FIRST STEPS

1. DSGVO nicht unterschätzen!

Die DSGVO ist keine Revolution, sondern eine Evolution gegenüber den bestehenden Datenschutzregelungen im DSG 2000. Wer bisher gesetzeskonform war, ist das meist auch in der Zukunft. Jedoch ergeben sich teilweise neue oder andere administrative Pflichten, die mitunter auch einen größeren Aufwand bedeuten können. Neu sind vor allem aber die sehr hohen Strafen bei Verstößen (bis zu € 20 Mio. pro Verstoß oder 4 % des weltweiten Umsatzes). Auch die Möglichkeit von Schadenersatzklagen kann bei einer großen Zahl von Betroffenen beträchtliche Dimensionen annehmen.

2. Überblick über eigene Datenverwendung verschaffen

IT-Infrastruktur und Software sind oft über Jahrzehnte gewachsen. Um sich auf die DSGVO vorzubereiten ist daher zuerst ein Überblick über die Nutzung von „personenbezogenen Daten" (also Daten, die sich auf eine bestimmbare Person beziehen, siehe Artikel 4 Z 1 DSGVO) zu schaffen.

- Wo verarbeiten wir „personenbezogene Daten" (z. B. von Mitarbeitern und Kunden)?
- Haben wir, neben normalen Datenbanken, z. B. auch Kunden- oder Mitarbeiterdaten an unerwarteten Stellen (z. B. Metadaten in Dateien, Fotos von Personen etc.)?
- Wo liegen unsere Daten? Welche externen Dienstleister (z. B. Cloud-Dienste) nutzen wir?
- Verarbeitet man auch Daten als Auftragsdatenverarbeiter für jemand anderen (z. B. Betreuung einer Newsletter-Datenbank mit den Kundendaten eines Partners)?
- Für welchen Zweck bzw. welche Zwecke werden die Daten verwendet?
- Was sind unsere Datenquellen (z. B. direkter Kontakt, Datenhändler)?
- Geben wir Daten an Dritte als Empfänger weiter (z. B. Verkauf von Kundendaten, Hochladen von Kundendaten auf Plattformen, die diese Daten dann selbst weiterverwenden)?
- Übertragen wir Daten an Dienstleister oder Partner außerhalb der EU / des EWR (z. B. sehr häufig: amerikanische Cloud-Dienste)?
- Welche technischen und organisatorischen Maßnahmen haben wir für die Datensicherheit getroffen (z. B. Firewalls, Verschlüsselung, Back-ups, Zugangssysteme, Dienstanweisungen)?

Tipp: Nach Artikel 30 der DSGVO müssen gewisse Unternehmen (Ausnahmen siehe Artikel 32 Abs. 5) ein „Verarbeitungsverzeichnis" führen. Der Aufbau dieses Verzeichnisses kann hier gleich mit erledigt werden.

3. Überblick über DSGVO verschaffen

Nicht jedes Unternehmen ist von der DSGVO in gleichem Maß betroffen. Je nach Branche und Art der Nutzung von personenbezogenen Daten und Diensten kann die DSGVO

umfangreiche Änderungen oder auch nur kleine Anpassungen in der täglichen Praxis bedeuten.
Grundsätzlich gilt: Wenn man sich an das bisher gültige DSG 2000 gehalten hat oder personenbezogene Daten nur in absolut notwendigem Maß verwendet (z. B. zur Vertragserfüllung oder wegen gesetzlicher Speicherpflichten) bzw. der Betroffene zugestimmt hat, wird die DSGVO im Normalfall keine großen Umstellungen in der Datenverarbeitung bringen. Durch eine Veränderung in den Details und bei diversen Pflichten kann jedoch trotzdem Anpassungsbedarf gegeben sein.
Für einen allgemeinen Überblick zur DSGVO hilft dieser Folder. Für eine detaillierte Analyse, besonders bei umfangreichen Datenanwendungen, ist jedoch eine Beratung von einem Experten dringend zu empfehlen.

