WilhelmGilliéron
AVOCATS

Auteur: Wilhelm Gilliéron Avocats | Le : 3 Mai 2021

Das neue Bundesdatenschutzgesetz: Sorgen machen, ja! Kein Grund zur Panik!

„Was machen Sie mit meinen Daten? „Warum fragen Sie mich nach meiner Telefonnummer? „Muss ich Ihre Kundendatei ausfüllen? Muss ich Ihnen all diese Informationen geben? „. All diese Fragen, denen sich viele Einzelhändler heute stellen müssen, wurden vor ein paar Jahren noch nicht gestellt.

Im digitalen Zeitalter ist es schwierig, sich dem Bewusstsein zu entziehen, das rund um den Datenschutz besteht, verstärkt durch das Interesse der Medien, über den kleinsten Vorfall zu berichten. Die Beschleunigung der Digitalisierung als Folge der Pandemie hat diese Aufmerksamkeit nur noch verstärkt.

Obwohl oft als „*Gasfabrik*" bezeichnet, kann dem Datenschutz eine fundamentale Schutzfunktion im Kampf gegen die immer größer werdende Informationsasymmetrie zwischen Anbietern und Individuen nicht abgesprochen werden, eine Disparität, die angesichts der vorherrschenden Rolle von Big Tech offensichtlich ist.

In einer Zeit, in der gerade ein neues Bundesgesetz über den Datenschutz verabschiedet wurde und der Bundesrat an Verordnungsentwürfen arbeitet, die bis Ende 2022 oder Anfang 2023 in Kraft treten sollen, stellt sich die Frage, welche Schritte unternommen werden sollen, um den guten Willen in diesem Bereich zu demonstrieren.

In der Realität muss daraus keine „*Gasfabrik*" werden, denn die zu treffenden Maßnahmen hängen weitgehend von der Einschätzung des Risikoniveaus in Bezug auf die verarbeiteten Daten, ihre Kategorien, Volumina, Zwecke usw. ab.

In den allermeisten Fällen reichen die folgenden sechs Maßnahmen, die mit vertretbarem Aufwand ergriffen werden können, aus, um die Einhaltung der Vorschriften zu gewährleisten

1. Inventarisierung von persönlichen Daten

Die Erstellung eines Inventars besteht aus der Auflistung der verschiedenen Arten der Datenverarbeitung, die das Unternehmen durchführt. Auch wenn es für viele Unternehmen, die keine kritische Größe erreichen, nicht erforderlich sein wird, scheint seine Einrichtung eine Best Practice zu sein, die es ermöglicht, sich intern über die durchgeführten Verarbeitungen bewusst zu werden und das Management und die Mitarbeiter für das Thema Datenschutz zu sensibilisieren. Sich dafür die nötige Zeit zu nehmen, ist also alles andere als Zeitverschwendung.

Die Arten der Verarbeitung können mehr oder weniger zahlreich sein. Für die überwiegende Mehrheit der KMU werden sie typischerweise zwei Hauptkategorien von Personen betreffen, nämlich einerseits die Mitarbeiter (Zahlung von Gehältern und Sozialversicherungsbeiträgen, Abwicklung von Krankheitsurlaub, Urlaub, Vorstellungsgesprächen usw.) und andererseits die Kunden (Auftragserteilung, Kundendienst, Marketing).

Für jede Art der Verarbeitung werden die Unterauftragnehmer, die im Bereich der IT immer zahlreicher werden (z. B. Microsoft im Falle des Rückgriffs auf eine Plattform wie Azure oder O365 oder SAP im Bereich der Personalverwaltung, um nur zwei Beispiele zu nennen), und die mögliche Übermittlung der verarbeiteten Daten ins Ausland ermittelt. Die Erstellung des Inventars ist somit eine Gelegenheit, die bestehenden Dienstleister, das Vorhandensein ordnungsgemäßer Verträge (einschließlich Datenschutz- und Sicherheitsklauseln) sowie die Dauer der Aufbewahrung der Daten zu hinterfragen, was oft völlig außer Acht gelassen wird.

Bei kleineren Unternehmen, die ein solches Inventar durchführen wollen, kann diese Aufgabe von einer Person übernommen werden. Bei größeren KMU sollte sie an Abteilungsleiter delegiert werden, die in direktem Kontakt mit den Datenverarbeitungsvorgängen stehen, denen ihre Abteilung zugeordnet ist. Wenn diese Aufgabe intern durchgeführt werden soll, ist nach meiner Erfahrung die Unterstützung und Überprüfung durch einen Anwalt nicht nutzlos, da interne Teams oft große Schwierigkeiten haben, alle Dienstleister zu identifizieren, die ihre Daten verarbeiten, insbesondere im Bereich der IT.

Das Dokument ist nicht statisch, sondern dynamisch und entwickelt sich weiter. Sie sollte daher bei neuen Verarbeitungsvorgängen

ergänzt werden.

Die Behörden stellen oft nützliche Dokumente zur Verfügung, die bei der Erstellung der Bestandsaufnahme helfen und die richtigen Fragen stellen; dies gilt insbesondere für die CNIL in Frankreich.

2. Datenschutzrichtlinie und andere Vertragsdokumente

Um eine saubere Bilanz vorzuweisen, scheint die Erstellung bestimmter Vertragsdokumente unerlässlich zu sein, ohne viel Aufwand zu erfordern. Hier kann zwischen internen und externen Dokumenten unterschieden werden.

Intern ist es sinnvoll, eine Datenschutzrichtlinie zu haben (die normalerweise auf der Website erwähnt und durch einen Cookie-Hinweis ergänzt wird), die in allgemeiner Form die Art der erhobenen Daten und die durchgeführte Verarbeitung definiert. Es ist mittlerweile auch üblich, eine Richtlinie für die Verarbeitung von Mitarbeiterdaten zu erstellen.

