Datenschutz

Booklet

STADLER VÖLKEL
RECHTSANWÄLTE · ATTORNEYS AT LAW

Hi there, welcome to #svlove

Intro

„Big Brother is watching you" ist wohl eines der bekanntesten Zitate von George Orwell und seit langem keine Fiktion mehr. Zugegeben, von der dystopischen Welt, welche uns sein zeitloser Klassiker „1984" präsentierte, sind wir auch im 21. Jahrhundert noch weit entfernt. Dennoch erfassen staatliche und vermehrt auch private Akteure mit stetig fortentwickelten Methoden und Technologien Unmengen an Daten für die eigenen Interessen. Daher ist es wenig verwunderlich, dass der Datenschutz eine immer wesentlichere Rolle in unserer Gesellschaft einnimmt.

Nicht zuletzt wird die zugrundeliegende Bedeutsamkeit durch rechtliche Schutzvorkehrungen herausgestrichen, denen praktische Erkenntnisse vorausgehen. Dabei bringt der technologische Fortschritt unentwegt neue Herausforderungen und auch Bestrebungen mit sich, technologieneutrale Ansätze zu definieren – eine zunehmend abstrakte Sprache und daraus resultierender Interpretationsspielraum bilden die für den Einzelnen unschönen Konsequenzen. Als Thema und Rechtsgebiet unserer Epoche wird der Datenschutz jedenfalls auch in den nächsten Jahrzehnten nicht an Relevanz verlieren.

Dieses Booklet soll die zentralen Aspekte des Datenschutzrechts auf verständliche Weise vermitteln. Für eine Behandlung von Detailfragen oder eine rechtliche Beratung in Zusammenhang mit konkreten Projekten stehen die Datenschutzexperten von STADLER VÖLKEL Rechtsanwälte jederzeit zur Verfügung.

Datenschutz(-Recht)

Ein allgemeines Verständnis des Begriffs „Datenschutz" lässt sich rasch gewinnen: In einem weiten Sinn kann darunter alles aufgefasst werden, was sich – aus welchem Grund auch immer – mit dem Schutz von Informationen durch bestimmte Vorkehrungen beschäftigt. Im Detail wird die Begrifflichkeit allerdings weder einheitlich definiert noch verstanden.

Eine besondere Schutzbedürftigkeit ist traditionell vor allem dort gegeben, wo Informationen in den falschen Händen das Potential aufweisen, die Rechte und Freiheiten von Individuen zu beeinträchtigen. Gefahr kann von staatlichen Stellen (Stichwort: Überwachungsstaat) oder privaten Akteuren (Stichwort: Big Data und Datenhandel) ausgehen. Längst sind Daten zu Wertträgern geworden, deren missbräuchlicher Verwendung oder Weitergabe mit rechtlichen Spielregeln (dem Datenschutzrecht) entgegengetreten werden muss, um die gerade in westlichen Demokratien extrem kritisch betrachtete Ausformung des sog. „gläsernen Menschen" hintanzuhalten.

Auf der anderen Seite führt ein Mehr an Datenschutz zu einer erschwerten Verfolgung anderweitiger legitimer Anliegen, wie z.B. dem Recht auf freie Meinungsäußerung, der Kriminalitätsbekämpfung oder wissenschaftlicher Forschungsarbeit. Der sohin erforderliche Ausgleich widerstreitender Interessen wird global durch verschiedenartige Wertungen und Gewichtungen erschwert. In den USA etwa gibt es bundesweit nur sehr wenige Datenschutzvorgaben, die sich vorrangig auf spezifische Sektoren beziehen, ohne allgemeine Vorschriften zu schaffen.

Im Fokus des Datenschutzes steht seit Anbeginn jedenfalls die Verhinderung von Missbrauch und ungewollten Abflüssen von als schutzwürdig anerkannten Datensätzen, was sowohl durch technische wie auch organisatorische Maßnahmen sichergestellt werden soll – dies naturgemäß unter Berücksichtigung der zunehmenden Digitalisierung (Stichwort: Datensicherheit).

Was sind personenbezogene Daten

und warum wird diese Unterscheidung getroffen?

