economiesuisse

Datenschutz: Eine Übersicht zum neuen Gesetz

Die Revision des Schweizer Datenschutzgesetzes (DSG) wurde abgeschlossen. Die neuen Regeln des DSG und die Ausführungsbestimmungen in der neuen Datenschutzverordnung (DSV) und der neuen Verordnung über Datenschutzzertifizierungen (VDSZ) treten per 1. September 2023 in Kraft. Übergangsfristen sind keine vorgesehen.

Mit den neu geltenden Datenschutz-Bestimmungen ist es für Schweizer Unternehmen dringend zu empfehlen, sich spätestens jetzt mit dem neuen Gesetz und seinen Anforderungen auseinanderzusetzen und die erforderlichen Anpassungen am Datenschutz-Setup, insbesondere an den Datenschutzerklärungen und Verträgen, vorzunehmen. Gemeinsam mit Anwältin Cornelia Stengel und Anwalt Luca Stäuble hat economiesuisse in der nachfolgenden Übersicht die Antworten auf die drängendsten Fragen zusammengestellt, um die Schweizer Unternehmen auf die Handlungsdringlichkeit in Bezug auf das Inkrafttreten des neuen Datenschutzgesetzes hinzuweisen.

Diese Übersicht dient nur zur Information und Sensibilisierung. Sie ist kein Ersatz für eine Rechtsberatung. economiesuisse übernimmt keine Haftung für Handlungen oder Unterlassungen im Zusammenhang mit der Konsultation dieser Zusammenstellung.

FAQ

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

Das neue Gesetz (nDSG) 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) 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 Personendaten nur dann ohne weiteres in einen Drittstaat 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.

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 Schweiz dürfte jedoch mit der Revision des DSG die Voraussetzungen dafür geschaffen haben, damit die EU-Kommission das (revidierte) Schweizer Datenschutzgesetz weiterhin als angemessen qualifiziert. Der (neue) Angemessenheitsbeschluss steht derzeit noch aus.

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 Neuseeland. Auch in Kalifornien wurde inzwischen ein strengeres Datenschutzgesetz, das sich teilweise am EU-Standard orientiert, umgesetzt.

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

Obwohl das nDSG primär für das Territorium der Schweiz gilt, hat das Gesetz auch einen extraterritorialen Anwendungsbereich (sog. Auswirkungsprinzip). Es kann sich namentlich auf Sachverhalte erstrecken, die sich zwar im Ausland ereignen, aber Auswirkungen in der Schweiz haben (Art. 3 nDSG). 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, muss der betreffende Datenbearbeiter im Ausland das nDSG einhalten. Darüber hinaus muss er unter bestimmten Voraussetzungen einen gesetzlichen Vertreter in der Schweiz bestellen (Art. 14 und Art. 15 nDSG).

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 nDSG zur Anwendung – das dürfte in der Regel jedenfalls bereits dann der Fall sein, wenn eine Datenbearbeitung mit Blick auf eine gewisse Anzahl Personen, die sich in der Schweiz befinden, erfolgt. Im Unterschied dazu stellt die DSGVO – sofern keine Niederlassung in der EU besteht – darauf ab, ob die Datenbearbeitung im Zusammenhang mit der "offensichtlich beabsichtigten" Ausrichtung des Angebots von Waren oder Dienstleistungen auf Personen in der EU (z.B. durch entsprechende Ausrichtung des Onlineshops) oder eine Verhaltensbeobachtung in Bezug auf Personen in der EU (z.B. Einsatz von Webtracking-Technologien) erfolgt. Insofern ist der räumliche Anwendungsbereich gemäss der neuen schweizerischen Regelung noch weiter gefasst als derjenige gemäss DSGVO.

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

Der Bundesrat hat am 31. August 2022 die Datenschutzverordnung (DSV) veröffentlicht und das Inkrafttreten der neuen Regeln per 1. September 2023 beschlossen. Weil keine Übergangsfristen vorgesehen sind, ist jetzt der richtige Zeitpunkt, um sich mit der Umsetzung der erforderlichen Anpassungen auseinanderzusetzen.

