www.pwc.ch

Was bringt die Revision des Schweizer Datenschutz-gesetzes 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 präsentierte im September 2017 einen Entwurf für ein totalrevidiertes Datenschutzgesetz (E-DSG), das erhöhte Transparenz schaffen und die Mitbestimmungsrechte von betroffenen Personen[1], über die Daten bearbeitet werden, stärken soll. Dabei ist der Entwurf stark an die Datenschutz-Grundverordnung (DSGVO) angelehnt, welche seit dem 25. Mai 2018 anwendbar ist**.** Auch die ePrivacy-Verordnung ist eng damit verknüpft, die ebenfalls von der EU verabschiedet wurde (noch nicht in Kraft) und als Lex Specialis die Privatsphäre im Internet und bei der elektronischen Kommunikation regeln soll. Diese Publikation soll aufzeigen, was Schweizer Unternehmen von der Revision des DSG erwarten können, inwiefern sich die Gesetzgebung von der DSGVO unterscheidet und welche Herausforderungen bei der Implementierung anstehen können.

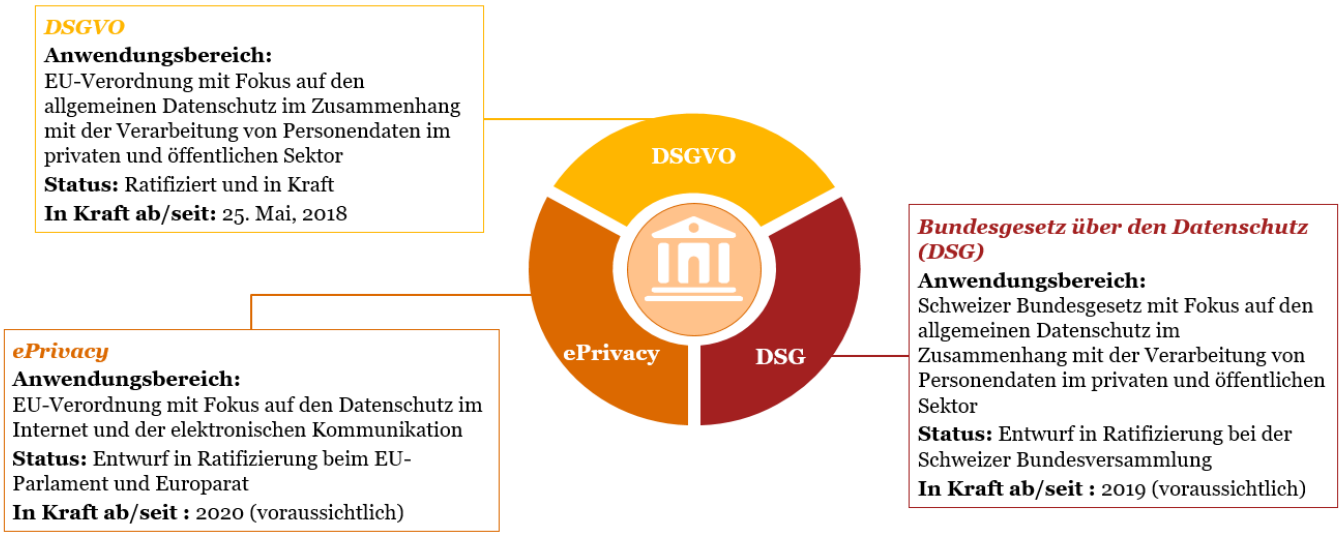
1. Überblick über die aktuelle Situation des Datenschutzes in der Schweiz

Mit der zunehmenden Verbreitung digitaler Technologien während der letzten drei Jahrzehnte stiegen die Anforderungen an den Datenschutz fortlaufend an. Das Inkrafttreten der europäischen Regulierung DSGVO im Mai 2018 sowie die erwartete ePrivacy-Verordnung (voraussichtlich 2020) stellen eine Welle von europäischen Massnahmen dar, die zum Ziel haben, die Persönlichkeit und Freiheiten von Datensubjekten zu schützen. Aufgrund der rasant steigenden Entwicklung von Kommunikations- und Vertriebskanälen, sowie der fortgeschrittenen Kapazitäten von Unternehmen, persönliche Daten sammeln und verarbeiten zu können, steht der Schutz der Datensubjekte, über die Daten bearbeitet werden, im Zentrum der neuen Regulierungen.

