Unternehmensberatung · Buchhaltung · IT
STEIERMARK

Datenschutzgrundverordnung DSGVO

WIR NEHMEN **WISSEN** IN BETRIEB.

Inhaltsverzeichnis

Vorwort

Die Autoren ***DI(FH) Harald Schenner, CMC*** und ***DI Gerald Kortschak, BSc, CMC*** sind als zertifizierte Unternehmensberater und zertifizierte IT-Konsulenten im Themengebiet des Datenschutzes und der Daten- sowie IT-Sicherheit am österreichischen Markt aktiv. Dieses Werk stellt somit keine juristische Beratung dar, sondern soll die rechtlichen Vorgaben anhand notwendiger Maßnahmen erklären. Konkret geht es den beiden Autoren dabei um die Übersetzung, welche Prozesse und Strukturen geschaffen werden müssen, wo es in der technischen Umsetzung Handlungsbedarf geben wird und wie Sie als Unternehmen die Anwendungsfehler vermeiden können. Mit praktischen Tipps wird das Werk abgerundet.

Für die rechtliche Verifikation Ihrer Umsetzungsplanung konsultieren Sie entweder den Rechtsbeistand Ihres Vertrauens, oder den von den Autoren empfohlenen Experten für geistiges Eigentum.

Sie finden die Autoren und weitere Informationen zum Thema Datenschutzgrundverordnung auf www.dsgvo2018.at bzw. die Autoren und deren Partner-Netzwerk auf www.digital-coaches.at

„Datenschutz ist keine reine technologische Implementierung, es ist vielmehr ein strategischer und organisatorischer Ansatz, bei dessen Umsetzung jeder einzelne Mitarbeiter und externe Dienstleister mit eingebunden werden muss. Kümmern Sie sich rechtzeitig um Ihre Abläufe und Sie sparen sich viel Ärger, Zeit und Geld!“

Harald Schenner

„Datenschutz ist das Grundgerüst einer digitalen Gesellschaft wodurch die Umsetzungsmaßnahmen zur DSGVO in Form von flacheren Datenstrukturen und klaren Abläufen nicht nur einen Aufwand im Rahmen der Erstellung bedeutet, sondern auch eine große Chance darstellt.“

Gerald Kortschak

Kapitel 1: Situation und Problematik

Der Countdown läuft – ab 25. Mai 2018 gilt die EU-Datenschutzgrundverordnung. So neu ist das Thema zwar nicht, jedoch ergeben sich ein paar einschneidende Veränderung gegenüber der alten gesetzlichen Regelung. Sich darum nicht zu kümmern, wäre ein fataler Fehler. Es stellt sich nämlich nicht die Frage, ob die Behörde auf Sie als Unternehmen aufmerksam wird, sondern nur wann dies passiert. Das enorme in Aussicht gestellte Strafmaß entscheidet dann wahrscheinlich über Ihren unternehmerischen Fortbestand. Und wenn nicht das Strafmaß über den Fortbestand entscheidet, so vielleicht die Schadensersatzforderungen der betroffenen Personen.

Welche zusätzlichen oder neuen Aufgaben kommen nun auf Sie zu? Neben umfangreichen Dokumentationspflichten und notwendigen organisatorischen Maßnahmen sind einige weitere wichtige Vorschriften im Umgang mit personenbezogenen Daten einzuhalten. Dabei spielt es keine Rolle, ob es sich hierbei um Kundendaten, Mitarbeiterdaten oder um Daten anderer Personen handelt. Wesentlich ist, dass nach der EU-DSGVO alle natürlichen Personen das Schutzrecht genießen.

ACHTUNG: Die EU-DSGVO bezieht sich nur auf die personenbetroffenen Daten einer natürlichen Person. **ABER**: Das österreichische Anpassungsgesetz DSG2018 hat das DSG2000 NICHT abgelöst, sondern nur in einzelnen Paragrafen verändert bzw. angepasst. Somit gilt in Österreich weiterhin der §1 DSG2000, der im Geltungsbereich juristische Personen (der Begriff „jedermann“ ist formuliert) miteinbezieht. Somit bleiben in Österreich auch personenbezogene Daten juristischer Personen inbegriffen!
Quelle: „Datenschutz konkret“, Interview mit Dr. Eckhard Riedl (Leiter der Datenschutzabteilung des BKA), geführt von Dr. Rainer Knyrim

Bedenken Sie dabei, dass Sie als Geschäftsführer in dieser Thematik auch die sogenannte Geschäftsführerhaftung innehaben, aufgrund derer auch auf Ihr Privatvermögen zugegriffen werden kann.

Grundlegende, einleitende Informationen zur DSGVO

Zum Themenstart ist es hilfreich, sich mit den theoretischen Bestandteilen der Verordnung zu befassen, um diese im weiteren Gebrauch nachvollziehen zu können. Dies wird zwar auf den nächsten wenigen Seiten etwas „trocken“ im Stoff, erleichtert aber danach die praxisorientierte Darlegung der Anforderungen, Systemanpassungen und der Umsetzungsschritte.