4. Maßnahmenplan bis 25.05.2018

Entsprechend der Analyse von Ist-Zustand und Soll-Zustand nach DSGVO sollte man umgehend einen Maßnahmenplan anlegen und den Anpassungsbedarf nach entsprechenden Prioritäten reihen. Wenn möglich, kann eine Umstellung von Abläufen im Rahmen der DSGVO-Implementierung auch mit Effizienzsteigerungen in den Abläufen oder Produktverbesserungen kombiniert werden.

ÜBERSICHT ÜBER DIE DSGVO

Überblick: Wo finde ich welche Themen in der DSGVO?

Die DSGVO ist mit über 80 Seiten ein umfangreiches Gesetz, aber nur bestimmte Teile sind für Unternehmen relevant. Neben den 99 Artikeln gibt es auch noch über 170 Erwägungsgründe, die zwar nicht rechtlich verbindlich sind, aber beim Verständnis der DSGVO helfen können.

- Kapitel I (Artikel 1 bis 4) beschäftigt sich mit den Definitionen und dem Anwendungsbereich.
- Kapitel II (Artikel 5 bis 11) erklärt, wann man Daten verarbeiten darf und wann nicht.
- Kapitel III (Artikel 12 bis 23) deckt die Rechte von Betroffenen ab.
- Kapitel IV (Artikel 24 bis 43) deckt die Pflichten des Verantwortlichen ab.
- Kapitel V (Artikel 44 bis 50) sind relevant, wenn man Daten außerhalb des EWR übermittelt.

Daneben gilt in Österreich ab 25.05.2018 ein nationales Datenschutzgesetz („DSG"), das einige Anpassungen der DSGVO und auch Ausnahmen von der DSGVO vorsieht.

Tipp: Viele Artikel der DSGVO sind nicht klar formuliert. Oft hilft es in die entsprechenden „Erwägungsgründe" am Anfang des Gesetzes zu blicken. Diese Gründe sind nicht rechtlich verbindlich, aber helfen bei der Interpretation der DSGVO. Online finden sich Tabellen, die erläutern, welche Erwägungsgründe zu welchem Artikel der DSGVO gehören.

Regelungsansatz der DSGVO

Die DSGVO folgt einem gewissen Regelungsansatz, der sich mitunter von anderen Gesetzen und dem DSG 2000 unterscheidet:

- Die DSGVO ist „**technologieneutral**". Es gibt abstrakte Regeln (z. B. Daten müssen nach dem Prinzip der Datenminimierung nach Zweckerfüllung gelöscht werden), die für jeden Anwendungsfall andere Lösungen (hier z. B. Löschzeiten von Sekunden bis zu Jahrzehnten) bedeuten.
- Die DSGVO versucht „**risikobasiert**" zu sein. Mit flexiblen Regelungen wird versucht, in einem Gesetz Weltkonzerne und EPUs gleichzeitig zu reglementieren. Viele Pflichten sind daher für KMUs nur eingeschränkt anwendbar oder praktisch irrelevant.
- Die DSGVO folgt der Idee der „**Selbstregulierung**" von Unternehmen. Systeme, wie das staatliche Datenverarbeitungsregister, werden durch interne Prozesse in Unternehmen ersetzt und von hohen Strafen begleitet. Das erlaubt schnelle interne Entscheidungen, bedeutet aber auch deutlich mehr Verantwortung für Unternehmen.

Zusammengefasst bedeutet das, dass die DSGVO meistens etwas Interpretation des Verantwortlichen erfordert und eine fehlerhafte Interpretation mitunter massive Konsequenzen hat.

