenschutzgesetzen lassen sich nur mithilfe eines gesicherten IT-Systems implementieren und einhalten. IT-Sicherheit wird somit zu einem festen Bestandteil, wenn es darum geht, der Gesetzgebung zu entsprechen. Der Compliance Officer allein wird die Aufgabe nicht mehr bewältigen können. Er benötigt die Unterstützung und die Zusammenarbeit vonseiten des IT-Spezialisten.

Datenschutzrechte für Datensubjekte

Je nach Geschäftsmodell, Kundensegmentierung und Risikobereitschaft lassen sich die Prozesse zur Einhaltung der Rechte der Datensubjekte in unterschiedlichem Ausmass automatisieren. Die Erfahrung mit der DSGVO zeigt, dass bestehende Lösungen wie E-Banking verwendet werden können, um das Auskunftsrecht spezifisch mit einer automatischen Vorgehensweise abzudecken.

Unternehmen, die die Anfragen der Datensubjekte manuell bearbeiten wollen, bauen in der Regel eine zentrale Anlaufstelle auf, die alle Anfragen auffängt und behandelt. Ebenso kann die Tätigkeit bestehender Einheiten, die sich üblicherweise mit Beschwerden von Kunden befassen, ausgeweitet werden, um Datenschutzanfragen abzudecken.

Die Erfahrung zeigt, dass ein grosser Teil der Firmen derzeit kaum durchgehende Prozesse etabliert haben, die dem Umgang mit den erweiterten Datenschutzanforderungen sowie den Anfragen der Datensubjekte Rechnung tragen. In der Regel empfiehlt es sich, je nach Automatisierungsgrad Arbeitsgruppen zu erstellen und auszubilden, um allgemeine Datenschutzanfragen bezüglich DSGVO, E-DSG und ePrivacy abzufangen und in einem einheitlichen Format zu beantworten.

Ein Weg, die Beantwortung der Anfragen möglichst kosteneffizient zu gestalten, sind standardisierte Berichte, die eigens als Antwort für betroffene Personen entwickelt werden. Auch die Erfahrung mit der DSGVO zeigt, dass solche Berichte einen effizienten Antwortprozess ermöglichen. Die Voraussetzung dafür ist allerdings eine Abgrenzung der Datenstruktur (strukturierte vs. unstrukturierte Daten). Auch Umfang und Integration der Metadaten und der Transaktionsdaten im Bericht sind unbedingt in Betracht zu ziehen.

Der Umfang der erwarteten Anfragen von betroffenen Personen ist nicht nur anspruchsvoll zu prognostizieren, sondern hängt zudem von zahlreichen Schlüsselentscheidungen von Unternehmen ab. Die Erfahrung mit der DSGVO zeigt aber, dass mit regelmässigen Anfragen zu rechnen ist, wobei beim Go-Live ein Peak besteht.

3. Spezifische Herausforderungen zur Compliance mit Anfragen zur Datenlöschung («right to be forgotten») und Ausbau der Löschungskapazitäten für Prinzipien der Speicherbegrenzung

3.1 Compliance mit Anfragen zur Datenlöschung

Das Recht auf Löschung ist ein absolutes Recht. Es kann allerdings nur dann ausgeübt werden, wenn die personenbezogenen Daten für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden und keine anderen Anforderungen, z.B. Archivierung, diesem Recht entgegenstehen. Unternehmen müssen somit aufzeigen können, weshalb die Daten gesammelt und verarbeitet werden und was die rechtliche Grundlage hierfür ist. Falls das Recht auf Löschung ausgeübt werden kann, müssen Unternehmen in der Lage sein, die betroffenen Daten auf Anhieb zu löschen.

In diesem Zusammenhang sehen sich Firmen häufig mit mangelnden Systemfähigkeiten konfrontiert. Bestehende Systeme sind im Hinblick auf das Löschen von Daten, die das Stammdatenintegritätsmodell unterstützen, oft eingeschränkt. Im Finanzsektor wird zwar erwartet, dass nur wenige betroffene Personen von diesem Recht Gebrauch machen werden.

