(Protection des données:) tour d’horizon de la nouvelle loi

19.05.2021

D'un coup d'oeil

Le Parlement a adopté la nouvelle loi sur la protection des données en automne 2020. Le délai référendaire a expiré en janvier 2021 sans qu’un référendum ait été lancé. Les travaux relatifs à l’ordonnance d’exécution (OLPD) étant encore en cours, il faut s’attendre à ce que la nouvelle loi entre en vigueur au second semestre 2022.

Il est recommandé aux entreprises suisses de se familiariser dès aujourd'hui avec la nouvelle loi et ses exigences et d'adapter leur dispositif de protection des données, en particulier en ce qui concerne leurs dispositions relatives à la protection des données et contrats. economiesuisse répond aux questions les plus pressantes en collaboration avec deux avocats, Me Cornelia Stengel et Me Luca Stäuble, afin de signaler aux entreprises suisses les mesures à prendre en lien avec l'entrée en vigueur de la nouvelle loi sur la protection des données (LPD).

Le présent tour d'horizon a pour seul but d'informer et de sensibiliser les personnes intéressées. Il ne remplace pas un conseil juridique. economiesuisse ne pourra être tenue pour responsable des actions ou omissions consécutives à la lecture de cet article.

1) Was sind Zweck und Anwendungsbereich des neuen Gesetzes (revDSG)?

Das neue Gesetz (revDSG) bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, die sich in der Schweiz befinden und deren Daten durch Private oder den Staat bearbeitet werden. Daten von juristischen Personen sind neu nicht mehr geschützt. Die zugrundeliegende Idee ist es, den betroffenen Personen mehr Transparenz und damit eine Stärkung ihrer Rechte in Bezug auf ihre eigenen Daten zu geben („informationelle Selbstbestimmung"). Weiter soll dadurch auch eine Förderung der Prävention und der Eigenverantwortung der Datenbearbeiter bewirkt werden. Damit verbunden sind die Stärkung der Datenschutzaufsicht und ein Ausbau der Strafbestimmungen. Für Unternehmen schafft das Gesetz ausserdem neue Pflichten, insbesondere bei der Erhebung, dem Verlust oder dem Missbrauch von Personendaten.

1) Was sind Zweck und Anwendungsbereich des neuen Gesetzes (revDSG)?

Das neue Gesetz (revDSG) bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, die sich in der Schweiz befinden und deren Daten durch Private oder den Staat bearbeitet werden. Daten von juristischen Personen sind neu nicht mehr geschützt. Die zugrundeliegende Idee ist es, den betroffenen Personen mehr Transparenz und damit eine Stärkung ihrer Rechte in Bezug auf ihre eigenen Daten zu geben („informationelle Selbstbestimmung“). Weiter soll dadurch auch eine Förderung der Prävention und der Eigenverantwortung der Datenbearbeiter bewirkt werden. Damit verbunden sind die Stärkung der Datenschutzaufsicht und ein Ausbau der Strafbestimmungen. Für Unternehmen schafft das Gesetz ausserdem neue Pflichten, insbesondere bei der Erhebung, dem Verlust oder dem Missbrauch von Personendaten.

1) Was sind Zweck und Anwendungsbereich des neuen Gesetzes (revDSG)?

Das neue Gesetz (revDSG) bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, die sich in der Schweiz befinden und deren Daten durch Private oder den Staat bearbeitet werden. Daten von juristischen Personen sind neu nicht mehr geschützt. Die zugrundeliegende Idee ist es, den betroffenen Personen mehr Transparenz und damit eine Stärkung ihrer Rechte in Bezug auf ihre eigenen Daten zu geben („informationelle Selbstbestimmung“). Weiter soll dadurch auch eine Förderung der Prävention und der Eigenverantwortung der Datenbearbeiter bewirkt werden. Damit verbunden sind die Stärkung der Datenschutzaufsicht und ein Ausbau der Strafbestimmungen. Für Unternehmen schafft das Gesetz ausserdem neue Pflichten, insbesondere bei der Erhebung, dem Verlust oder dem Missbrauch von Personendaten.

2) Für welches Territorium kommt das neue Gesetz zur Anwendung?

Obwohl das revDSG primär für das Territorium der Schweiz gilt, hat das Gesetz auch einen extraterritorialen Anwendungsbereich. Es kann sich namentlich auf Sachverhalte erstrecken, die sich zwar im Ausland ereignen, aber Auswirkungen in der Schweiz haben (Art. 3). Mit anderen Worten: Wenn die Bearbeitung von Personendaten ausserhalb der Schweiz stattfindet, aber natürliche Personen in der Schweiz betrifft und die Auswirkungen davon in der Schweiz spürbar sind (dieses Kriterium sollte in der Verordnung noch konkretisiert werden), muss der betreffende Datenbearbeiter im Ausland das neue Schweizer Recht einhalten. Darüber hinaus muss er unter bestimmten Voraussetzungen einen gesetzlichen Vertreter in der Schweiz bestellen (Art. 14 und Art. 15 revDSG).

Beispiel: Ein Unternehmen hat seinen Sitz im Ausland und bearbeitet vom Ausland aus Daten von natürlichen Personen in der Schweiz. In diesem Fall muss eine Einzelfallprüfung vorgenommen werden. Je nachdem, ob die Datenbearbeitung in der Schweiz „spürbar“ ist oder nicht, käme das revDSG zur Anwendung. Die DSGVO stellt bspw. darauf ab, ob die Datenbearbeitung im Zusammenhang mit der Ausrichtung des Angebots von Waren oder Dienstleistungen auf Personen in der EU erfolgt.

2) Für welches Territorium kommt das neue Gesetz zur Anwendung?

Obwohl das revDSG primär für das Territorium der Schweiz gilt, hat das Gesetz auch einen extraterritorialen Anwendungsbereich. Es kann sich namentlich auf Sachverhalte erstrecken, die sich zwar im Ausland ereignen, aber Auswirkungen in der Schweiz haben (Art. 3). Mit anderen Worten: Wenn die Bearbeitung von Personendaten ausserhalb der Schweiz stattfindet, aber natürliche Personen in der Schweiz betrifft und die Auswirkungen davon in der Schweiz spürbar sind (dieses Kriterium sollte in der Verordnung noch konkretisiert werden), muss der betreffende Datenbearbeiter im Ausland das neue Schweizer Recht einhalten. Darüber hinaus muss er unter bestimmten Voraussetzungen einen gesetzlichen Vertreter in der Schweiz bestellen (Art. 14 und Art. 15 revDSG).

Beispiel: Ein Unternehmen hat seinen Sitz im Ausland und bearbeitet vom Ausland aus Daten von natürlichen Personen in der Schweiz. In diesem Fall muss eine Einzelfallprüfung vorgenommen werden. Je nachdem, ob die Datenbearbeitung in der Schweiz „spürbar“ ist oder nicht, käme das revDSG zur Anwendung. Die DSGVO stellt bspw. darauf ab, ob die Datenbearbeitung im Zusammenhang mit der Ausrichtung des Angebots von Waren oder Dienstleistungen auf Personen in der EU erfolgt.

2) Für welches Territorium kommt das neue Gesetz zur Anwendung?

Obwohl das revDSG primär für das Territorium der Schweiz gilt, hat das Gesetz auch einen extraterritorialen Anwendungsbereich. Es kann sich namentlich auf Sachverhalte erstrecken, die sich zwar im Ausland ereignen, aber Auswirkungen in der Schweiz haben (Art. 3). Mit anderen Worten: Wenn die Bearbeitung von Personendaten ausserhalb der Schweiz stattfindet, aber natürliche Personen in der Schweiz betrifft und die Auswirkungen davon in der Schweiz spürbar sind (dieses Kriterium sollte in der Verordnung noch konkretisiert werden), muss der betreffende Datenbearbeiter im Ausland das neue Schweizer Recht einhalten. Darüber hinaus muss er unter bestimmten Voraussetzungen einen gesetzlichen Vertreter in der Schweiz bestellen (Art. 14 und Art. 15 revDSG).

Beispiel: Ein Unternehmen hat seinen Sitz im Ausland und bearbeitet vom Ausland aus Daten von natürlichen Personen in der Schweiz. In diesem Fall muss eine Einzelfallprüfung vorgenommen werden. Je nachdem, ob die Datenbearbeitung in der Schweiz „spürbar“ ist oder nicht, käme das revDSG zur Anwendung. Die DSGVO stellt bspw. darauf ab, ob die Datenbearbeitung im Zusammenhang mit der Ausrichtung des Angebots von Waren oder Dienstleistungen auf Personen in der EU erfolgt.

3) Warum war eine Überarbeitung des aktuellen Gesetzes notwendig?

Das aktuelle Schweizer Datenschutzgesetz stammt aus dem Jahr 1992. Seither nahmen die Erhebung und Nutzung von Personendaten im Zuge der fortschreitenden Digitalisierung von Wirtschaft und Gesellschaft rasant zu. Auf globaler Ebene und insbesondere im EU-Raum wurde der Datenschutz stark ausgebaut und internationale Organisationen haben ihre datenschutzrechtlichen Mindeststandards verschärft. Für die Schweiz war es daher notwendig, das 30 Jahre alte Gesetz an die neuen Formen des Konsums (Online-Shopping, soziale Netzwerke usw.), an die technologischen Entwicklungen (Digitalisierung, künstliche Intelligenz usw.) sowie an die internationalen Standards anzupassen.