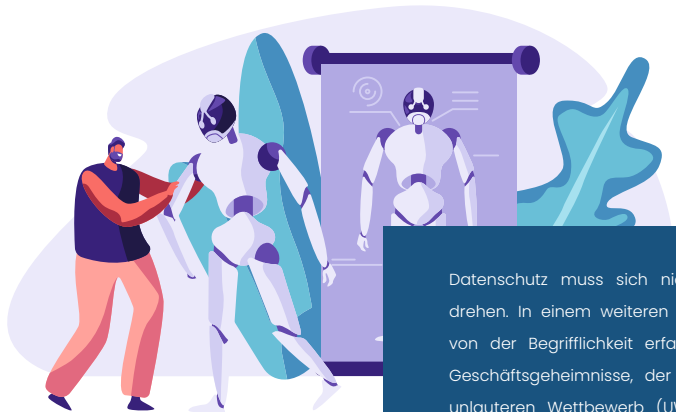
Einen umfassenden und weitreichenden Schutz genießen grundsätzlich nur jene Daten, die „personenbezogen" sind. Nach europäischem Verständnis sind damit Informationen gemeint, welche sich eignen, eine sog. natürliche Person (d.h. einen Menschen) zu identifizieren oder identifizierbar zu machen – selbst wenn diese Möglichkeit nur gemeinsam mit zusätzlichen Informationen besteht. So bildet der Name einer solchen Person ein personenbezogenes Datum, der Name eines Druckers aber bspw. nicht.

Das erhöhte Schutzbedürfnis personenbezogener Daten liegt vor allem in ihrer Nähe zu den Rechten, Freiheiten und der Privatsphäre der Menschen begründet. Ursprünglich wurde ein Anspruch von Individuen auf den Schutz ihrer durch die undifferenzierte Verarbeitung von personenbezogenen Daten beeinträchtigten Privatsphäre schon aus allgemeinen Persönlichkeitsrechten abgeleitet. Auch soll ihnen im Sinne der sog. „informationellen Selbstbestimmung" Entscheidungsfreiheit in Zusammenhang mit ihnen zugehörigen Informationen zukommen.

Diese Einordnungen haben etwa in der EU und ihren Mitgliedsstaaten zur umfassenden Regulierung des personenbezogenen Datenschutzes geführt, welcher den Großteil aller datenschutzrechtlichen Vorschriften ausmacht und von entsprechenden Grundrechten des Einzelnen – in Österreich insbesondere dem Grundrecht auf Datenschutz gemäß § 1 Datenschutzgesetz (DSG) – flankiert wird.