Was ist die DSGVO?

Die **Datenschutzgrundverordnung** (kurz DSGVO) ist eine Regelung der Europäischen Union, um im gesamten Rechtsgebiet der EU eine einheitliche Basis zum Thema Datenschutz zu schaffen. Bislang wurde dieses Thema nationalstaatlich in eigenen gesetzlichen Vorschriften geregelt. In Österreich beispielsweise gilt aktuell (bis 25.05.2018) noch das DSG 2000 (Datenschutzgesetz 2000). Geregelt wurden in diesem Gesetz die rechtmäßige Verwendung und Verarbeitung von personenbezogenen Daten.

Neben dem Aspekt, eine gemeinschaftliche Basis auf europäischer Ebene zu schaffen, wurden in der DSGVO im Unterschied zum DSG2000 ein paar grundlegende Veränderungen durchgeführt. Darunter fallen das in Aussicht gestellte Strafmaß, das einem Vielfachen des bisherigen Strafmaßes entspricht, die *Auskunftspflicht*, das *Recht auf „Vergessenwerden“* (Löschpflicht), *Privacy by Design* und *Privacy by Default*, sowie einige Punkte mehr, auf die wir im Folgenden näher eingehen werden.

> Grundlegend ist die DSGVO ein Verbotsgesetz, das generell die Verarbeitung von personenbezogenen Daten verbietet, sie jedoch für einige Anwendungsfälle erlaubt und vom Verbot ausnimmt. Daher ist auch wirklich alles, das nicht explizit erlaubt ist, implizit verboten!

Eine wesentliche, und somit fundamentale Veränderung liegt jedoch in der Auslegungs- oder Anwendungsverantwortung. Die DSG2000 verlangte eine Meldung (ein Ansuchen) an die Datenschutzbehörde, in der die gewünschte Datenerhebung und Datensammlung dargestellt werden musste. Gab die Behörde „grünes Licht“ und somit eine DVR-Melderegisternummer, so war das Unternehmen auf der sicheren Seite, diese Daten erheben und verarbeiten zu dürfen. In der neuen Regelung der DSGVO hat das Unternehmen selbst diese Sorgfalt wahrzunehmen und auf Basis der gesetzlichen Bestimmung zu erwägen, ob und in welcher Form eine Datenerhebung und Datenspeicherung zulässig ist. Zudem hat das Unternehmen jederzeit abrufbar nachzuweisen, welche Daten es warum, wozu, womit und auf welche Weise erhebt, speichert oder weiterverarbeitet. Dieses sogenannte ***„Verzeichnis der***

Verarbeitungstätigkeiten" ist vom Unternehmen zu erstellen und aktuell zu halten und muss bei entsprechender Prüfung durch die Aufsichtsbehörde vorgelegt werden.

Der Gesetzgeber legt die Verantwortung somit gänzlich in die Hände der Unternehmen. Ob dies nun einen Vorteil oder einen Nachteil für die Unternehmen darstellt, wird hier nicht behandelt. Welche Möglichkeiten sich dadurch ergeben, ist aus unserer Sicht der interessantere Blickwinkel. Auch dazu kommen wir später im Detail.

Zukünftig werden keine DVR-Nummern vergeben. Die Verantwortung fällt dem Datenverantwortlichen zu.

Österreichisches Anpassungsgesetz

Die DSGVO schafft für nationale Anpassungen den notwendigen Raum, um Details konkretisieren oder nachschärfen zu können. In Österreich kommt daher ein Anpassungsgesetz zur Anwendung (Datenschutz-Anpassungsgesetz 2018, BGBLA 2017/I/120 vom 31.07.2017 = DSG2018), welches das DSG2000 NICHT ablöst, sondern nur anpasst.

Wesentliche Änderung in der österreichischen Gesetzgebung gegenüber der EU-DSGVO ist, dass juristische Personen weiterhin das Recht auf Schutz personenbezogener Daten genießen.

Die einzelnen Anpassungen zur DSGVO werden in den entsprechenden nachfolgenden Kapiteln nähergebracht, bzw. der jeweilige Bezug hergestellt.

Die Intention der DSGVO

Neben dem bereits erwähnten Interesse, ein Union-weites Fundament für die Regelung von Datenschutz-Themen zu schaffen, waren noch weitere Aspekte für das Zustandekommen der EU-DSGVO wesentlich. ***Datenschutz als Grundrecht*** anzuerkennen, ist bereits in der „Charta der Grundrechte der Europäischen Union" verankert und findet in der DSGVO die entsprechende rechtliche Umsetzung. Im Zeitalter der Digitalisierung und des rasanten Technologie-Fortschritts wird auch das Datenschutzniveau auf den „***aktuellen Stand der Technik***" festgelegt, was jedenfalls bedeutet, dass sich jedes Unternehmen auch bei Ihren entsprechenden Dienstleistern rückversichern muss. Ebenfalls wird der ***Grundsatz der Transparenz*** eingeführt, sodass sämtliche für betroffene Personen bestimmte Informationen präzise, leicht zugänglich und leicht verständlich, in klarer und einfacher Sprache gefasst zur Verfügung gestellt werden müssen. Diese Transparenz ist auch notwendig, da die betroffenen Personen spezielle Rechte genießen, die ein schnelles Auffinden der jeweiligen personenbezogenen Daten voraussetzt. Das ***Auskunftsrecht*** spricht den betroffenen Personen das Recht zu, jederzeit ein Auskunftsbegehren an ein Unternehmen stellen und somit in Erfahrung bringen zu können, welche Daten für welchen Zweck in welcher Form gespeichert und verarbeitet werden. Weiters besteht das ***Recht auf Berichtigung***, sollten die

