DOMENIG PARTNER
RECHTSANWÄLTE AG

Europäische Datenschutzgrundverordnung (DSGVO) – Relevanz und Herausforderungen für Schweizerische Klein- und Mittelunternehmen

Benjamin Domenig, Rechtsanwalt
Bern, 18. Januar 2018

Am 25. Mai 2018 tritt die neue Datenschutz-Grundverordnung (DSGVO) der EU in Kraft. Die DSGVO ist auch für Schweizerische Unternehmen relevant, sofern Waren- oder Dienstleistungen an Personen in der EU angeboten werden (beispielsweise über die Homepage des Unternehmens) oder das Verhalten von Personen in der EU analysiert wird (beispielsweise bei Webtracking oder Location Based Services).

Die neue DSGVO schreibt den Unternehmen vor, dass jederzeit der Nachweis erbracht werden muss, dass die Vorschriften eingehalten werden. Das bringt erheblichen Dokumentationsaufwand mit sich, was bei vielen Unternehmen eine Überarbeitung jener Arbeitsprozesse verlangt, die den Umgang mit personenbezogenen Daten definieren. Bei Nichteinhaltung der DSGVO drohen hohe Geldbussen von bis zu EUR 20 Mio. oder, falls höher, 4% des weltweiten Umsatzes des Unternehmens. Die Umsetzung durch die betroffenen Unternehmen bedarf in vielen Fällen organisatorischer oder technischer Anpassungen.

Die Schweiz ist gestützt auf das Schengen-Abkommen gezwungen, den ersten Teil der DSGVO (dieser regelt den Datenaustausch zwischen Behörden) in nationales Recht umzusetzen. Der zweite Teil der DSGVO (Regeln für Unternehmen für den Umgang mit Daten) muss die Schweiz ebenfalls umsetzen, wenn der Zugang für Schweizer Unternehmen zum EU-Markt erhalten bleiben soll. Die Revision des Schweizerischen Datenschutzgesetzes (DSG) ist bereits fortgeschritten, tritt aber voraussichtlich erst im Jahr 2019 in Kraft. Schweizerische Unternehmen sind gut beraten, wenn sie sich bereits jetzt mit den neuen Bestimmungen auseinandersetzen und entsprechende Änderungen in ihren Compliance-Strukturen vornehmen.

DOMENIG & PARTNER RECHTSANWÄLTE AG
Hirschengraben 2 | Postfach 2276 | CH-3001 Bern
Tel.: +41 31 380 11 00 | Fax: +41 31 380 11 09 | info@domenig.law
www.domenig.law

CHE-284.941.671 MWST

A. Ausgangslage

Die EU hat im April 2016 die neue **Datenschutz-Grundverordnung DSGVO** erlassen (die offizielle und etwas schwerfälligere Bezeichnung lautet «Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG. Diese tritt in der EU am **25. Mai 2018** in Kraft.

Ziel dieser Verordnung ist, dass die Bürgerinnen und Bürger der EU mehr Kontrolle über ihre Personendaten haben. Dies soll dadurch erreicht werden, dass die Unternehmen zur Verantwortung gezogen werden und der Rolle der Datenschutzbehörde eine grössere Bedeutung zukommt.

Die **EU-Länder** haben bis am 6. Mai 2018 Zeit, die Richtlinie in ihrem nationalen Recht umzusetzen. Selbst wenn diese Länder die Umsetzung noch nicht vollzogen haben, ist die DSGVO im ganzen Raum der EU uneingeschränkt anwendbar.

Die DSGVO wird auch für **Schweizerische Unternehmen** eine **direkte Auswirkung haben**, selbst wenn die Revision des Schweizerischen Datenschutzgesetzes (DSG) erst später in Kraft tritt.

Die vorliegende Information legt die Herausforderungen für Schweizerische Unternehmen dar und soll insbesondere die Frage beantworten, **welche Schweizerische Unternehmen von der DSGVO betroffen sind**.