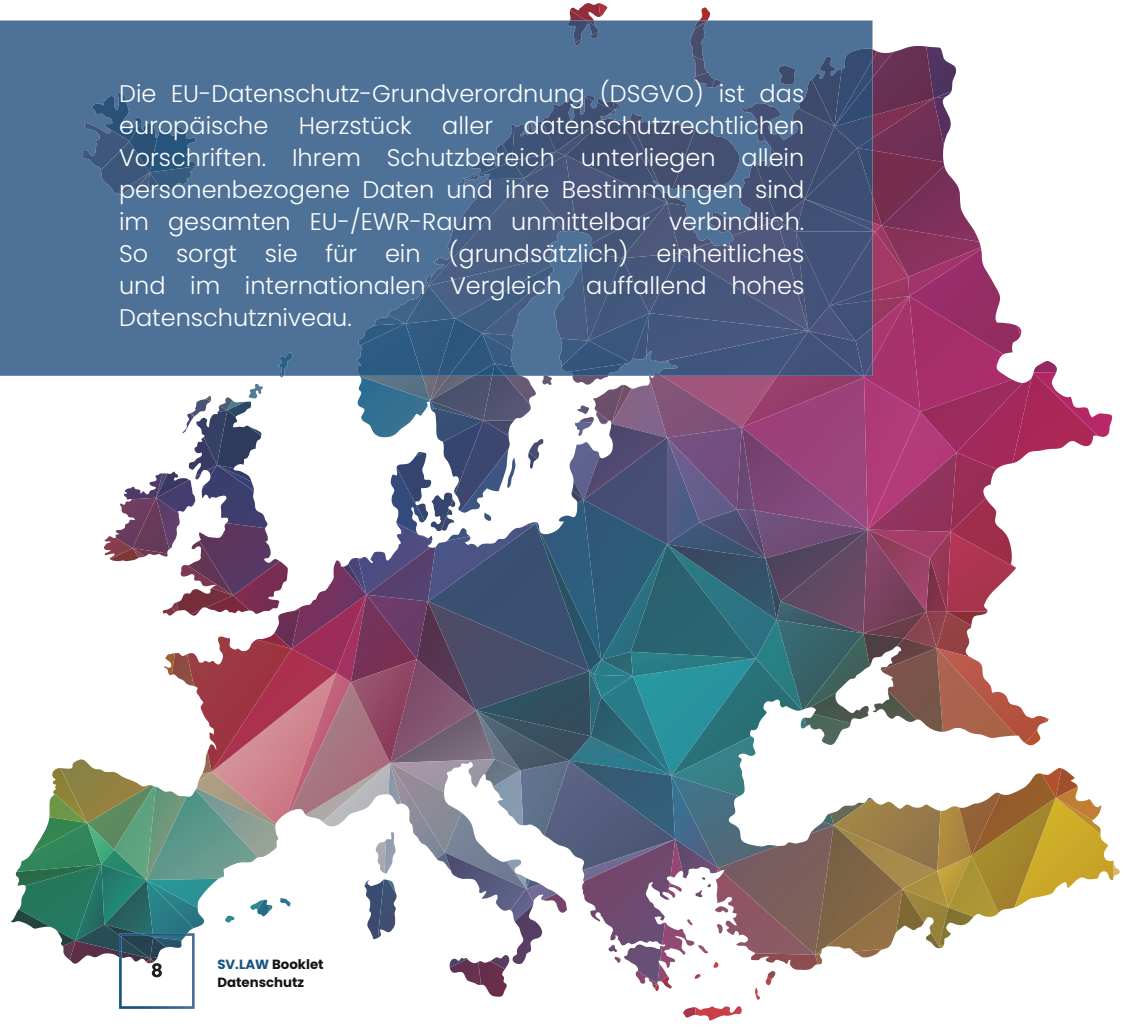
Was ist mit dem Schutz von Daten

ohne Personenbezug?



Datenschutz muss sich nicht immer um den Schutz von Individuen drehen. In einem weiteren Sinn können auch gänzlich andere Bereiche von der Begrifflichkeit erfasst sein. So etwa der Schutz (technischer) Geschäftsgeheimnisse, der in Österreich im Bundesgesetz gegen den unlauteren Wettbewerb (UWG) oder in (besonders schwerwiegenden) Teilaspekten sogar im Strafgesetzbuch (StGB) angesiedelt ist. Spezielle Anforderungsprofile formen sich ebenfalls im Hinblick auf neue Technologien und den Vormarsch künstlicher Intelligenz. Im Umfang dieses Booklets wird auf diese Art von Datenschutz jedoch nicht näher eingegangen, um eine gründlichere Betrachtung des weitaus präsenteren personenbezogenen Datenschutzes zu ermöglichen.

Die EU-Datenschutz-Grundverordnung (DSGVO) ist das europäische Herzstück aller datenschutzrechtlichen Vorschriften. Ihrem Schutzbereich unterliegen allein personenbezogene Daten und ihre Bestimmungen sind im gesamten EU-/EWR-Raum unmittelbar verbindlich. So sorgt sie für ein (grundsätzlich) einheitliches und im internationalen Vergleich auffallend hohes Datenschutzniveau.



Was ist die DSGVO und wann kommt sie zur Anwendung?

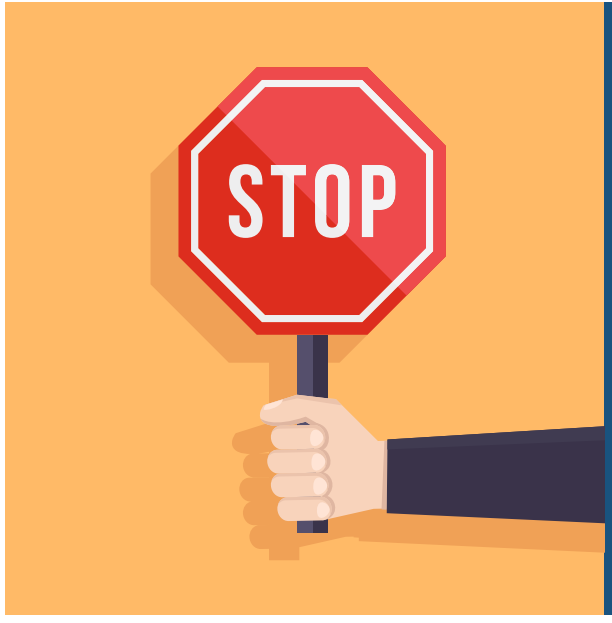
„70 % der Welt sind von Wasser bedeckt, der Rest von N'Golo Kanté." Dieser Spruch ist aufgrund der allumfassenden Präsenz des Chelsea-Stars auf dem Fußballplatz weit verbreitet. Ähnliches könnte man wohl auch über die DSGVO sagen, deren Anwendbarkeit gleichfalls einen enormen Bereich abdeckt.