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

Die Revision des Schweizer DSG orientierte 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. So gilt etwa weiterhin das Prinzip, dass eine Bearbeitung von Personendaten zulässig ist, sofern die Grundsätze der Bearbeitung eingehalten werden (Art. 6 nDSG). Anders als in der EU bedarf es daher grundsätzlich keines Rechtfertigungsgrundes (Art. 6 DSGVO) für die Bearbeitung von Personendaten.

Es gibt jedoch einige wenige Punkte, in denen das neue DSG strenger ist als die DSGVO. Dazu gehören etwa der räumliche (vgl. dazu Ziff. 3) sowie der sachliche Anwendungsbereich (Art. 2 nDSG). Letzterer umfasst gemäss nDSG sämtliche (automatisierte und manuelle) Datenbearbeitungen, wohingegen die DSGVO bei manuellen Datenbearbeitungen nur für Dateisysteme gilt. Sodann geht die Informationspflicht bei der Erhebung von Personendaten unter dem nDSG insofern über die Regelung in der DSGVO hinaus, als bei einer Datenübermittlung ins Ausland über sämtliche Empfängerstaaten informiert werden muss (Art. 19 nDSG). Auch besteht unter dem nDSG eine Pflicht zur Protokollierung und Führung eines Bearbeitungsreglements für automatisierte Datenbearbeitungen (Art. 4 und 5 f. DSV). Weiter gelten unter dem nDSG – im Unterschied zur DSGVO, welche ausschliesslich Bussen für Unternehmen vorsieht – Sanktionen für natürliche Personen (Art. 60 ff. nDSG) und schliesslich beinhaltet der Begriff der «besonders schützenswerten Personendaten» zwei zusätzliche Kategorien: die administrative oder strafrechtliche Verfolgung und Sanktionen sowie Massnahmen der sozialen Hilfe.

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 bearbeitenden Personendaten in den Unternehmen, auch bei den KMU, weiter zunehmen. Einige der (neuen) Pflichten unter dem nDSG richten sich jedoch nach dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt. Dieser risikobasierte Ansatz, der unter anderem bei der Datensicherheit gilt, lässt eine einzelfallgerechte Ergreifung von Massnahmen zu. Allerdings können selbstredend auch KMU in grossem Umfang besonders schützenswerte Personendaten bearbeiten oder andere Bearbeitungsaktivitäten ausüben, die ein hohes Risiko für die Persönlichkeit der betroffenen Personen mit sich bringen

Entsprechend sollten sich alle Unternehmen – auch KMU – auf das Inkrafttreten des neuen Gesetzes adäquat 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.

Die einzige «KMU-Ausnahme» besteht in Bezug auf die Pflichten zur Führung eines Bearbeitungsverzeichnisses. KMUs mit weniger als 250 Mitarbeitenden per 1. Januar sind von dieser Pflicht befreit, soweit keine «besonders schützenswerten Personendaten» in grossem Umfang bearbeitet werden und kein «Profiling mit hohem Risiko» erfolgt. Grundsätzlich tut ein Unternehmen dennoch gut daran, auf freiwilliger Basis ein solches Bearbeitungsverzeichnis zu führen, da dieses einen wertvollen Überblick über die Datenbearbeitungen im Betrieb schaffen und damit als Grundlage für die Erfüllung anderer Verpflichtungen, wie etwa der Informationspflichten gegenüber den betroffenen Personen, dienen kann.

7) Was sind die wichtigsten neuen Pflichten für Unternehmen?

Mit dem neuen Datenschutzgesetz werden unter anderem folgende Pflichten 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 nDSG) (vgl. dazu die neuen Begriffe unter Ziff. 12);

- die bisher aufgrund des Verhältnismässigkeitsgrundsatzes bereits geltende Pflicht zur Löschung (oder Anonymisierung) von Personendaten, welche für die verfolgten Zwecke nicht mehr benötigt werden und keinen gesetzlichen Aufbewahrungspflichten unterliegen, ist neu explizit im Gesetz verankert (Art. 6 Abs. 4 nDSG);