Auf internationaler Ebene hat insbesondere die Europäische Union (EU) mit der seit 25. Mai 2018 gültigen Datenschutz-Grundverordnung (DSGVO oder „GDPR“) einen neuen, hohen Standard gesetzt, der aufgrund seines extraterritorialen Geltungsbereichs weltweit Beachtung findet. Auch viele Schweizer Unternehmen fallen aufgrund ihrer Ausrichtung auf den EU- bzw. EWR-Raum in den Anwendungsbereich der DSGVO. Zudem verlangt die DSGVO, dass Daten nur dann ohne weiteres in einen anderen Staat übermittelt werden dürfen, wenn dieser über ein aus Sicht der EU „angemessenes“ Datenschutzniveau verfügt. Der problemlose Datenfluss aus der EU ist für Länder wie die Schweiz, welche sehr enge wirtschaftliche Beziehungen zur EU führen von besonders grosser Bedeutung.

Ein wichtiges Ziel der Revision des Schweizer DSG war daher, eine international abgestimmte – aus Sicht der EU „gleichwertige“ – Lösung zu erarbeiten, welche die technologischen Entwicklungen im Zusammenhang mit der Datenwirtschaft fördert und gleichzeitig die Stärken der bisherigen Gesetzgebung nicht aufgibt.

Mit dem neuen Gesetz werden insbesondere die Informationspflichten sowie die Betroffenenrechte ausgebaut. Ausserdem wird neu das sogenannte „Profiling“ geregelt. Unter Profiling wird jede Art der automatisierten Bearbeitung von Personendaten verstanden, mit welcher bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen (z.B. Arbeitsleistung, wirtschaftliche Situation, Gesundheit, Interessen, Aufenthaltsort), bewertet, analysiert oder vorhergesagt wird. Verschärfte

Rechtsfolgen gelten indes nur beim Profiling mit hohem Risiko für die Persönlichkeit der betroffenen Person.

Verfügt die Schweiz aus Sicht der EU über ein „angemessenes" Datenschutzniveau?

Die Schweiz ist aus der Sicht der EU ein „Drittland". Damit der Datentransfer in ein Drittland ohne weiteres möglich ist, braucht es einen Angemessenheitsbeschluss der EU-Kommission. Aktuell liegt dieser Beschluss für die Schweiz zwar vor, allerdings erfolgte die Prüfung nach altem EU-Recht. Die EU prüft derzeit, ob das (revidierte) Schweizer Datenschutzgesetz auch unter der DSGVO als angemessen qualifiziert. Die Schweiz dürfte mit der Revision die Voraussetzungen geschaffen haben, damit die EU die Angemessenheit bejaht. Aufgrund der neuesten EU-Rechtsprechung zum Datenfluss in Drittstaaten, wohl aber auch aus politischen Gründen verzögert sich die auf letztes Jahr angekündigte Beschlussfassung.

Schliesslich darf nicht vergessen werden, dass die Modernisierung des Schweizer Rechts in einem globalen Kontext stattfindet, in dem Bürger und Verbraucher weltweit mehr Schutz und Kontrolle über ihre persönlichen Daten fordern. Dieser Trend ist nicht auf die EU beschränkt, sondern beeinflusste zahlreiche andere Länder, darunter etwa auch Japan. Auch in Kalifornien wurde inzwischen ein strengeres Datenschutzgesetz, das sich teilweise am europäischen Standard orientiert, umgesetzt.

3) Warum war eine Überarbeitung des aktuellen Gesetzes notwendig?

Das aktuelle Schweizer Datenschutzgesetz stammt aus dem Jahr 1992. Seither nahmen die Erhebung und Nutzung von Personendaten im Zuge der fortschreitenden Digitalisierung von Wirtschaft und Gesellschaft rasant zu. Auf globaler Ebene und insbesondere im EU-Raum wurde der Datenschutz stark ausgebaut und internationale Organisationen haben ihre datenschutzrechtlichen Mindeststandards verschärft. Für die Schweiz war es daher notwendig, das 30 Jahre alte Gesetz an die neuen Formen des Konsums (Online-Shopping, soziale Netzwerke usw.), an die technologischen Entwicklungen (Digitalisierung, künstliche Intelligenz usw.) sowie an die internationalen Standards anzupassen.

Auf internationaler Ebene hat insbesondere die Europäische Union (EU) mit der seit 25. Mai 2018 gültigen Datenschutz-Grundverordnung (DSGVO oder „GDPR“) einen neuen, hohen Standard gesetzt, der aufgrund seines extraterritorialen Geltungsbereichs weltweit Beachtung findet. Auch viele Schweizer Unternehmen fallen aufgrund ihrer Ausrichtung auf den EU- bzw. EWR-Raum in den Anwendungsbereich der DSGVO. Zudem verlangt die DSGVO, dass Daten nur dann ohne weiteres in einen anderen Staat übermittelt werden dürfen, wenn dieser über ein aus Sicht der EU „angemessenes“ Datenschutzniveau verfügt. Der problemlose Datenfluss aus der EU ist für Länder wie die Schweiz, welche sehr enge wirtschaftliche Beziehungen zur EU führen von besonders grosser Bedeutung.

Ein wichtiges Ziel der Revision des Schweizer DSG war daher, eine international abgestimmte – aus Sicht der EU „gleichwertige“ – Lösung zu erarbeiten, welche die technologischen Entwicklungen im Zusammenhang mit der Datenwirtschaft fördert und gleichzeitig die Stärken der bisherigen Gesetzgebung nicht aufgibt.

Mit dem neuen Gesetz werden insbesondere die Informationspflichten sowie die Betroffenenrechte ausgebaut. Ausserdem wird neu das sogenannte „Profiling“ geregelt. Unter Profiling wird jede Art der automatisierten Bearbeitung von Personendaten verstanden, mit welcher bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen (z.B. Arbeitsleistung, wirtschaftliche Situation, Gesundheit, Interessen, Aufenthaltsort), bewertet, analysiert oder vorhergesagt wird. Verschärfte Rechtsfolgen gelten indes nur beim Profiling mit hohem Risiko für die Persönlichkeit der betroffenen Person.

Verfügt die Schweiz aus Sicht der EU über ein „angemessenes“ Datenschutzniveau?

Die Schweiz ist aus der Sicht der EU ein „Drittland“. Damit der Datentransfer in ein Drittland ohne weiteres möglich ist, braucht es einen Angemessenheitsbeschluss der EU-Kommission. Aktuell liegt dieser Beschluss für die Schweiz zwar vor, allerdings erfolgte die Prüfung nach altem EU-Recht. Die EU prüft derzeit, ob das (revidierte) Schweizer Datenschutzgesetz auch unter der DSGVO als angemessen qualifiziert. Die Schweiz dürfte mit der Revision die Voraussetzungen geschaffen haben, damit die EU die Angemessenheit bejaht. Aufgrund der neuesten EU-Rechtsprechung zum Datenfluss in Drittstaaten, wohl aber auch aus

politischen Gründen verzögert sich die auf letztes Jahr angekündigte Beschlussfassung.

Schliesslich darf nicht vergessen werden, dass die Modernisierung des Schweizer Rechts in einem globalen Kontext stattfindet, in dem Bürger und Verbraucher weltweit mehr Schutz und Kontrolle über ihre persönlichen Daten fordern. Dieser Trend ist nicht auf die EU beschränkt, sondern beeinflusste zahlreiche andere Länder, darunter etwa auch Japan. Auch in Kalifornien wurde inzwischen ein strengeres Datenschutzgesetz, das sich teilweise am europäischen Standard orientiert, umgesetzt.

3) Warum war eine Überarbeitung des aktuellen Gesetzes notwendig?

Das aktuelle Schweizer Datenschutzgesetz stammt aus dem Jahr 1992. Seither nahmen die Erhebung und Nutzung von Personendaten im Zuge der fortschreitenden Digitalisierung von Wirtschaft und Gesellschaft rasant zu. Auf globaler Ebene und insbesondere im EU-Raum wurde der Datenschutz stark ausgebaut und internationale Organisationen haben ihre datenschutzrechtlichen Mindeststandards verschärft. Für die Schweiz war es daher notwendig, das 30 Jahre alte Gesetz an die neuen Formen des Konsums (Online-Shopping, soziale Netzwerke usw.), an die technologischen Entwicklungen (Digitalisierung, künstliche Intelligenz usw.) sowie an die internationalen Standards anzupassen.

Auf internationaler Ebene hat insbesondere die Europäische Union (EU) mit der seit 25. Mai 2018 gültigen Datenschutz-Grundverordnung (DSGVO oder „GDPR“) einen neuen, hohen Standard gesetzt, der aufgrund seines extraterritorialen Geltungsbereichs weltweit Beachtung findet. Auch viele Schweizer Unternehmen fallen aufgrund ihrer Ausrichtung auf den EU- bzw. EWR-Raum in den Anwendungsbereich der DSGVO. Zudem verlangt die DSGVO, dass Daten nur dann ohne weiteres in einen anderen Staat übermittelt werden dürfen, wenn dieser über ein aus Sicht der EU „angemessenes“ Datenschutzniveau verfügt. Der problemlose Datenfluss aus der EU ist für Länder wie die Schweiz, welche sehr enge wirtschaftliche Beziehungen zur EU führen von besonders grosser Bedeutung.

Ein wichtiges Ziel der Revision des Schweizer DSG war daher, eine international abgestimmte – aus Sicht der EU „gleichwertige“ – Lösung zu erarbeiten, welche die technologischen Entwicklungen im Zusammenhang

mit der Datenwirtschaft fördert und gleichzeitig die Stärken der bisherigen Gesetzgebung nicht aufgibt.

Mit dem neuen Gesetz werden insbesondere die Informationspflichten sowie die Betroffenenrechte ausgebaut. Ausserdem wird neu das sogenannte „Profiling“ geregelt. Unter Profiling wird jede Art der automatisierten Bearbeitung von Personendaten verstanden, mit welcher bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen (z.B. Arbeitsleistung, wirtschaftliche Situation, Gesundheit, Interessen, Aufenthaltsort), bewertet, analysiert oder vorhergesagt wird. Verschärfte Rechtsfolgen gelten indes nur beim Profiling mit hohem Risiko für die Persönlichkeit der betroffenen Person.

