Welche Auswirkungen hat die DSGVO auf Schweizer Unternehmen?

Es gibt zahlreiche Schweizer Unternehmen, die ohne besondere Aufmerksamkeit darauf zu verwenden, persönliche Daten von Personen mit Wohnsitz in der EU verarbeiten. Seit dem 25. Mai 2018 ist jedoch die neue Europäische Grundverordnung DSGVO in Kraft getreten, die zum Ziel hat, den Bewohnern der EU zu mehr Sichtbarkeit und einer besseren Kontrolle ihrer personenbezogenen Daten zu verhelfen. Gilt diese Verordnung auch für Ihr Unternehmen? Und wenn ja, welche Massnahmen sind zu treffen?

Worum handelt es sich bei der DSGVO?

Die DSGVO bezweckt den Schutz von natürlichen Personen im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten. Sie gilt für alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.[1] Anders ausgedrückt ist die Anwendung der Verordnung abhängig von der Möglichkeit, die betroffene Person direkt oder indirekt anhand von einzelnen oder mehreren Daten, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen und Vornamen, E-Mail-Adresse, Telefonnummer, Standortdaten, IBAN-Nummer sowie IP-Adresse, zu identifizieren. Hingegen gilt die Verordnung nicht bei anonymen Daten, noch bei Daten, die juristische Personen oder verstorbene natürliche Personen betreffen.

Die Verordnung gilt auch nicht für die Verarbeitung von personenbezogenen Daten, die im Rahmen von Grenzkontrollen, Asyl- und Einwanderungsmassnahmen vorgenommen wird. Sie gilt ebenfalls nicht für Kontrollen, die von den zuständigen Behörden zum Zwecke der Verhütung und Aufdeckung, Ermittlung und Verfolgung von Straftaten oder der Strafvollstreckung, einschliesslich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit durchgeführt werden[2].

Nichtsdestotrotz ist das Konzept der personenbezogenen Daten, das vom europäischen Gesetzgeber angewendet wird, besonders breit gefasst. Der Anwendungsbereich dieser Verordnung umfasst im Übrigen alle Formen, die eine Information unabhängig vom vermittelten Inhalt annehmen kann. Dabei kann es sich um Bild- oder Tondokumente handeln, wie bei Telefongesprächen, die Hinweise auf das Privat- oder Berufsleben sowie bestimmte Aspekte des öffentlichen Lebens der betroffenen Person geben.

Konkret gibt die DSGVO Massnahmen mit gesundem Menschenverstand in Bezug auf personenbezogene Datensicherheit vor, indem die Sammlung der Daten verringert wird, die nicht mehr nützlichen gelöscht werden, der Zugang zu diesen Daten eingeschränkt und diese so lange sie zweckdienlich sind, gesichert werden sollen. Je sensibler die personenbezogenen Daten eingestuft werden, desto grösser der gesetzlich vorgeschriebene Schutz. Unter sensiblen Daten versteht man jedwede personenbezogene Daten, die direkt oder indirekt Informationen in Zusammenhang mit der Gesundheit, der Intimsphäre, der Rasse oder ethnischen

[1] Art. 4 – DSGVO
[2] Art. 2 – DSGVO

Zugehörigkeit, sozialen Massnahmen, Meinungen oder Tätigkeiten im religiösen, philosophischen, politischen oder gewerkschaftlichen Spektrum liefern, ebenso wie strafrechtliche Verfolgung oder verwaltungsrechtliche oder strafrechtliche Sanktionen und biometrische und genetische Daten aufdecken.

Die Verarbeitung der Daten im Sinne der europäischen Verordnung besteht nicht nur in der Sammlung, Nutzung und Löschung von personenbezogenen Daten durch das Unternehmen, sondern betrifft beispielsweise auch die einfache Speicherung von personenbezogenen Daten. Angesichts der schieren Menge an elektronischen Daten, die von Unternehmen täglich verarbeitet werden, versteht man leicht, welche Auswirkung eine solche Verordnung auf ein ihr unterstelltes Unternehmen hätte.

Kann die DSGVO auf Schweizer Unternehmen angewandt werden?

Die wichtigste Frage ist zweifelsohne, ob Ihr Unternehmen von der DSGVO betroffen ist. Nach Untersuchung des sachlichen Anwendungsbereichs mit dem Begriff der personenbezogenen Daten für die die Verordnung gilt, muss man die Anwendung vom territorialen Standpunkt aus betrachten. Die Verordnung gilt in erster Linie für die Bearbeitung von personenbezogenen Daten, die auf dem Gebiet der Europäischen Union vorgenommen wird. Die Auswirkung auf Schweizer Unternehmen mit Zweigstellen in Europa ist offensichtlich, doch sie ist es weit weniger bei Unternehmen, deren Hauptsitz in der Schweiz liegt. Da die Schweiz kein Mitglied der Europäischen Union ist, wird die DSGVO nicht in das schweizerische Recht übernommen. Dennoch enthält die DSGVO ein Kriterium der extraterritorialen Anwendung und kann in den folgenden vier Fällen für ein Unternehmen gelten, dass seinen Sitz in der Schweiz hat[3]:

- Ein Schweizer Unternehmen verkauft online Artikel an Kundschaft in einem EU-Mitgliedstaat, via eine Website, die für die Kundschaft in der Union bestimmt ist. In diesem Zusammenhang muss man klarstellen, ob das Unternehmen Dienstleistungen an betroffene Personen in einem, oder mehreren EU-Mitgliedstaaten anbieten möchte. Bei der Beurteilung dieser Absicht muss man ein Bündel an Indizien miteinbeziehen, beispielsweise die Verwendung einer anderen Sprache oder einer Währung, die in einem oder mehreren EU-Ländern verwendet wird, die Möglichkeit Waren und Dienstleistungen in dieser anderen Sprache zu bestellen, die Erwähnung von Kunden oder Nutzern, die sich in der EU befinden, eine Telefonnummer mit einer internationalen Vorwahl, oder die Nutzung einer Internetdomäne auf oberster Stufe, die nicht zum EU-Land gehört, in dem die Dienste angeboten werden.

- Ein in der europäischen Union ansässiger Nutzer surft auf einer Schweizer Website, die einen Cookie[4] enthält, um das Verhalten des Nutzers zu verfolgen.

---

[3] Art. 3 und Art. 27 DSGVO

[4] Ein Cookie ist eine kleine Textdatei die auf dem Terminal des Internetnutzers gespeichert wird. Sie erlaubt den Entwicklern von Websites, Daten des Nutzers zu speichern, um die Navigation zu vereinfachen und bestimmte Funktionen zu ermöglichen. Cookies waren stets mehr oder weniger umstritten, da sie Reste von persönlichen Informationen enthalten, die von Dritten genutzt werden könnten.

- Ein Schweizer Unternehmen vergibt die Bearbeitung personenbezogener Daten weiter an ein Unternehmen, das sich in einem Land der EU befindet.[5]

- Ein Schweizer Unternehmen bearbeitet die personenbezogenen Daten als Subunternehmer einer Firma in der EU.

Im Hinblick auf das obgenannte muss man feststellen, dass die Verordnung, allgemein betrachtet, natürliche Personen unabhängig von ihrer Staatsangehörigkeit oder ihres Wohnsitzes schützt. Jedes Schweizer Unternehmen muss folglich überprüfen, ob es die neuen Vorgaben der DSGVO beachten muss, oder nicht.

Welche Konsequenzen wird die Umsetzung der DSGVO haben?

Die von der neuen Europäischen Verordnung betroffenen Schweizer Unternehmen werden die folgenden zusätzlichen Pflichten erfüllen müssen[6]:

a) Betroffene Personen informieren und ihre Einwilligung einholen

Bevor jedwede personenbezogene Daten erhoben und genutzt werden, muss den betroffenen Personen mitgeteilt werden, wozu diese Daten genutzt werden und ihre Einwilligung muss eingeholt werden. Diese Personen behalten das Recht, auf ihre Daten zuzugreifen, sie zu berichtigen, ihre Nutzung zu verbieten, oder sie zu löschen. Beim Datenschutzgesetz der EU ist nämlich, im Gegensatz zum Schweizer Recht, die Bearbeitung der Daten allgemein untersagt, so lange sie nicht ausdrücklich durch ein Gesetz erlaubt ist, oder so lange die betroffene Person nicht ihre Einwilligung zur Bearbeitung gegeben hat. Die Einwilligung ist nur dann gültig, wenn die betroffene Person diese freiwillig gegeben hat. Die Person muss wirklich die Wahl haben, das heisst sie darf im Moment der Einwilligung nicht vor vollendete Tatsachen gestellt, oder in ihrer Entscheidungsfreiheit eingeschränkt werden. Die betroffene Person muss im Vorhinein über den Zweck der Erhebung und Bearbeitung ihrer personenbezogenen Daten informiert werden, um nicht allgemein ihre Einwilligung zu geben, sondern für jede einzelne Aktion im Zusammenhang mit ihren personenbezogenen Daten. Die Einwilligung kann sowohl schriftlich, wie auch mündlich erteilt werden, sofern dies ausdrücklich und aktiv geschieht. Die betroffene Person kann aber ihre Einwilligung jederzeit zurückziehen.

b) Sicherstellen von „privacy by design“ und „privacy by default“

„Privacy by design“ (integrierter Datenschutz) bedeutet, dass der Datenverantwortliche das Risiko der Persönlichkeitsverletzung oder des Verstosses gegen die Grundrechte der betroffenen Person verringern muss und solche Verstösse schon in der Planungsphase der Datenbearbeitung verhindern muss. Ein Beispiel für die Grundrechte ist das Recht jeder Person auf ihre Daten zuzugreifen, sie zu berichtigen, zu erneuern, oder zu löschen. Jedes Unternehmen muss folglich sicherstellen, dass die Daten einfach zugänglich gespeichert werden, damit beispielsweise Zugangsanfragen schnell entsprochen werden kann. Es muss zudem alle notwendigen Massnahmen ergreifen, um die Sicherheit der Daten, die der

[5] Die Schweizer Tochtergesellschaft einer Unternehmensgruppe speichert zum Beispiel alle Daten ihrer Mitarbeiter in einer zentralen Datei, die bei der Muttergesellschaft der Gruppe in der EU untergebracht ist.
[6] Art. 5 DSGVO

Datenverantwortliche gesammelt hat zu gewährleisten, ebenso wie deren Vertraulichkeit, d.h. er muss sicherstellen, dass nur die autorisierten Personen Zugang haben. Sobald der Zweck, zu dem die Daten gesammelt wurden, erreicht ist, besteht kein Grund mehr die Daten zu bewahren und sie müssen gelösch werden.