Im Wesentlichen muss die DSGVO bei jedem (!) Vorgang im Zusammenhang mit personenbezogenen Daten berücksichtigt werden (also bspw. bereits beim Speichern einer Telefonnummer oder beim Fotografieren einer Person), soweit dieser Vorgang von Individuen oder Entitäten durchgeführt wird, die (i) ihren (Wohn-)Sitz bzw. eine Niederlassung im EU-/EWR-Raum haben oder (ii) ohne derartige Ansässigkeit unter gewissen Voraussetzungen Daten von Personen verarbeiten, welche sich im EU-/EWR-Raum befinden. Aber bevor jetzt alle nur noch unter Beiziehung eines Rechtsbeistandes den Auslöser ihrer Kamera betätigen, können wir beruhigen: Der Anwendungsbereich der DSGVO kennt auch (in sachlicher Hinsicht) einige Ausnahmen. So müssen etwa Hobbyfotografen die DSGVO bei Schnappschüssen auf privaten Feiern nicht beachten, da diese Aufnahmen ausschließlich zu persönlichen oder familiären Zwecken angefertigt werden. Hier spricht man von der sog. „Haushaltsausnahme".

Verarbeitung von Daten nach den Regeln der DSGVO

Der sehr weit gefasste Anwendungsbereich der DSGVO stellt Rechtsunterworfenen vor einige Hürden. Im Zeitalter des Internets fließen Daten nämlich im Bruchteil von Sekunden – oftmals ungefragt und unbemerkt – ans andere Ende der Welt. Die Einfachheit Daten zu verarbeiten steht dabei in einem starken Kontrast zu den restriktiven Regeln der DSGVO, welche beinahe immer beachtet werden muss.

Deshalb ist Vorsicht geboten! Die DSGVO folgt nämlich dem sog. „Verbotsprinzip mit Erlaubnisvorbehalt", welches besagt, dass jede Verarbeitung personenbezogener Daten untersagt ist – es sei denn, es liegt einer der abschließend geregelten Ausnahmefälle vor.



Wann können Daten also verarbeitet werden?

Zunächst findet sich in Artikel 6 Absatz 1 DSGVO eine Reihe sog. Rechtmäßigkeitsgrundlagen, welche eine eigentlich unzulässige Datenverarbeitung rechtfertigen können. Wichtig ist, dass hier Nägel mit Köpfen gemacht werden: Jede zulässige Verarbeitung erfordert zwingend das Vorliegen einer solchen Grundlage, bspw. die Einwilligung jener natürlichen Person, deren Daten verarbeitet werden („betroffene Person").

Zusätzliche Anforderungen bestehen darüber hinaus im Hinblick auf besondere Kategorien personenbezogener Daten (z.B. Informationen zum Gesundheitszustand) oder im Falle der Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten, da ihre sensible Natur bei einer Verarbeitung zu einem höheren Risiko für die betroffene Person führt.

In jedem Fall sind die Grundsätze für die Verarbeitung personenbezogener Daten des Artikel 5 DSGVO einzuhalten. Diese Verarbeitungsgrundsätze sind das historisch gewachsene Grundgerüst jedweder datenschutzrechtlicher Überlegungen und trotz ihrer abstrakten Formulierung unmittelbar verbindlich und durchsetzbar!

Informationspflichten

Eine Verordnung mit fast 100 Seiten wie die DSGVO ist mit dem Vorliegen einer passenden Rechtmäßigkeitsgrundlage natürlich noch lange nicht eingehalten. Vielmehr bestehen zahlreiche weitere Pflichten, deren Erfüllung die Voraussetzung für ein vollständig datenschutzkonformes Verhalten bildet.

Allen voran setzt die DSGVO fest, dass betroffenen Personen umfassende Informationen über die (geplante) Verarbeitung ihrer Daten zu erteilen sind. Besonders bekannt sind in diesem Zusammenhang die Informationserteilungen auf Websites, die zumeist als „Datenschutzerklärungen" bezeichnet werden.

Welche Informationen müssen bereitgestellt werden?