Verfügt die Schweiz aus Sicht der EU über ein „angemessenes“ Datenschutzniveau?

Die Schweiz ist aus der Sicht der EU ein „Drittland“. Damit der Datentransfer in ein Drittland ohne weiteres möglich ist, braucht es einen Angemessenheitsbeschluss der EU-Kommission. Aktuell liegt dieser Beschluss für die Schweiz zwar vor, allerdings erfolgte die Prüfung nach altem EU-Recht. Die EU prüft derzeit, ob das (revidierte) Schweizer Datenschutzgesetz auch unter der DSGVO als angemessen qualifiziert. Die Schweiz dürfte mit der Revision die Voraussetzungen geschaffen haben, damit die EU die Angemessenheit bejaht. Aufgrund der neuesten EU-Rechtsprechung zum Datenfluss in Drittstaaten, wohl aber auch aus politischen Gründen verzögert sich die auf letztes Jahr angekündigte Beschlussfassung.

Schliesslich darf nicht vergessen werden, dass die Modernisierung des Schweizer Rechts in einem globalen Kontext stattfindet, in dem Bürger und Verbraucher weltweit mehr Schutz und Kontrolle über ihre persönlichen Daten fordern. Dieser Trend ist nicht auf die EU beschränkt, sondern beeinflusste zahlreiche andere Länder, darunter etwa auch Japan. Auch in Kalifornien wurde inzwischen ein strengeres Datenschutzgesetz, das sich teilweise am europäischen Standard orientiert, umgesetzt.

4) Wann wird das neue Gesetz (revDSG) in Kraft treten?

Aller Voraussicht nach wird das revDSG in der zweiten Hälfte des Jahres 2022 in Kraft treten. Da die Arbeiten an den Verordnungen noch nicht abgeschlossen sind (Vernehmlassung für Juni 2021 geplant), steht dieser Termin aber noch nicht fest und einzelne Quellen gehen momentan von einem späteren Inkrafttreten aus. Das Gesetz sieht aber keine relevanten Übergangsfristen vor, weshalb eine Umsetzung der erforderlichen Anpassungen durch die Unternehmen frühzeitig erfolgen sollte.

4) Wann wird das neue Gesetz (revDSG) in Kraft treten?

Aller Voraussicht nach wird das revDSG in der zweiten Hälfte des Jahres 2022 in Kraft treten. Da die Arbeiten an den Verordnungen noch nicht abgeschlossen sind (Vernehmlassung für Juni 2021 geplant), steht dieser Termin aber noch nicht fest und einzelne Quellen gehen momentan von einem späteren Inkrafttreten aus. Das Gesetz sieht aber keine relevanten Übergangsfristen vor, weshalb eine Umsetzung der erforderlichen Anpassungen durch die Unternehmen frühzeitig erfolgen sollte.

4) Wann wird das neue Gesetz (revDSG) in Kraft treten?

Aller Voraussicht nach wird das revDSG in der zweiten Hälfte des Jahres 2022 in Kraft treten. Da die Arbeiten an den Verordnungen noch nicht abgeschlossen sind (Vernehmlassung für Juni 2021 geplant), steht dieser Termin aber noch nicht fest und einzelne Quellen gehen momentan von einem späteren Inkrafttreten aus. Das Gesetz sieht aber keine relevanten Übergangsfristen vor, weshalb eine Umsetzung der erforderlichen Anpassungen durch die Unternehmen frühzeitig erfolgen sollte.

5) In welchen Bereichen geht das überarbeitete Schweizer Gesetz weiter als die EU-DSGVO?

Die Revision des Schweizer DSG orientiert sich grundsätzlich an den inhaltlichen Vorgaben der DSGVO, weist aber einige Besonderheiten auf. In den meisten Fällen ist das Schweizer Gesetz weniger formalistisch und hat weniger spezifische Regelungsinhalte als die DSGVO. Es gibt jedoch einige wenige Punkte, in denen das neue DSG strenger sein wird als die DSGVO. Dazu gehören etwa der sachliche Anwendungsbereich (Art. 2 revDSG), die Informationspflicht bei der Erhebung von Personendaten (Art. 19 revDSG), die Sanktionen für natürliche Personen (Art. 60 ff. revDSG) und die Definition der besonders schützenswerten Personendaten.

5) In welchen Bereichen geht das überarbeitete Schweizer Gesetz weiter als die EU-DSGVO?

Die Revision des Schweizer DSG orientiert sich grundsätzlich an den inhaltlichen Vorgaben der DSGVO, weist aber einige Besonderheiten auf. In den meisten Fällen ist das Schweizer Gesetz weniger formalistisch und hat weniger spezifische Regelungsinhalte als die DSGVO. Es gibt jedoch einige wenige Punkte, in denen das neue DSG strenger sein wird als die DSGVO. Dazu gehören etwa der sachliche Anwendungsbereich (Art. 2 revDSG), die Informationspflicht bei der Erhebung von Personendaten (Art. 19 revDSG), die Sanktionen für natürliche Personen (Art. 60 ff. revDSG) und die Definition der besonders schützenswerten Personendaten.

5) In welchen Bereichen geht das überarbeitete Schweizer Gesetz weiter als die EU-DSGVO?

Die Revision des Schweizer DSG orientiert sich grundsätzlich an den inhaltlichen Vorgaben der DSGVO, weist aber einige Besonderheiten auf. In den meisten Fällen ist das Schweizer Gesetz weniger formalistisch und hat weniger spezifische Regelungsinhalte als die DSGVO. Es gibt jedoch einige wenige Punkte, in denen das neue DSG strenger sein wird als die DSGVO. Dazu gehören etwa der sachliche Anwendungsbereich (Art. 2 revDSG), die Informationspflicht bei der Erhebung von Personendaten (Art. 19 revDSG), die Sanktionen für natürliche Personen (Art. 60 ff. revDSG) und die Definition der besonders schützenswerten Personendaten.

6) Schliesst das neue Gesetz KMUs aus? Werden nur grosse Unternehmen betroffen sein?

Nein. Alle Unternehmen, ohne Ausnahme, sind von dem neuen Datenschutzgesetz betroffen. Unabhängig von seiner Grösse verfügt jedes Unternehmen über eine Vielzahl von Daten seiner Kunden, Partner, Lieferanten und Mitarbeiter. Mit der Digitalisierung der Wirtschaft wird die Menge der zu verarbeitenden Daten in den Unternehmen, auch bei den KMU, weiter zunehmen. Entsprechend sollten sich alle Unternehmen auf das Inkrafttreten des neuen Gesetzes vorbereiten. Da sich das Gesetz an den EU-Standards orientiert, gilt dies umso mehr für Unternehmen, die ihr Datenschutz-Konzept noch nicht an die DSGVO angepasst haben.

Dabei sollte auch berücksichtigt werden, dass Kriminalität im digitalen Raum konstant zunimmt. So steigt die Anzahl Cyberangriffe und kein Unternehmen kann davor bewahrt werden. Das neue Datenschutzgesetz verpflichtet Unternehmen dazu, die notwendigen organisatorischen und technischen Massnahmen zu ergreifen, um die Datensicherheit sicherzustellen und den Datenmissbrauch möglichst zu verhindern.

6) Schliesst das neue Gesetz KMUs aus? Werden nur grosse Unternehmen betroffen sein?

Nein. Alle Unternehmen, ohne Ausnahme, sind von dem neuen Datenschutzgesetz betroffen. Unabhängig von seiner Grösse verfügt jedes Unternehmen über eine Vielzahl von Daten seiner Kunden, Partner, Lieferanten und Mitarbeiter. Mit der Digitalisierung der Wirtschaft wird die Menge der zu verarbeitenden Daten in den Unternehmen, auch bei den KMU, weiter zunehmen. Entsprechend sollten sich alle Unternehmen auf das Inkrafttreten des neuen Gesetzes vorbereiten. Da sich das Gesetz an den EU-Standards orientiert, gilt dies umso mehr für Unternehmen, die ihr Datenschutz-Konzept noch nicht an die DSGVO angepasst haben.

Dabei sollte auch berücksichtigt werden, dass Kriminalität im digitalen Raum konstant zunimmt. So steigt die Anzahl Cyberangriffe und kein Unternehmen kann davor bewahrt werden. Das neue Datenschutzgesetz verpflichtet Unternehmen dazu, die notwendigen organisatorischen und technischen Massnahmen zu ergreifen, um die Datensicherheit sicherzustellen und den Datenmissbrauch möglichst zu verhindern.

6) Schliesst das neue Gesetz KMUs aus? Werden nur grosse Unternehmen betroffen sein?

Nein. Alle Unternehmen, ohne Ausnahme, sind von dem neuen Datenschutzgesetz betroffen. Unabhängig von seiner Grösse verfügt jedes Unternehmen über eine Vielzahl von Daten seiner Kunden, Partner, Lieferanten und Mitarbeiter. Mit der Digitalisierung der Wirtschaft wird die Menge der zu verarbeitenden Daten in den Unternehmen, auch bei den KMU, weiter zunehmen. Entsprechend sollten sich alle Unternehmen auf das Inkrafttreten des neuen Gesetzes vorbereiten. Da sich das Gesetz an den EU-Standards orientiert, gilt dies umso mehr für Unternehmen, die ihr Datenschutz-Konzept noch nicht an die DSGVO angepasst haben.

Dabei sollte auch berücksichtigt werden, dass Kriminalität im digitalen Raum konstant zunimmt. So steigt die Anzahl Cyberangriffe und kein Unternehmen kann davor bewahrt werden. Das neue Datenschutzgesetz verpflichtet Unternehmen dazu, die notwendigen organisatorischen und technischen Massnahmen zu ergreifen, um die Datensicherheit sicherzustellen und den Datenmissbrauch möglichst zu verhindern.