Jedoch ist die Anzahl der manuell bearbeiteten Anfragen zu berücksichtigen. Auch hier spielt die Komplexität der Systemarchitektur eine Rolle, ebenso wie die Anzahl der betroffenen Systeme.

3.2 Ausbau der Löschungskapazitäten für Prinzipien der Speicherbegrenzung

Die Löschkapazitäten für Prinzipien der Speicherbegrenzung erweisen sich in der Industrie als eine grosse Herausforderung. Die meisten Institute haben eine fragmentierte Systemlandschaft und verfügen nicht über ein einheitliches und holistisches Systeminventar, das aufzeigt:

(i) welche Datenattribute in welcher Anwendung gespeichert/bearbeitet werden,

(ii) welche Datenquellen benötigt werden,

(iii) was der Zweck der Bearbeitung auf Attributebene ist und

(iv) wie und wann die Daten pro System archiviert werden.

Eine automatische Löschfunktionalität ist empfehlenswert, da die manuelle Bearbeitung mit hohen Kosten und grossem Aufwand verbunden sein kann. Für eine strategisch automatisierte Löschfunktionalität braucht es unter anderem eine klare Analyse, die Folgendes aufzeigt:

1. Welche Anwendungen welche Attribute verarbeiten.
2. Link der Attribute zur Datentaxonomie, um den Zweck und die rechtliche Grundlage festzulegen.
3. Datenquelle per Anwendung.
4. Aufräumen der Archive (Legacy).
5. Aktualisierung der Datenrichtlinien.
6. Anforderungen definieren, die sicherstellen, dass die Daten beim Archivieren in der Hauptanwendung gelöscht werden.
7. Anforderungen an das Archiv definieren, sodass die rechtliche Haltungsfrist der Attribute betrachtet und an den Zweck sowie die rechtlichen Grundlagen zur Verarbeitung/Haltung angepasst wird.
8. Anforderungen zur Löschung von persönlichen Daten im Archivsystem definieren und sicherstellen, dass zwischen Archiv und operativen Anwendungen keine Überlappungen der persönlichen Daten bestehen. Hier lohnt es sich im Hinblick auf die ePrivacy-Verordnung, nicht nur auf persönliche Daten einzugehen, sondern Daten generell zu überprüfen.

Eine Umgehungslösung, die in Erwägung gezogen werden kann, besteht darin, die Daten durch Pseudonyme zu ersetzen und zu verschlüsseln. Dadurch werden die verschiedenen Datenattribute geschützt, die möglicherweise gelöscht werden müssen.

4. Umgang mit unstrukturierten Daten

Wie im vorherigen Kapitel erwähnt, ist es zentral, beim Design und bei der Definition des Konzepts der Löschkapazitäten unstrukturierte Daten zu berücksichtigen. Wie die Erfahrung zeigt, besteht die Komplexität jedoch darin, die unstrukturierten Daten zu lokalisieren. Die Thematik unstrukturierter Daten wird als Teil der DSGVO-Themen als zentral betrachtet. Folglich sind dafür analog die Regelungen der Datensubjektrechte, Übertragungen und strukturierten Datenprozesse anzuwenden. Bestimmte Elemente von unstrukturierten Daten (z.B. Kundenlisten für Marketing-Events, die in Excel gepflegt werden) werden im Wesentlichen ausserhalb von strukturierten Systemen verwaltet. Daher ist es wichtig, den Umfang und den Ansatz frühzeitig zu definieren.

Zusätzlich zeigt die Erfahrung mit der DSGVO, dass Anfragen von betroffenen Personen zu unstrukturierten Daten manuell abgerufen und überprüft werden müssen. Die manuelle Handhabung der unstrukturierten Daten führt zu erheblichem Mehraufwand. Um diesen Aufwand zu verringern, können Teams, die Rechtsstreitigkeiten behandeln, sowie Forensikteams die Funktion im Falle von überverhältnismässigen Anfragen betroffener Personen unterstützen.