Der Bundesrat beschloss bereits 2011, das 1992 in Kraft getretene Datenschutzgesetz zu revidieren. Aufgrund der Veröffentlichung der DSGVO im Jahr 2016 beschloss der Schweizer Nationalrat, nun die Revision des Datenschutzgesetzes unter Einbezug der DSGVO vorzunehmen. Davon sind alle Schweizer Unternehmen betroffen, die personenbezogene Daten bearbeiten (z.B. von Kunden oder von Mitarbeitenden). Jeder Umgang mit Personendaten stellt eine Bearbeitung dar, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten. Aufgrund des breiten Anwendungsbereichs wird es wohl nur sehr wenige Unternehmen in der Schweiz geben, die von der Revision nicht betroffen sind.

Die Erfahrung mit der DSGVO für betroffene Unternehmen, sowie der Revisionsentwurf des DSG zeigen, dass die Implementierung der neuen Vorgaben eine grosse Herausforderung für Unternehmen darstellt. Ein dringender Handlungsbedarf ist somit notwendig. Dabei ist eine holistische Betrachtung der kommenden Regulierungen zentral, um möglichst kosteneffizient und marktkonform zu sein. Die Markterfahrung zeigt, dass die fachlichen und zeitlichen Abhängigkeiten zwischen revidiertem Datenschutzgesetz (E-DSG), ePrivacy und DSGVO bei der Implementierung berücksichtigt werden sollten.

[1] Siehe Glossar



Was die neuen Gesetze zum Schutz der Personendaten für Schweizer Unternehmen konkret bedeuten, welche Massnahmen ergriffen werden müssen und was es bei der bevorstehenden Entwicklung zu beachten gilt, wird in den folgenden Kapiteln dargestellt. Dabei steht der Fokus dieses Dokuments primär auf dem E-DSG und welche Abhängigkeiten zur DSGVO bestehen.

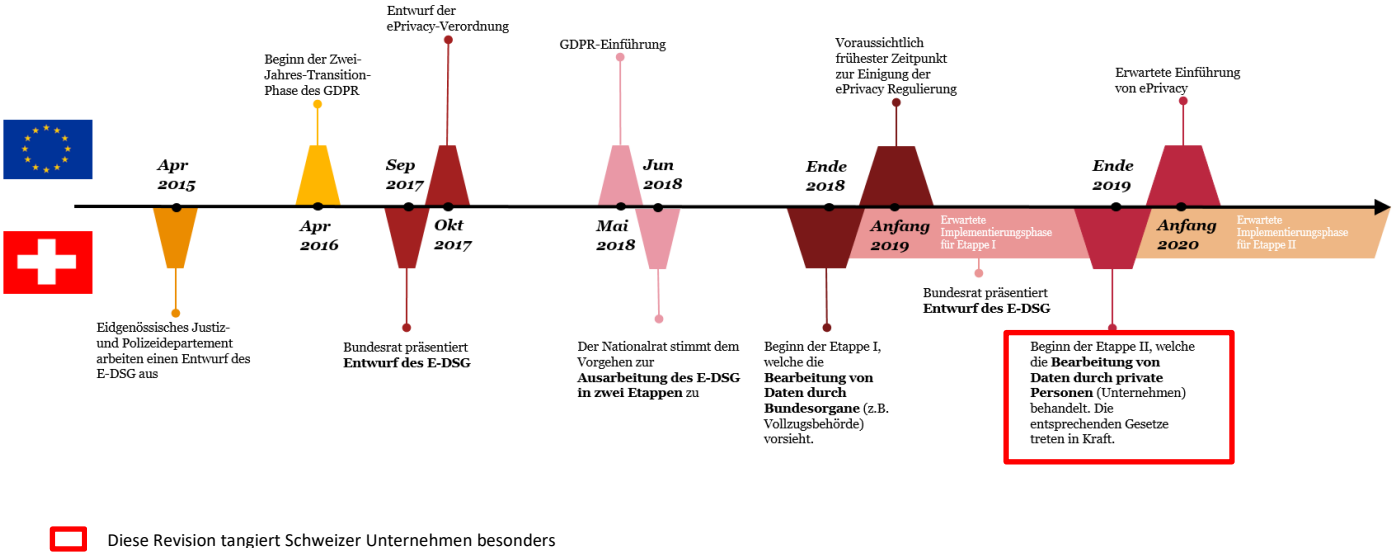
2. Die Revision des Schweizer DSG

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 dabei inhaltlich an die DSGVO anlehnen.