- die Erstellung und Führung eines Verzeichnisses der Datenbearbeitungstätigkeiten. Eine Ausnahme hiervon gilt für Unternehmen mit weniger als 250 Mitarbeiter, wenn deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt (Art. 12 nDSG, vgl. dazu auch vorangehende Ziff. 6). Die DSV führt aus, dass ein hohes Risiko besteht, wenn besonders schützenswerte Personendaten in grossem Umfang bearbeitet werden oder ein Profiling mit hohem Risiko durchführt wird (Art. 24 DSV);

- die Meldepflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sowie gegenüber der betroffenen Person im Falle einer Datensicherheitsverletzung (Art. 24 nDSG und Art. 15 DSV). Im Gegensatz zur DSGVO (bei der eine 72-Stunden-Frist für die Meldung gilt) statuiert das nDSG keine explizite Frist, die Meldung hat jedoch «so rasch als möglich» zu erfolgen. In der DSV werden sodann Pflichtinhalt und Dokumentation der Meldung geregelt (Art. 15 DSV);

- die Verpflichtung, vorgängig eine Datenschutz-Folgenabschätzung durchzuführen, wenn aufgrund einer Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person besteht (Art. 22 nDSG und Art. 14 DSV);

- die Informationspflicht bei der Beschaffung von Personendaten, unabhängig davon, ob die Daten direkt bei der betroffenen Person oder bei Dritten beschafft werden (Art. 19 ff. nDSG und Art. 13 DSV). Dabei ist zu beachten, dass die Information über die Beschaffung von Personendaten muss für die betroffenen Personen, einfach und verständlich sein muss. Dies ist insbesondere im Hinblick auf die Gestaltung von Datenschutzerklärungen zu beachten. In Bezug auf die Informationspflicht ist das nDSG ausnahmsweise strenger als die DSGVO (vgl. auch vorstehende Ziff. 5). Die (eventual-)vorsätzliche Verletzung dieser Pflicht wird strafrechtlich sanktioniert;

- die Informationspflicht im Falle einer automatisierten Einzelentscheidung – d.h. einer Entscheidung, welche ausschliesslich auf einer automatisierten Bearbeitung beruht und mit einer Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt (Art. 21 nDSG). Die (eventual-)vorsätzliche Verletzung dieser Pflicht wird strafrechtlich sanktioniert;

- die Pflicht, automatisierte Bearbeitungen von besonders schützenswerten Personendaten in grossem Umfang oder Profiling mit hohem Risiko zu protokollieren, wenn die ergriffenen präventiven Massnahmen den Datenschutz nicht zu gewährleisten vermögen (Art. 4 DSV) sowie ein Reglement für solche automatisierten Bearbeitungen zu erstellen und regelmässig zu aktualisieren (Art. 5 DSV).

8) Was sind die neuen Rechte von betroffenen Privatpersonen?

Das Hauptziel der neuen Regelungen ist es, die Transparenz zu erhöhen und den Schutz der persönlichen Daten von betroffenen Personen zu stärken. Dies soll u.a. dadurch erreicht werden, dass Unternehmen die Informationen über die Beschaffung von Personendaten in verständlicher und leicht zugänglicher Form mitteilen (Art. 13 DSV) und die Rechte des Einzelnen ausgebaut werden. So profitiert der Einzelne beispielsweise von folgenden Rechten:

- Recht auf Auskunft über die Bearbeitung seiner Personendaten (Art. 25-27 nDSG)
- Recht auf Herausgabe oder Übermittlung seiner Daten (Datenübertragbarkeit) (Art. 28 und 29 nDSG)
- das Recht, nicht einer automatisierten Einzelentscheidung unterworfen zu werden (Art. 21 nDSG)

Gewisse (eventual-)vorsätzliche Verstösse gegen das Auskunftsrecht sind sanktionsbedroht (Art. 60 nDSG). Unternehmen sollten daher sicherstellen, dass sie jederzeit einen Überblick über die von ihnen bearbeiteten Personendaten haben und Begehren von betroffenen Personen frist- und formgerecht beantworten können.

9) Brauche ich eine Einwilligung von der betroffenen Person, um ihre Daten zu bearbeiten?