Daten lückenhaft oder falsch sein. Das ***Recht auf Widerruf*** (Widerruf der einstmals erteilten Einwilligung der Datenerfassung und Verarbeitung) ist neben dem ***Recht auf „Vergessenwerden“*** (also sowohl die automatische als auch die manuelle Löschung der personenbezogenen Daten) ebenfalls in der DSGVO verankert.

Zudem werden in der DSGVO auch weitreichende Verantwortungen an die Unternehmen delegiert, was Meldepflicht und Folgenabschätzung bei Datendiebstahl oder –verlust anbelangt.

Wen betrifft die DSGVO?

Hartnäckig hält sich das Gerücht, dass die DSGVO nur für Unternehmen mit mindestens 250 Mitarbeitern Gültigkeit besitzt. Das ist leider ein fataler Irrtum. **Die DSGVO gilt grundsätzlich für ALLE Unternehmen**, die mit personenbezogenen Daten natürlicher Personen „arbeiten“. Ob dies nun Mitarbeiterdaten, Kunden- oder Lieferantendaten sind, ist ebenso unerheblich wie die Unterscheidung nach digitaler oder analoger Verarbeitung. Sobald Sie als Unternehmen die Daten strukturiert oder durchsuchbar erheben, speichern oder verarbeiten, gilt die Regelung für Sie – unabhängig davon, ob Sie die Daten in einem Software-System speichern, oder dies in einem Aktenordner aufbewahren. Tatsächlich wird es sehr wenige Unternehmen geben, für die die DSGVO keine Relevanz haben wird.

Die DSGVO betrifft praktisch alle Unternehmen!

Ob Sie nun auch ein Verfahrensverzeichnis (Verzeichnis über die Verarbeitungstätigkeiten) führen müssen, oder explizit einen Datenschutzbeauftragten benötigen werden, hängt von weiteren Kriterien ab. Soviel sei an dieser Stelle vorweggenommen: das Verfahrensverzeichnis werden Sie wahrscheinlich führen müssen – abgesehen davon, dass dieses Verzeichnis auch eine hervorragende Möglichkeit darstellt, die internen Daten-Verarbeitungstätigkeiten transparent und detailliert darzustellen und somit das Bewusstsein im Umgang mit personenbezogenen und schützenwerten Daten zu sensibilisieren.

Folgen einer Nichtumsetzung

Auch in puncto Folgen und Strafausmaß lässt der rechtliche Handlungsspielraum der DSGVO die Intention der Europäischen Union erkennen. Wer sich eklatant außerhalb der gesetzlichen Vorschrift bewegt, hat mit weitreichenden Strafen (bis zu 20 Mio. EUR oder 4% des Jahresumsatzes des gesamten Konzerns) zu rechnen. Das Österreichische Anpassungsgesetz zeigt hier seinerseits auch die österreichische Gesinnung: dieses hohe EU-Strafmaß gilt nur für

juristische Personen, Einzelunternehmen werden mit bis zu 50.000 EUR belangt.

Welche Chancen bringt die DSGVO für Sie als Unternehmen?

Neben den vielen Anforderungen und Vorgaben durch die DSGVO bestehen aber auch einige Chancen für das Unternehmen. Chancen in Hinblick auf die eigene Datenhaltung, die Eindämmung dezentraler, redundanter Datenstämme und die Transparenz der eigenen Datenverarbeitungssysteme.

Audit der Unternehmensdaten: die System- und Bezugsgruppenanalyse

Ein Audit der Unternehmensdaten beantwortet die wichtigen Fragen rund um die Datenverwendung und –Verarbeitung innerhalb des Unternehmens: Welche Daten werden erhoben und -verarbeitet, wo werden die Daten gespeichert, wer hat Zugriff in welcher Form oder werden die Daten für den eigentlichen Zweck verarbeitet?

Die Erhebung der IST-Situation und der Abgleich mit der SOLL-Situation ergibt sowohl Ausgangspunkt als auch Richtung Ihrer Prozess- und IT-Korrekturen.