B. Was sind «personenbezogene Daten» und was fällt unter die «Verarbeitung» von Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine natürliche Person (nachfolgend sprechen wir daher von der «betroffenen Person») beziehen, wenn diese identifizierbar ist. Identifizierbar ist die Person, wenn sie aufgrund von den zur Verfügung stehenden Informationen bestimmt werden kann. Kann die Person beispielsweise mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer (Passport-Nr., IP-Adresse, etc.), zu Standortdaten oder zu einer Online-Kennung bestimmt werden, so handelt es sich dabei um personenbezogenen Daten.

Als **«Verarbeitung»** von Daten wird das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von personenbezogenen Daten verstanden. Der Begriff wird offensichtlich ausserordentlich breit verstanden und umfasst vereinfacht gesagt **jede Tätigkeit in Zusammenhang mit den personenbezogenen Daten**.

C. Ist meine Unternehmung von der Datenschutz-Grundverordnung der EU (DSGVO) betroffen?

Sachlicher Anwendungsbereich der DSGVO

Die DSGVO hat einen ausserordentlich breiten Anwendungsbereich. Sie ist **anwendbar sobald personenbezogene Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen** (Art. 2 § 1 DSGVO). Es spielt keine Rolle, ob die personenbezogenen Daten von einer natürlichen oder einer juristischen Person bearbeitet werden. Ebenfalls nicht relevant ist, ob eine natürliche oder juristische Person des öffentlichen Rechts (Staat, Behörden, Departemente, etc.) oder des privaten Rechts (Unternehmen und Privatpersonen) die Daten verarbeitet.

In **vier Fällen** ist die DSGVO allerdings **nicht anwendbar** (sog. **Ausnahmetatbestände** gemäss Art. 2 § 2 DSGVO):

a. *Im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrecht fällt;*
b. *Durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen;*
c. *Durch natürliche Personen zur Ausübung ausschliesslich persönlicher oder familiärer Tätigkeiten*
d. *Durch die zuständige Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschliesslich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.*

Für **Schweizerische Unternehmen** sind diese Ausnahmetatbestände weitgehend **irrelevant**.

Räumlicher Anwendungsbereich der DSGVO

Im Zusammenhang mit dem räumlichen Anwendungsbereich erfährt die DSGVO **extraterritoriale Wirkung**. Das heisst, dass die Anwendung nicht auf das Territorium der EU beschränkt ist. Massgebend ist, wie sich die personenbezogene Bearbeitung der Daten auf den Raum der EU auswirkt, unabhängig davon, ob die Bearbeitung der Daten in der EU oder ausserhalb der EU (wie beispielsweise in der Schweiz) stattfindet.

Anhand der folgenden **Kriterien** kann geprüft werden, ob Ihre Unternehmung von der DSGVO betroffen ist:

- **Kriterium der Niederlassung.** Hat der Verantwortliche (derjenige, der die Daten bearbeitet) oder der Auftragsbearbeiter (wenn der Verantwortliche die Bearbeitung der Daten an einen Dritten überträgt) seine Niederlassung in der **Europäischen Union**, dann findet die DSGVO ohne Weiteres Anwendung.

- **Kriterium des Zielmarktes (auch Marktortprinzip).** Hier ist die Beantwortung folgender Frage relevant: «Wo hat die Person, deren Daten bearbeitet werden, ihren Wohnort?». Befindet sich der **Wohnort in der EU**, dann ist die **DSGVO anwendbar** und zwar unabhängig davon, ob die Bearbeitung ausserhalb der EU erfolgt. Damit sind insbesondere **Internetnutzerinnen und Internetnutzer** gemeint, deren Daten von ausserhalb der EU bearbeitet werden.

Für **Schweizerische Unternehmen** ist das **Kriterium des Zielmarktes** von grosser Bedeutung: Wenn das Schweizerische Unternehmen beispielsweise über das Internet **Waren oder Dienstleistungen** an Personen mit Sitz in der EU anbietet (oder deren Verhalten beobachtet), dann ist die **DSGVO** in aller Regel **anwendbar**. Irrelevant ist, ob für die Waren und Dienstleistungen ein Entgelt verlangt wird. Das heisst, dass auch das Anbieten von Gratisprodukten und Gratisdienstleistungen in den Anwendungsbereich der DSGVO fallen, wenn sich das Angebot an Personen mit Wohnsitz in der EU richtet.