Nein. Die Bearbeitung von Personendaten ist sowohl unter geltendem als auch unter neuem Recht grundsätzlich erlaubt, solange die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzt wird. Eine Persönlichkeitsverletzung liegt insbesondere vor, wenn:

- Personendaten entgegen den Grundsätzen der Datenbearbeitung (Art. 6 nDSG) und der Datensicherheit (Art. 8 nDSG) bearbeitet werden,
- Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden,
- Dritten besonders schützenswerte Personendaten bekanntgegeben werden.

Ein Rechtfertigungsgrund ist – im Unterschied zur DSGVO – grundsätzlich nicht erforderlich (vgl. dazu auch vorgehende Ziff. 5). Nach dem nDSG gilt demnach weiterhin das «Erlaubnisprinzip mit Verbotsvorbehalt» während nach der DSGVO das «Verbotsprinzip mit Erlaubnisvorbehalt» gilt (Art. 6 und 9 DSGVO).

10) Was muss ich beim Beizug von Dienstleistern, die für uns Personendaten bearbeiten (z.B. Cloud-Provider, HR-Dienstleister etc.), beachten?

Dienstleister, die im Auftrag und auf Weisung des Auftraggebers bzw. des «Verantwortlichen» (vgl. dazu nachfolgende Ziff. 12) Personendaten bearbeiten, z.B. Cloud-Dienstleister, Webhosting-Agenturen, Payroll-Provider etc. gelten als «Auftragsbearbeiter» (Art. 5 lit. k nDSG).

Die Bearbeitung von Personendaten kann – wie bereits heute – vertraglich oder durch Gesetz einem Auftragsbearbeiter übertragen werden, wenn dieser die Daten so bearbeitet, wie der Verantwortliche selbst es tun dürfte, und keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet (Art. 9 nDSG). Der Beizug eines Auftragsbearbeiters setzt also in der Regel einen (schriftlichen) Vertrag (Auftragsbearbeitungsvertrag, «ADV) voraus. Der Auftraggeber bzw. Verantwortliche muss vor der Übertragung sicherstellen, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit (Art. 8 nDSG und Art. 1 ff. DSV) zu gewährleisten. Der Auftragsbearbeiter ist gesetzlich verpflichtet, die vorgängige (allgemeine oder spezifische) Genehmigung des Verantwortlichen einholen, bevor er einen Unterauftragnehmer für die Datenbearbeitung beizieht (Art. 7 DSV). Die Parteien können weitere Punkte in den ADV aufnehmen (z.B. Vorgehen bei Betroffenenbegehren und Verletzungen der Datensicherheit, Audit- und Kontrollrechte, Haftung, Gerichtsstand etc.). In der Praxis werden regelmässig Musterverträge verwendet, die sich nach dem Mindestinhalt gemäss DSGVO richten.

Das vorsätzliche Übergeben einer Datenbearbeitung an einen Auftragsdatenbearbeiter, ohne dass die Voraussetzungen nach Art. 9 Abs. 1 und 2 erfüllt sind, wird unter Strafe gestellt (Art. 61 lit. b nDSG).

11) Darf ich Personendaten ins Ausland bekanntgeben bzw. übermitteln?

Als Bekanntgabe von Personendaten gilt das «Übermitteln oder Zugänglichmachen von Personendaten» (Art. 5 lit. b nDSG). Damit stellt auch die blosse Zugriffsmöglichkeit durch eine Stelle im Ausland (z.B. Support-Team) eine

Bekanntgabe im Sinne des nDSG dar.

Die Bekanntgabe von Personendaten ins Ausland ist zulässig, sofern der Empfängerstaat (aufgrund seiner Gesetzgebung) über ein «angemessenes» Datenschutzniveau verfügt (Art. 16 Abs. 1 nDSG). Welche Staaten diese Voraussetzung erfüllen, wird vom Bundesrat festgelegt und im Anhang 1 der Datenschutzverordnung publiziert.