DIE ZWEI KERNBESTIMMUNGEN DER DSGVO

Kernbestimmung 1: Grundprinzipien der DSGVO

Eine Datenverarbeitung nach der DSGVO muss vor allem zwei Artikeln entsprechen: In Artikel 5 werden zuerst die sechs Grundprinzipen zur Datenverwendung der DSGVO festgeschrieben:

a) **Rechtmäßige und transparente Verarbeitung nach „Treu und Glauben":** Man darf Daten nicht entgegen den Gesetzen verarbeiten und die Verarbeitung muss allgemein „fair" sein (also z. B. nicht heimtückisch oder trickreich sein). In der Praxis ist das selten ein Problem.
b) **Zweckbindung:** Die Zweckbestimmung ist das Rückgrat der DSGVO. Daten dürfen nur für einen oder mehrere bestimmte Zwecke verarbeitet werden (z. B. für eine Bestellung) und dürfen nicht für andere Zwecke (z. B. Marketing) weiterverwendet werden. Eine „Sekundärnutzung" von Daten (nach dem Motto: „Die Daten haben wir ja schon!") widerspricht der Zweckbindung. Ausnahmen für die „vereinbarte" Nutzung gibt es in Artikel 6 Abs. 4.
c) **Datenminimierung:** Daten müssen für den Zweck notwendig sein (z. B. sind „Zusatzinfos" bei Bestellungen, die irrelevant für die Abwicklung sind, nicht zu erheben).
d) **Richtigkeit:** Daten müssen richtig und (soweit erforderlich) am neuesten Stand sein. Falsche Informationen zu Betroffenen können deren Rechte schädigen.

e) **Speicherbegrenzung:** Daten müssen gelöscht werden, sobald der Zweck erfüllt wurde und es keine Speichergründe mehr gibt (z. B. mit Ablauf der steuerrechtlichen Aufbewahrungspflicht). Hier sind automatische Löschungen vorzusehen.
f) **Integrität und Vertraulichkeit:** Man muss die Datensicherheit (z. B. vor externen Hackern, unbefugten Mitarbeitern oder technischen Fehlern) entsprechend der Verarbeitung sicherstellen.

Kernbestimmung 2: Verbotsausnahmen

Auch wenn man den Grundprinzipien in Artikel 5 entspricht, ist laut DSGVO eine Datenverarbeitung immer verboten („Verbotsprinzip"), wenn nicht eine der Ausnahmen des Artikel 6 erfüllt ist:

a) **Einwilligung:** Eine gültige (!) Einwilligung des Betroffenen erlaubt die Datennutzung. Die DSGVO stellt strenge Bedingungen für eine Einwilligung in Artikel 7 und 8 auf. Schon zuvor haben die österreichischen Gerichte sehr genaue und klare Einwilligungen verlangt. Wenn eine gültige Einwilligung leicht zu erhalten ist, ist das eine sehr sichere Rechtsgrundlage. Eine Einwilligung kann jederzeit zurückgezogen werden – die Verarbeitung der Daten muss dann gestoppt werden.
b) **Erfüllung eines Vertrags:** In der wirtschaftlichen Praxis ist die „Vertragserfüllung" eine sehr gute Rechtsgrundlage für die Verarbeitung (z. B. bei einer Bestellung sind alle nötigen Schritte der Abwicklung erlaubt, auch ohne Einwilligung). Diese Rechtsgrundlage ist solide und benötigt wenig Administration.
c) **Rechtliche Verpflichtung:** Ebenso solide und einfach ist die Verarbeitung wegen rechtlicher Pflichten (z. B. Aufbewahrungspflichten, Dokumentationspflichten).
d) **Berechtigtes Interesse:** In Fällen, in denen keine Einwilligung möglich ist und keine andere Rechtsgrundlage vorliegt, kann ein „berechtigtes Interesse" weiterhelfen. Hier wird das Interesse des Unternehmens mit jenem des Betroffenen abgewogen. Dem Betroffenen bleibt jedoch ein Widerspruchsrecht nach Artikel 21. Diese Rechtsgrundlage ist in einigen Bereichen klar (z. B. Verarbeitung von Daten, um einen Anspruch gerichtlich geltend zu machen) und in anderen Bereichen relativ unklar (z. B. Marketing, Big-Data-Analysen, Datenhandel). Erwägungsgrund 47 der DSGVO gibt teilweise mehr Aufschluss, ist aber teilweise selbst unklar (z. B. „Direktwerbung kann (!) [...] ein berechtigtes Interesse" darstellen).

