

Datenschutz für KMU

1. Datenschutz – geht mich das etwas an?

Kurze Antwort: Ja. Das Datenschutzgesetz ("DSG") geht alle etwas an, die Personendaten bearbeiten, sprich alle Unternehmen, die Mitarbeiter, Kunden, Lieferanten, Webseiten, Partner oder IT-Lösungen haben. Warum ist das so? Weil das Datenschutzgesetz die Rechte der betroffenen Personen schützt, von welchen Sie Daten bearbeiten, egal ob Sie ein einzelner Uhrmacher, eine lokale Autogarage, eine regionale Bank oder ein globaler Software-Riese sind.

2. Warum jetzt?

In der Tat, Datenschutz gibt es in der Schweiz schon länger, auch das entsprechende Gesetz dazu: Das DSG von 1992. Dieses wird nun auf den 1. September 2023 revidiert. Das hat auch damit zu tun, dass die Schweiz gegenüber der EU weiterhin ein angemessenes Datenschutzniveau halten will und dass der freie Datenfluss mit unserem wichtigsten Handelspartner nicht gekappt wird. Dies hat einerseits zur Folge, dass ein paar neue Grundsätze und Pflichten Einzug ins DSG finden. Andererseits erhalten die Behörden neue Kompetenzen, um die Einhaltung des DSG zu überprüfen und gegebenenfalls Verfehlungen zu bestrafen.

3. Was will es denn von mir, dieses DSG?

Grundsätzlich will das DSG von Ihnen zwei Dinge. Erstens verlangt es, dass Sie sich als Datenbearbeiter bewusst sind, wie Sie welche Daten wozu bearbeiten. Zweitens verlangt es, dass Sie die Rechte der Personen respektieren, von welchen Sie Daten bearbeiten. Als Datenbearbeiter sind Sie wie ein Treuhänder. Ihnen werden Personendaten anvertraut, freiwillig oder gestützt auf eine vertragliche oder gesetzliche Pflicht. Folglich müssen Sie diese Daten sicher und vertraulich behandeln. Weiter müssen Sie wissen welche Daten Sie von wem und wozu verwalten. Letztlich müssen Sie jederzeit darüber Auskunft geben können, was Sie mit den Daten machen, und informieren, wenn etwas mit den Daten schiefgelaufen ist.

4. Was heisst das nun für mich?

Als Einstieg müssen Sie sich eine Übersicht verschaffen, welche Abläufe in Ihrem Unternehmen Personendaten bearbeiten, in Zusammenarbeit mit wem und unter welchem Rahmenbedingungen.

- Solche Abläufe sind z.B. der Bewerbungsprozess, das Online-Geschäft, die Kundenverwaltung, die Video-Überwachung, die Spesen-Bewirtschaftung, der Newsletter-Versand, usw. Ziel der Bestandesaufnahme ist es, diese zu dokumentieren und allfällige datenschutzrechtliche Lücken festzustellen.
- Weiter relevant ist es, mit welchen Dritten Sie zusammenarbeiten (und gestützt auf welchen Vertrag), um diese Daten zu bearbeiten (z.B. Cloud-Lösung, externer Lohnbuchhalter, Sicherheitsdienst oder Aussendienst oder IT-Firma). Auch diese werden in der Bestandesaufnahme erfasst.

- Auch Teil dieser Übersicht ist die Bestandesaufnahme hinsichtlich der technischen und organisatorischen Massnahmen ("TOM") in Ihrem Unternehmen, welche die vertrauliche und korrekte Bearbeitung von Personendaten ermöglichen und sicherstellen. Solche können z.B. sein wie Sie Ihr Unternehmen gegen physische und digitale Eindringlinge schützen, wie Sie Schlüssel und Batches verwalten, welche Schulungen und Prozesse im Unternehmen existieren, um Sicherheit und Datenschutz zu fördern, oder wie Sie Ihre Daten sichern, verwalten und teilen.

Gestützt auf diese Übersicht der relevanten Abläufe, der Zusammenarbeit mit Dritten und Ihrer TOM können Sie nun die nächste Schritte machen.

5. Was setze ich dann bei mir um?

Nun können Sie Ihre datenschutzrechtlichen Pflichten gezielt, effizient und mit dem nötigen Pragmatismus erfüllen. Das heisst:

- Die betroffenen Personen richtig informieren, wo es angezeigt ist (z.B. Mitarbeiter, Kunden Geschäftspartner oder Webseiten-Besucher)
- Verträge mit den relevanten Dienstleistern auf Datenschutz hin überprüfen
- Die Datensammlung und -nutzung auf der Webseite anpassen, wo nötig
- Intern Datenschutz als Kompetenz einführen, schulen und dokumentieren
- Aufbewahrungsfristen definieren und einhalten
- Datensicherheit dort stärken, wo sie Schwächen hat
- Anfragen von betroffenen Personen richtig und zeitgerecht beantworten

6. Danach ist aber gut, oder?

Datenschutz gehört als Disziplin ins Denken des Unternehmens. Das bedeutet, dass Datenschutz Teil der Gesamtüberlegung und -beurteilung werden muss, zum Beispiel bei:

- Änderung von bestehenden Prozessen
- Einführung von neuen Abläufen
- Anpassungen der Webseite
- Aufnahme von neuen Online-Produkten/Dienstleistungen
- Anschaffungen oder Einbindungen von neuer IT
- Datenrelevante Zusammenarbeit mit neuen Partnern oder Erweiterung bestehender Zusammenarbeit
- Einführungen eines Systems zur Kundenbewirtschaftung oder zur Zeit-/Ferien-Management der Mitarbeiter
- Planung von Marketing-Massnahmen

Dadurch wird von Anfang an und immer wieder gefragt, welchen Einfluss die Tätigkeiten Ihres Unternehmen auf die betroffenen Personen haben und gleichzeitig sichergestellt wie Sie dabei Ihre datenschutzrechtlichen Pflichten erfolgreich erfüllen können; nahtlos eingebunden in Ihre Geschäftstätigkeit.

Autor: Denis F. Berger