Automatisierte Datenspeicherung und sinnvolle Datenverwaltung

Prüfen Sie die Datenablage und die Datenströme im Unternehmen. Automatisierte Prozesse führen zu mehr Effizienz im Unternehmen. Darüber hinaus werden überflüssige und doppelte Datensätze vermieden. Klar vorgegebene Datenstrukturen und Erhebungs- als auch Verarbeitungsprozesse vereinfachen die Datenverwaltung. Mehrfach erstellte und abgelegte Excel-Dateien, die über diverse Abteilungen und verschiedene Hardware verteilt sind, könnten vermieden werden.

Transparenz der Datensysteme

Ein genauer Überblick über Ihre Datenverarbeitungsprozesse ist die Basis für die Datensystem-Transparenz. Dies bedeutet vor allem, dass Sie jederzeit Auskunft darüber erteilen können, welche Daten, wann und wo und zu welchem Zweck bei Ihnen im Unternehmen verarbeitet werden. Sie können sofort die Fragen nach Backup- oder Löschkonzept beantworten und wissen, wo erhöhtes Risiko in Ihrer Datenverarbeitung besteht. Somit wissen Sie auch, wo Sie angreifen müssen, wenn es notwendig wird.

Die DSGVO ist nicht nur Vorschrift, sondern auch Chance!

Begriffsdefinition und Rollen in der DSGVO

Um in weiterer Folge die jeweiligen Bereiche der Datenschutzgrundverordnung besser verstehen zu können, wollen wir uns nun den wesentlichen Begriffen und Rollen widmen. Dabei zitiere ich auszugsweise (wenn erforderlich) aus dem Gesetz, werde jedoch vorrangig auf verständliche Darstellung achten.

Personenbezogene Daten, betroffene Person

Die EU-DSGVO bezieht sich ausschließlich auf alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (= betroffene Person) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt durch Namen, Kennnummer, Standortdaten, Online-Kennung oder besonderen Merkmalen (wie physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität) identifiziert werden kann.

Worauf die Verordnung im Anwendungsbereich abzielt, wird später erläutert. Wesentlich ist jedoch, dass die Daten juristischer Personen in der EU-DSGVO somit nicht geregelt werden.

ACHTUNG: An dieser Stelle verweise ich noch einmal auf das eingangs erwähnte Spezialthema des österreichischen Anpassungsgesetzes:

> **ACHTUNG**: Die EU-DSGVO bezieht sich nur auf die personenbetroffenen Daten einer natürlichen Person. **ABER**: Das österreichische Anpassungsgesetz DSG2018 hat das DSG2000 NICHT abgelöst, sondern nur in einzelnen Paragrafen verändert bzw. angepasst. Somit gilt in Österreich weiterhin der §1 DSG2000, der im Geltungsbereich juristische Personen (der Begriff „jedermann“ ist formuliert) miteinbezieht. Somit bleiben in Österreich auch personenbezogene Daten juristischer Personen inbegriffen!
> **Quelle**: „Datenschutz konkret“, Interview mit Dr. Eckhard Riedl (Leiter der Datenschutzabteilung des BKA), geführt von Dr. Rainer Knyrim

Verarbeitung

Als Verarbeitung gilt jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben oder Erfassen, die Organisation, das Ordnen oder Speichern, Anpassen oder Verändern, Auslesen oder Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Einschränkung der Verarbeitung

Dies bezeichnet die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Das kann bedeuten, dass die Verwendung der personenbezogenen Daten die betroffene Person zwar die Einwilligung zum Zweck X gegeben hat, jedoch zum Zweck Y. (Bsp: zur Rechnungslegung schon, zu Marketingzwecken nicht).

Profiling

Mit Profiling ist jede Art der automatisierten Verarbeitung personenbezogener Daten gemeint, die darin besteht, die Daten dahingehend zu verwenden, um persönliche Aspekte (Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort und Ortswechsel) einer betroffenen Person zu bewerten, zu analysieren oder vorherzusagen. Dies betrifft vor allem, aber nicht nur, die Bereiche Web-Analytics, Affiliate-Marketing, Zutrittskontrollsysteme und vieles mehr.

Verantwortlicher

Als Verantwortlicher gilt eine „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

Auftragsverarbeiter

Als Auftragsverarbeiter gilt jemand, der „die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet“. Dies können IT-Dienstleister oder andere Dienstleister sein (Buchhaltung, Lohnverrechnung, ...).

Einwilligung

Als Einwilligung gilt die in „informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.“

Diese Willensbekundung gilt ausschließlich für den in der Einwilligung genannten Zweck der Verarbeitung. Es reicht nicht aus, diese notwendige Einwilligung als passiv akzeptierten Bereich in den Allgemeinen Geschäftsbedingungen unterzubringen.

Gesundheitsdaten

... sind „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.“

Vertreter

Als Vertreter gilt eine von Verantwortlichen oder Auftragsverarbeiter beauftragte – in der Union niedergelassene – natürliche oder juristische Person, die den Auftraggeber „in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflicht vertritt."

