Neues Datenschutzrecht – Wichtige Änderungen für Unternehmen

Im Herbst 2020 hat das Bundesparlament den Entwurf des neuen Datenschutzgesetzes (nDSG) verabschiedet. Das nDSG soll voraussichtlich Ende 2022 in Kraft treten und das bisherige DSG von 1992 ersetzen.

Das nDSG führt zu zahlreichen Angleichungen an die Datenschutz-Grundverordnung der Europäischen Union (DSGVO). Das Schweizer Grundkonzept wird allerdings beibehalten und weicht in verschiedenen Punkten von der DSGVO ab.

Diese Aspekte sind für Unternehmen wichtig:

1. **Daten juristischer Personen nicht erfasst**: Das nDSG schützt die Daten juristischer Personen (also z.B. einer AG oder GmbH) nicht mehr.

2. **Streng vertrauliche Personendaten**: Die Liste streng vertraulicher Personendaten wird ausgeweitet und wird auch genetische und biometrische Daten, die eine natürliche Person eindeutig identifizieren (z. B. Fingerabdrücke, Netzhaut-Scans), erfassen.

3. **Sicherstellung von Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen**: Insbesondere, damit die Bearbeitungsgrundsätze (Transparenz, Zweckgebundenheit, Verhältnismässigkeit und Datensicherheit) eingehalten werden und sich die Datenbearbeitungen auf das für den Verwendungszweck nötige Mindestmass beschränken.

4. **Erweiterte Informationspflichten**: Wenn Personendaten erhoben werden, müssen die betroffenen Personen in Kenntnis gesetzt werden über a.) die Identität und Kontaktdaten des Datenverarbeiters, b.) den Zweck der Verarbeitung und c.) alle Empfängerinnen und Empfänger oder Empfangskategorien, denen Personendaten mitgeteilt werden. Im Fall der Offenlegung im Ausland sind ausserdem das Land oder die internationale Einrichtung und gegebenenfalls die Garantien des Personendatenschutzes anzugeben.

   Betroffene Personen haben Anspruch auf alle Informationen, die wichtig für sie sind, um ihre Rechte gemäss nDSG geltend zu machen. Die der betroffenen Person mitgeteilten Informationen können daher nicht in allen Fällen auf dem im nDSG aufgeführten Mindestkatalog beschränkt werden.

5. **Recht auf Datenübertragbarkeit**: Eine betroffene Person kann verlangen, dass die oder der Datenverantwortliche ihre Personendaten in maschinenlesbarer Form - für die Betroffenen kostenlos - an eine andere für die Daten verantwortliche Person übermittelt oder überträgt.

6. **Automatisierte Entscheidungsfindung**: Basiert eine Entscheidung ausschliesslich auf automatisierter Verarbeitung und zieht rechtliche Folgen für die betroffene Person nach sich oder beeinträchtigt diese erheblich, so ist die oder der Datenverantwortliche dazu verpflichtet, die betroffene Person darüber in Kenntnis zu setzen. Der betroffenen

Person muss die Möglichkeit gegeben werden, ihre Position darzulegen. Ausserdem kann sie oder er verlangen, dass die Entscheidung durch eine natürliche Person überprüft wird.

7. **Exterritorialität**: Ausweitung des Anwendungsumfangs des nDSG auf Sachverhalte, die im Ausland geschehen und sich auf die Schweiz auswirken.

8. **Repräsentanz in der Schweiz**: Datenverantwortliche im Ausland müssen unter bestimmten Bedingungen einen Vertreter in der Schweiz benennen, falls sie Personendaten von Personen in der Schweiz verarbeiten.

9. **Datenschutzfolgenabschätzung**: Die oder der Datenverantwortliche ist verpflichtet, eine Datenschutzfolgenabschätzung durchzuführen, falls die Datenverarbeitung ein Risiko für die Persönlichkeits- oder Grundrechte der betroffenen Person darstellt. Die geplante Verarbeitung, die entstehenden Risiken und geeignete Massnahmen, um den Risiken entgegenzuwirken, müssen dargestellt werden.

10. **Meldung von Datenschutzverletzungen**: Im Falle einer Datenschutzverletzung, welche eine erhebliche Gefahr der Verletzung der Persönlichkeits- oder Grundrechte der betroffenen Person darstellt, muss die oder der Datenverantwortliche den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) schnellstmöglich darüber in Kenntnis setzen. Die betroffenen Personen müssen ebenfalls informiert werden, falls dies für ihren persönlichen Schutz notwendig erscheint.