Im Umkehrschluss bedeutet dies, dass alle Staaten, welche nicht auf dieser Liste aufgeführt sind, über kein «angemessenes» Datenschutzniveau verfügen und eine Bekanntgabe – wenn überhaupt – nur unter zusätzlichen Schutzmassnahmen möglich ist (Art. 16 Abs. 2 und Art. 17 nDSG sowie Art. 9 DSV). Dazu werden typischerweise die sog. Standardvertragsklauseln (SCC) verwendet. Der Datenexporteur muss dabei durch geeignete Massnahmen sicherstellen, dass der Datenempfänger die SCC einhält (Art. 10 DSV). Weil die SCC nur den Empfänger als Vertragspartner, nicht aber die lokalen Behörden binden und folglich die übermittelten Personendaten nicht vor staatlichen Zugriffen geschützt sind, hat der Datenexporteur vorgängig mittels Durchführung eines sog. «Transfer Risk Assessment» (TIA) (Klausel 14 der SCC), das Risiko von aus schweizerischer Sicht inakzeptablen Zugriffen durch Behörden einzuschätzen. Je nach Risiko, sind zusätzliche Schutzmassnahmen (z.B. Pseudonymisierung, Verschlüsselung der Daten) zu treffen oder es ist gänzlich vom Datentransfer abzusehen.

Die (eventual-)vorsätzliche Verletzung der Bestimmungen über die Bekanntgabe von Personendaten ins Ausland ist sanktionsbedroht (Art. 61 lit. a nDSG).

In Bezug auf die Bekanntgabe von Personendaten in die USA ist auf das neue EU-US Data Privacy Framework (DPF) hinzuweisen, unter welchem sich US-Unternehmen als Datenimporteure zertifizieren lassen können. Seit dem Angemessenheitsbeschluss der EU-Kommission vom 10. Juli 2023 gelten Datenübermittlungen aus der EU an US-Unternehmen, die unter dem DPF zertifiziert sind, als Datenübermittlungen in ein Land mit «angemessenem» Datenschutzniveau (Link zur Pressemitteilung). Es ist zu erwarten, dass auch der EDÖB in absehbarer Zukunft für die Schweiz (CH-US Data Privacy Framework) die Angemessenheit von Datentransfers unter dem DPF feststellen wird.

12) Welche neuen Begriffe sind wichtig für das Verständnis des Datenschutzrechts?

Mit dem neuen Datenschutzgesetz wurden einige neue Begriffe eingeführt bzw. teilweise an die DSGVO angeglichen. Die Wichtigsten sind:

- Personendaten: Der Begriff wird auf natürliche Personen begrenzt. Daten von juristischen Personen sind also nicht mehr erfasst und folglich vom Schutzbereich des DSG ausgeschlossen (Art. 1 und Art. 5 lit. a nDSG);
- besonders schützenswerte Personendaten: Hierunter fallen neu zusätzlich auch Daten über die Zugehörigkeit zu einer Ethnie, genetische und (eindeutig identifizierende) biometrische Daten (Art. 5 lit. c nDSG);
- Verantwortlicher: Entspricht dem „Inhaber der Datensammlung“ unter dem geltenden Recht 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 nDSG). Z.B. ein Arbeitgeber für die Bearbeitung von Personendaten seiner Angestellten im Rahmen der Durchführung des Arbeitsvertrags oder ein Händler für die Bearbeitung von Personendaten seiner Kunden im Rahmen der Abwicklung des Kaufvertrags;