Hier hilft ein Blick auf die in Artikel 13 DSGVO (Datenerhebung bei der betroffenen Person selbst) und Artikel 14 DSGVO (Datenerhebung aus dritter Quelle) enthaltenen Aufzählungen weiter. Um nur ein paar Beispiele zu nennen: Name und Kontaktdaten des datenverarbeitenden „Verantwortlichen", Zweck und Rechtmäßigkeitsgrundlage sowie die Speicherdauer der verarbeiteten Daten bzw. die Kriterien, nach denen diese festgelegt wird.

Auch auf die Art der Informationserteilung ist Bedacht zu nehmen: Die DSGVO fordert eine präzise, transparente, verständliche und leicht zugängliche Form sowie eine klare und einfache Sprache.

Privacy by Design und Privacy by Default

Was haben fähige Fußballtrainer, historische Feldherren und fleißige Studenten gemeinsam? Sie alle wissen, dass die Wiege des späteren Erfolges eine anständige Vorbereitung ist! Auch die Köpfe hinter der DSGVO haben dies erkannt. Die Verordnung beschränkt sich daher nicht auf die eigentliche Verarbeitungstätigkeit, sondern setzt bedeutend früher an.

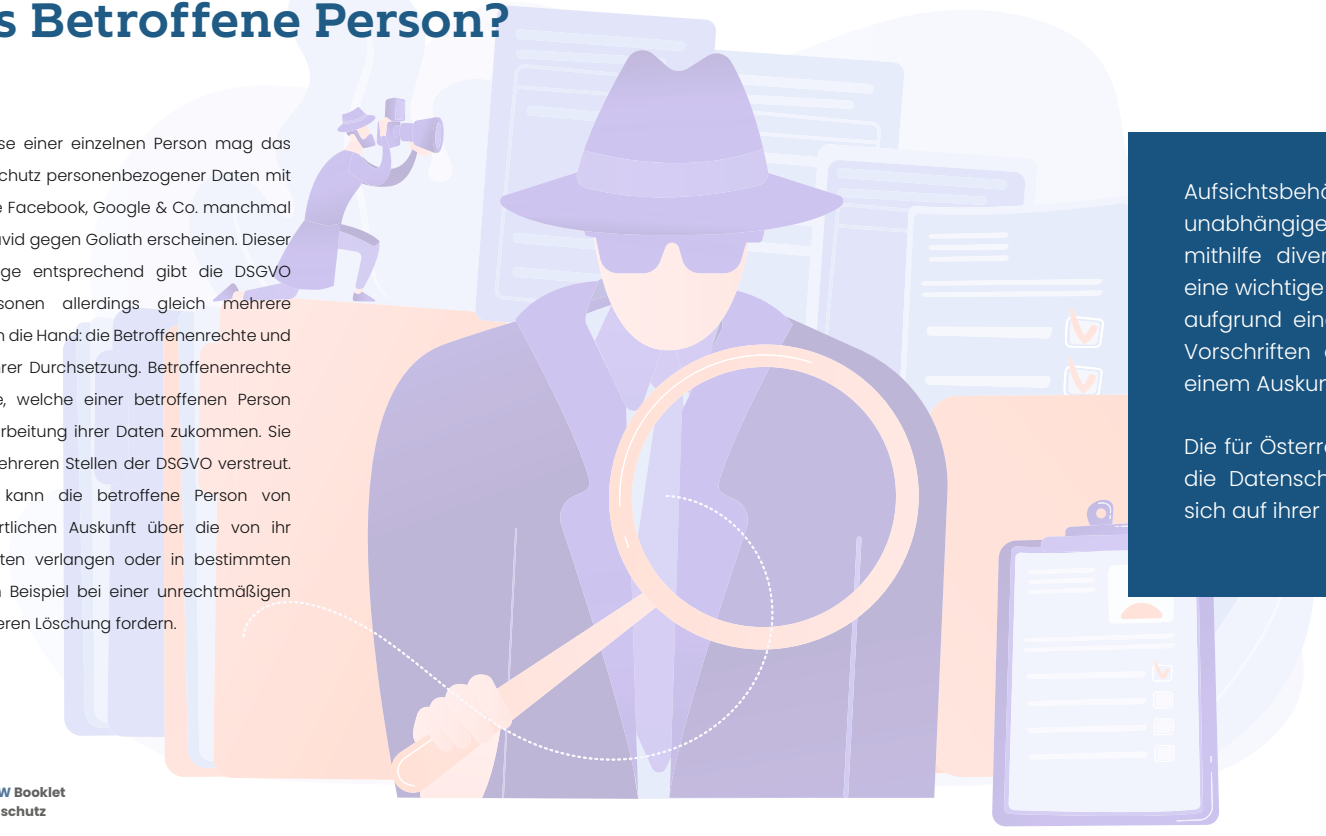
Zusammengefasst unter den Schlagworten „Privacy by Design" (Datenschutz durch Technikgestaltung) und „Privacy by Default" (Datenschutz durch datenschutzfreundliche Voreinstellungen) statuiert die DSGVO zwei Konzepte, welche Verantwortliche zu einer möglichst datenschutzfreundlichen Ausgestaltung ihrer Verarbeitungsumgebung animieren sollen.