7) Was müssen Unternehmen nun tun, um mit dem neuen DSG konform zu werden?

Jedes Unternehmen muss sich auf das Inkrafttreten des neuen Gesetzes vorbereiten. Eine Bestandsaufnahme der Bearbeitung von Personendaten im Unternehmen und eine Risikobewertung sind erforderlich, um die Anforderungen an die Datenschutz-Compliance zu bestimmen. Ausserdem können mittels Gap-Analyse (Vergleich Ist- und Sollzustand) die erforderlichen Umsetzungsarbeiten identifiziert werden. Höhere Compliance-Anforderungen liegen z.B. vor, wenn:

- Unternehmen eine grosse Menge an Personendaten bearbeiten. Zum Beispiel haben Unternehmen, die sich auf Online-Verkäufe oder Import/Export spezialisiert haben, einen grossen Kundenstamm, der eine beträchtliche Menge an Personendaten generiert.
- Unternehmen besonders schützenswerte Personendaten (wie in Art. 5 lit. c revDSG definiert) bearbeiten. Betroffen sind z.B. Unternehmen, die Personendaten über politische oder religiöse Meinungen, Gesundheit, genetische oder rassische Daten, Sozialhilfe, Strafverfolgung, Profiling usw. bearbeiten.

In diesen Fällen sind die Anforderungen an die rechtmässige Bearbeitung von Personendaten bzw. das Risiko der Verletzung von Persönlichkeitsrechten höher als bspw. bei Unternehmen, die Daten einer begrenzten Anzahl Mitarbeiter, Lieferanten, Kunden etc. bearbeiten.

Die Datenschutz-Compliance-Arbeit erfordert je nach Art und Umfang der bearbeiteten Personendaten die Entwicklung oder Beiziehung von Datenschutz-Knowhow sowie die Einrichtung interner Prozesse, um die Anforderungen des neuen Gesetzes zu erfüllen. Nicht zu unterschätzen sind die materiellen Ressourcen (Datenverwaltungssoftware etc.), die personellen

Ressourcen (Data Protection Officer bzw. für den Datenschutz zuständige Mitarbeiter etc.) und die Zeit, die dafür aufgewendet werden muss.

Je nach Umfang der Compliance-Anforderungen wird den Unternehmen dringend empfohlen, die Dienste von IT-Experten, Anwälten und Schulungsangeboten der Handelskammern in Anspruch zu nehmen.

7) Was müssen Unternehmen nun tun, um mit dem neuen DSG konform zu werden?

Jedes Unternehmen muss sich auf das Inkrafttreten des neuen Gesetzes vorbereiten. Eine Bestandsaufnahme der Bearbeitung von Personendaten im Unternehmen und eine Risikobewertung sind erforderlich, um die Anforderungen an die Datenschutz-Compliance zu bestimmen. Ausserdem können mittels Gap-Analyse (Vergleich Ist- und Sollzustand) die erforderlichen Umsetzungsarbeiten identifiziert werden. Höhere Compliance-Anforderungen liegen z.B. vor, wenn:

- Unternehmen eine grosse Menge an Personendaten bearbeiten. Zum Beispiel haben Unternehmen, die sich auf Online-Verkäufe oder Import/Export spezialisiert haben, einen grossen Kundenstamm, der eine beträchtliche Menge an Personendaten generiert.
- Unternehmen besonders schützenswerte Personendaten (wie in Art. 5 lit. c revDSG definiert) bearbeiten. Betroffen sind z.B. Unternehmen, die Personendaten über politische oder religiöse Meinungen, Gesundheit, genetische oder rassische Daten, Sozialhilfe, Strafverfolgung, Profiling usw. bearbeiten.

In diesen Fällen sind die Anforderungen an die rechtmässige Bearbeitung von Personendaten bzw. das Risiko der Verletzung von Persönlichkeitsrechten höher als bspw. bei Unternehmen, die Daten einer begrenzten Anzahl Mitarbeiter, Lieferanten, Kunden etc. bearbeiten.

Die Datenschutz-Compliance-Arbeit erfordert je nach Art und Umfang der bearbeiteten Personendaten die Entwicklung oder Beiziehung von Datenschutz-Knowhow sowie die Einrichtung interner Prozesse, um die Anforderungen des neuen Gesetzes zu erfüllen. Nicht zu unterschätzen sind die materiellen Ressourcen (Datenverwaltungssoftware etc.), die personellen Ressourcen (Data Protection Officer bzw. für den Datenschutz zuständige Mitarbeiter etc.) und die Zeit, die dafür aufgewendet werden muss.

Je nach Umfang der Compliance-Anforderungen wird den Unternehmen dringend empfohlen, die Dienste von IT-Experten, Anwälten und Schulungsangeboten der Handelskammern in Anspruch zu nehmen.

7) Was müssen Unternehmen nun tun, um mit dem neuen DSG konform zu werden?

Jedes Unternehmen muss sich auf das Inkrafttreten des neuen Gesetzes vorbereiten. Eine Bestandsaufnahme der Bearbeitung von Personendaten im Unternehmen und eine Risikobewertung sind erforderlich, um die Anforderungen an die Datenschutz-Compliance zu bestimmen. Ausserdem können mittels Gap-Analyse (Vergleich Ist- und Sollzustand) die erforderlichen Umsetzungsarbeiten identifiziert werden. Höhere Compliance-Anforderungen liegen z.B. vor, wenn:

- Unternehmen eine grosse Menge an Personendaten bearbeiten. Zum Beispiel haben Unternehmen, die sich auf Online-Verkäufe oder Import/Export spezialisiert haben, einen grossen Kundenstamm, der eine beträchtliche Menge an Personendaten generiert.
- Unternehmen besonders schützenswerte Personendaten (wie in Art. 5 lit. c revDSG definiert) bearbeiten. Betroffen sind z.B. Unternehmen, die Personendaten über politische oder religiöse Meinungen, Gesundheit, genetische oder rassische Daten, Sozialhilfe, Strafverfolgung, Profiling usw. bearbeiten.

In diesen Fällen sind die Anforderungen an die rechtmässige Bearbeitung von Personendaten bzw. das Risiko der Verletzung von Persönlichkeitsrechten höher als bspw. bei Unternehmen, die Daten einer begrenzten Anzahl Mitarbeiter, Lieferanten, Kunden etc. bearbeiten.

Die Datenschutz-Compliance-Arbeit erfordert je nach Art und Umfang der bearbeiteten Personendaten die Entwicklung oder Beiziehung von

Datenschutz-Knowhow sowie die Einrichtung interner Prozesse, um die Anforderungen des neuen Gesetzes zu erfüllen. Nicht zu unterschätzen sind die materiellen Ressourcen (Datenverwaltungssoftware etc.), die personellen Ressourcen (Data Protection Officer bzw. für den Datenschutz zuständige Mitarbeiter etc.) und die Zeit, die dafür aufgewendet werden muss.

Je nach Umfang der Compliance-Anforderungen wird den Unternehmen dringend empfohlen, die Dienste von IT-Experten, Anwälten und Schulungsangeboten der Handelskammern in Anspruch zu nehmen.

8) Warum ist es wichtig, sich bereits jetzt vorzubereiten?

Mit Ausnahme bestimmter Verpflichtungen sieht das neue Gesetz keine relevanten Übergangsvorschriften vor. Somit wird ein Grossteil der im Gesetz festgelegten Pflichten mit Inkrafttreten des revDSG sofort gelten. Es ist daher wichtig und wird empfohlen, sich frühzeitig vorzubereiten und bereits jetzt allfälligen Handlungsbedarf zu eruieren. Dadurch kann erreicht werden, dass im Zeitpunkt des Inkrafttretens des revDSG ein effektiver Datenschutz besteht (rechtzeitiger Aufbau von internem Fachwissen, Erstellung von internen Richtlinien sowie Anpassung von Dokumenten wie Datenschutzerklärungen und Verträgen mit Partnern und Datenbearbeitern).

8) Warum ist es wichtig, sich bereits jetzt vorzubereiten?

Mit Ausnahme bestimmter Verpflichtungen sieht das neue Gesetz keine relevanten Übergangsvorschriften vor. Somit wird ein Grossteil der im Gesetz festgelegten Pflichten mit Inkrafttreten des revDSG sofort gelten. Es ist daher wichtig und wird empfohlen, sich frühzeitig vorzubereiten und bereits jetzt allfälligen Handlungsbedarf zu eruieren. Dadurch kann erreicht werden, dass im Zeitpunkt des Inkrafttretens des revDSG ein effektiver Datenschutz besteht (rechtzeitiger Aufbau von internem Fachwissen, Erstellung von internen Richtlinien sowie Anpassung von Dokumenten wie Datenschutzerklärungen und Verträgen mit Partnern und Datenbearbeitern).

8) Warum ist es wichtig, sich bereits jetzt vorzubereiten?

Mit Ausnahme bestimmter Verpflichtungen sieht das neue Gesetz keine relevanten Übergangsvorschriften vor. Somit wird ein Grossteil der im Gesetz festgelegten Pflichten mit Inkrafttreten des revDSG sofort gelten. Es ist daher wichtig und wird empfohlen, sich frühzeitig vorzubereiten und bereits jetzt allfälligen Handlungsbedarf zu eruieren. Dadurch kann erreicht werden, dass im Zeitpunkt des Inkrafttretens des revDSG ein effektiver Datenschutz besteht (rechtzeitiger Aufbau von internem Fachwissen, Erstellung von internen Richtlinien sowie Anpassung von Dokumenten wie Datenschutzerklärungen und Verträgen mit Partnern und Datenbearbeitern).

9) Was sind die wichtigsten neuen Pflichten für Unternehmen?