- Auftragsdatenbearbeiter: Als Auftragsbearbeiter gilt, wer im Auftrag des Verantwortlichen Personendaten bearbeitet, z.B. Cloud-Dienstleister (Art. 5 lit. k DSG, vgl. auch vorangehende Ziff. 10).
- Profiling: Unter Profiling wird jede Art der automatisierten Bearbeitung von Personendaten verstanden, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen (z.B. Arbeitsleistung, wirtschaftliche Situation, Gesundheit, Interessen, Aufenthaltsort, persönliche Vorlieben), zu bewerten, zu analysieren oder vorherzusagen. Verschärfte Rechtsfolgen gelten indes nur beim «Profiling mit hohem Risiko», das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person. Dieses ist vergleichbar mit dem heutigen Konzept des «Persönlichkeitsprofils». Es ist darauf hinzuweisen, dass das nDSG kein Einwilligungserfordernis für das Profiling mit hohem Risiko einführt, sondern lediglich fordert, dass eine Einwilligung, sofern diese als Rechtfertigungsgrund nach Art. 31 nDSG erforderlich sein sollte, «ausdrücklich» erfolgen muss. In diesem Zusammenhang sei daran erinnert, dass die Bearbeitung von Personendaten sowohl unter geltendem als auch unter neuem Recht grundsätzlich keines Rechtfertigungsgrundes bedarf (vgl. vorstehende Ziff. 5 und 9).
- «Privacy by Design» und «Privacy by Default»: Unter nDSG werden die Grundsätze «Privacy by Design» und «Privacy by Default» eingeführt. Wie der Name bereits andeutet, bedeutet «Privacy by Design» (Datenschutz durch Technikgestaltung), dass bereits zum Zeitpunkt der Planung eines Bearbeitungssystems technische und organisatorische Massnahmen getroffen werden sollen, um insbesondere die Sicherheit der Personendaten zu gewährleisten. Der Grundsatz «Privacy by Default» (Datenschutz durch Voreinstellung) besagt, dass die Voreinstellungen eines Datenbearbeitungssystems so zu konfigurieren sind, dass nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen bestimmten Verarbeitungszweck tatsächlich erforderlich sind. Damit sollen auch wenig technik-affine Nutzer/innen geschützt werden, die selbst keine Datenschutzeinstellungen nach ihren Präferenzen anpassen können. Es gilt anzumerken, dass ausschliesslich dort eine datenschutzfreundliche Voreinstellung getroffen werden muss, wo die Einstellungen überhaupt angepasst werden können.

13) 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 zu CHF 250'000.00 (z.B. wenn sie gegen Ihre Informations- oder Auskunftspflichten (Art. 19 ff. bzw. 25 ff. nDSG) verstossen oder Ihre Sorgfaltspflichten verletzen, namentlich Personendaten unrechtmässig ins Ausland (Art. 16 f. nDSG) oder an einen Auftragsbearbeiter (Art. 9 nDSG) bekanntgeben oder die Mindestanforderungen an die Datensicherheit (Art. 8 nDSG

i.V.m. Art. 1 ff. DSV) nicht einhalten). Im Gegensatz zur DSGVO richten sich die Sanktionen unter dem nDSG nicht gegen das fehlbare Unternehmen, sondern gegen die für die Einhaltung des Datenschutzes verantwortliche natürliche Person (z.B. Geschäftsführer oder Verwaltungsrat, aber unter Umständen auch andere Mitarbeitende). Es wird ausschliesslich (eventual-)vorsätzliches Verhalten bestraft (Art. 60 ff. nDSG). Ausnahmsweise können Unternehmen auch direkt in die Pflicht genommen werden, falls eine Busse von höchstens CHF 50'000.00 in Betracht fällt und die Ermittlung der strafbaren natürlichen Person innerhalb des Unternehmens oder der Organisation einen unverhältnismässigen Untersuchungsaufwand mit sich ziehen würde (Art. 64 abs. 2 nDSG)

Das Ignorieren des (neuen) Datenschutzgesetzes kann jedoch nicht nur für die verantwortliche Person in einem Unternehmen, sondern auch für das Unternehmen selbst Folgen haben, insbesondere für seine Reputation. Auch wurden die Kompetenzen des Eidgenössischen Datenschutzbeauftragen (EDÖB) erweitert (Art. 51 nDSG). Neu kann er nicht nur Empfehlungen aussprechen, sondern auch Verwaltungsmassnahmen verfügen (z.B. Anordnung, dass eine Bearbeitung angepasst, unterbrochen oder abgebrochen wird oder Personendaten gelöscht werden), was für Unternehmen ebenfalls eine einschneidende Massnahme darstellen kann.

14) Wie kann man sich auf die Änderungen vorbereiten?

Zunächst sollte baldmöglichst ein Aktionsplan mit Hilfe einer GAP-Analyse definiert werden, um die Datenschutz-Compliance Schritt für Schritt an das neue Gesetz anzupassen. Je nach Grösse des Unternehmens und dem Umfang von Datenbearbeitungen kann dieser Prozess einige Tage oder aber mehrere Monate dauern. Unternehmen, die bereits DSGVO-compliant sind, werden selbstredend weniger Aufwand haben solche, die auf Feld eins beginnen. Nichtsdestotrotz sind pragmatische Lösungen erforderlich, d.h. es sollten vorderhand die gesetzlich zwingenden Mindestvorgaben (z.B. Verzeichnis, Informationspflicht, Auftragsbearbeitungsverträge, Datenübermittlungen in Drittländer etc.) umgesetzt werden.