Anwendungsbereiche der Verordnung

Gemäß Artikel 2 der DSGVO erschließt sich der ***sachliche Anwendungsbereich*** auf die *„ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen."* Damit sind also sowohl automatisierte als auch manuelle Verarbeitungsschritte in digitaler aber auch analoger Form inkludiert! Das bedeutet, dass Akten oder Aktensammlungen, die nach bestimmten Kriterien geordnet sind, ebenfalls in den Anwendungsbereich dieser Verordnung fallen.

Eine der wenigen genannten ***Ausnahmefälle*** betrifft die Verarbeitung durch natürliche Personen zur Ausübung ausschließlich ***persönlicher oder familiärer Tätigkeiten***. Jedoch gilt die Verordnung für Verantwortliche oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung zu persönlichen oder familiären Zwecken bereitstellen!

Der Artikel 3 der DSGVO beschreibt den ***räumlichen Anwendungsbereich*** und bezieht sich einerseits auf die *„Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet."*, und andererseits auf die *„Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist, oder b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt."*

Zusammengefasst betrifft die Verordnung also einerseits die ***Unternehmen mit Sitz in der Union*** und diejenigen Unternehmen, die Daten von sich in der ***Union befindlichen betroffenen Personen*** verarbeiten. Vereinfacht könnte man sagen, die DSGVO gilt, wenn sich Datenquelle oder Datenziel innerhalb der Europäischen Union befinden.

Dabei gilt ein Nicht-Unions-Ort, der aufgrund geltenden Völkerrechts dem Recht eines Mitgliedsstaats unterliegt, ebenfalls als betroffen.

Themenschwerpunkt: Rechte der betroffenen Personen

Die Rechte der betroffenen Personen gegenüber den Datenverantwortlichen sind mit der DSGVO weitreichend und ergeben sohin die Pflichten der Unternehmen. Diese betreffen einerseits die Vorgaben für die Einwilligung zur Verarbeitung der Daten, als auch die Pflicht zur Auskunftserteilung, Berichtigung, Löschung und Widerruf. Welche Rechte sind das im Detail? Und was bedeuten diese Rechte der betroffenen Personen als Pflichten für die Unternehmen? Nachfolgend erhalten Sie eine Übersicht der wesentlichen Rechte:

Rechtmäßigkeit der Verarbeitung (Art. 6)

Vereinfacht gibt es 6 Bedingungen, die eine Rechtmäßigkeit der Verarbeitung darstellen:

a) Einwilligung zur Verarbeitung durch die betroffene Person
b) Verarbeitung ist aufgrund eines Vertrags mit der betroffenen Person oder zur Erfüllung vorvertraglicher Maßnahmen, die die betroffene Person in Auftrag gegeben hat, erforderlich
c) Verarbeitung ist aufgrund einer rechtlichen Verpflichtung, die der Verantwortliche einzuhalten hat, erforderlich
d) Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen
e) Verarbeitung ist für Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt
f) Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Bedingungen für die Einwilligung (Art. 7)

Der Verantwortliche muss den Nachweis erbringen, dass die betroffene Person ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten ausdrücklich gegeben hat, wenn die Verarbeitung auf Basis der Einwilligung beruht.

Bedingungen für die Einwilligung eines Kindes (Art. 8)

Eine gem. Art. 7 erfüllte Einwilligung eines Kindes gilt durch das Anpassungsgesetz DSG2018 nur dann, wenn das Kind das 14 Lebensjahr bereits vollendet hat. Andernfalls ist die Einwilligung der Träger der elterlichen Verantwortung entsprechend einzuholen.

Informationspflicht bei Erhebung (Art. 13)

Zum Zeitpunkt der Erhebung von personenbezogenen Daten muss der betroffenen Person folgendes mitgeteilt werden:

- Name und Kontaktdaten des Verantwortlichen oder Vertreters
- Kontaktdaten des Datenschutzbeauftragten (so es einen gibt)
- Die Zwecke der Verarbeitung und die Rechtsgrundlage der Verarbeitung
- Wenn die Verarbeitung auf Art. 6, Abs. 1, Buchstabe f (Wahrung berechtigter Interessen ...) beruht, die berechtigten Interessen
- Empfänger der Daten
- Absicht des Verantwortlichen, Daten an Drittländer oder internationale Organisationen zu übermitteln, sowie das Fehlen oder Vorhandensein eines Angemessenheitsbeschlusses
- Die Dauer der Speicherung bzw. die Kriterien für die Festlegung der Dauer
- Das Bestehen der Rechte gem. Art. 15-21
- Bestehen des Beschwerderechts bei der Aufsichtsbehörde
- Wofür die Verarbeitung notwendig ist (gesetzlich oder vertraglich vorgeschrieben) und welche möglichen Folgen eine Nichtbereitstellung hätte
- Bestehen von automatisierten Entscheidungsfindungen einschließlich Profiling und aussagekräftige Informationen zur involvierten Logik sowie Tragweite und angestrebte Auswirkung

Diese Informationspflicht bei der Erhebung von Daten stellt einen wesentlichen und wichtigen Bereich der DSGVO dar. Die betroffene Person soll damit über die Verwendung und Verarbeitung ihrer personenbezogenen Daten transparent aufgeklärt werden. Um diese Information im Zuge der Einwilligung richtig zur Verfügung stellen zu können, bedarf es umfangreicher Kenntnis der eigenen Verarbeitungsprozesse und Datenverwendungen im Unternehmen, etwaiger Weitergaben an Dritte oder Datenempfänger bzw. auch der eigenen Auftragsverarbeiter.