Privacy by Design beschreibt die datenschutzfreundliche Ausgestaltung der internen Prozesse und Systeme. Dadurch sollen bereits im Konzeptionsstadium und während der Produktentwicklung – also von Beginn an (!) – Datenschutzüberlegungen einfließen.

Privacy by Default verlangt indes, dass durch Voreinstellungen nur die für den speziellen Zweck unbedingt erforderlichen Daten verarbeitet werden sollen. Sind auf einer Social-Media-Plattform etwa standardmäßig nicht die datenschutzfreundlichsten Voreinstellungen ausgewählt, wurde das Konzept nicht im Sinne der DSGVO realisiert.

Welche Rechte habe ich ich als Betroffene Person?

Aus der Sichtweise einer einzelnen Person mag das Ringen um den Schutz personenbezogener Daten mit Konzernriesen wie Facebook, Google & Co. manchmal wie der Kampf David gegen Goliath erscheinen. Dieser biblischen Passage entsprechend gibt die DSGVO betroffenen Personen allerdings gleich mehrere Steinschleudern in die Hand: die Betroffenenrechte und die Möglichkeit ihrer Durchsetzung. Betroffenenrechte sind jene Rechte, welche einer betroffenen Person im Falle der Verarbeitung ihrer Daten zukommen. Sie finden sich an mehreren Stellen der DSGVO verstreut. Unter anderem kann die betroffene Person von einem Verantwortlichen Auskunft über die von ihr verarbeiteten Daten verlangen oder in bestimmten Fällen – wie zum Beispiel bei einer unrechtmäßigen Verarbeitung – deren Löschung fordern.



Aufsichtsbehörden

Aufsichtsbehörden sind von den Mitgliedsstaaten errichtete, unabhängige Behörden, welche die Anwendung der DSGVO mithilfe diverser Befugnisse überwachen. Außerdem sind sie eine wichtige Anlaufstelle für betroffene Personen. Bei ihnen kann aufgrund einer behaupteten Verletzung datenschutzrechtlicher Vorschriften eine Beschwerde eingebracht werden (z.B. wenn einem Auskunftsbegehren nicht entsprochen wird).

Die für Österreich ausschließlich zuständige Aufsichtsbehörde ist die Datenschutzbehörde. Weiterführende Informationen finden sich auf ihrer Website unter www.dsb.gv.at.

www.dsb.gv.at

Meldung von Datenschutzverletzungen

Ozzy Osbourne sagte einst: „Von allem, was ich verloren habe, vermisse ich meinen Verstand am meisten!". Auch personenbezogene Daten haben es an sich, teilweise verloren zu gehen – sei es ungewollt, bspw. durch Sicherheitslücken in datenverarbeitenden Systemen, oder im Zuge der Nachlässigkeit eines Verantwortlichen bewusst in Kauf genommen. Zwar sind Daten zum Glück nicht gleich der Verstand – aber auch sie werden von den Betroffenen oft schmerzhaft vermisst. Dabei könnte deren Verlust gerade mit vorausschauendem Scharfsinn allzu oft verhindert werden. Was muss ich tun, wenn mir Daten abhandenkommen? Sollte es zu einer Verletzung des Schutzes personenbezogener Daten kommen (sog. „Data Breach"), ist schnelles und entschlossenes Handeln gefragt!

Zunächst muss in den allermeisten Fällen innerhalb von 72 Stunden ab Kenntnis der Verletzung eine Meldung an die zuständige Aufsichtsbehörde vorgenommen werden. In ihr müssen bestimmte Mindestangaben über den Vorfall enthalten sein; so etwa die Art der Verletzung, ihre wahrscheinlichen Folgen und die zu ihrer Beseitigung angedachten Maßnahmen.