Mit dem neuen Datenschutzgesetz werden unter anderem folgende Pflichten für Unternehmen eingeführt:

- Sicherstellung von Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, insbesondere damit die Bearbeitungsgrundsätze eingehalten werden und sich die Datenbearbeitungen auf das für den Verwendungszweck nötige Mindestmass beschränkt (Art. 7 revDSG)
- die Erstellung und Führung eines Verzeichnisses der Datenbearbeitungstätigkeiten. Eine Ausnahmen hiervon gilt für Unternehmen mit weniger als 250 Mitarbeiter, allerdings nur dann, wenn deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt (das wird in der Verordnung noch präzisiert werden, Art. 12 revDSG).
- die Meldepflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sowie gegenüber der betroffenen Person im Falle einer Datensicherheitsverletzung (Art. 24 revDSG)
- die Verpflichtung, in bestimmten Fällen eine Folgenabschätzung zum Schutz der Personendaten durchzuführen, wenn aufgrund einer Bearbeitung ein hohes Risiko besteht (Art. 22 revDSG)

- die Informationspflicht bei der Datenerhebung und die Pflicht zur Nennung des/der Staates/Staaten im Falle eines Transfers ins Ausland (Art. 19 revDSG). Hier ist das revDSG ausnahmsweise strenger als die DSGVO.
- die Informationspflicht im Falle einer automatisierten Einzelentscheidung - d.h. einer Entscheidung, welche in Bezug auf eine Person mit Hilfe von Algorithmen getroffen und auf ihre persönlichen Daten angewendet werden, ohne dass ein Mensch in den Prozess eingreift (Art. 21 revDSG)

9) Was sind die wichtigsten neuen Pflichten für Unternehmen?

Mit dem neuen Datenschutzgesetz werden unter anderem folgende Pflichten für Unternehmen eingeführt:

- Sicherstellung von Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, insbesondere damit die Bearbeitungsgrundsätze eingehalten werden und sich die Datenbearbeitungen auf das für den Verwendungszweck nötige Mindestmass beschränkt (Art. 7 revDSG)
- die Erstellung und Führung eines Verzeichnisses der Datenbearbeitungstätigkeiten. Eine Ausnahmen hiervon gilt für Unternehmen mit weniger als 250 Mitarbeiter, allerdings nur dann, wenn deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt (das wird in der Verordnung noch präzisiert werden, Art. 12 revDSG).
- die Meldepflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sowie gegenüber der betroffenen Person im Falle einer Datensicherheitsverletzung (Art. 24 revDSG)
- die Verpflichtung, in bestimmten Fällen eine Folgenabschätzung zum Schutz der Personendaten durchzuführen, wenn aufgrund einer Bearbeitung ein hohes Risiko besteht (Art. 22 revDSG)
- die Informationspflicht bei der Datenerhebung und die Pflicht zur Nennung des/der Staates/Staaten im Falle eines Transfers ins Ausland (Art. 19 revDSG). Hier ist das revDSG ausnahmsweise strenger als die DSGVO.

- die Informationspflicht im Falle einer automatisierten Einzelentscheidung - d.h. einer Entscheidung, welche in Bezug auf eine Person mit Hilfe von Algorithmen getroffen und auf ihre persönlichen Daten angewendet werden, ohne dass ein Mensch in den Prozess eingreift (Art. 21 revDSG)

9) Was sind die wichtigsten neuen Pflichten für Unternehmen?

Mit dem neuen Datenschutzgesetz werden unter anderem folgende Pflichten für Unternehmen eingeführt:

- Sicherstellung von Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, insbesondere damit die Bearbeitungsgrundsätze eingehalten werden und sich die Datenbearbeitungen auf das für den Verwendungszweck nötige Mindestmass beschränkt (Art. 7 revDSG)
- die Erstellung und Führung eines Verzeichnisses der Datenbearbeitungstätigkeiten. Eine Ausnahmen hiervon gilt für Unternehmen mit weniger als 250 Mitarbeiter, allerdings nur dann, wenn deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt (das wird in der Verordnung noch präzisiert werden, Art. 12 revDSG).
- die Meldepflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sowie gegenüber der betroffenen Person im Falle einer Datensicherheitsverletzung (Art. 24 revDSG)
- die Verpflichtung, in bestimmten Fällen eine Folgenabschätzung zum Schutz der Personendaten durchzuführen, wenn aufgrund einer Bearbeitung ein hohes Risiko besteht (Art. 22 revDSG)
- die Informationspflicht bei der Datenerhebung und die Pflicht zur Nennung des/der Staates/Staaten im Falle eines Transfers ins Ausland (Art. 19 revDSG). Hier ist das revDSG ausnahmsweise strenger als die DSGVO.
- die Informationspflicht im Falle einer automatisierten Einzelentscheidung - d.h. einer Entscheidung, welche in Bezug auf eine Person mit Hilfe von Algorithmen getroffen und auf ihre persönlichen Daten angewendet werden, ohne dass ein Mensch in den Prozess eingreift (Art. 21 revDSG)

10) Was sind die neuen Rechte von betroffenen Privatpersonen?

Das Hauptziel dieses Gesetzes ist es, die Transparenz und den Schutz der persönlichen Daten von betroffenen Personen zu stärken. In dieser Hinsicht wird der Einzelne von neuen Rechten profitieren, wie z.B. in Bezug auf

- sein Recht auf Auskunft über die Bearbeitung seiner Personendaten (Art. 25-27 revDSG)
- sein Recht auf Herausgabe oder Übermittlung seiner Daten (Datenübertragbarkeit)) (Art. 28 und 29 revDSG)
- das Recht, nicht einer automatisierten Einzelentscheidung unterworfen zu werden, d. h. einer Entscheidung, welche in Bezug auf eine Person mit Hilfe von Algorithmen getroffen und auf ihre persönlichen Daten angewendet werden, ohne dass ein Mensch in den Prozess eingreift (Art. 21 revDSG)

10) Was sind die neuen Rechte von betroffenen Privatpersonen?

Das Hauptziel dieses Gesetzes ist es, die Transparenz und den Schutz der persönlichen Daten von betroffenen Personen zu stärken. In dieser Hinsicht wird der Einzelne von neuen Rechten profitieren, wie z.B. in Bezug auf

- sein Recht auf Auskunft über die Bearbeitung seiner Personendaten (Art. 25-27 revDSG)
- sein Recht auf Herausgabe oder Übermittlung seiner Daten (Datenübertragbarkeit)) (Art. 28 und 29 revDSG)
- das Recht, nicht einer automatisierten Einzelentscheidung unterworfen zu werden, d. h. einer Entscheidung, welche in Bezug auf eine Person mit Hilfe von Algorithmen getroffen und auf ihre persönlichen Daten angewendet werden, ohne dass ein Mensch in den Prozess eingreift (Art. 21 revDSG)

10) Was sind die neuen Rechte von betroffenen Privatpersonen?

Das Hauptziel dieses Gesetzes ist es, die Transparenz und den Schutz der persönlichen Daten von betroffenen Personen zu stärken. In dieser Hinsicht wird der Einzelne von neuen Rechten profitieren, wie z.B. in Bezug auf

- sein Recht auf Auskunft über die Bearbeitung seiner Personendaten (Art. 25-27 revDSG)
- sein Recht auf Herausgabe oder Übermittlung seiner Daten (Datenübertragbarkeit)) (Art. 28 und 29 revDSG)
- das Recht, nicht einer automatisierten Einzelentscheidung unterworfen zu werden, d. h. einer Entscheidung, welche in Bezug auf eine Person mit Hilfe von Algorithmen getroffen und auf ihre persönlichen Daten angewendet werden, ohne dass ein Mensch in den Prozess eingreift (Art. 21 revDSG)

11) Weitere Änderungen im Vergleich zum aktuellen Gesetz?

Weitere Änderungen gegenüber dem geltenden Recht betreffen:

- Personendaten: Der Begriff wird auf natürliche Personen begrenzt, erfasst Daten von juristischen Personen also nicht mehr und schliesst diese damit vom Schutzbereich des DSG aus (Art. 1 und Art. 5 lit. a revDSG).
- besonders schützenswerte Personendaten: Hierunter fallen neu zusätzlich auch genetische und (eindeutig identifizierende) biometrische Daten (Art. 5 lit. c revDSG)
- Verantwortlicher: Entspricht dem heutigen „Inhaber der Datensammlung“ und dem „Verantwortlichen“ nach DSGVO. Dabei handelt es sich um eine private Person (insbesondere Unternehmen) oder ein Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung von Personendaten entscheidet (Art. 5 lit. j revDSG)
- Extraterritorialität: Ausdehnung des Geltungsbereichs des DSG auf Sachverhalte, die sich im Ausland ereignen und Auswirkungen in der Schweiz haben (Art. 3 Abs. 1 revDSG)

- Bezeichnung einer Vertretung in der Schweiz für Verantwortliche im Ausland: Diese Verpflichtung gilt, wenn ein privater Verantwortlicher seinen Sitz oder Wohnsitz im Ausland hat, Personendaten von Personen in der Schweiz bearbeitet und weitere Voraussetzungen erfüllt sind (Art. 14 f. revDSG)

11) Weitere Änderungen im Vergleich zum aktuellen Gesetz?