Um einen umfassenden Ansatz zu garantieren, der unstrukturierte Daten berücksichtigt, müssen die Systemlandschaft und das operative Geschäftsmodell umfänglich analysiert werden. Richtlinien, Verfahren und Verhaltensregeln müssen überarbeitet und durchgesetzt werden, um die Einhaltung der Datenschutzgrundsätze sicherzustellen. Dies erleichtert die Identifikation von unstrukturierten Daten substanziell. Ausserdem kann für eine taktische Lösung die Unterstützung durch Dritte in Betracht gezogen werden. Ergänzend dazu können Scanning-Tools implementiert werden, um Diskrepanzen in Bezug auf unstrukturierte Datenrichtlinien und -verfahren aufzuspüren oder sie auszulagern.

5. Management persönlicher Daten an Drittparteien

Personenbezogene Daten werden übertragen, wenn sie Dritten (einschliesslich konzerninterner Stellen) ausserhalb der Infrastruktur/des Systems/der Netzwerke zugänglich gemacht werden, zum Beispiel durch Zulassen der Übertragung, Offenlegung oder anderweitige Übermittlung der Personendaten. Es findet jedoch keine Übertragung statt, wenn die gesendeten oder abgefragten Daten anonymisiert sind (eine erneute Identifizierung also nicht möglich ist).

Die Herausforderung liegt hautsächlich darin, die Daten, die transferiert werden, zu identifizieren. Konkret geht es darum, festzulegen, welche Drittpartei für welchen Zweck welche Daten bearbeitet. Ausserdem braucht es im operativen Geschäftsmodell Prozesse sowie Kontrollen, um die Datenbearbeitung durch Drittanbieter und deren Verträge zu überprüfen und den Transfer von Personendaten zu überwachen. Die Prozesse sollen auch den Bezug/die Verknüpfung zu den Prozessen bezüglich der Rechte von Datensubjekten (z.B. Recht auf Löschung) herstellen.

Zusätzlich müssen bestehende Verträge mit Drittanbietern aktualisiert und neue verfasst werden, um:

1. die Art und Weise der Datenbearbeitung zu bestimmen,
2. die Art der betroffenen Daten und die Kategorien der Datensubjekte zu definieren sowie Massnahmen zur Kontrolle festzulegen, und
3. die Anforderungen und Pflichten festzulegen, falls Anfragen von Datensubjekten eintreffen.

Zusätzlich ist sicherzustellen, dass neue Richtlinien oder Gesetzesänderungen rasch berücksichtigt und eingehalten werden.

Zu bedenken ist, dass auch die Drittanbieter selbst teilweise nicht identifiziert sind, beispielsweise bei der Erstellung einer Webseite. In die Entwicklung sind typischerweise 10 bis 20, teilweise sogar über 50 verschiedene Dritt- und Werbeanbieter (z.B. für Online-Tracking) involviert, die den Unternehmen meist nicht oder lediglich teilweise bekannt sind.

6. Informations- und Cybersicherheit: Herausforderungen und Chancen

«Es geht nicht mehr darum, ob – es geht darum, wann» – diesem Satz wird man schon häufig begegnet sein. Angriffe auf die Infrastruktur grosser Organisationen sind wöchentlich in den Schlagzeilen. Das Bekenntnis, dass sich Angriffe niemals verhindern lassen und dass nie von hundertprozentiger Sicherheit ausgegangen werden darf, bedeutet, dass Unternehmen ihre Fähigkeit verbessern sollten, solche Vorfälle zu erkennen, um eine effektive und schnelle Aufdeckung und Eindämmung sowie eine angemessene Reaktion zu ermöglichen. Dazu gehört, die Datenpanne innerhalb von 72 Stunden den Aufsichtsbehörden zu melden, wie es in der DSGVO gefordert wird. Die DSGVO spricht von der sog. «Verletzung des Schutzes personenbezogener Daten»; diese ist als eine Verletzung der Sicherheit zu verstehen, die – ob nun unbeabsichtigt oder unrechtmässig – zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von verarbeiteten Daten führt. Auch der unbefugte Zugang von Unberechtigten fällt darunter. Datenpannen haben erhebliche Folgen für das Unternehmen, das Opfer eines solchen Angriffs geworden ist. Oftmals geht es um vertrauliche Informationen, die in die Hände unbefugter Dritter geraten.

