PROBSTPARTNER

Newsletter Datenschutzrecht

Revision des Datenschutzgesetzes in der Schweiz – Wie umsetzen?

von Kaj Seidl-Nussbaumer

Juni 2021

Nachdem wir im letzten Datenschutznewsletter eine Übersicht über das neue, voraussichtlich 2022 ohne Übergangsfrist in Kraft tretende Datenschutzgesetz (nDSG) und die Änderungen, die es mit sich bringt, gegeben haben, widmen wir uns in diesem Newsletter der Frage, wie man diese neuen Anforderungen effizient umsetzen kann.

Jedes Unternehmen bringt eine ganz individuelle Ausgangslage mit sich. Es ist zu unterscheiden zwischen Unternehmen, die bereits DSGVO-compliant sind (Ziff. 1) oder sich bereits umfassend mit dem Datenschutz (aber nicht DSGVO) befasst haben (Ziff. 4), und solchen, für die das Thema (fast) ganz neu ist (Ziff. 3).

1. Erste Weichenstellung: DSGVO-Compliance

1.1 DSGVO Anwendbarkeit in der Schweiz

Seit Mai 2018 ist in der EU deren neues, einheitliches Datenschutzrecht, die Datenschutzgrundverordnung (DSGVO) bzw. die General Data Protection Regulation (GDPR) anwendbar. Die DSGVO beansprucht unter gewissen Umständen auch Geltung ausserhalb der EU und damit auch in der Schweiz, nämlich falls:

- ein Angebot von Waren oder Dienstleistungen an Personen in der EU gemacht wird; oder
- das Verhalten von Personen in der EU beobachtet wird.

Dies trifft auf viele Schweizer Unternehmen und in der Schweiz beheimatete Konzerne zu. Sie stellten sich daher bereits 2018 die Frage, was sie unternehmen müssen, um den neuen EU-Regeln zu genügen und Risiken für Klagen und Bussen zu minimieren. Diese Unternehmen haben sich also bereits detailliert mit ihrer Datenbearbeitung befasst und Massnahmen implementiert.

1.2 Empfohlenes Vorgehen für Unternehmen mit DSGVO-Compliance

Für Unternehmen mit DSGVO-Compliance, d.h. Unternehmen, die die Vorschriften der DSGVO bereits einhalten, ist der Handlungsbedarf im Hinblick auf die Einführung des nDSG in der Regel eher klein. Sie sollten die getroffenen Massnahmen überprüfen und die nötigen Anpassungen vornehmen, um die zum Teil weitergehenden oder abweichenden Anforderungen des neuen Schweizer Rechts umzusetzen. Insbesondere sollten folgende Anpassungen geprüft werden:

- bezüglich der **internationalen Datentransfers** prüfen, ob die vom nDSG geforderten, gegenüber der DSGVO weitergehenden, Informationspflichten eingehalten sind und allfällige Datenschutzerklärungen erweitern;
- **Datenschutzerklärungen und Auftragsdatenbearbeitungsverträge prüfen** und, falls sie ausschliesslich auf die DSGVO Bezug nehmen, Anpassungen durch Generalisierung oder Miteinbezug des Schweizer Rechts erwägen;

- implementierte **Prozesse prüfen** auf Übereinstimmung mit Anforderungen des Schweizer Rechts und gegebenenfalls anpassen (z.B. Beantwortung Auskunftsgesuch, Vorgehen bei Feststellung und Meldung einer Datenschutzverletzung, Prozess zur Erstellung einer Datenschutzfolgenabschätzung etc.);
- prüfen, ob für **ausländische Konzerngesellschaften** eine Vertretung in der Schweiz ernannt werden muss, und diese gegebenenfalls ernennen;
- Einsetzung eines **Datenschutzberaters** prüfen.

2. Zweite Weichenstellung: Vorbefassung mit Datenschutzrecht

Die übrigen Unternehmen lassen sich im Wesentlichen in zwei Gruppen einteilen:

a) Unternehmen, die sich bereits einmal umfassend mit ihren Datenbearbeitungen und den Anforderungen des (bisherigen) Datenschutzrechtes befasst haben; und

b) Unternehmen, die sich erst punktuell bezüglich einzelner Fragen (z.B. bezüglich HR, Kundendaten, E-Mail Marketing o.ä.) oder noch gar nicht konzeptuell mit dem Datenschutzrecht und ihren Datenbearbeitungen auseinandergesetzt haben.