2.1 Der Zeitplan der Totalrevision

Ursprünglich war beabsichtigt, in einem einzigen Schritt durch die Totalrevision des DSG sowohl den Verpflichtungen aus dem Schengen-Besitzstand sowie jenen der DSGVO nachzukommen. Streng genommen ist die Schweiz aber lediglich zur Übernahme jener datenschutzrechtlichen Bestimmungen verpflichtet, die aus den Schengen-Verträgen resultieren. Um allerdings als ein Drittstaat mit einem der EU vergleichbaren Datenschutzniveau anerkannt zu werden, sollen auch die relevanten Anpassungen an das europäische Recht vorgenommen werden. Andernfalls besteht das Risiko, dass Daten zwischen der Schweiz und der EU nur mit erschwerenden Auflagen ausgetauscht werden können. Es wurde dann allerdings entschieden, die Totalrevision in zwei Etappen aufzuteilen: Die Teilung soll es erlauben, die aufgrund der Schengen-Verträge innert einer bestimmten Frist notwendige Umsetzung von EU-Recht (Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts) vorab zu beraten. Anschliessend könne die Totalrevision des Datenschutzgesetzes «ohne Zeitdruck» angegangen werden. Für Schweizer Unternehmen ist entsprechend insbesondere die zweite Etappe relevant, welche voraussichtlich bis Ende 2020 abgeschlossen werden soll.

[2] Siehe Glossar



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 verstärkt 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 folgenden Kernpunkten von der bestehenden Gesetzgebung (DSG):

- ***Schutzobjekt: natürliche Personen***

Während das DSG aus dem Jahre 1992 den Schutz von Daten von sowohl natürlichen als auch juristischen Personen regelte, beschränkt sich das E-DSG auf Daten von natürlichen Personen.

- ***Sanktionen***

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

- ***Besonders schützenswerte Personendaten***

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

- ***Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellung***

Datenverarbeitern werden erhöhte Sorgfaltspflichten auferlegt, die zudem genauer definiert sind. So müssen Datenverantwortliche und -verarbeiter bereits bei der Planung von Datenbearbeitungen das Risiko von Verletzungen der Persönlichkeit durch angemessene Massnahmen verringern. Zudem sind sie verpflichtet, mittels geeigneten Voreinstellungen sicherzustellen, dass standardmässig nur solche Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.

- ***Datenschutz-Folgenabschätzung***

Datenverantwortliche oder Datenverarbeiter 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 als möglich eine Meldung zu erstatten, wenn ein hohes

Risiko für die Persönlichkeit oder Grundrechte der betroffenen Person 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.

Doch auch wenn das E-DSG inhaltlich an die DSGVO angelehnt ist, gibt es Unterschiede zwischen den beiden Richtlinien zum Datenschutz. Die wichtigsten Unterschiede zwischen dem E-DSG und der DSGVO sind nachstehend aufgeführt:

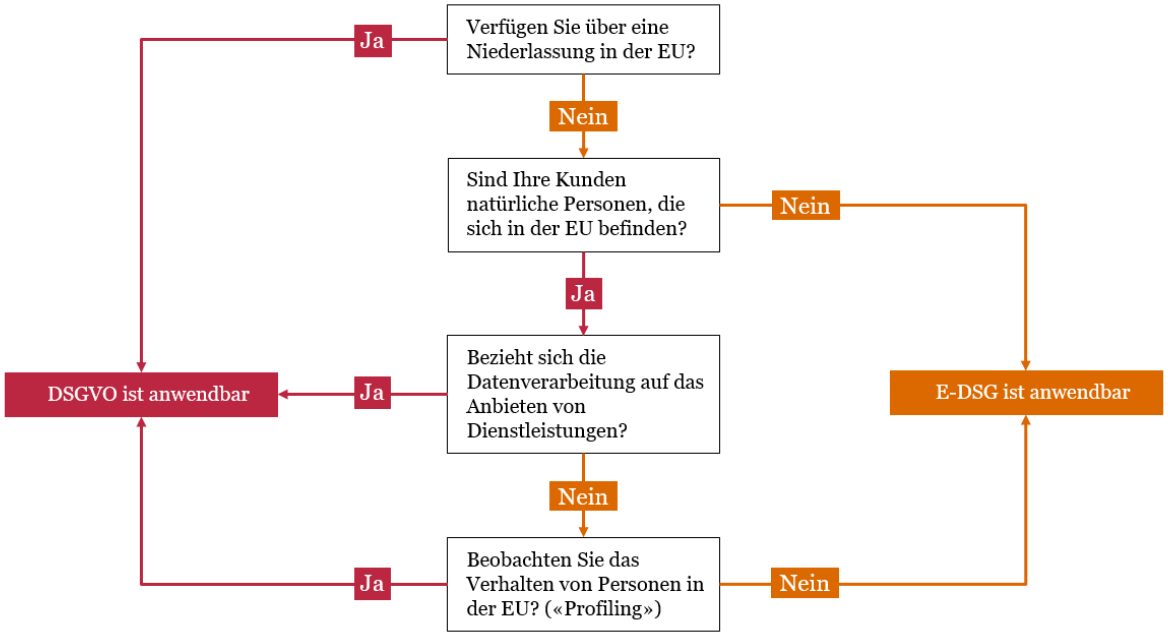
Hauptkriterien		DSGVO	E-DSG
Kategorien	**Spezifizierung**		
Allgemeine Vorschriften	**Geografische Reichweite**	Einheiten in der EU und/oder Einheiten, die Daten von natürlichen Personen innerhalb der EU bearbeiten	Einheiten, die in der Schweiz ansässig sind
	Bussgelder	Bis zu EUR 20 Millionen oder 4% 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, in Betracht gezogen 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, in Betracht gezogen 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 72 Stunden	«so rasch als 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 zur 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?

Abhängig von den spezifischen Marktaktivitäten von Schweizer Unternehmen gelten entweder ausschliesslich die Vorschriften nach dem E-DSG oder es gelten sowohl das E-DSG als auch die DSGVO. Die nachfolgende Grafik gibt Ihnen einen Überblick, welche Regelwerke zum Datenschutz speziell für Ihr Unternehmen relevant sind.



3.2 Herausforderungen bei der Implementierung des neuen Datenschutzgesetzes

PwC begleitete seit mehreren Jahren zahlreiche Unternehmen in der Schweiz und innerhalb der EU bei der Analyse, Konzeptdefinierung und Implementierung der Anforderungen der DSGVO. Parallel führte PwC bei diversen Finanzdienstleistungsunternehmen eine Benchmarking-Analyse durch, um Markteinblicke über die Design- und Umsetzungsfortschritte zur 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 die Bildung eines Verzeichnisses von Verarbeitungstätigkeiten

Die Herausforderung beim Management der persönlichen Daten besteht darin:
a) Ein Verzeichnis von Verarbeitungstätigkeiten zu bilden
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 deren Zweck sowie rechtliche 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. Diese sollen sicherzustellen, dass bei jeglicher Änderung in der Verarbeitung von persönlichen Daten innerhalb der Geschäftstätigkeiten 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. Dabei stellt ebenfalls die Aufrechterhaltung und Integration des BAU eine zentrale Herausforderung für Finanzdienstleister dar.

2. Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellung

Datenschutz durch Technikgestaltung bezieht sich auf die Umsetzung organisatorischer und technischer Massnahmen, 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 Voreinstellung besagt, dass als Standardeinstellung nur jene 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 ein klares Verständnis darüber vorhanden sein, welche Daten zu welchem Zweck verwendet werden.