Das „lebenswichtige Interesse" und das „öffentliche Interesse" nach Litera d) und e) sind in der wirtschaftlichen Praxis selten relevant. Etwas strenger sind die Vorschriften für „sensible Daten" (z. B. Gesundheitsdaten) in Artikel 9 und für strafrechtliche Daten in Artikel 10.

SONSTIGE WICHTIGE BESTIMMUNGEN DER DSGVO

Auslagerung und Auslandsdatenverkehr

In der Praxis werden Daten oft nicht lokal oder nur vom Verantwortlichen selbst verarbeitet. Regelmäßig werden externe Dienste (z. B. Clouds) genutzt. Dabei werden Daten auch oft in andere Länder übertragen, die keine dem europäischen Datenschutz entsprechende Gesetze haben.

- **Auftragsdatenverarbeitung.** Verarbeitet ein Dienstleister (z. B. ein Cloud-Dienst) Daten für einen fremden Verantwortlichen (z. B. Verarbeitung eines Newsletters für einen Kunden), so liegt eine Auftragsdatenverarbeitung vor (Artikel 38). Der Auftragsdatenverarbeiter muss dabei garantieren können, dass er die Vorschriften der DSGVO einhält und die Daten z. B. nur im Auftrag des Verarbeiters nutzt. Ein Vertrag ist abzuschließen, der den Vorgaben der DSGVO entspricht.
- **Datenübermittlung in einen Drittstaat.** Generell dürfen Daten den EWR / die EU nicht verlassen, um sicherzustellen, dass der Schutz in der Union nicht unterlaufen wird. Gerade Auftragsdatenverarbeitung kann auch bei an sich nationaler Datenverarbeitung zur Datenübermittlung außerhalb der EU / des EWR führen (z. B. große US-Anbieter). Hierfür gibt es eine Reihe von Voraussetzungen in Artikel 44 bis 50.

Pflichten des Verantwortlichen

- **Informationspflichten.** Nach Artikel 13 oder 14 ist dem Betroffenen eine Liste von Informationen zur Verfügung zu stellen. Üblicherweise erfolgt das durch eine Datenschutzrichtlinie.
- **Verarbeitungsverzeichnis.** Nach Artikel 30 ist ein Verzeichnis der Verarbeitungstätigkeiten anzulegen. Unternehmen unter 250 Mitarbeitern können unter die Ausnahme in Absatz 5 fallen.
- **Privacy by Design.** Systeme und Grundeinstellungen müssen nach Artikel 25 „datenschutzfreundlich“ gestaltet werden (z. B. „Opt-in“ statt „vorgewählte“ Datenverwendung).
- **Datensicherheit**. Der Verantwortliche muss laut Artikel 32 für eine dem Stand der Technik und der Bedrohungslage angemessene Datensicherheit (z. B. mit Firewalls, Verschlüsselung, Dienstanweisungen) sorgen. Versagen diese Vorkehrungen, müssen die Betroffenen und / oder die Behörde informiert werden („Data Breach Notification“).
- **Folgenabschätzung.** Nach Artikel 35 ist mitunter bei umfangreicheren Datenanwendungen vorab eine Folgenabschätzung durchzuführen.
- **Datenschutzbeauftragter.** Unternehmen, die als Kerntätigkeit eine umfangreiche Überwachung oder eine Verarbeitung von sensiblen Daten betreiben, müssen einen Datenschutzbeauftragten ernennen. Andere Unternehmen können das tun.

Rechte der Betroffenen

- **Auskunftsrecht und Datenübertragbarkeit.** Betroffene haben nach Artikel 15 das Recht, eine Kopie ihrer Daten und diverse Informationen zur Datenverarbeitung zu erhalten. Nach Artikel 20 haben sie in bestimmten Fällen auch das Recht, die Daten in einem gängigen maschinenlesbaren Format zu erhalten.
- **Berichtigung, Löschung, Einschränkung und Widerspruch.** Nach Artikel 16 bis 18 haben Betroffene das Recht, dass falsche oder rechtswidrig gespeicherte Daten richtiggestellt werden, die Daten gelöscht werden oder die Verarbeitung eingeschränkt wird. Der Betroffene kann auch Widerspruch zur Datenverarbeitung einlegen.
- **Automatisierte Entscheidung und Profiling.** Automatisierte Entscheidungen, die eine rechtliche Wirkung entfalten oder den Betroffenen ähnlich erheblich beeinträchtigen (z. B. Entscheidung über die Kreditwürdigkeit), sind nach Artikel 22 nur in bestimmten Fällen erlaubt.