Informationspflicht, wenn die Daten indirekt ermittelt wurden (Art. 14)

Wenn die personenbezogenen Daten nicht direkt bei der betroffenen Person eingehoben wurden, so ist neben den Informationen von Art. 13 zusätzlich der Quellennachweis zu erbringen. Diese gesamten Informationen sind der betroffenen Person innerhalb eines angemessenen Zeitraums, längstens jedoch innerhalb eines Monats nach Erlangen der personenbezogenen Daten, zu erteilen. Ausnahmen von dieser Informationspflicht gibt es, wenn sich die Erteilung als unmöglich darstellt oder einen unverhältnismäßigen Aufwand erfordern würde.

Die juristische Auslegung eines „unverhältnismäßigen Aufwands“ ist unbedingt individuell und pro Anlassfall zu betrachten!

Auskunftsrecht der betroffenen Person (Art. 15)

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf weitere Informationen, die im Kapitel 2 detailliert dargestellt werden.

Recht auf Berichtigung (Art. 16)

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.

Recht auf Löschung (Art. 17)

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, soferne einige Gründe zutreffen, die in Kapitel 2 genau erläutert werden.

Recht auf Einschränkung der Verarbeitung (Art. 18)

Unter bestimmten Voraussetzungen – die in Kapitel 2 näher betrachtet werden – hat die betroffene Person das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen.

Mitteilungspflicht (Art. 19)

Der Verantwortliche teilt allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

Recht auf Datenübertragbarkeit (Art. 20)

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern die Verarbeitung auf Einwilligung oder einem Vertrag beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Widerspruchsrecht (Art. 21)

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen. Die genaueren Bedingungen zum Widerspruchsrecht werden in Kapitel 2 erläutert.

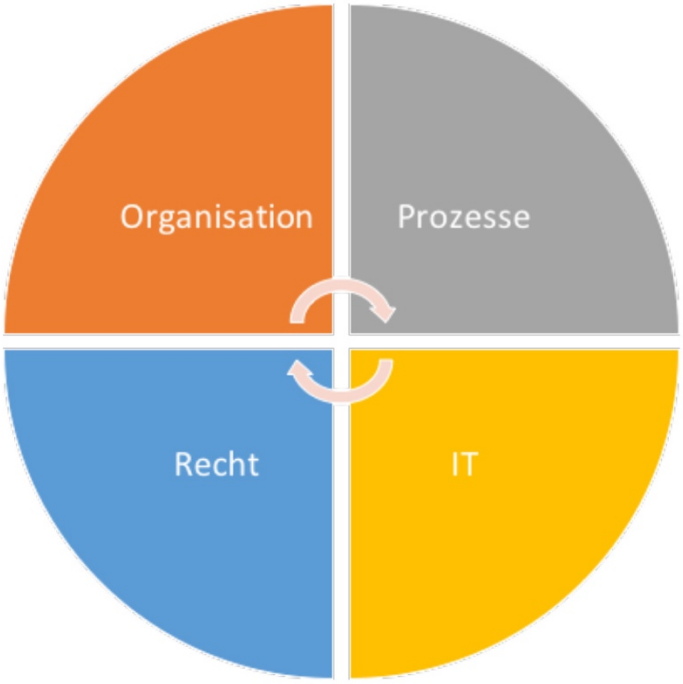
Umfangreiche Rechte der betroffenen Personen bedeuten entsprechend umfangreiche Pflichten für die Unternehmen. Bereiten Sie sich früh genug darauf vor, um unnötige Strafen vermeiden zu können!

Kapitel 2: Bedeutung und Auswirkung

Im Kapitel 1 sind wir näher auf die Begriffe und die einzelnen wichtigen Artikel der DSGVO eingegangen. Wir haben auch auf einige Irrtümer hingewiesen und die österreichische Ausnahme (Datenschutz in Österreich gilt auch für juristische Personen) erläutert. Im Kapitel 2 nähern wir uns nun der konkreten Bedeutung und der Auswirkungen auf Ihr „daily-business“. Wir sehen uns die Prozesse an, die durch die DSGVO und das DSG2018 betroffen sind. Dazu betrachten wir die Auswirkungstiefe der gesetzlichen Vorschrift, die in den IT-Systemen bis hin zum Betreiber Ihrer Infrastruktur reicht. Zusätzlich wird das „Recht auf Vergessenwerden“ in Bezug auf Regellöschfristen konkretisiert.