Um die Einhaltung des Grundsatzes der Datenminimierung zu überprüfen, wird antizipiert, ein Benchmark bezüglich der Datenminimierung aus der Industrie zu verwenden. Dabei gibt es zurzeit 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 stellt aus der Erfahrung mit der DSGVO das Design und die Implementierung von Konzepten, Policen und Kontrollen dar, die eine 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 soll darauf geachtet werden, dass bei den zu implementierenden Massnahmen ein konkreter «Audit-Trail» vorgewiesen wird, um die kontinuierliche Einhaltung der Regulierung zu gewährleisten.
Dabei spielt gerade das Thema Cybersicherheit zunehmend eine wichtige und ergänzende Rolle im Datenschutz. Die zu ergreifenden technischen und organisatorischen Massnahmen zum Schutz der Daten und die damit einhergehende Compliance mit den Datenschutzgesetzen kann nur mittels gesichertem IT-System erreicht und eingehalten werden. IT-Sicherheit wird somit ein fester Bestandteil bei der Einhaltung der Gesetzgebung. Der Compliance Officer allein wird die Aufgabe nicht mehr bewältigen können. Er benötigt die Unterstützung und Zusammenarbeit des fachkundigen IT-Spezialisten.

Datenschutz-Rechte für Datensubjekte

Abhängig von Geschäftsmodell, Kundensegmentierung und Risikobereitschaft kann der Grad der Automatisierung der Prozesse, um die Rechte der Datensubjekte einzuhalten, stark variieren. Die Erfahrung bei der DSGVO zeigt, dass bereits bestehende Lösungen wie E-Banking verwendet werden können, um das Auskunftsrecht mit einer automatischen Vorgehensweise spezifisch abzudecken.
Unternehmen, die eine manuelle Bearbeitung der Anfragen der Datensubjekte wählen, bauen in der Regel eine zentrale Anlaufstelle auf, die alle Anfragen auffangen und entsprechend bearbeiten. Dabei wird aber auch beobachtet, dass die Arbeitstätigkeiten bestehender Einheiten, die üblicherweise Beschwerden von Kunden behandeln, ausgeweitet werden, um Datenschutzanfragen zu decken.

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 Datensubjekten 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.

Um die Beantwortung der Anfragen möglichst kosteneffizient zu gestalten, können standardisierte Berichte produziert werden, die eigens als Antwort für betroffene Personen entwickelt werden. Auch die Erfahrung mit der DSGVO zeigt, dass solche Berichte einen effizienten Antwortprozess ermöglichen. Hierfür muss allerdings eine Abgrenzung der Datenstruktur (strukturierte vs. unstrukturierte Daten) erfolgen. Auch Umgang und Integration der Metadaten und Transaktionsdaten im Bericht sollten unbedingt in Betracht gezogen werden.

Den Umfang der erwarteten Anfragen von betroffenen Personen zu prognostizieren, ist nicht nur eine grosse Herausforderung, sondern zusätzlich an zahlreiche Schlüsselentscheidungen von Unternehmen gekoppelt. 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, das allerdings nur dann ausgeübt werden kann, wenn personenbezogene Daten für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden oder andere 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 stehen Firmen häufig vor der Herausforderung eingeschränkter Systemfähigkeiten. Bestehende Systeme sind häufig im Hinblick auf das Löschen von Daten, die das Stammdatenintegritätsmodell unterstützten, eingeschränkt. Im Finanzsektor wird zwar erwartet, dass nur wenige betroffene Personen von diesem Recht Gebrauch machen werden.

Jedoch muss die Anzahl der manuell bearbeiteten Anfragen berücksichtigt werden. Hier spielt ebenfalls die Komplexität der Systemarchitektur eine Rolle sowie die Anzahl der betroffenen Systeme.

3.2 Ausbau der Löschungskapazitäten für Prinzipien der Speicherbegrenzung

Die Löschkapazitäten für Prinzipien der Speicherbegrenzung zeigt sich in der Industrie als eine grosse Herausforderung. Die meisten Institute haben oft fragmentierte Systemlandschaften und verfügen nicht über einheitliche und holistische Systeminventare, die aufzeigen:

(i) welche Datenattribute in welcher Anwendung gespeichert/bearbeitet werden;
(ii) welche Datenquellen benötigt wird;
(iii) welches der Zweck der Bearbeitung auf Attribut-Ebene ist; und
(iv) wie und wann die Daten pro System archiviert werden.

Eine automatische Löschfunktionalität ist empfehlenswert, da die manuelle Arbeit mit sehr hohen Kosten und sehr hohem 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 wird und an den Zweck und den 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 Konzeptdefinition der Löschkapazitäten unstrukturierte Daten in Betracht zu ziehen. Jedoch zeigt die Erfahrung, dass die Komplexität darin besteht, 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 von betroffenen Personen unterstützen.