Weitere Änderungen gegenüber dem geltenden Recht betreffen:

- Personendaten: Der Begriff wird auf natürliche Personen begrenzt, erfasst Daten von juristischen Personen also nicht mehr und schliesst diese damit vom Schutzbereich des DSG aus (Art. 1 und Art. 5 lit. a revDSG).
- besonders schützenswerte Personendaten: Hierunter fallen neu zusätzlich auch genetische und (eindeutig identifizierende) biometrische Daten (Art. 5 lit. c revDSG)
- Verantwortlicher: Entspricht dem heutigen „Inhaber der Datensammlung“ und dem „Verantwortlichen“ nach DSGVO. Dabei handelt es sich um eine private Person (insbesondere Unternehmen) oder ein Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung von Personendaten entscheidet (Art. 5 lit. j revDSG)
- Extraterritorialität: Ausdehnung des Geltungsbereichs des DSG auf Sachverhalte, die sich im Ausland ereignen und Auswirkungen in der Schweiz haben (Art. 3 Abs. 1 revDSG)
- Bezeichnung einer Vertretung in der Schweiz für Verantwortliche im Ausland: Diese Verpflichtung gilt, wenn ein privater Verantwortlicher seinen Sitz oder Wohnsitz im Ausland hat, Personendaten von Personen in der Schweiz bearbeitet und weitere Voraussetzungen erfüllt sind (Art. 14 f. revDSG)

11) Weitere Änderungen im Vergleich zum aktuellen Gesetz?

Weitere Änderungen gegenüber dem geltenden Recht betreffen:

- Personendaten: Der Begriff wird auf natürliche Personen begrenzt, erfasst Daten von juristischen Personen also nicht mehr und schliesst diese damit vom Schutzbereich des DSG aus (Art. 1 und Art. 5 lit. a revDSG).
- besonders schützenswerte Personendaten: Hierunter fallen neu zusätzlich auch genetische und (eindeutig identifizierende) biometrische Daten (Art. 5 lit. c revDSG)
- Verantwortlicher: Entspricht dem heutigen „Inhaber der Datensammlung“ und dem „Verantwortlichen“ nach DSGVO. Dabei handelt es sich um eine private Person (insbesondere Unternehmen) oder ein Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung von Personendaten entscheidet (Art. 5 lit. j revDSG)
- Extraterritorialität: Ausdehnung des Geltungsbereichs des DSG auf Sachverhalte, die sich im Ausland ereignen und Auswirkungen in der Schweiz haben (Art. 3 Abs. 1 revDSG)
- Bezeichnung einer Vertretung in der Schweiz für Verantwortliche im Ausland: Diese Verpflichtung gilt, wenn ein privater Verantwortlicher seinen Sitz oder Wohnsitz im Ausland hat, Personendaten von Personen in der Schweiz bearbeitet und weitere Voraussetzungen erfüllt sind (Art. 14 f. revDSG)

12) Welche Risiken bestehen bei einem Verstoss gegen das neue Gesetz?

Im Falle eines Verstosses gegen das neue Gesetz drohen Sanktionen in Form von Bussgeldern bis CHF 250‘000 . Im Gegensatz zur DSGVO richten sich die Sanktionen unter dem revDSG nicht gegen das fehlbare Unternehmen, sondern gegen die für die Einhaltung des Datenschutzes verantwortliche natürliche Person (z.B. Geschäftsführer oder Verwaltungsrat). Es wird ausschliesslich (eventual-)vorsätzliches Verhalten bestraft (Art. 60 ff. revDSG).

12) Welche Risiken bestehen bei einem Verstoss gegen das neue Gesetz?

Im Falle eines Verstosses gegen das neue Gesetz drohen Sanktionen in Form von Bussgeldern bis CHF 250‘000 . Im Gegensatz zur DSGVO richten sich die Sanktionen unter dem revDSG nicht gegen das fehlbare Unternehmen, sondern gegen die für die Einhaltung des Datenschutzes verantwortliche natürliche Person (z.B. Geschäftsführer oder Verwaltungsrat). Es wird ausschliesslich (eventual-)vorsätzliches Verhalten bestraft (Art. 60 ff. revDSG).

12) Welche Risiken bestehen bei einem Verstoss gegen das neue Gesetz?

Im Falle eines Verstosses gegen das neue Gesetz drohen Sanktionen in Form von Bussgeldern bis CHF 250‘000 . Im Gegensatz zur DSGVO richten sich die Sanktionen unter dem revDSG nicht gegen das fehlbare Unternehmen, sondern gegen die für die Einhaltung des Datenschutzes verantwortliche natürliche Person (z.B. Geschäftsführer oder Verwaltungsrat). Es wird ausschliesslich (eventual-)vorsätzliches Verhalten bestraft (Art. 60 ff. revDSG).

13) Was steht für Unternehmen auf dem Spiel?

Das Ignorieren des (neuen) Datenschutzgesetzes kann nicht nur für die verantwortliche Person in einem Unternehmen, sondern auch für das Unternehmen selbst Folgen haben, insbesondere für seine Reputation. Auch der Eidgenössische Datenschutzbeauftrage (EDÖB) kann sich einschalten und Verwaltungsmassnahmen treffen (z.B. Anordnung, dass eine Bearbeitung angepasst, unterbrochen oder abgebrochen wird oder Personendaten gelöscht werden).

13) Was steht für Unternehmen auf dem Spiel?

Das Ignorieren des (neuen) Datenschutzgesetzes kann nicht nur für die verantwortliche Person in einem Unternehmen, sondern auch für das Unternehmen selbst Folgen haben, insbesondere für seine Reputation. Auch der Eidgenössische Datenschutzbeauftrage (EDÖB) kann sich einschalten und Verwaltungsmassnahmen treffen (z.B. Anordnung, dass eine Bearbeitung angepasst, unterbrochen oder abgebrochen wird oder Personendaten gelöscht werden).

13) Was steht für Unternehmen auf dem Spiel?

Das Ignorieren des (neuen) Datenschutzgesetzes kann nicht nur für die verantwortliche Person in einem Unternehmen, sondern auch für das Unternehmen selbst Folgen haben, insbesondere für seine Reputation. Auch der Eidgenössische Datenschutzbeauftrage (EDÖB) kann sich einschalten und Verwaltungsmassnahmen treffen (z.B. Anordnung, dass eine Bearbeitung angepasst, unterbrochen oder abgebrochen wird oder Personendaten gelöscht werden).

14) Wie kann man sich auf die Änderungen vorbereiten?

Zunächst sollte baldmöglichst ein Aktionsplan mit Hilfe einer GAP-Analyse definiert werden, um sich Schritt für Schritt an das neue Gesetz anzupassen. Je nach Grösse des Unternehmens kann dies mehrere Monate dauern. Nichtsdestotrotz sind pragmatische Lösungen erforderlich, d.h. es sollten vorderhand die gesetzlich zwingenden Mindestvorgaben (z.B. Verzeichnis, Informationspflicht etc.) umgesetzt werden.

14) Wie kann man sich auf die Änderungen vorbereiten?

Zunächst sollte baldmöglichst ein Aktionsplan mit Hilfe einer GAP-Analyse definiert werden, um sich Schritt für Schritt an das neue Gesetz anzupassen. Je nach Grösse des Unternehmens kann dies mehrere Monate dauern. Nichtsdestotrotz sind pragmatische Lösungen erforderlich, d.h. es sollten vorderhand die gesetzlich zwingenden Mindestvorgaben (z.B. Verzeichnis, Informationspflicht etc.) umgesetzt werden.

14) Wie kann man sich auf die Änderungen vorbereiten?

Zunächst sollte baldmöglichst ein Aktionsplan mit Hilfe einer GAP-Analyse definiert werden, um sich Schritt für Schritt an das neue Gesetz anzupassen. Je nach Grösse des Unternehmens kann dies mehrere Monate dauern. Nichtsdestotrotz sind pragmatische Lösungen erforderlich, d.h. es sollten vorderhand die gesetzlich zwingenden Mindestvorgaben (z.B. Verzeichnis, Informationspflicht etc.) umgesetzt werden.

15) Wie definiert man einen Aktionsplan?

Ein Aktionsplan sollte auf den folgenden drei Säulen basieren: IT-Sicherheit, rechtliche Aspekte und Data Governance. Zum letzten Punkt hat economiesuisse eine Unternehmenscharta erstellt. Falls nötig, sollten Unternehmen IT-Sicherheits- und Datenschutzexperten beiziehen, um detaillierte Compliance-Programme zu entwickeln, welche die neuen Anforderungen erfüllen.

15) Wie definiert man einen Aktionsplan?

Ein Aktionsplan sollte auf den folgenden drei Säulen basieren: IT-Sicherheit, rechtliche Aspekte und Data Governance. Zum letzten Punkt hat economiesuisse eine Unternehmenscharta erstellt. Falls nötig, sollten Unternehmen IT-Sicherheits- und Datenschutzexperten beiziehen, um detaillierte Compliance-Programme zu entwickeln, welche die neuen Anforderungen erfüllen.

15) Wie definiert man einen Aktionsplan?

Ein Aktionsplan sollte auf den folgenden drei Säulen basieren: IT-Sicherheit, rechtliche Aspekte und Data Governance. Zum letzten Punkt hat economiesuisse eine Unternehmenscharta erstellt. Falls nötig, sollten Unternehmen IT-Sicherheits- und Datenschutzexperten beiziehen, um detaillierte Compliance-Programme zu entwickeln, welche die neuen Anforderungen erfüllen.

16) Welche Prinzipien sollten beibehalten werden? Und welche Massnahmen sind erforderlich?