Auswirkungen der DSGVO

Die Datenschutzgrundverordnung, das Datenschutzgesetz 2000 und das Datenschutz-Anpassungsgesetz 2018 nehmen weitreichenden Einfluss auf Ihr Unternehmen. Da mehrfach in der DSGVO auch Bezug auf organisatorische Maßnahmen genommen wird, ist die reine technische Betrachtung nicht ausreichend. Es ist vielmehr notwendig, sich die gesamte Organisation, deren Prozesse und IT-Systeme näher vor Augen zu führen und diese anzupassen. Dies auf Grundlage des geltenden Rechts.



Sehen wir uns dazu noch genauer die Rechtmäßigkeit der Verarbeitung an.

Rechtmäßigkeit der Verarbeitung

Unter welchen Voraussetzungen dürfen welche Daten erhoben und verarbeitet werden?

Auf das notwendige Maß reduziert, rechtmäßig und nachvollziehbar, mittels angemessener Sicherheit, durch Einwilligung oder Verpflichtung oder erfüllungsnotwendig

Gemäß Artikel 5 der DSGVO (Grundsätze für die Verarbeitung personenbezogener Daten) müssen personenbezogene Daten auf rechtmäßige und für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Weiters dürfen die Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden, sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein, und dürfen nicht zu anderen Zwecken weiterverarbeitet werden (wörtlich: *„... nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise ...“*). Zudem müssen die Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet (einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen).

Gemäß Artikel 6 ist eine Verarbeitung nur rechtmäßig, wenn entweder eine Einwilligung der betroffenen Person vorliegt (wie diese auszusehen hat, wird nachfolgend erläutert), oder die Verarbeitung für die Erfüllung eines Vertrages erforderlich ist (bzw. zur Durchführung von vorvertraglichen Maßnahmen auf Anfrage der betroffenen Person), oder die Verarbeitung aufgrund einer rechtlichen Verpflichtung erforderlich ist. Weitere rechtmäßige Bedingungen beziehen sich vor allem auf den Gesundheitssektor (lebenswichtige Interessen).

Einwilligung

Wir raten davon ab, Einwilligungen mündlich einzuholen, da der Verantwortliche jederzeit nachweisen können muss, dass die betroffene Person in die Verarbeitung eingewilligt hat. Zudem hat diese Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen. Die „Unterbringung“ der Einwilligung in die Allgemeinen Geschäftsbedingungen ist sohin keine adäquate Form[1].

Am besten schriftlich, in klarer Sprache, alle Zwecke auflistend und auf notwendige Daten beschränkt

[1] Erwägungsgrund 32 der DSGVO: *„Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, ...*
Stillschweigen, ... sollte daher keine Einwilligung darstellen. Wenn die Verarbeitung mehreren Zwecken dient, sollte für ALLE diese Verarbeitungszwecke eine Einwilligung gegeben werden.“

Weiters hat die betroffene Person gemäß Artikel 7 Absatz 3 der DSGVO (Bedingungen für die Einwilligung) das Recht, ihre Einwilligung jederzeit zu widerrufen. Dabei muss der Widerruf der Einwilligung so einfach wie die Erteilung der Einwilligung sein!

Zusätzlich legt der Art.7, Abs. 4 fest, dass bei der Beurteilung der „freiwilligen Einwilligung" genau darauf zu achten ist, ob in die Verarbeitung etwaiger für die Erfüllung des Vertrages nicht erforderlichen personenbezogenen Daten eingewilligt werden muss. Kurz formuliert ist darauf zu achten, dass Sie keine Personen von einem Angebot ausschließen, nur weil diese nicht in die Verarbeitung personenbezogener Daten (die nicht zur Vertragserfüllung erforderlich sind) einwilligen!

Für Kinder, die das vierzehnte[2] Jahr nicht vollendet haben, muss die Einwilligung durch den „Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung" erteilt werden.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)

Einige Branchen arbeiten mit besonderen Kategorien personenbezogener Daten (sogenannte sensible Daten). Vor allem der Gesundheitsbereich (Diagnostik, Pflege, Betreuung, ...) ist damit betraut und dahingehend auch legitimiert (Art. 9, Abs. 2, Ziff c DSGVO: zum Schutz lebenswichtiger Interessen).

Jedoch haben Arbeitgeber-Betriebe (meist) ebenfalls sensible Daten ihrer MitarbeiterInnen gespeichert – zumindest die Sozialversicherungsnummer gehört zu den Gesundheitsdaten und ist sohin sensibel. Weiters könnte zur Geltendmachung verschiedener religiöser Ansprüche (Feiertage, Verfügbarkeits- oder Einsatzlimitierung aufgrund religiöser Fastenzeiten, ...) das Religionsbekenntnis im Unternehmen erfasst sein, welches ebenso gem. Art. 9, Abs. 1 DSGVO zu den sensiblen Daten gehört.

Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO)

Weitestgehend dürfen Daten über strafrechtliche Verurteilungen und Straftaten nur unter behördlicher Aufsicht verarbeitet werden.