Die betroffenen Personen sind von der Verletzung hingegen grundsätzlich nur dann zu unterrichten, wenn daraus ein hohes Risiko für ihre Rechte und Freiheiten resultiert.

Zuckerbrot und Peitsche:

Sanktionen und Rechtsdurchsetzung

Obgleich die DSGVO die Konformität mit datenschutzrechtlichen Bestimmungen fröhlich der Selbstverantwortung der Rechtsunterworfenen überlässt, straft sie aufgedeckte Verfehlungen umso hemmungsloser ab. Selbst amerikanische Großkonzerne, die geübt darin sind, sich aus der Affäre zu ziehen, durften die scharfen Zähne ihres Sanktionsregimes bereits kennenlernen.

Das betraf vor allem die „üblichen Verdächtigen" wie Facebook, Amazon, Google & Co., bei welchen datenschutzrechtliche Überlegungen lange Zeit keinen allzu hohen Stellenwert eingenommen haben – aber auch kleine und mittelgroße Unternehmen bekamen den Zorn der Aufsichtsbehörden schon zu spüren.

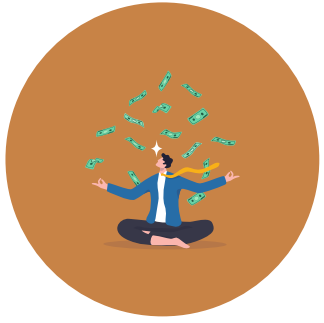
Der Rahmen der verhängten Sanktionen reichte dabei von bloßen Verwarnungen bis zu Strafen im Bereich mehrerer hundert Millionen Euro!

Trotz der für den einfachen Mann astronomischen Summen bleibt allerdings dennoch zu bedenken: Auch die höchsten der bisherigen Bußgelder fallen speziell für die abgestraften Großkonzerne aufgrund ihrer enormen wirtschaftlichen Kapazitäten nicht wirklich ins Gewicht. Es ist damit fraglich, ob sie ein effektives Mittel darstellen, die angestrebten Ziele (Konformität mit datenschutzrechtlichen Vorschriften) gerade gegenüber den bedeutsamsten „Datenkraken" durchzusetzen.

Wie kommt es zu derartigen Summen?

Die Höhe der Bußgelder wird von Aufsichtsbehörden – mit einem weiten Ermessenspielraum – festgelegt (bis zu EUR 20 Millionen oder 4 % des weltweiten Jahresumsatzes). Außerdem stehen diesen Behörden zusätzliche Werkzeuge zur Reaktion auf Verstöße gegen das Datenschutzrecht, wie etwa die Untersagung von weiteren Verarbeitungen zur Verfügung. Probleme für Verantwortliche können sich dabei schon dadurch ergeben, dass sie ihr gegebenenfalls datenschutzkonformes Verhalten nicht nachzuweisen vermögen und damit die allgemeine Rechenschaftspflicht der DSGVO verletzen.

Aber auch betroffene Personen müssen bei einer Verletzung datenschutzrechtlicher Vorschriften nicht tatenlos zusehen: Zum einen können sie auf ihr Beschwerderecht bei einer Aufsichtsbehörde zurückgreifen, sollten datenschutzrechtliche Pflichten nicht eingehalten werden, oder sie machen eine Verletzung ihrer subjektiven Rechte als betroffene Personen vor den ordentlichen Gerichten geltend. Auch können sie unter gewissen Voraussetzungen Schadenersatz verlangen.



Ein Blick in die Praxis:

Website und Cookies

In der Praxis erweist sich oftmals das Betreiben einer rechtlich konformen Website als besonders herausfordernd, da hier die datenschutzrechtlichen Problemstellen auf den ersten Blick nicht sofort ersichtlich sind. Was manche vielleicht nicht wissen: Schon beim Zugriff auf eine Website kommt es zur automatisierten Verarbeitung personenbezogener Daten (insbesondere der IP-Adresse). Ebenfalls können häufig eingesetzte Cookies oder vergleichbare Speichertechnologien Daten erfassen.

Was muss beim Einsatz von Cookies beachtet werden?

Zur Erklärung: Cookies sind kleine Datensätze, die beim Zugriff auf eine Website auf dem Endgerät des Nutzers gespeichert werden. Sie haben eine große Spannweite an Einsatzmöglichkeiten. So können sie etwa die Website um besondere Funktionen erweitern oder aber auch Daten über ihre Nutzer sammeln, die zu Profilen verknüpft und im Weiteren für interessenbezogene Werbeschaltungen verwendet werden.