Ohne auf die technischen, rechtlichen und IT-Überlegungen zur Einhaltung des revDSG einzugehen, sollte ein pragmatischer Aktionsplan mindestens die folgenden Prinzipien beibehalten:

1. **Eine umfassende Bestandsaufnahme ist zentral**
   Unternehmen müssen unter dem revDSG bestimmte Informationspflichten erfüllen, d.h. sie müssen bei der Beschaffung von Personendaten über die Identität des Verantwortlichen, den Bearbeitungszweck, allfällige Datenempfänger usw. informieren. Zudem müssen sie in der Lage sein, die Betroffenenrechten zu erfüllen, etwa einer betroffenen Person Auskünfte zur Bearbeitung ihrer Personendaten zu erteilen. Das alles setzt voraus, dass Unternehmen wissen, welche Personendaten zu welchen Zwecken bearbeitet werden, ob die Daten in andere Länder und an weitere Personen transferiert werden etc. Demzufolge sollten Unternehmen zunächst eine Bestandsaufnahme aller Datenbearbeitungen durchzuführen. Dabei kann das gesetzlich neu vorgeschriebene Verzeichnis als Vorlage dienen.
   Eine solche Bestandsaufnahme ist eine kollektive Anstrengung, die alle Mitarbeiter, die in die Bearbeitung von Personendaten involviert sind, einbeziehen muss.
2. **Abschätzung der Risiken**
   Je grösser das Volumen der von einem Unternehmen bearbeiteten Personendaten und/oder je sensibler die die Personendaten sind, desto höher sind die Anforderungen an die Datenschutz-Compliance bzw. desto grösser sind die potentiellen Sanktionen und Reputationsschäden bei einem Verstoss (siehe Frage 6).

3. **Bewusstsein wecken**
   Sowohl für kleine als auch grosse Unternehmen gilt: alle Mitarbeiter, vom Lehrling bis zum Geschäftsführer, müssen für das Thema Datenschutz sensibilisiert werden. Empfangsmitarbeiter, Projektleiter, Personalleiter, Berater, Freiberufler, Geschäftsführer – Mitarbeiter auf allen Ebenen eines Unternehmens bearbeiten regelmässig Personendaten und tragen hierfür ggf. sogar eine strafbewehrte Verantwortung. Beispiel: Eine Empfangsdame führt ein Register der Besucher eines Unternehmens. Indem sie den Vor- und Nachnamen von Personen, die das Unternehmen besuchen, erfasst und archiviert, bearbeitet sie bereits Personendaten.
4. **Transparenz und Information**
   Transparenz bei der Datenbearbeitung ist auch unter dem neuen DSG nach wie vor ein wichtiger Grundsatz. Hinzu kommt die Informationspflicht bei der Datenbeschaffung. Der Verantwortliche muss die betroffenen Personen über verschiedene Aspekte der Datenbearbeitung(en) zwingend informieren. Deshalb ist die Erstellung bzw. Aktualisierung von Datenschutzerklärungen mit Blick auf das Inkrafttreten des revDSG unerlässlich (auf der Unternehmenswebsite, aber auch in der physischen Korrespondenz).
5. **IT-Sicherheit**
   Unternehmen müssen sicherstellen, dass die Sicherheit ihrer IT-Systeme und Software-Anwendungen den Vorgaben des neuen Gesetzes entspricht. Dazu gehören insbesondere technische und organisatorische Massnahmen zur Verhinderung von Cyberattacken, Datendiebstahl und anderweitigen Datenverlust.

6. **Interne Organisation und Abläufe**
   Um auf Betroffenenanfragen (z.B. Auskunfts- oder Löschbegehren eines Kunden) oder auf eine Verletzung der Datensicherheit („Datenpannen"), bei denen Personendaten verloren gehen, gestohlen oder missbraucht werden, gesetzeskonform reagieren zu können, müssen klare interne Prozesse festgelegt werden. Diese Prozesse sollten je nach Vorfall insbesondere definieren, welcher Mitarbeiter (inkl. Vertretung) welche Massnahmen innert welcher Frist treffen muss. Beispiel: Verletzung der Datensicherheit: Überblick von Fallbeispielen bzw. Kriterien, nach denen zu beurteilen ist, ob ein Vorfall einer Behörde gemeldet werden muss. Klare Ausführungen dazu, welcher Mitarbeiter diese Meldung innert welcher First und in welcher Form an welche Behörde vornehmen muss (Checklisten).
7. **Erstellung und Führung eines Verzeichnisses der Bearbeitungstätigkeiten**
   Das revDSG sieht vor, dass sowohl der Verantwortliche als auch der Auftragsbearbeiter je ein Verzeichnis über ihre Bearbeitungstätigkeiten führen muss. Diese Pflicht gilt grundsätzlich für alle Unternehmen.
   Der Bundesrat kann jedoch Ausnahmen vorsehen für Unternehmen mit weniger als 250 Mitarbeitern (Art 12 Abs. 2 revDSG). Diese Ausnahmen werden in der Verordnung festgehalten, deren Entwurf noch immer ausstehend ist. Das Erstellen solcher Verzeichnisse setzt voraus, dass sämtliche Bearbeitungen von Personendaten innerhalb eines Unternehmens identifiziert und systematisch zusammengetragen werden. Gerade in Fällen, wo noch keine entsprechenden Verzeichnisse geführt werden und viele verschiedene Bearbeitungen durchgeführt werden, ist dieser Prozess mit einem beträchtlichen Aufwand verbunden und sollte daher frühzeitig angegangen werden.
8. **Überprüfung von Verträgen**
   Bis zum Inkrafttreten des neuen Gesetzes sollten Unternehmen ihre Verträge mit Kunden, Lieferanten und Dienstleistern sowie Arbeitnehmern mit Blick auf die Neuerungen überprüfen und ggf. anpassen. Dies setzt frühzeitige Vorkehrungen voraus. Eine rasche Umsetzung ist auch deshalb angezeigt, weil damit gerechnet werden muss, dass viele Vertragspartner in den kommenden Monaten Verträge bzw. Vertragsanpassungen verlangen werden, um ihrerseits Datenschutz-Compliance sicherzustellen.

9. **Informiert bleiben**
   Um sich dem Thema Datenschutz-Compliance unter dem revDSG bewusst zu werden, muss man in der Lage sein, die konkreten Auswirkungen des neuen Gesetzes auf die eigenen Bearbeitungsprozesse zu verstehen. Informieren Sie sich auf den Internetseiten der Datenschutzbehörde (EDÖB), auf einschlägigen Blogs, in Fachzeitschriften und nehmen Sie an den verschiedenen Schulungen teil (z.B. von Industrie- und Handelskammern).

16) Welche Prinzipien sollten beibehalten werden? Und welche Massnahmen sind erforderlich?

Ohne auf die technischen, rechtlichen und IT-Überlegungen zur Einhaltung des revDSG einzugehen, sollte ein pragmatischer Aktionsplan mindestens die folgenden Prinzipien beibehalten:

1. **Eine umfassende Bestandsaufnahme ist zentral**
   Unternehmen müssen unter dem revDSG bestimmte Informationspflichten erfüllen, d.h. sie müssen bei der Beschaffung von Personendaten über die Identität des Verantwortlichen, den Bearbeitungszweck, allfällige Datenempfänger usw. informieren. Zudem müssen sie in der Lage sein, die Betroffenenrechten zu erfüllen, etwa einer betroffenen Person Auskünfte zur Bearbeitung ihrer Personendaten zu erteilen. Das alles setzt voraus, dass Unternehmen wissen, welche Personendaten zu welchen Zwecken bearbeitet werden, ob die Daten in andere Länder und an weitere Personen transferiert werden etc. Demzufolge sollten Unternehmen zunächst eine Bestandsaufnahme aller Datenbearbeitungen durchzuführen. Dabei kann das gesetzlich neu vorgeschriebene Verzeichnis als Vorlage dienen.
   Eine solche Bestandsaufnahme ist eine kollektive Anstrengung, die alle Mitarbeiter, die in die Bearbeitung von Personendaten involviert sind, einbeziehen muss.
2. **Abschätzung der Risiken**
   Je grösser das Volumen der von einem Unternehmen bearbeiteten Personendaten und/oder je sensibler die die Personendaten sind, desto höher sind die Anforderungen an die Datenschutz-Compliance bzw. desto grösser sind die potentiellen Sanktionen und Reputationsschäden bei einem Verstoss (siehe Frage 6).

3. **Bewusstsein wecken**
   Sowohl für kleine als auch grosse Unternehmen gilt: alle Mitarbeiter, vom Lehrling bis zum Geschäftsführer, müssen für das Thema Datenschutz sensibilisiert werden. Empfangsmitarbeiter, Projektleiter, Personalleiter, Berater, Freiberufler, Geschäftsführer – Mitarbeiter auf allen Ebenen eines Unternehmens bearbeiten regelmässig Personendaten und tragen hierfür ggf. sogar eine strafbewehrte Verantwortung. Beispiel: Eine Empfangsdame führt ein Register der Besucher eines Unternehmens. Indem sie den Vor- und Nachnamen von Personen, die das Unternehmen besuchen, erfasst und archiviert, bearbeitet sie bereits Personendaten.
4. **Transparenz und Information**
   Transparenz bei der Datenbearbeitung ist auch unter dem neuen DSG nach wie vor ein wichtiger Grundsatz. Hinzu kommt die Informationspflicht bei der Datenbeschaffung. Der Verantwortliche muss die betroffenen Personen über verschiedene Aspekte der Datenbearbeitung(en) zwingend informieren. Deshalb ist die Erstellung bzw. Aktualisierung von Datenschutzerklärungen mit Blick auf das Inkrafttreten des revDSG unerlässlich (auf der Unternehmenswebsite, aber auch in der physischen Korrespondenz).
5. **IT-Sicherheit**
   Unternehmen müssen sicherstellen, dass die Sicherheit ihrer IT-Systeme und Software-Anwendungen den Vorgaben des neuen Gesetzes entspricht. Dazu gehören insbesondere technische und organisatorische Massnahmen zur Verhinderung von Cyberattacken, Datendiebstahl und anderweitigen Datenverlust.