Die Schweizerischen Unternehmen können die Anwendung des DSGVO nicht vermeiden, indem sie bspw. auf ihrer **Homepage erklären, dass keine Waren oder Dienstleistungen** an Kunden in der Union angeboten werden, diese aber dennoch bestellt werden können. Wird hingegen durch technische Massnahmen sichergestellt, dass Personen mit Sitz in der EU nicht auf die Homepage zugreifen können, resp. keine Bestellungen ausführen können, ist die DSGVO nach der hier vertretenen Ansicht nicht anwendbar.

Wenn das Unternehmen mit Sitz in der Schweiz zwar keine Waren und/oder Dienstleistungen anbietet, aber das **Verhalten von Personen** innerhalb der EU **beobachtet**, dann ist die **DSGVO** ebenfalls **anwendbar**. Das ist dann der Fall, wenn Daten erhoben werden, um über die Internetaktivitäten der Benutzer Profile bezüglich der Vorlieben und Verhaltensweisen zu erstellen. Letzteres betrifft vor allem Betreiber sozialer Netzwerke, Webtracking-Unternehmen und das Anbieten von Location Based Services.

D. Ist meine Unternehmung von der Datenschutz-Grundverordnung der EU (DSGVO) auch dann betroffen, wenn ich nur als Auftragsbearbeiter Daten bearbeite?

- Ja. Wenn ein Auftragsbearbeiter im EU-Gebiet personenbezogene Daten für ein Schweizer Unternehmen bearbeitet, ist die DSGVO anwendbar, unabhängig davon, ob er Daten von betroffenen Personen in der Schweiz oder in der EU bearbeitet.

- Ja. Wenn Ihre Schweizerische Unternehmung personenbezogene Daten im Auftrag eines europäischen Unternehmens bearbeitet, ist die DSGVO anwendbar.

E. Was sind die Pflichten meiner Unternehmung, wenn die DSGVO für uns anwendbar ist?

Haben Sie gestützt auf die obigen Ausführungen festgestellt, dass Ihre Unternehmung die DSGVO beachten muss? Nachstehend finden Sie eine Übersicht über die wichtigsten Pflichten, die die Anwendung der DSGVO mit sich bringt. Beachten Sie unbedingt, dass diese Ausführungen aufgrund der umfangreichen DSGVO nicht abschliessend sind und weitere Verpflichtungen zu beachten sind.

Grundsatz

Die DSGVO sieht neu die sog. **Rechenschaftspflicht** des Verantwortlichen (der natürlichen oder juristischen Person, die über die Zwecke und Mittel der Verarbeitung der Daten entscheidet) vor. Die Rechenschaftspflicht bedeutet, dass das Unternehmen, welches die Daten bearbeitet jederzeit den Nachweis erbringen können muss, dass die allgemeinen Grundsätze der DSGVO eingehalten werden. Dies führt zu einer **Beweislastumkehr**: Nicht die betroffenen Personen oder die Aufsichtsbehörde müssen beweisen, dass das Unternehmen das DSGVO einhält. Die Beweislast hierfür liegt ausschliesslich beim Unternehmen, das personenbezogene Daten bearbeitet.

Übersicht über die Pflichten, die die Anwendung der DSGVO mit sich bringt (nicht abschliessend)

1. Der Verantwortliche muss **technische** und **organisatorische Massnahmen** umsetzen, um sicherzustellen dass die DSGVO eingehalten wird und, dass jederzeit der Nachweis über die Erfüllung der DSGVO erbracht werden kann (Art. 24 DSGVO);

2. Dem Datenschutz ist bereits bei der Neuentwicklung von Produkten und Dienstleistungen hinreichend Rechnung zu tragen. Wird vom Verantwortlichen ein neues Produkt entwickelt oder eine neue Dienstleistung angeboten, ist er also verpflichtet, durch technische und organisatorische Massnahmen einen möglichst hohen Datenschutzgrad zu erreichen (sog. **Privacy by Design**). Das geschieht beispielsweise durch Minimierung der bearbeiteten Daten und Pseudonymisierung. Produkte und Dienstleistungen müssen zudem mit datenschutzfreundlichen Voreinstellungen (z.B. vorangekreuzte Kästchen) angeboten werden (sog. **Privacy by Default**), vgl. hierzu Art. 25 DSGVO.