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 mangels interner Expertise und/oder Resourcen nötig, sollten Unternehmen IT-Sicherheits- und Datenschutzexperten beiziehen, sei es, um die Ausarbeitung oder punktuelle Überprüfungen von Dokumenten (z.B. Datenschutzerklärungen) oder Verträgen (ADVs) vornehmen zu lassen oder um detaillierte Compliance-Programme (z.B. Weisungen, Prozesse) zu entwickeln.

15) Welche Schritte sind nötig, um mit dem neuen DSG konform zu werden? Welche Massnahmen sind erforderlich?

Ohne auf die einzelnen technischen, rechtlichen und IT-Aspekte zur Einhaltung des nDSG einzugehen, sollte ein pragmatischer Aktionsplan mindestens die folgenden Massnahmen beinhalten:

1. **Verantwortlichkeiten und Funktionen festlegen**
   Für die Projektplanung ist es wichtig, vorgängig die Verantwortlichkeiten

festzulegen und Funktionen zu vergeben. Es sollte eine zentrale Datenschutzstelle (Koordinator, Ansprechperson) geschaffen werden.

In diesem Zusammenhang kann sogleich geprüft werden, ob ein Datenschutzberater ernannt werden muss oder soll (im Gegensatz zur DSGVO ist dies unter dem nDSG für Private freiwillig – nur Bundesorgane sind gesetzlich dazu verpflichtet, Art. 10 nDSG und Art. 23 DSV)

2. **Eine umfassende Bestandsaufnahme ist zentral**
   Unternehmen müssen unter dem nDSG bestimmte Informationspflichten erfüllen, d.h. sie müssen bei der Beschaffung von Personendaten über die Identität des Verantwortlichen, den Bearbeitungszweck, allfällige Datenempfänger usw. informieren (Art. 19 ff. nDSG und Art. 13 DSV). Zudem müssen sie in der Lage sein, die Betroffenenrechten zu erfüllen, etwa einer betroffenen Person Auskünfte zur Bearbeitung ihrer Personendaten zu erteilen (Art. 25 ff. nDSG und Art. 16 ff. DSV). 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 (sog. Bearbeitungsverzeichnis) als Vorlage dienen. Damit wird nicht nur eine gute Ausgangslage für die Erarbeitung weiterer (zwingender) datenschutzrechtlicher Dokumente (z.B. Datenschutzerklärung, ADVs etc.) geschaffen, sondern es kann zugleich die (allfällige) Pflicht zur Führung eines Bearbeitungsverzeichnisses wahrgenommen werden. Eine solche Bestandsaufnahme ist eine kollektive Anstrengung, die alle Mitarbeiter, die in die Bearbeitung von Personendaten involviert sind, einbeziehen muss.

3. **GAP-Analyse und Abschätzung der Risiken**
   Mittels Gap-Analyse (Vergleich Ist- und Sollzustand) können die erforderlichen Umsetzungsarbeiten identifiziert und anschliessend dokumentiert werden. Für diese Zwecke kann ebenfalls auf Vorlagen für Bearbeitungsverzeichnisse zurückgegriffen werden.

   Einige Pflichten des nDSG, wie bspw. die Anforderungen an die Datensicherheit, die Pflicht von KMU zur Führung von Bearbeitungsverzeichnissen oder die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung sind abhängig vom Risiko, welches die Datenbearbeitungen des Unternehmens mit sich bringen. Aus diesem Grund ist eine vorgängige Risikobewertung erforderlich, um die konkreten Umsetzungsmassnahmen zu bestimmen. Zur Gewährleistung einer angemessenen Datensicherheit müssen der Schutzbedarf der Personendaten bestimmt und die im Hinblick auf das Risiko geeigneten technischen und organisatorischen Massnahmen festlegt werden. Für die Kriterien zur Bestimmung des Schutzbedarfs der Personendaten kann auf die Kriterien von Art. 1 Abs. 2 DSV, für diejenigen zur Beurteilung des Risikos für die Persönlichkeit oder die Grundrechte der betroffenen Person auf die Kriterien in Art. 1 Abs. 3 DSV abgestellt werden. Bei der Festlegung der technischen und organisatorischen Massnahmen sind zudem der

Stand der Technik sowie die Implementierungskosten zu berücksichtigen (Art. 1 Abs. 4 DSV).