11. **Sanktionen**: Für natürliche Personen kann die maximale Geldbusse im Fall einer vorsätzlichen Verletzung der Informations- und Offenlegungspflichten sowie bestimmter Sorgfaltspflichten bis zu CHF 250'000 je Verstoss betragen. Im Gegensatz zur DSGVO, die eine Verantwortung von Unternehmen vorsieht, können verantwortliche Personen innerhalb des Unternehmens, wie z.B. der Verwaltungsrat oder der Geschäftsführer, direkt sanktioniert werden.

Was ist Unternehmern zu empfehlen?

Das nDSG sieht keine Übergangsfristen vor. Das bedeutet, dass das Gesetz nach dem Inkrafttreten sofort angewendet werden muss. Daraus folgt, dass sich Unternehmen bereits heute mit dem Thema auseinanderzusetzen haben.

Ein pragmatischer Aktionsplan kann wie folgt aussehen[1]:

1. **Bestandsaufnahme:** Unternehmen müssen unter dem nDSG bestimmte Informationspflichten erfüllen, d.h. sie müssen bei der Beschaffung von Personendaten über die Identität der oder des Verantwortlichen, den Bearbeitungszweck, allfällige Datenempfangende usw. informieren. Zudem müssen sie in der Lage sein, die Betroffenenrechte zu erfüllen, etwa einer betroffenen Person Auskünfte zur Bearbeitung

[1] Basierend auf dem Merkblatt von economiesuisse unter www.economiesuisse.ch

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 durchführen. Dabei kann das gesetzlich neu vorgeschriebene Verzeichnis als Vorlage dienen. Eine solche Bestandesaufnahme ist eine kollektive Anstrengung, die alle Mitarbeitenden, 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 Personendaten sind, desto höher sind die Anforderungen an die Datenschutz-Compliance bzw. desto grösser sind die potenziellen Sanktionen und Reputationsschäden bei einem Verstoss.

3. **Bewusstsein wecken**: Sowohl für kleine als auch grosse Unternehmen gilt: alle Mitarbeitenden, von den Lernenden bis zur Geschäftsführung, müssen für das Thema Datenschutz sensibilisiert werden. Empfangsmitarbeitende, Projektleitetende, Personalleitende, Beraterinnen und Berater, Freiberuflich tätige Personen, Geschäftsführung – Mitarbeitende auf allen Ebenen eines Unternehmens bearbeiten regelmässig Personendaten und tragen hierfür ggf. sogar eine strafbewehrte Verantwortung.

4. **Transparenz und Information:** Transparenz bei der Datenbearbeitung ist auch unter dem neuen DSG ein wichtiger Grundsatz. Hinzu kommt die Informationspflicht bei der Datenbeschaffung. Die oder 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).

5. **IT-Sicherheit**: Unternehmen müssen sicherstellen, dass die Sicherheit ihrer IT-Systeme und Software-Anwendungen den Vorgaben des neuen Gesetzes entsprechen. 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, welche Mitarbeitenden (inkl. Vertretung) welche Massnahmen innert welcher Frist treffen müssen. 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, welche Mitarbeitenden diese Meldung innert welcher First und in welcher Form an welche Behörde vornehmen müssen.

7. **Erstellung und Führung eines Verzeichnisses der Bearbeitungstätigkeiten**: Das nDSG sieht vor, dass sowohl die oder der Verantwortliche als auch die Auftragsbearbeitenden je ein Verzeichnis über ihre Bearbeitungstätigkeiten führen müssen. Diese Pflicht gilt grundsätzlich für alle Unternehmen. Der Bundesrat kann jedoch Ausnahmen vorsehen für Unternehmen mit weniger als 250 Mitarbeitenden (Art 12 Abs. 2 nDSG). 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 Kundinnen und Kunden, Liefernden und Dienstleistenden sowie Arbeitnehmenden 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 nDSG bewusst zu werden, muss man in der Lage sein, die konkreten Auswirkungen des neuen Gesetzes auf die eigenen Bearbeitungsprozesse zu verstehen.

Kontakt

Wirtschaftskammer Baselland
Rechtsberatung
Haus der Wirtschaft
4133 Pratteln
061 927 64 64
info@kmu.org