3. Der Verantwortliche muss ein **Register** führen (Art. 30 DSGVO). Dieses Register muss ein Verzeichnis **aller Verarbeitungstätigkeiten** aufführen und hat einen hohen – von der DSGVO –

vorgeschriebenen Detailierungsgrad (Zweck der Verarbeitung; Beschreibung der Kategorien personenbezogener Daten; Kategorien von Empfängern; Fristen für vorgesehene Löschungen; etc.). Auf Anfrage der **Aufsichtsbehörde** muss dieses Register zur Verfügung gestellt werden.

4. Hat die Bearbeitung der Daten ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person zur Folge, so ist der Verantwortliche verpflichtet, eine **sog. Datenschutz-Folgenabschätzung** vorzunehmen (Art. 35 DSGVO). Führt eine solche Datenschutz-Folgenabschätzung zur Einsicht, dass die Bearbeitung der Daten einer Person bspw. zu Diskriminierungen, Identitätsdiebstahl oder –betrug, finanziellen Verlusten oder Rufschädigung führen kann, so ist der Verantwortliche verpflichtet, vor der Bearbeitung die Datenschutzbehörde zu konsultieren. Ist im Unternehmen ein Datenschutzverantwortlicher ernannt worden, so ist dieser zu konsultieren.

5. In folgenden Fällen ist die Benennung eines **Datenschutzbeauftragten** zwingend erforderlich:

   a. Für Behörden oder öffentliche Stellen;

   b. Für Unternehmen, die Bearbeitungen durchführen, die eine umfangreiche, regelmässige und systematische Überwachung der betroffenen Personen erfordern. Dies ist beispielsweise der Fall, wenn ein Unternehmen systematisch personenbezogene Daten auswertet, um darauf gestützt Werbung zu versenden;

   c. Für Unternehmen, die sensible Datenbearbeitungsvorgänge durchführen. Dabei handelt es sich üblicherweise um Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen.

F. Was passiert, wenn ich die DSGVO nicht einhalte?

Die **Sanktionen** der DSGVO sind drastisch. Die Aufsichtsbehörden der EU können direkt **Geldbussen verhängen**. Die Geldbussen werden gegen die Verantwortlichen ausgesprochen und betragen **bis zu 20 Millionen Euro** oder **4 Prozent des weltweiten Jahresumsatzes.**

G. Wie können Sie mir in Bezug auf die Herausforderungen der DSGVO helfen?

Unsere Kanzlei verfügt als eine der wenigen Kanzleien in der Schweiz über Erfahrung in der Implementierung der Vorschriften des DSGVO.

Die Implementierung erfolgt regelmässig im Rahmen eines Projektes. Das Projektteam setzt sich aus Schlüsselfiguren Ihres Unternehmens und unseren Experten zusammen. Gemeinsam wird die aktuelle Situation in Ihrer Unternehmung analysiert und gestützt auf eine GAP-Analyse werden die erforderlichen Massnahmen geplant und umgesetzt. Dabei ist der Grösse und den Herausforderungen Ihres Unternehmens im Einzelfall Rechnung zu tragen.

H. Welche Relevanz hat das Schweizerische Datenschutzgesetz (DSG)?

Das Schweizerische Datenschutzgesetz (DSG) ist veraltet. Deshalb ist der Bundesrat daran, das DSG zu revidieren. Nach der Revision wird das DSG mit der DSGVO gleichwertig sein müssen, da die EU den Datenverkehr zwischen der EU und der Schweiz sonst untersagen könnte. Letzteres wäre für international tätige Unternehmen fatal. Folglich müssen selbst jene Unternehmen, die vorerst von der DSGVO nicht betroffen sind, die Regeln der DSGVO dennoch implementieren, da diese in Schweizerisches Recht überführt werden.