Es entstehen beträchtliche finanzielle Schäden, die juristische Konsequenzen und einen anhaltenden Imageschaden nach sich ziehen. Nicht zuletzt wird der Betroffene selbst in Mitleidenschaft gezogen. Seine dem Unternehmen anvertrauten Daten kursieren im Netz und bieten eine ideale Angriffsfläche. Die Folgen eines Cyberangriffs schlagen somit hohe Wellen. Eine Organisation muss sich auf solche Vorfälle einstellen und vorbereiten.

Absolute Sicherheit lässt sich nie gewährleisten, doch zumindest ist es möglich, das Risiko eines Angriffs beträchtlich zu verringern und die Reaktionszeit zu verkürzen. Eine Organisation kann ihre Cyberresilienz stärken, d.h. ihre Fähigkeit, ihre Steuerung und ihre Reaktion schnell wieder ins Gleichgewicht zu bringen und somit zum Alltagsgeschäft zurückzukehren. Dadurch lassen sich die Schäden gering halten.

Um Cyberrisiken effektiv zu managen, müssen Unternehmen eine Reihe von Faktoren berücksichtigen. So sollten zunächst abteilungsübergreifend einheitliche Sicherheitspraktiken vorliegen, mit Fokus auf datenspezifische Schutzpraktiken. Auch Sicherheitskonzepte sollten flächendeckend in Projekte, Produkte und Prozesse eingebaut werden (Security by Design). Ein besonderes Augenmerk sollte der Bedrohungslandschaft und den Bedrohungsakteure gelten, die auf die Infrastruktur der Organisation abzielen. Solche Erkenntnisse und das daraus gewonnene Know-how sind kosteneffizient in der Sicherheitsarchitektur des Unternehmens zu operationalisieren.

Zu guter Letzt empfiehlt es sich, häufig Disaster-Recovery-Übungen durchzuführen, frei nach dem Motto «Übung macht den Meister». So wird das Personal geschult, sensibilisiert und die allgemeine Einsatzbereitschaft innerhalb der Organisation gestärkt. Grundsätzlich sollten regelmässig Schulungen stattfinden, um die Sensibilität und das Risikobewusstsein der Angestellten zu erhöhen. Die beste IT-Sicherheitsinfrastruktur allein nützt wenig, denn es bedarf nur eines Einzelnen, um Angreifern Tür und Tor zu öffnen, etwa indem er versehentlich auf einen Link klickt und Opfer einer Phishing-Attacke wird.

4. Ausblick

4.1 ePrivacy

Die ePR, die das Recht auf Achtung des Privatlebens und der Kommunikation schützt, gehört zu den Eckpfeilern der EU-Strategie für einen digitalen Binnenmarkt.

Diese neue Regelung soll «zukunftssicher» sein: Sie bezieht sich auf alle bestehenden und zukünftigen Kommunikationstechnologien. Dies wird sich jedoch störend auf die digitalen Strategien der Unternehmen auswirken, die mit Blick auf die neuen Anforderungen neu definiert werden müssen.

Die ePrivacy-Verordnung wird die bestehende ePrivacy-Richtlinie ersetzen, die 2009 überarbeitet wurde. Die neue Verordnung umfasst mehrere Anpassungen, um den aktuellen Trends auf den digitalen Märkten Rechnung zu tragen, und weitet den Anwendungsbereich erheblich aus. Das Hauptziel der ePrivacy-Verordnung besteht darin, die elektronische Kommunikation natürlicher und juristischer Personen sowie die in ihren Endgeräten gespeicherten Informationen zu schützen.