Das empfohlene Vorgehen unterscheidet sich für diese beide Gruppen. Da für Unternehmen der zweiten Gruppe ein grösserer Aufwand anfällt, gehen wir zunächst auf diese ein (Ziff. 3). Der Handlungsbedarf für Unternehmen, die sich bereits einmal umfassend mit dem Datenschutz befasst haben, wird daran anschliessend (Ziff. 4) aufgezeigt.

3. Was muss ein Unternehmen tun, das sich noch nicht (im Detail) mit Datenschutz befasst hat?

Wenn Ihr Unternehmen sich noch nicht oder erst punktuell mit Datenschutz befasst hat, empfehlen wir ein Vorgehen in drei Schritten:

In einer ersten Phase sollte eine Bestandesaufnahme über die aktuell stattfindenden Datenbearbeitungen und bestehende Dokumentation gemacht werden (Feststellung

des IST-Zustandes). Anschliessend sind die rechtlichen Anforderungen an die Bearbeitungen für Ihr Unternehmen individuell zu klären (Festhalten SOLL-Zustand) und Compliance-Lücken zu identifizieren (GAP-Analyse). Abschliessend sind die angesichts einer Risikobeurteilung passenden Massnahmen zur Schliessung der Lücken umzusetzen (Umsetzungsphase).

3.1 Feststellung des IST-Zustands

Ziel dieser Phase ist, dass das Unternehmen die folgende Frage beantworten kann:

Welche Personendaten werden in meinem Unternehmen zu welchem Zweck wie durch wen und wo bearbeitet?

Um dies beantworten zu können, müssen sich die Bereichsverantwortlichen (z.B. Operations, HR, IT, Marketing etc.) mit den unter ihnen laufenden Datenbearbeitungen auseinandersetzen und es wird auch geklärt, in welchen Teilbereichen allenfalls schon Massnahmen getroffen wurden (z.B. Datenschutzerklärung auf Webseite oder für Mitarbeiter). Zur Orientierung hilft, bereits in dieser Phase einen Entwurf des Datenbearbeitungsverzeichnisses zu erstellen. Diese Phase, d.h. die Abklärung des IST-Zustands, ist häufig der aufwändigste Teil, weil es allenfalls nicht ganz einfach ist, die tatsächlich stattfindenden Datenbearbeitungen zu benennen, zu lokalisieren und richtig einzuordnen.

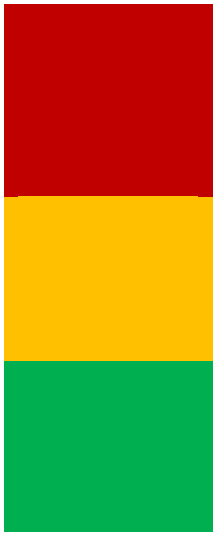
Wird externe Hilfe in Anspruch genommen, z.B. von unserem Datenschutzteam, wird der IST-Zustand in der Regel mit Interviews des Führungsteams oder Fragebögen ermittelt, je nach Setup und Bedürfnissen des Kunden.

3.2 Festhalten SOLL-Zustand und GAP-Analyse

Nachdem Sie sich ein Bild über die aktuellen Datenbearbeitungen gemacht haben, muss geklärt werden, welche rechtlichen Anforderungen konkret für Ihr Unternehmen bestehen (SOLL-Zustand) und wo sich daraus Lücken gegenüber dem IST-Zustand ergeben (GAP-Analyse).

Unser Datenschutzteam schliesst diese Phase jeweils mit einem Bericht ab, in dem die Lücken aufgezeigt und Massnahmen zu deren Schliessung empfohlen werden.