Damit befindet sich der Betreiber der Website nicht nur im Anwendungsbereich der DSGVO, sondern hat auch das für den Bereich der elektronischen Kommunikation bestehende Sonderdatenschutzrecht zu berücksichtigen. Für Cookies & Co. bedeutet dies, dass ihr Einsatz einwilligungspflichtig ist, soweit sie nicht zur Aufrechterhaltung der Funktionalität der Website unbedingt erforderlich sind – und zwar völlig unabhängig davon, ob erfasste Informationen personenbezogen sind oder nicht.

...und was beim sonstigen Betrieb einer Website?

Für jeden auf der Website auslösbaren Verarbeitungsvorgang müssen passende Rechtmäßigkeitsgrundlagen identifiziert und gemeinsam mit den übrigen verpflichtend bereitzustellenden Informationen im Wege einer Datenschutzerklärung an die betroffenen Personen (Websitenutzer) herangetragen werden.

Des Weiteren bereiten zumeist Drittanbieter-Dienste wie „Google Analytics" Probleme. Für Websitebetreiber sind Funktionsweise und Datenflüsse oft nicht im Detail nachzuvollziehen, weswegen sie ihren eigenen Informationspflichten oftmals nur unzureichend nachkommen können.

Hinzu kommt, dass der Großteil dieser Dienste von Anbietern außerhalb des EU-/EWR-Raums stammt. Die DSGVO begegnet dem zusätzlichen Risiko einer Datenübertragung in solche „Drittländer" (z.B. die USA) mit zusätzlichen Anforderungen an die Verantwortlichen, welche in einigen Fällen – mangels ausreichenden Datenschutzniveaus des Ziellandes – nur sehr schwer zu erfüllen sind.

Dein SV.LAW-Team

für den Bereich Datenschutz


Arthur Stadler


Tamino Chochola


Jacqueline Bichler


Andreas Pfeil


Felix Bauer


Lukas Pachschwöll


Veronika Krickl


Lukas Ragl


Seda Scheripova

Unsere Checkliste zur DSGVO-Compliance für Verantwortliche:

1. **Wo finden sich datenschutzrechtlich relevante Anknüpfungspunkte (Problembewusstsein)?**
2. **Sind meine technischen Systeme standardmäßig datenschutzfreundlich eingerichtet?**
3. **Bin ich mir bewusst, welche Daten in welcher Form und zu welchen Zwecken von mir verarbeitet werden?**
4. **Habe ich geeignete Rechtmäßigkeitsgrundlagen für meine Datenverarbeitungen identifiziert und Kriterien für die Speicherdauer der verschiedenen Datensätze festgelegt?**
5. **Weiß ich, woher die verarbeiteten Daten stammen und an wen sie übermittelt werden?**
6. **Habe ich die notwendigen technischen und organisatorischen Maßnahmen für ein angemessenes Schutzniveau getroffen?**
7. **Sind in die Verarbeitung nur unbedingt notwendige Personen involviert und unterliegen diese entsprechenden Geheimhaltungsmaßnahmen?**
8. **Wurden angemessene Prozesse für die zeitnahe Wahrnehmung von Betroffenenrechten sowie die Meldung von Datenschutzverletzungen eingerichtet?**
9. **Gibt es datenschutzfreundlichere Alternativen für Dienste von Drittanbietern?**
10. **Habe ich für den Fall eines Drittlandtransfers alle zusätzlichen Anforderungen berücksichtigt?**
11. **Erfordert der Umfang meiner Verarbeitungsaktivitäten die Ausarbeitung einer innerbetrieblichen Datenschutz-Policy?**
12. **Müssen im speziellen Fall besondere von der DSGVO vorgesehene Vorkehrungen berücksichtigt werden (Bestellung eines Datenschutzbeauftragten etc.)?**
13. **Wurden alle als notwendig festgestellten Maßnahmen auch faktisch implementiert?**

STADLER VÖLKEL
RECHTSANWÄLTE - ATTORNEYS AT LAW

IMPRESSUM
STADLER VÖLKEL Rechtsanwälte GmbH
Seilerstätte 24, 1010 Wien

Tel.: +43 1 997 1025
Fax: +43 1 997 1025 99

office@sv.law
www.sv.law

Bildnachweise
Adobe Stock
Iconfinder
FontAwesome

Druckhersteller
online Druck GmbH
Brown-Boveri-Straße 8
2351 Wr. Neudorf