Die Eckpfeiler[3] der vorgeschlagenen Regeln für Datenschutz und elektronische Kommunikation sind:

- **Die gesamte elektronische Kommunikation erfordert ein hohes Mass an Vertraulichkeit**
  Das Anhören, Abhören, Scannen und Speichern von beispielsweise Textnachrichten, E-Mails oder Sprachanrufen ist ohne die Zustimmung des Benutzers nicht erlaubt. Der neu eingeführte Grundsatz der Vertraulichkeit der elektronischen Kommunikation gilt für gegenwärtige und künftige Kommunikationsmittel – einschliesslich aller mit dem IoT («Internet der Dinge») verbundenen Geräte.
- **Die Vertraulichkeit des Online-Verhaltens und der Geräte der Nutzer muss gewährleistet sein**
  Für den Zugriff auf Informationen eines Benutzergeräts ist die Zustimmung des Nutzers erforderlich. Benutzer müssen auch Webseiten zustimmen, die Cookies oder andere Technologien verwenden, um auf die auf ihrem Computer gespeicherten Informationen zuzugreifen oder um ihr Online-Verhalten zu verfolgen.
- **Die Verarbeitung von Kommunikationsinhalten und Metadaten erfordert die Zustimmung der betroffenen Person**
  Der Datenschutz ist somit sowohl für den Inhalt der Kommunikation als auch für die Metadaten gewährleistet – zum Beispiel, wer angerufen wurde, Zeitpunkt, Ort und Dauer des Anrufs sowie alle besuchten Webseiten.
- **Spam- und Direktmarketing-Kommunikation erfordern vorherige Zustimmung**
  Unabhängig von der verwendeten Technologie (z.B. Anrufautomaten, SMS oder E-Mail) müssen Benutzer ihre Zustimmung geben, bevor sie zu kommerziellen Zwecken kontaktiert werden. Werbeanrufer müssen ihre Telefonnummer anzeigen oder eine spezielle Vorwahlnummer verwenden, die auf einen Marketing-Anruf hinweist.

Die ePR soll die Anforderungen der DSGVO ergänzen und präzisieren. Die beiden Regelungen können jedoch Überschneidungen aufweisen. Im Konfliktfall haben die Entscheidungen gemäss ePR Vorrang vor der DSGVO (vorausgesetzt, sie verringern nicht das Schutzniveau, das natürliche Personen im Rahmen der DSGVO geniessen). Damit stellt die ePR eine Lex Specialis für die DSGVO dar. Für Schweizer Unternehmen wird die ePrivacy-Verordnung von Relevanz sein. Es ist zu empfehlen, bei der Analyse für das E-DSG Schnittstellen zur ePrivacy-Verordnung zu berücksichtigen, die auf dem vorhandenen Entwurf basieren.

Basierend auf den neuesten Informationen bestehen zusammengefasst folgende Parallelen zwischen E-DSG und ePrivacy.

3 Basierend auf Entwurf ePrivacy 5. Dezember 2017

Kriterien		DSGVO/E-DSG	Privacy
Kategorien	**Betroffene**	Natürliche Personen	Natürliche und juristische Personen
	Anwendungs-bereich	Allgemeiner Datenschutz im Zusammenhang mit der Verarbeitung personen¬bezogener Daten durch juristische Personen des privaten Sektors und gesetzgebende Körperschaften (öffentlicher Sektor)	Verarbeitung von elektronischen Daten und Informationen in Bezug auf Endgeräte
	Geografische Reichweite	Einheiten in der EU und/oder Einheiten, die Daten von natürlichen Personen innerhalb der EU bearbeiten (Schweiz: nur Einheiten, die in der Schweiz ansässig sind)	Ort, an dem der Nutzer den Dienst nutzt: Erbringung von Online-Kommunikationsdienstleistung, Online-Tracking-Technologien oder elektronisches Marketing
Personen-bezogenes Dateninventar	**Rechtmässige Grundlage**	(i) Zustimmung der betroffenen Personen, (ii) vertragliche Ver-pflichtung, (iii) Ein-haltung der gesetzlichen Verpflichtung, (iv) erforderlich, aufgrund weniger, öffentlicher und/oder berechtigter Interessen	Zustimmung ist erforderlich für jede Art von Datenverarbei¬tung, wenn die Verarbeitung über die angeforderte Dienstleistung hinausgeht (z.B. ist Bearbeitung ohne Zustimmung gestattet, wenn sie für die Kommunikationsübertragung erforderlich ist)
Grundsätze der Bearbeitung von persönlichen Daten		Recht auf Löschung (DSGVO), kein Recht auf Löschung beim E-DSG	Sofortige Löschung bestimmter Daten (z.B. Inhalte der Kommunikation), andere Daten werden nicht länger als notwendig gespeichert (z.B. Metadaten für die Rechnungsbegleichung)
		Recht auf Widerspruch gegen Verarbeitung	Recht auf Steuerung elektronischer Kommunikation inkl. Verbieten unerwünschter Kommunikation/Werbung
		Recht auf Datenzugang, Recht auf Übertragbar-keit, Recht auf Berichtigung, Recht auf Wider¬ruf von Zustimmung, Recht auf Widerspruch gegen automatisierte Ent-scheidungsfindung, Anspruch auf Ein-schränkung der Bearbeitung	Zwei Rechte sind geschützt: • Recht eines jeden Menschen auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seiner Kommunikation • Recht auf Privatsphäre und vertrauliche Kommunikation