Extern sollte eine Standard-Datenverarbeitungsvereinbarung erstellt werden, um sicherzustellen, dass externe Anbieter einen bestimmten Standard einhalten. Zwar haben viele Anbieter inzwischen ihre eigene Datenverarbeitungsvereinbarung, doch ein Standarddokument stellt sicher, dass die Vereinbarung des Anbieters den Anforderungen des Unternehmens entspricht und gegebenenfalls dem Unternehmen zur Verfügung gestellt wird, wenn es keine solche Vereinbarung hat.

3. Folgenabschätzung der Datenverarbeitung

Wenn eine vorgeschlagene Datenverarbeitung wahrscheinlich ein hohes Risiko für den Einzelnen birgt (z. B. eine groß angelegte Verarbeitung medizinischer Daten), muss eine Folgenabschätzung durchgeführt werden. Der Zweck einer solchen Analyse ist es, den Risikograd der Verarbeitung zu bestimmen, auch wenn dies bedeutet, dass die vorherige Zustimmung des Datenschutzbeauftragten eingeholt werden muss. In diesem Fall wird die multidisziplinäre Übung meistens die Unterstützung eines Anwalts erfordern, der in dieser Angelegenheit Fachwissen bereitstellen kann.

Für die überwiegende Mehrheit der KMU sollte sich ein solches Vorgehen jedoch in Grenzen halten, mit Ausnahme einiger spezifischer Bereiche wie dem Gesundheitswesen.

4. Verfahren zur Ausübung der dem Einzelnen zustehenden Rechte

Mit dem Inkrafttreten des neuen Bundesgesetzes werden die Rechte des Einzelnen erweitert. Im Wesentlichen muss jedes Unternehmen in der Lage sein, jeder Person, die dies wünscht, mitzuteilen, ob es Daten über sie verarbeitet und wenn ja, welche Daten.

Es ist dann sinnvoll, sicherzustellen, dass diese Daten leicht identifiziert werden können, was bei kleinen KMUs der Fall sein sollte, aber manchmal schwieriger sein kann, wenn die Daten von Einzelpersonen auf verschiedenen Ebenen von verschiedenen Akteuren verarbeitet werden. Das Inventar ist dann ein nützliches Werkzeug zum Auffinden dieser Daten im Hinblick auf die durchgeführte Verarbeitung.

Die Etablierung von Standardprozessen und Antwortvorlagen kann dann sinnvoll sein, um die Bearbeitung solcher Anfragen auf einheitliche und konsistente Weise zu erleichtern und zu systematisieren.

5. Erstellung eines Reaktionsplans für Sicherheitsvorfälle

Da heutzutage jeder Sicherheitsvorfall erhebliche Auswirkungen auf den Ruf haben kann, wenn er nicht operativ ist, ist es von grundlegender Bedeutung, dass die verarbeiteten Daten von angemessenen Sicherheitsvorkehrungen umgeben sind, die dem Risiko Rechnung tragen.

Entweder beauftragt das betreffende Unternehmen einen Dritten mit dem Betrieb seiner IT-Infrastruktur und ist dann dafür verantwortlich, dass der betreffende Dienstleister vertraglich die notwendigen Sicherheitsgarantien bietet (z.B. durch bestimmte Zertifizierungen, oder dass sich das verwendete Rechenzentrum in der Schweiz oder zumindest in Europa befindet, oder dass ein Datenwiederherstellungsplan vorhanden ist, usw.); oder das Unternehmen betreibt seine eigene IT-Infrastruktur und muss dann dafür sorgen, dass das Sicherheitsniveau bei der Verarbeitung der Daten ausreichend ist.

Es wird heute oft die Ansicht vertreten, dass die Frage nicht lautet, ob ein Sicherheitsvorfall eintreten wird, sondern wann. Dies wirft eine Reihe von Fragen auf: Wie soll man reagieren? Wer sollte reagieren? Was sollte zuerst getan werden? Soll ich die Konten schließen, das System isolieren? Wer sollte informiert werden? Sollen Mitarbeiter, Behörden, die Öffentlichkeit informiert werden? Die Formalisierung des Prozesses, der im Falle eines solchen Vorfalls zu befolgen ist, ist daher ein Zeichen der Vorsicht und, einmal mehr, des Bewusstseins, wie wichtig der Schutz von Daten ist.

6. Ausbildung

Schließlich ist es sinnvoll, die Mitarbeiter durch Schulungen für dieses Thema zu sensibilisieren, die einheitlich sein können oder ggf. je nach Position des Mitarbeiters (z. B. Empfangsmitarbeiter, Personalabteilung, Marketing usw.) spezifiziert werden. Die Erfahrung hat mich gelehrt, dass eine Basisschulung leicht in 1 bis 1,5 Stunden durchgeführt werden kann, eine angemessene Zeitspanne, um jedem

Mitarbeiter seine Verantwortung bewusst zu machen.

7. Fazit

Unwissenheit ist oft eine Quelle der Ablehnung. Der Datenschutz bildet da keine Ausnahme. Unbekannt, wird es oft abgelehnt aus Angst vor den Anstrengungen und Budgets, die wir glauben, dafür aufwenden zu müssen. Einige einfache Maßnahmen zu vertretbaren Kosten reichen jedoch aus, um ein akzeptables Maß an Compliance für die große Mehrheit der KMUs zu erreichen, deren Verarbeitung oft begrenzt ist und deren Risiken leicht zu begrenzen sind.

Source : https://www.wg-avocats.ch/de/nachrichten/datenschutz/neue-bundesdatenschutzgesetz/