Am 15. September 2017 hat der Bundesrat die Botschaft zur Totalrevision des Datenschutzgesetzes verabschiedet. Die Revision wurde aber in der Woche vom 8. Januar 2018 von der vorberatenden Kommission des Nationalrates verzögert. Nunmehr ist davon auszugehen, dass der Schengen-Teil (dieser regelt den Datenaustausch zwischen den Behörden) frühestens in der Sommersession behandelt wird und Anfang 2019 in Kraft tritt. Wann der zweite Teil (dabei handelt es sich um die Vorschriften, wie Unternehmen mit Daten umgehen müssen) in Schweizerisches Recht übernommen wird, kann zum jetzigen Zeitpunkt noch nicht definiert werden.

I. Autor

Benjamin Domenig
Rechtsanwalt, Partner

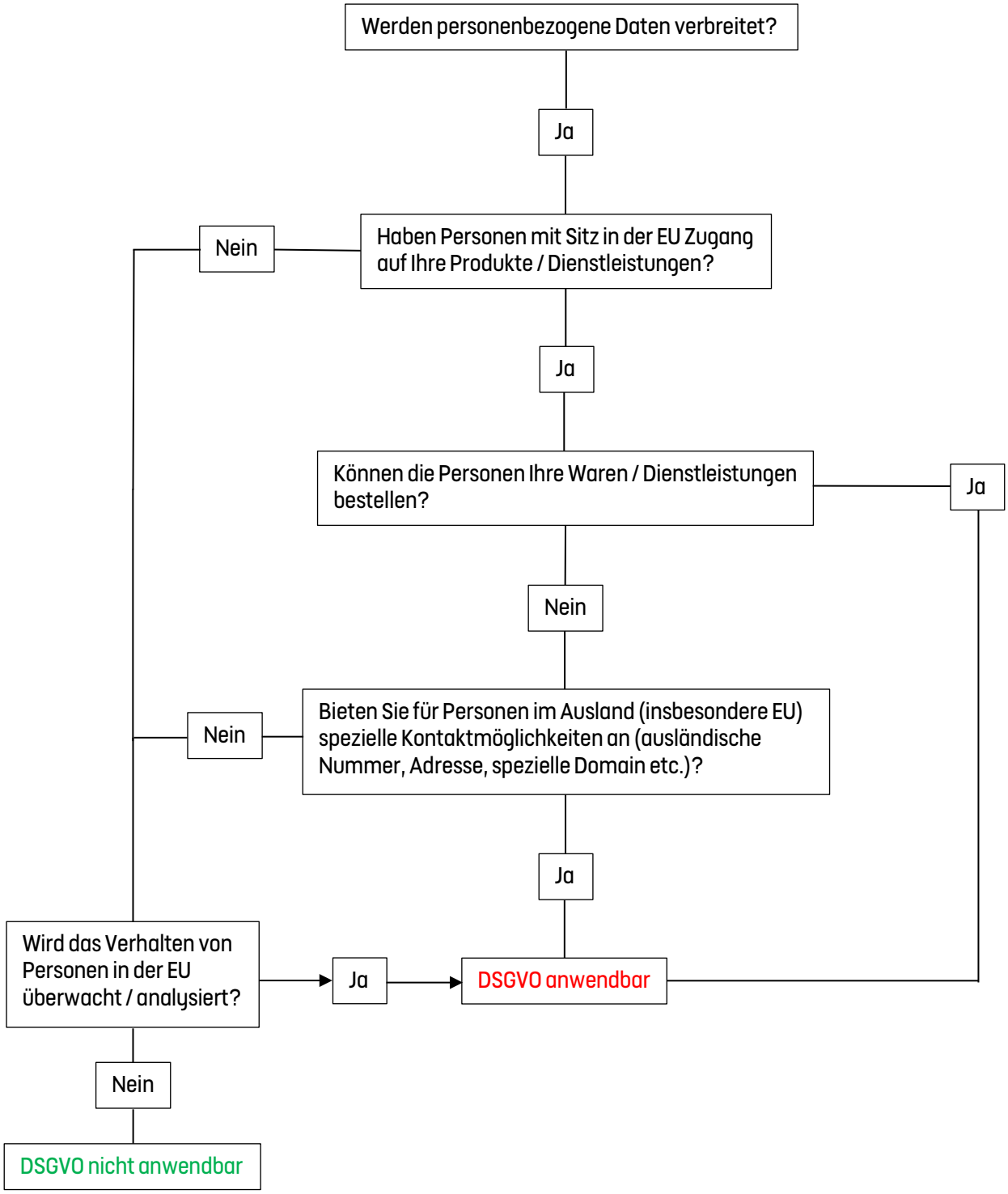
domenig@domenig.law

Domenig & Partner Rechtsanwälte AG
Hirschengraben 2, Postfach 2276
3001 Bern

Telefon: +41 31 380 11 00
Fax: +41 31 380 11 09
E-Mail: info@domenig.law

DOMENIG PARTNER
RECHTSANWÄLTE AG

Anwendungsbereich DSGVO für Schweizerische Unternehmen



DOMENIG & PARTNER RECHTSANWÄLTE AG
Hirschengraben 2 | Postfach 2276 | CH-3001 Bern
Tel.: +41 31 380 11 00 | Fax: +41 31 380 11 09 | info@domenig.law
www.domenig.law

CHE-284.941.671 MWST

DOMENIG PARTNER
RECHTSANWÄLTE AG

Projektphasen für die Implementierung der Europäischen Datenschutz-Grundverordnung (DSGVO)

Vorphase	Priorität
Bildung eines Projektteams	
Festlegung von Projektzielen	
Planung der Ressourcen für die einzelnen Projektphasen	
Festsetzung des Budgets	
Voruntersuchung	
Bestandsaufnahme bestehender Datenschutzstrukturen	
Verzeichnis aller Verarbeitungsvorgänge	
Prüfung der Rechtmässigkeitsgrundlagen	