„Privacy by default“ (datenschutzfreundliche Voreinstellungen) ist ein Prinzip, das vom Verantwortlichen fordert, die Bedeutung der Daten zu überprüfen und nur die zur Verwirklichung der Ziele absolut notwendigen Daten zu sammeln. Der Datenverantwortliche darf somit nicht mehr Daten sammeln, als er wirklich benötigt. Darüber hinaus muss er auf besonders empfindliche Daten achten und sicherstellen, dass sie richtig und aktuell sind.

c) Ernennung eines Repräsentanten in der EU

Diese Verpflichtung entfällt, sobald die Verarbeitung nur gelegentlich geschieht, keine empfindlichen Daten betrifft und kein wirkliches Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt.

d) Führung eines Verzeichnisses der Verarbeitungen

Der Verantwortliche muss ein Verzeichnis der Verarbeitungen führen. Dieses Verzeichnis muss die wichtigsten Informationen über die Datenverarbeitung enthalten, insbesondere die Kategorien der Daten, die betroffenen Personenkreise, die Ziele der Verarbeitung sowie mögliche Adressaten der Daten.

e) Meldung von Fällen der Datenschutzverletzung an die Kontrollbehörde

Bei Datenverlust muss umgehend der Datenschutzbeauftragte des Unternehmens informiert werden. Das Unternehmen hat 72 Stunden Zeit, um zu reagieren und um eine Verletzung, die ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellen könnte, der zuständigen Kontrollbehörde mitzuteilen.

Es gilt zu beachten, dass die Verantwortung für die Daten auch bei Weitervergabe nach wie vor beim Unternehmen liegt. Es muss sicherstellen, dass der Subunternehmer die gleichen Regeln in Bezug auf den Datenschutz beachtet.

Welche Konsequenzen wird die Umsetzung der DSGVO haben?

Die DSGVO überlässt es den Kontrollbehörden Verwaltungsbussen zu verhängen, sobald eine bestimmte Anzahl an Voraussetzungen erfüllt wurde. Im Falle der Datenschutzverletzung von persönlichen Daten riskiert das Unternehmen eine Verwaltungsbusse von maximal 20 Millionen Euro, oder bei Unternehmen von maximal 4 % des globalen Jahresumsatzes des Vorjahresergebnisses, wobei der höhere Betrag von beiden berücksichtigt wird. Für die Berechnung der Busse ist folglich der Umsatz der Gruppe ausschlaggebend und nicht nur der Umsatz der von der Verletzung betroffenen Einheit. Das Unternehmen riskiert ebenfalls organisationelle Strafen, wie einen vorläufigen oder endgültigen Entzug der Genehmigung zur Datenverarbeitung. Bei schwerwiegenden Verstössen kann ein EU-Land eine komplette Einstellung sämtlicher Tätigkeiten der Datenverarbeitung aussprechen. Die Verordnung bietet eine ganze Pallette an

Abschreckungsmassnahmen, wie die Verwarnung, die Mahnung, die zeitliche oder endgültige Einschränkung der Verarbeitung sowie die Abmahnungen, bevor zum letzten Mittel der Busse gegriffen wird.

Schlusswort

Der Schweizer Unternehmer, der die neuen Vorschriften einhalten muss, sollte zunächst untersuchen, wie das Unternehmen die Daten verarbeitet und abklären, welche Daten in welchem Bereich verarbeitet werden. Anschliessend, und um den Vorgang zu optimieren und eventuelle Mängel des Unternehmens zu beheben, sollten die abgeklärten Daten näher untersucht werden. Folgende Fragen sollten gestellt werden: Woher kommen die Daten? Wer verarbeitet sie? Mit welchen Datenträgern werden sie bearbeitet? Weshalb werden sie bearbeitet? Wie werden sie bearbeitet? Wann werden sie gelöscht? Wo werden sie aufbewahrt? Musste man die betroffene Person im Hinblick auf deren Verarbeitung um Erlaubnis fragen? Dann sollte man festlegen, welche Kategorien von persönlichen Daten besonders schützenswert sind, darunter solche, die auf die rassische oder ethnische Abstammung, die politischen oder religiösen Meinungen, philosophischen Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hinweisen, oder die medizinische Daten oder Informationen über die sexuelle Orientierung der betroffenen Person preisgeben. Da es sich bei der Verordnung um eine europäische Rechtsvorschrift handelt, sollte man sich bei Fragen an die europäischen Datenschutzbehörden wie die CNIL, die belgische CPVP oder die luxemburgische CNDP wenden.