Um einen umfassenden Ansatz zu garantieren, der unstrukturierte Daten beinhaltet, muss 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 ebenfalls eine 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 diese auszulagern.

5. Management persönlicher Daten an Drittparteien

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

Die Hauptherausforderung liegt darin, die Daten, die transferiert werden, zu identifizieren. Konkret geht es darum, festzulegen, welche Drittpartei für welchen Zweck welche Daten bearbeitet. Weiterhin 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 Kategorien der Datensubjekte zu definieren sowie Massnahmen zur Kontrolle festzulegen; und
3. die Anforderungen und Pflichten festzulegen, falls Anfragen von Datensubjekten eintreffen.

Zusätzlich soll sichergestellt werden, dass neue Richtlinien oder Gesetzesänderungen rasch berücksichtigt und eingehalten werden.

Dabei sind auch die Drittanbieter selbst teilweise nicht identifiziert, beispielsweise bei der Erstellung einer Webseite. Zur Entwicklung benötigt es typischerweise 10 bis 20, teilweise sogar über 50 verschiedene Dritt- und Werbeanbieter (z.B. für Online-Tracking), 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 …» – dieser Satz wird einem schon des Öfteren begegnet sein. Angriffe auf die Infrastruktur von grossen Organisationen tauchen wöchentlich auf den Titelseiten der Zeitungen auf. Mit dem Bekenntnis, dass Angriffe niemals verhindert werden können und dass nie von einer hundertprozentigen Sicherheit ausgegangen werden darf, sollten Unternehmen ihre Fähigkeiten, Vorfälle zu erkennen, verbessern, um eine effektive und schnelle Aufdeckung, Eindämmung und angemessene Reaktion auf diese zu ermöglichen. Dazu gehört die Benachrichtigung der Datenpanne an die Aufsichtsbehörden innerhalb von 72 Stunden, wie es in der DSGVO gefordert wird. Die DSGVO spricht von der sog. «Verletzung des Schutzes personenbezogener Daten», die als eine Verletzung der Sicherheit zu verstehen ist, 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 wird davon erfasst. Datenpannen haben erhebliche Folgen auf das Unternehmen, das Opfer eines solchen Angriffs wird. So geht es oftmals um vertrauliche Informationen, die in die Hände unbefugter Dritter geraten.

Es entstehen Finanzschäden in beträchtlichen Summen, die juristische Konsequenzen und anhaltende Imageschäden nach sich ziehen. Zu guter Letzt wird auch der Betroffene selbst in Mitleidenschaft gezogen. Seine dem Unternehmen anvertrauten Daten kursieren nun durch das Netz und bieten eine ideale Angriffsfläche für Angriffe dar. Folgen eines Cyberangriffs schlagen somit hohe Wellen. Eine Organisation muss sich auf solche Vorfälle einstellen und vorbereiten.

Absolute Sicherheit kann nie gewährleistet werden, doch zumindest ist es möglich, das Risiko eines Angriffs beträchtlich zu verringern und die Reaktionszeit zu erhöhen. 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 können die Schäden geringgehalten werden.

Um Cyberrisiken effektiv zu managen, müssen Unternehmen eine Reihe unterschiedlicher Faktoren berücksichtigen: So sollte zunächst eine abteilungsübergreifende Einheitlichkeit in Sachen Sicherheitspraktiken vorliegen, mit Fokus auf datenspezifischen Schutzpraktiken. Auch Sicherheitskonzepte sollten flächendeckend in Projekte, Produkte und Prozesse eingebaut werden (Security by design). Ein besonderes Augenmerk sollte auf die Bedrohungslandschaft und die Bedrohungsakteure gelegt werden, die auf die Infrastruktur der Organisationen abzielen. Solche Erkenntnisse und das gewonnene Know-how sollten in der Sicherheitsarchitektur eines Unternehmens kosteneffizient operationalisiert werden.

Zu guter Letzt sollten noch häufige Disaster-Recovery-Übungen durchgeführt werden, frei nach dem Motto: «Übung macht den Meister». Dadurch 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 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 beinhaltet eine erhebliche Ausweitung des Anwendungsbereichs. 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**
  Um auf Informationen eines Benutzergerätes zuzugreifen, ist eine Zustimmung des Nutzers erforderlich. Benutzer müssen auch Webseiten zustimmen, die Cookies oder andere Technologien verwenden, um auf die auf ihren Computern 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.