Wir ordnen die Empfehlungen anhand der möglichen zivil- und strafrechtlichen Risiken und teilen diese mittels eines einfachen Ampelsystems in drei Kategorien ein:



sofortiger Handlungsbedarf
(z.B. wegen grossem Bussenrisiko und hoher Eintretenswahrscheinlichkeit. Anwendungsbeispiele: gänzlich fehlende Information bei ausgeprägtem Newslettertracking, Nutzung US-amerikanischer SaaS Dienste ohne weitere Sicherheitsvorkehrungen)

mittelfristiger Handlungsbedarf
(z.B. wegen Prozessgefahr mit mittlerer Eintretenswahrscheinlichkeit. Anwendungsbeispiele: fehlender Prozess für Meldung von Datenschutzverletzungen, Mängel bei Beauftragung von Subunternehmern)

langfristiger Handlungsbedarf oder nützliche, aber nicht zwingende Massnahmen
(Anwendungsbeispiele: Datenschutzhandbuch, Einsetzung eines Datenschutzberaters etc.)

3.3 Umsetzungsphase

In der Umsetzungsphase setzen Sie die von Ihnen ausgewählten Massnahmen um. Dies können Sie wiederum mit oder ohne externe Hilfe tun.

3.4 Mögliche Themenfelder

Um eine Vorstellung zu erhalten, welche Themen überhaupt anzupacken sind, können Sie in unserem Newsletter vom Mai 2021 die Übersicht über das neue Datenschutzgesetz durchgehen. Zusammenfassend sollten Sie sich mit folgenden Themenfeldern befassen:

a) Gesamtüberblick / Bearbeitungsverzeichnis
Welche Personendaten *(normal/besonders schützenswert)* werden zu welchem Zweck (*Abwicklung Kundenverträge, Marketing, gesetzliche Pflichten etc.)* wie *(normale Bearbeitung / Profiling / Profiling mit hohem Risiko)* durch wen *(inhouse / Gruppengesellschaften / Outsourcings)* wo *(Schweiz / EU und EWR / Rest der Welt)* bearbeitet? Muss ich ein Bearbeitungsverzeichnis führen? Muss ich ein weiteres Bearbeitungsverzeichnis führen für Kunden, die ihrerseits Personendatenbearbeitungen an mich ausgelagert haben?

b) Datenschutzerklärungen
Informiere ich die Betroffenen *(Kunden, User, Mitarbeiter, Lieferanten etc.)*

angemessen und zum richtigen Zeitpunkt über die Bearbeitung? Habe ich – wo nötig – die Einwilligung richtig eingeholt?

c) Auftragnehmer, Subunternehmer / Internationaler Datentransfer
Habe ich Personendatenbearbeitungen ausgelagert *(z.B. Newsletterversand mittels Online-Dienst)*? Liegt der Bearbeitungsort in der Schweiz, der EU und EWR oder ausserhalb? Habe ich die gesetzlichen Vorgaben eingehalten *(z.B. Information über den Serverstandort, zusätzliche Schutzmassnahmen)*? Entsprechen die geschlossenen Verträge den Anforderungen des Gesetzes?

d) Vertreter in der Schweiz
Habe ich ausländische Tochter- oder Schwestergesellschaften, die allenfalls einen Vertreter in der Schweiz ernennen müssen?

e) Prozesse
Habe ich die nötigen Prozesse implementiert, um im Ernstfall schnell und richtig reagieren zu können *(z.B. bei Datenschutzverletzungen, Auskunfts- oder Löschgesuchen, Datenportabilitätsgesuchen etc.)*?

f) Datenschutzfolgenabschätzung
Einführung eines Prozesses; Bestehen bei mir Datenbearbeitungen, für die eine DSFA vorgenommen werden muss?

g) Technische und organisatorische Massnahmen (TOM)
Habe ich angemessene technische und organisatorische Massnahmen zum Datenschutz getroffen? Sind meine Mitarbeiter entsprechend ausgebildet *(z.B. erkennen sie Social Hacking und Phishing-Versuche, die auf Erlangung von Personendaten abzielen?)*

Diese Liste ist nicht abschliessend, soll aber einen Eindruck geben, mit welchen Fragestellungen Sie sich als Unternehmer im Zusammenhang mit der Herstellung der Datenschutz-Compliance Ihres Unternehmens auseinandersetzen sollten.

4. …und ein Unternehmen, das sich bereits mit Datenschutz befasst hat?