GAP-Analyse zwischen IST-Zustand und SOLL-Zustand	
Entwicklung von Lösungsoptionen	
Einbindung des Datenschutzbeauftragten	
Umsetzungsphase	
Risikoanalyse DSGVO	**Hoch**
Datenschutzkommunikation im Unternehmen	**Mittel**
Einrichtung einer Datenschutzberatung im Unternehmen	**Mittel**
Kommunikation mit der Belegschaft, bzw. mit Betriebsräten	**Hoch**
Schulung und Sensibilisierung der Mitarbeiter	**Hoch**
Einführung eines Datenschutz-Management-Systems (DMS)	**Hoch**
– Zweckfestlegung und -änderung	**Hoch**
– Löschkonzepte	**Hoch**
– Datenschutz-Folgenabschätzung	**Hoch**
– Sicherheit der Verarbeitung	**Hoch**
– Aktualität des Verarbeitungsverzeichnisses	**Mittel**
– Sicherstellung der Betroffenenrechte	**Hoch**
– Kommunikation mit der Aufsichtsbehörde	**Niedrig**
– Datentransfers in Drittländer	**Mittel**
– Dokumentation sämtlicher relevanter Prozesse	**Hoch**
– Privacy by design and by default	**Mittel**
– Big data	**Mittel**
Anpassung der Auftragsverarbeitungen	**Hoch**
Vereinbarung über gemeinsame Verantwortliche	**Mittel**
Einrichtung eines Beschwerdemanagements	**Hoch**
Überprüfung bestehender Verträge	**Hoch**
Einwilligungsmanagement	**Hoch**

Darstellung in Anlehnung an WYBITUL/BREUNIG/STRÖBEL, Praktische Hinweise zur DSGVO-Umsetzung, in: Baeriswyl et. al. (Hrsg.), DIGMA, Zeitschrift für Datenrecht und Informationssicherheit, 17. Jahrgang, Heft. 1, März 2017, S. 27.

DOMENIG & PARTNER RECHTSANWÄLTE AG
Hirschengraben 2 | Postfach 2276 | CH-3001 Bern
Tel.: +41 31 380 11 00 | Fax: +41 31 380 11 09 | info@domenig.law
www.domenig.law

CHE-284.941.671 MWST