Ziel der ePR ist es, die Anforderungen der DSGVO zu ergänzen und zu 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 ein 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 aktuellsten Informationen bestehen zusammengefasst folgende Parallelen zwischen E-DSG und ePrivacy.

[3] Basierend auf Entwurf ePrivacy 5. Dezember 2017

Kriterien		DSGVO/E-DSG	ePrivacy
Allgemeine Vorschriften	Betroffene	Natürliche Personen	Natürliche und juristische Personen
	Anwendungsbereich	Allgemeiner Datenschutz im Zusammenhang mit der Verarbeitung personenbezogener Daten durch juristische Personen des privaten Sektors und gesetzgebenden 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 Nutzer den Dienst nutzt: Erbringung von Online-Kommunikationsdienstleistung, Online-Tracking-Technologien oder elektronisches Marketing
Personenbezogenes Dateninventar	Rechtmässige Grundlage	(i) Zustimmung der betroffenen Personen, (ii) vertragliche Verpflichtung, (iii) Einhaltung der gesetzlichen Verpflichtung, (iv) erforderlich, aufgrund weniger, öffentlicher und/oder berechtigter Interessen	Zustimmung ist erforderlich für jede Art von Datenverarbeitung, wenn die Verarbeitung über die angeforderte Dienstleistung hinausgeht (z.B. Bearbeitung gestattet ohne Zustimmung, wenn es für Kommunikationsübertragung erforderlich ist)
Rechte der Betroffenen		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)
		Widerspruchsrecht zur Verarbeitung	Recht auf Steuerung elektronischer Kommunikation inkl. das Verbieten ungewünschter Kommunikation/Werbung
		Recht auf Datenzugang, Recht auf Übertragbarkeit, Recht auf Berichtigung, Recht auf Widerruf von Zustimmung, Widerspruchsrecht zur automatisierten Entscheidungsfindung, Anspruch auf Einschränkung 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 nächste Schritte bezüglich des E-DSG ergreifen und dabei von taktischen temporären Lösungen wegkommen und zu langfristigen strategischen Lösungen übergehen. 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: z.B. E-DSG vs. DSGVO/ePrivacy. Dabei ist die Unsicherheit bezüglich der finalen Version der Regulierungen und die Kosten-/Aufwandschätzung zentral, um effizient konform zu sein.
Eine individuell auf das Unternehmen gerichtete Gap-Analyse zum E-DSG ist ein erster Schritt, um Handlungsbedarf zu ermitteln und entsprechende unternehmensadäquate Massnahmen zu entwickeln.
Bezüglich der ePrivacy-Richtlinien müssen Unternehmen ihren Standpunkt analysieren und bei Bedarf ihre Prozesse auf den Datenschutz im Internet und bei der elektronischen Kommunikation gemäss ePrivacy anpassen. In einem ersten Schritt sollte eine unternehmensweite Analyse der konkreten Betroffenheit durchgeführt werden. Dabei sind insbesondere folgende Fragen von Relevanz (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 Rechten 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 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 schon in meinem Unternehmen?
- Wie werden die Informationspflichten erfüllt (Datenschutzerklärungen)?
- 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 kundenidentifizierender Daten. So können neue Technologien wie maschinelles Lernen und AI Datenklassifizierungsprozesse automatisieren und somit manuelle Prozesse stark reduzieren, wenn nicht gänzlich obsolet machen.
Neue Technologien können weiter 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 können. Zu den weiteren Rechten, die eine betroffene Person geniesst, gehören der unentgeltliche Zugang zu den Inhalten, die Berichtigung der Daten und das Widerspruchsrecht gegenüber der Datenverarbeitung. Um die Anfragen von betroffenen Personen effizient zu bearbeiten, können effiziente IT-Lösungen einen systembasierten Workflow anbieten, der den Prozess vom Eingang bis zum Abschluss einer Anfrage unterstützt.
«Last but not least» sorgen innovative IT-Lösungen gepaart mit einer effektiven Data Governance dafür, dass ein unerwünschter Datenabfluss mittels Erkennung von Anomalien verhindert wird.

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
marc.lehmann@ch.pwc.com

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 79 297 42 10
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.