Wenn Datenschutz-Compliance für Sie kein Fremdwort ist und Sie das Thema in Ihrem Unternehmen bereits früher einmal angepackt haben, sollten Sie sich ein Bild

über die Neuerungen machen und diese wo nötig umsetzen. Die wichtigsten Neuerungen, die es zu prüfen gilt, sind:

- **erweiterte Informationspflichten** (sowohl inhaltlich als auch auslösende Umstände): werden alle Betroffenen angemessen und zum richtigen Zeitpunkt über die Datenbearbeitungen informiert? Hierzu sind die bestehenden **Datenschutzerklärungen** (insb. bezüglich internationalem Datentransfer: werden die Zielländer genannt?) und deren Abgabepunkte (z.B. Webseite, Beginn des Arbeitsverhältnisses etc.) zu **überprüfen**;
- Prüfen von **Erleichterungen**: können gewisse Prozesse vereinfacht oder abgeschafft werden, weil **Personendaten juristischer Personen** nicht mehr unter das nDSG fallen und **keine Registrierungspflicht für Datensammlungen mehr** besteht?
- **Auftragsbearbeitungsverträge** prüfen: ist bereits festgehalten, dass die Übertragung der Bearbeitung auf einen Dritten (sog. **Unterauftragnehmer**) **nur mit vorgängiger Genehmigung** des Verantwortlichen zulässig ist? Sind Meldepflichten bei **Feststellung von Datenschutzverletzungen** durch den Auftragsbearbeiter geregelt?
- Neue Kategorien besonders schützenswerter Personendaten: bearbeiten Sie **genetische oder biometrische Daten**, die neu als besonders schützenswerte Personendaten gelten? Überprüfen Sie Ihre Datenschutzdokumentation, ob diese Datenkategorien allenfalls bereits bisher erfasst waren oder neu aufzunehmen sind (z.B. in Datenschutzerklärungen);
- Ist **Profiling** (d.h. automatisierte Auswertung von gewissen Persönlichkeitsaspekten) ein Thema in Ihrem Unternehmen? Sind die **neuen Anforderungen und Differenzierungen** (Profiling / Profiling mit hohem Risiko) in Datenschutzdokumentation und -prozessen berücksichtigt?
- Werden im Unternehmen **automatisierte Einzelentscheidungen** (d.h. Entscheidungen, die ausschliesslich auf einer automatisierten Datenbearbeitung beruhen und für die Betroffenen mit einer Rechtsfolge verbunden sind oder sie erheblich beeinträchtigen) getroffen? Wird über diese angemessen informiert?
- Überprüfung und Aktualisierung bzw. Erstellung des **Datenbearbeitungsverzeichnisses**;

- Einführung eines Prozesses bezüglich Bearbeitung und allenfalls Meldung von **Datenschutzverletzungen**;
- **Datenschutzfolgenabschätzungen (DSFA)**: Einführung eines Prozesses sowie Prüfung, ob Datenbearbeitungen bestehen, für die eine DSFA vorgenommen werden muss;
- Einführung eines Prozesses bezüglich **Datenportabilität** und technische Ermöglichung solcher Herausgaben durch Systemanpassungen;
- prüfen, ob für **ausländische Konzerngesellschaften** eine Vertretung in der Schweiz ernannt werden muss, und diese gegebenenfalls ernennen;
- Einsetzung eines **Datenschutzberaters** prüfen bzw. Umwandlung der Funktion des bisherigen "Datenschutzverantwortlichen" / "Data Protection Officer" (so die aktuelle Terminologie des DSG).

Je nachdem, wie lange es her ist, dass Ihr Unternehmen sich letztmals "datenschutzfit" gemacht hat, kann sich zudem eine umfassende Prüfung der bestehenden Dokumentation, Verträge und Prozesse empfehlen, um einerseits deren Aktualität zu gewährleisten und anderseits Anpassungen an den im Unternehmen gelebten Datenschutz vorzunehmen.

5. Fokusthema: Datenschutzerklärungen

In unserem nächsten Newsletter geht es darum, was bei Datenschutzerklärungen nach dem nDSG zu beachten ist. Falls Sie noch nicht auf dem Verteiler sind, aber eine Zustellung wünschen, senden Sie uns eine Nachricht an info@probstpartner.ch und wir nehmen Sie gerne auf.

Weitere Informationen zum Datenschutz finden Sie unter http://swissdataprotectionlaw.ch/

* * * * *