Praktische Beispiele

Kundenkarteien, Mitarbeiterdaten: Das Führen von Kundenkarteien, Mitarbeiterunterlagen, E-Mails, Dokumentationen oder das Abrechnungswesen sind – solang dieser Zweck nicht überschritten wird – ohne weitere Einschränkung erlaubt. Die Pflichten nach der DSGVO sind zu beachten.

Newsletter, Verteiler: Das Führen von Verteilern ist meist nur über ein „Opt-in" möglich. Hier ist eine Zustimmung zur Datennutzung leicht machbar. Eine Nutzung der Daten für den Zweck des Marketings ist dann unproblematisch. Eine Weitergabe von Daten (z. B. bei Verkauf an Partner) ist meist jedoch nicht zulässig.

Gewinnspieldaten: Daten können hier für den jeweiligen Zweck und mit Zustimmung leicht verarbeitet werden. Eine weitere Nutzung (z. B. über das jeweilige Gewinnspiel hinaus, für Werbung) muss klar als weiterer Zweck angegeben werden. Kunden können ihre Zustimmung jederzeit widerrufen, die Daten müssen dann gelöscht werden.

Social Media / Plattformen: Bei der Nutzung von Plattformen oder Social Media besteht oft das Problem, dass diese Dienste die DSGVO nicht beachten, aber der österreichische Verantwortliche diese Auftragsdatenverarbeiter nur nutzen dürfte, wenn sie die DSGVO vollinhaltlich einhalten.
Ein besonderes Problem ist der Import von Daten (z. B. Hochladen einer Kundenkarte), da damit diese Daten oft auch für andere Zwecke von den Plattformen genutzt werden, die dem ursprünglichen Zweck nicht mehr entsprechen. Häufig kommt es auch zur Datenübertragung in Drittstaaten, die rechtlich oft sehr komplex werden kann.

Cloud-Dienste: Cloud-Dienste können oft besseren Datenschutz und eine höhere Datensicherheit als lokale Verarbeitung bieten. Hier ist der Dienstleister auf eine

garantierte Einhaltung der DSGVO zu prüfen. Entsprechende Verträge / AGB sollten unterschrieben werden. Wichtig ist, dass eine „Sekundärnutzung" der Daten durch den Dienst ausgeschlossen ist – andernfalls „bezahlt" man meist rechtswidrig mit den Daten der eigenen Kunden. Die Nutzung von europäischen Anbietern vermeidet eine Problematik durch eine rechtlich oft problematische Übermittlung in ein Drittland.

Datensicherheit: Generell ist je nach Branche und System für die nötige Datensicherheit zu sorgen. Das ist insbesondere eine technische und organisatorische Frage. Auch Mobilgeräte mit Zugang zu Daten müssen gesichert werden. Die Anforderungen an die Datensicherheit wachsen mit der Sensibilität der Daten und dem Umfang der Datenverarbeitung.

Back-ups: Die Datensicherheitsmaßnahmen der DSGVO verpflichten dazu, auch für die Wiederherstellung von verlorenen oder zerstörten Daten zu sorgen. Back-ups dürfen jedoch nur so lange wie für eine mögliche Wiederherstellung nötig und nur für den Zweck der Wiederherstellung angelegt und genutzt werden und müssen danach ebenfalls gelöscht werden.

Maximilian Schrems
für die Fachgruppe Werbung und Marktkommunikation
Wirtschaftskammer Wien

Rückfragehinweis:

Fachgruppe Werbung und Marktkommunikation Wien
werbungwien@wkw.at