Erhöhte Risiken und damit höhere Anforderungen an die Datenschutz-Compliance (insb. Datensicherheit) können bspw. vorliegen, wenn:

- Unternehmen eine grosse Menge an Personendaten bearbeiten. Z.B. 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 nDSG definiert) bearbeiten. Betroffen sind z.B. Unternehmen, die Personendaten über politische oder religiöse Meinungen, Gesundheit, genetische oder rassische Daten, Sozialhilfe, Strafverfolgung usw. bearbeiten.
- Unternehmen ein Profiling mit hohem Risiko durchführen.
- Unternehmen automatisierte Einzelentscheidungen durchführen.

In diesen Fällen sind die Anforderungen an den Datenschutz und insbesondere an die Datensicherheit höher als beispielsweise 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 regelmässig 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.

4. **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.

   Zwar wird weder im nDSG noch in der DSGVO explizit verlangt, dass Schulungen durchgeführt werden, faktisch sind diese aber oft notwendig (und können sich bei einem strafrechtlich relevanten Verstoss allenfalls haftungsreduzieren auswirken), um im Unternehmen die erforderliche Sensibilität für das Thema zu schaffen.

   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.

5. **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 nDSG unerlässlich (auf der Unternehmenswebsite, aber auch in der physischen Korrespondenz).

6. **IT-Sicherheit**
   Unter dem Stichwort Datensicherheit müssen Unternehmen sicherstellen, dass die Sicherheit ihrer IT-Systeme und Software-Anwendungen den Vorgaben des neuen Gesetzes entspricht. Dazu gehören insbesondere technische und organisatorische Massnahmen (sog. TOMs, z.B. Zugriffsrechte, Pseudonymisierung) zur Verhinderung von Cyberattacken, Datenmanipulation, Datendiebstahl und anderweitigen Datenverlust. Mit den TOMs soll auf die Schutzziele der Datensicherheit nach Art. 2 DSV hingewirkt werden (Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit).

   In diesem Zusammenhang ist zu erwähnen, dass «über die gesamte Bearbeitungsdauer» eine Pflicht zur Überprüfung und gegebenenfalls Anpassung der getroffenen Massnahmen besteht und ein vorsätzlicher Verstoss gegen die Mindestanforderungen an die Datensicherheit sanktionsbewehrt ist (Art. 61 lit. c nDSG).

7. **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 und entsprechende Reglemente oder Weisungen ausgearbeitet werden. Diese 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).

8. **Erstellung und Führung eines Verzeichnisses der Bearbeitungstätigkeiten**
   Das nDSG 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 nDSG und Art. 24 DSV).

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.

9. **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 ihrerseits Verträge bzw. Vertragsanpassungen verlangen werden, um ihrerseits Datenschutz-Compliance sicherzustellen.

10. **Informiert bleiben**
    Um sich dem Thema Datenschutz-Compliance unter dem nDSG 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).

    Zu beachten ist, dass die Sicherstellung der Datenschutz-Compliance keine einmalige Übung ist. Vielmehr sollte diese u.a. aufgrund der technischen (z.B. neue IT-Systeme), rechtlichen (z.B. Gesetzesanpassungen oder Behördenpraxis) und unternehmerischen (z.B. neue Dienstleistungen, Niederlassungen in anderen Ländern) Entwicklung regelmässig überprüft und gegebenenfalls angepasst werden. Mit Blick auf die Datensicherheit schreibt Art. 1 Abs. 5 DSV explizit vor, dass der Schutzbedarf der Personendaten, das Risiko und die technischen und organisatorischen Massnahmen über die gesamte Bearbeitungsdauer hinweg zu überprüfen und die Massnahmen nötigenfalls anzupassen sind. Es bietet sich an, entsprechende Verfahren und Verantwortlichkeiten für diese Überprüfungen festzulegen.