5. Handlungsbedarf

Schweizer Unternehmen müssen zeitnah die nächsten Schritte bezüglich des E-DSG in Angriff nehmen. Dabei gilt es, von taktischen temporären Lösungen wegzukommen und zu langfristigen strategischen Lösungen überzugehen. Die Automatisierung von Anfragen muss vorangetrieben werden, um die Verarbeitung, das Case Management sowie die Löschung/Archivierung von persönlichen Daten effizienter, schneller und kostensparender zu bewerkstelligen.

Eine weitere Herausforderung stellt das Management von regulatorischen Zielkonflikten für Unternehmen dar, zum Beispiel E-DSG versus DSGVO/ePrivacy. Die Unsicherheit bezüglich der finalen Version der Regulierungen und die Kosten-Aufwand-Schätzung sind zentral, wenn es darum geht, effizient konform zu sein. Eine individuell auf das Unternehmen ausgerichtete Gap-Analyse zum E-DSG ist ein erster Schritt, um Handlungsbedarf zu ermitteln und entsprechende unternehmensadäquate Massnahmen zu entwickeln.

Mit Blick auf die ePrivacy-Richtlinien müssen Unternehmen ihren Stand analysieren und bei Bedarf ihre Prozesse an den Datenschutz im Internet und bei der elektronischen Kommunikation gemäss ePrivacy anpassen. Der erste Schritt sollte eine unternehmensweite Analyse der konkreten Betroffenheit sein. Dabei sind insbesondere folgende Fragen relevant (nicht abschliessend):

- Welche **personenbezogenen Daten** werden verarbeitet?
- Zu welchen Zwecken werden Personendaten erhoben und dann effektiv bearbeitet?
- Welche **sensiblen Daten** werden verarbeitet?
- Was ist die **Rechtsgrundlage** der Datenverarbeitung? Liegt eine **Einwilligung** vor?
- Welcher **Datenverkehr mit dem EU-Ausland und/oder Drittländern** besteht, und auf welcher Rechtsgrundlage?
- Wie werden die Rechte der Datensubjekte bearbeitet?
- Werden **Datenverarbeiter** (derzeit «Dienstleister») herangezogen?
  - Gibt es schriftliche Vereinbarungen für die Auftragsverarbeitung?
  - Wie werden die **Informationspflichten** erfüllt?
  - Wie werden die **Betroffenenrechte** erfüllt?
- Wer ist in meinem Unternehmen zuständig für den Datenschutz? An wen können sich z.B. die betroffenen Personen für die Ausübung ihrer Betroffenenrechte wenden?
- Welche **Datensicherheitsmassnahmen** sind vorhanden?
- Ist für meine Datenverarbeitung eine **Datenschutz-Folgenabschätzung** durchzuführen?
  - Welche Risiken aus der Datenverarbeitung ergeben sich für die Rechte und die Freiheiten der Betroffenen?
  - Wie kann ich den Risikoeintritt verhindern oder zumindest minimieren?
  - Ist eine vorherige **Konsultation** bei der Aufsichtsbehörde notwendig?
- Brauche ich einen **Datenschutzbeauftragten?**
- Welche Vorkehrungen gegen **Datenschutzverletzungen** existieren in meinem Unternehmen?
- Wie werden die Informationspflichten erfüllt (Datenschutzerklärung)?
- Besteht für meine Datenverarbeitung eine **Dokumentationspflicht?** Wie wird die Dokumentationspflicht erfüllt?