6. **Interne Organisation und Abläufe**
   Um auf Betroffenenanfragen (z.B. Auskunfts- oder Löschbegehren eines Kunden) oder auf eine Verletzung der Datensicherheit („Datenpannen"), bei denen Personendaten verloren gehen, gestohlen oder missbraucht werden, gesetzeskonform reagieren zu können, müssen klare interne Prozesse festgelegt werden. Diese Prozesse sollten je nach Vorfall insbesondere definieren, welcher Mitarbeiter (inkl. Vertretung) welche Massnahmen innert welcher Frist treffen muss. Beispiel: Verletzung der Datensicherheit: Überblick von Fallbeispielen bzw. Kriterien, nach denen zu beurteilen ist, ob ein Vorfall einer Behörde gemeldet werden muss. Klare Ausführungen dazu, welcher Mitarbeiter diese Meldung innert welcher First und in welcher Form an welche Behörde vornehmen muss (Checklisten).
7. **Erstellung und Führung eines Verzeichnisses der Bearbeitungstätigkeiten**
   Das revDSG sieht vor, dass sowohl der Verantwortliche als auch der Auftragsbearbeiter je ein Verzeichnis über ihre Bearbeitungstätigkeiten führen muss. Diese Pflicht gilt grundsätzlich für alle Unternehmen.
   Der Bundesrat kann jedoch Ausnahmen vorsehen für Unternehmen mit weniger als 250 Mitarbeitern (Art 12 Abs. 2 revDSG). Diese Ausnahmen werden in der Verordnung festgehalten, deren Entwurf noch immer ausstehend ist. Das Erstellen solcher Verzeichnisse setzt voraus, dass sämtliche Bearbeitungen von Personendaten innerhalb eines Unternehmens identifiziert und systematisch zusammengetragen werden. Gerade in Fällen, wo noch keine entsprechenden Verzeichnisse geführt werden und viele verschiedene Bearbeitungen durchgeführt werden, ist dieser Prozess mit einem beträchtlichen Aufwand verbunden und sollte daher frühzeitig angegangen werden.
8. **Überprüfung von Verträgen**
   Bis zum Inkrafttreten des neuen Gesetzes sollten Unternehmen ihre Verträge mit Kunden, Lieferanten und Dienstleistern sowie Arbeitnehmern mit Blick auf die Neuerungen überprüfen und ggf. anpassen. Dies setzt frühzeitige Vorkehrungen voraus. Eine rasche Umsetzung ist auch deshalb angezeigt, weil damit gerechnet werden muss, dass viele Vertragspartner in den kommenden Monaten Verträge bzw. Vertragsanpassungen verlangen werden, um ihrerseits Datenschutz-Compliance sicherzustellen.

9. **Informiert bleiben**
   Um sich dem Thema Datenschutz-Compliance unter dem revDSG bewusst zu werden, muss man in der Lage sein, die konkreten Auswirkungen des neuen Gesetzes auf die eigenen Bearbeitungsprozesse zu verstehen. Informieren Sie sich auf den Internetseiten der Datenschutzbehörde (EDÖB), auf einschlägigen Blogs, in Fachzeitschriften und nehmen Sie an den verschiedenen Schulungen teil (z.B. von Industrie- und Handelskammern).

16) Welche Prinzipien sollten beibehalten werden? Und welche Massnahmen sind erforderlich?

Ohne auf die technischen, rechtlichen und IT-Überlegungen zur Einhaltung des revDSG einzugehen, sollte ein pragmatischer Aktionsplan mindestens die folgenden Prinzipien beibehalten:

1. **Eine umfassende Bestandsaufnahme ist zentral**
   Unternehmen müssen unter dem revDSG bestimmte Informationspflichten erfüllen, d.h. sie müssen bei der Beschaffung von Personendaten über die Identität des Verantwortlichen, den Bearbeitungszweck, allfällige Datenempfänger usw. informieren. Zudem müssen sie in der Lage sein, die Betroffenenrechten zu erfüllen, etwa einer betroffenen Person Auskünfte zur Bearbeitung ihrer Personendaten zu erteilen. Das alles setzt voraus, dass Unternehmen wissen, welche Personendaten zu welchen Zwecken bearbeitet werden, ob die Daten in andere Länder und an weitere Personen transferiert werden etc. Demzufolge sollten Unternehmen zunächst eine Bestandsaufnahme aller Datenbearbeitungen durchzuführen. Dabei kann das gesetzlich neu vorgeschriebene Verzeichnis als Vorlage dienen.
   Eine solche Bestandsaufnahme ist eine kollektive Anstrengung, die alle Mitarbeiter, die in die Bearbeitung von Personendaten involviert sind, einbeziehen muss.
2. **Abschätzung der Risiken**
   Je grösser das Volumen der von einem Unternehmen bearbeiteten Personendaten und/oder je sensibler die die Personendaten sind, desto höher sind die Anforderungen an die Datenschutz-Compliance bzw. desto grösser sind die potentiellen Sanktionen und Reputationsschäden bei einem Verstoss (siehe Frage 6).

3. **Bewusstsein wecken**
   Sowohl für kleine als auch grosse Unternehmen gilt: alle Mitarbeiter, vom Lehrling bis zum Geschäftsführer, müssen für das Thema Datenschutz sensibilisiert werden. Empfangsmitarbeiter, Projektleiter, Personalleiter, Berater, Freiberufler, Geschäftsführer – Mitarbeiter auf allen Ebenen eines Unternehmens bearbeiten regelmässig Personendaten und tragen hierfür ggf. sogar eine strafbewehrte Verantwortung. Beispiel: Eine Empfangsdame führt ein Register der Besucher eines Unternehmens. Indem sie den Vor- und Nachnamen von Personen, die das Unternehmen besuchen, erfasst und archiviert, bearbeitet sie bereits Personendaten.
4. **Transparenz und Information**
   Transparenz bei der Datenbearbeitung ist auch unter dem neuen DSG nach wie vor ein wichtiger Grundsatz. Hinzu kommt die Informationspflicht bei der Datenbeschaffung. Der Verantwortliche muss die betroffenen Personen über verschiedene Aspekte der Datenbearbeitung(en) zwingend informieren. Deshalb ist die Erstellung bzw. Aktualisierung von Datenschutzerklärungen mit Blick auf das Inkrafttreten des revDSG unerlässlich (auf der Unternehmenswebsite, aber auch in der physischen Korrespondenz).
5. **IT-Sicherheit**
   Unternehmen müssen sicherstellen, dass die Sicherheit ihrer IT-Systeme und Software-Anwendungen den Vorgaben des neuen Gesetzes entspricht. Dazu gehören insbesondere technische und organisatorische Massnahmen zur Verhinderung von Cyberattacken, Datendiebstahl und anderweitigen Datenverlust.

6. **Interne Organisation und Abläufe**
   Um auf Betroffenenanfragen (z.B. Auskunfts- oder Löschbegehren eines Kunden) oder auf eine Verletzung der Datensicherheit („Datenpannen"), bei denen Personendaten verloren gehen, gestohlen oder missbraucht werden, gesetzeskonform reagieren zu können, müssen klare interne Prozesse festgelegt werden. Diese Prozesse sollten je nach Vorfall insbesondere definieren, welcher Mitarbeiter (inkl. Vertretung) welche Massnahmen innert welcher Frist treffen muss. Beispiel: Verletzung der Datensicherheit: Überblick von Fallbeispielen bzw. Kriterien, nach denen zu beurteilen ist, ob ein Vorfall einer Behörde gemeldet werden muss. Klare Ausführungen dazu, welcher Mitarbeiter diese Meldung innert welcher First und in welcher Form an welche Behörde vornehmen muss (Checklisten).
7. **Erstellung und Führung eines Verzeichnisses der Bearbeitungstätigkeiten**
   Das revDSG sieht vor, dass sowohl der Verantwortliche als auch der Auftragsbearbeiter je ein Verzeichnis über ihre Bearbeitungstätigkeiten führen muss. Diese Pflicht gilt grundsätzlich für alle Unternehmen.
   Der Bundesrat kann jedoch Ausnahmen vorsehen für Unternehmen mit weniger als 250 Mitarbeitern (Art 12 Abs. 2 revDSG). Diese Ausnahmen werden in der Verordnung festgehalten, deren Entwurf noch immer ausstehend ist. Das Erstellen solcher Verzeichnisse setzt voraus, dass sämtliche Bearbeitungen von Personendaten innerhalb eines Unternehmens identifiziert und systematisch zusammengetragen werden. Gerade in Fällen, wo noch keine entsprechenden Verzeichnisse geführt werden und viele verschiedene Bearbeitungen durchgeführt werden, ist dieser Prozess mit einem beträchtlichen Aufwand verbunden und sollte daher frühzeitig angegangen werden.
8. **Überprüfung von Verträgen**
   Bis zum Inkrafttreten des neuen Gesetzes sollten Unternehmen ihre Verträge mit Kunden, Lieferanten und Dienstleistern sowie Arbeitnehmern mit Blick auf die Neuerungen überprüfen und ggf. anpassen. Dies setzt frühzeitige Vorkehrungen voraus. Eine rasche Umsetzung ist auch deshalb angezeigt, weil damit gerechnet werden muss, dass viele Vertragspartner in den kommenden Monaten Verträge bzw. Vertragsanpassungen verlangen werden, um ihrerseits Datenschutz-Compliance sicherzustellen.

9. **Informiert bleiben**
   Um sich dem Thema Datenschutz-Compliance unter dem revDSG bewusst zu werden, muss man in der Lage sein, die konkreten Auswirkungen des neuen Gesetzes auf die eigenen Bearbeitungsprozesse zu verstehen. Informieren Sie sich auf den Internetseiten der Datenschutzbehörde (EDÖB), auf einschlägigen Blogs, in Fachzeitschriften und nehmen Sie an den verschiedenen Schulungen teil (z.B. von Industrie- und Handelskammern).

Erich Herzog
Responsable du département Concurrence et réglementation, General Counsel, membre de la direction élargie

Arnaud Midez
Responsable de projets Économie extérieure