Das Thema Datenschutz wird die Compliance-/Legal-Funktion sowie die IT auch in den kommenden Jahren beschäftigen. Effiziente IT-Lösungen rücken in den Fokus, insbesondere im Bereich Datenmanagement, -archivierung und -klassifizierung sowie Ausweitung der Definition von kundenidentifizierenden Daten. So können neue Technologien wie maschinelles Lernen und AI Datenklassifizierungsprozesse automatisieren und somit manuelle Prozesse reduzieren, wenn nicht gar obsolet machen.

Neue Technologien können die heutige IT-Infrastruktur und die Anwendungen für eine universelle Indizierung und Suche unterstützen, damit jegliche Personendaten schnell lokalisiert und z.B. Löschanfragen erfolgreich bearbeitet werden. Betroffene Personen haben das Recht auf unentgeltlichen Zugang zu den Inhalten, die Berichtigung der Daten und das Recht auf Widerspruch gegen die Datenverarbeitung. Um die Anfragen betroffener Personen effizient zu bearbeiten, können IT-Lösungen einen systembasierten Workflow anbieten, der den Prozess vom Eingang bis zum Abschluss der Anfrage unterstützt.

Nicht zuletzt können innovative IT-Lösungen, gepaart mit einer effektiven Data Governance, unerwünschten Datenabfluss verhindern, indem sie Anomalien erkennen.

Glossar

Datensubjekt	Eine Person, über die Daten bearbeitet werden
Datenverantwortlicher	Ein Unternehmen oder eine Person, die über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet
Datenverarbeiter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Datenverantwortlichen verarbeitet
DPO	Data Protection Officer (Datenschutzbeauftragter)
Juristische Person	Unternehmen
Natürliche Person	Privatpersonen bzw. Nutzer, die von Online-Diensten Gebrauch machen
Portabilität	Übertragung von Daten von einem Datenverantwortlichen zu einem anderen
Strukturierte Daten	Daten, aus welchen konkrete Informationen ausgelesen werden können
Transfer	Übertragung von Daten zwischen Datenverantwortlichem und Verarbeiter
Unstrukturierte Daten	Daten ohne identifizierbare Struktur (z.B. Bilder, Text, Sprachnachricht)

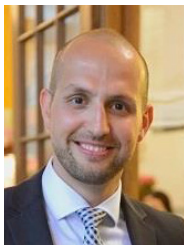
Notizen

Für weitere Informationen kontaktieren Sie bitte:

Regulatory Transformation

Patrick Akiki
Partner, Finance Risk and
Regulatory Transformation
+41 79 708 11 07
akiki.patrick@ch.pwc.com

Marc Lehmann
Director, Finance Risk and
Regulatory Transformation
+41 79 785 69 93



Morris Naqib
Senior Manager, Finance Risk and
Regulatory Transformation
+41 79 902 31 45
morris.naqib@ch.pwc.com

Legal

Susanne Hofmann
Director, Leader Legal
Compliance & Data Protection
+41 79 286 83 67
susanne.hofmann@ch.pwc.com

Michael Taschner
Director, Legal FS Regulatory &
Compliance Services
+41 79 757 95 53
michael.taschner@ch.pwc.com

Philipp Rosenauer
Manager, Legal FS Regulatory &
Compliance Services
+41 79 238 60 20
philipp.rosenauer@ch.pwc.com

PwC Digital Services

Wolfgang Schurr
Partner, Cybersecurity and Privacy
+41 79 545 77 71
wolfgang.schurr@ch.pwc.com

Sascha Sandragesan
Manager, Cybersecurity and Privacy
+41 58 792 50 56
sascha.sandragesan@ch.pwc.com

Hauptbeitragende:
Wir möchten uns bei Daniel Winteler, Philipp Schwarz, Chris Müller und Caroline Gigger für Ihren wertvollen Beitrag zu dieser Publikation bedanken.