Es gibt jedoch auch Branchen, die verpflichtet sind, neue Mitarbeiter einer ***behördlichen Zuverlässigkeitsprüfung*** unterziehen zu lassen, bevor diese in das aktive Arbeitsverhältnis einsteigen dürfen (Sicherheitsgewerbe, kritische öffentliche Infrastrukturbetreiber, ...). Die Antwort der Behörde ist hierbei zwar nicht detailliert (es gibt meist nur die Auskunft, ob eine

[2] EU-DSGVO schreibt im Art. 8 (Bedingungen für die Einwilligung eines Kindes) die Vollendung des 16. Lebensjahres vor – lässt jedoch der nationalstaatlichen Anpassung einen Rahmen bis minimal dem vollendeten 13. Lebensjahr. Das österreichische Datenschutz-Anpassungsgesetz 2018 (DSG2018) erfasst im §4, Abs. 4 das vollendete 14. Lebensjahr

Beschäftigung der überprüften Person möglich oder eben nicht möglich ist), dennoch aussagekräftig.

Welche Folgen könnten daraus abgeleitet werden, wenn diese Auskunft der Behörde, die Sie eventuell speichern, in falsche Hände gerät oder öffentlich gemacht wird? Welche Folgen hätte die veröffentlichte Antwort „Beschäftigung nicht möglich“ für die betroffene Person? Welche Information lässt sich daraus ableiten?

Wir werden uns noch später in diesem Kapitel mit dem Thema Folgenabschätzung und Risikobewertung beschäftigen.

Conclusio und Prüfung

Sind Sie sich sicher, dass Sie nur jene Daten erheben, die Sie wirklich benötigen (Datenminimierung)? Haben Sie dafür eine gesetzliche Erhebungspflicht oder die Willensbekundung der betroffenen Person (entweder als explizite Einwilligung oder als deren Auftrag zur Erfüllung eines Vertrages)? Welche besonderen Datenkategorien erheben und verarbeiten Sie? Welche rechtliche Grundlage legitimiert diese Datenerhebung und -verarbeitung?

Reduzieren Sie die Datenerhebung, prüfen Sie die Legitimität

Pflichten des Verantwortlichen

Die Pflichten des Verantwortlichen sind recht vielfältig, jedoch bei sorgsamen Umgang und entsprechender Vorbereitung auch hilfreich für interne Standardisierung.

Informationspflicht

Der Verantwortliche hat die betroffene Person bei deren Datenerhebung über einige Punkte zu informieren:

- Namen und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten (so es einen gibt)
- Verarbeitungszweck(e) und Rechtsgrundlagen der Verarbeitung
- Bei Datenverarbeitung im berechtigten Interesse des Verantwortlichen oder eines Dritten müssen diese berechtigten Interessen dargelegt werden
- Etwaige Empfänger der Daten
- Übermittlung an Drittland und Bestehen oder Fehlen eines Angemessenheitsbeschlusses seitens der Europäischen Union
- Dauer der Datenspeicherung bzw. Kriterien für die Festlegung der Dauer
- Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch/Widerruf, Datenübertragbarkeit)

- Ob die Erhebung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist (und die Folgen einer Nichtbereitstellung)

Werden die Daten nicht direkt bei der betroffenen Person erhoben, so ist die betroffenen Person neben den angeführten Punkten auch über die ***Datenquelle*** zu informieren. Die Information hat sofort nach Erhalt, allenfalls innerhalb eines Monats zu erfolgen. Ausnahmen davon bestehen, wenn die betroffene Person bereits über die Information verfügt, oder die Erteilung dieser Information unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert.

Wahrung der Betroffenenrechte

Eine betroffene Person hat das Recht auf Auskunft, Berichtigung/Löschung der Daten, Widerspruch der Einwilligung, Einschränkung der Verarbeitung und Datenübertragbarkeit. ***Innerhalb eines Monats*** ab Einlangen des Begehrens hat der Verantwortliche die angefragte Auskunft zu erteilen oder die Umsetzung des Begehrens bekannt zu geben. Bei mehrfachen parallelen Begehren kann ein Monat durchaus kurz werden, weswegen wir an dieser Stelle empfehlen, sämtliche Prozesse für derartige Begehren zu definieren und vorzubereiten. Wesentlich dabei ist auch, dass jegliche Datenempfänger über Berichtigung, Löschung oder Einschränkung der Verarbeitung informiert werden müssen!

Geeignete technische und organisatorische Maßnahmen

Der Verantwortlich trägt auch die Verantwortung für Datensicherheitsmaßnahmen, sowohl organisatorischer als auch IT-technischer Natur.

Datenschutz durch Technikgestaltung (Art. 25 DSGVO)

(1) Unter Berücksichtigung des ***Stands der Technik***, der ***Implementierungskosten*** und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der ***unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken*** für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum ***Zeitpunkt der Festlegung der Mittel*** für die Verarbeitung als auch zum ***Zeitpunkt der eigentlichen Verarbeitung*** geeignete ***technische und organisatorische Maßnahmen*** — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa ***Datenminimierung*** wirksam umzusetzen und die ***notwendigen Garantien*** in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass ***durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist***, verarbeitet werden. Diese Verpflichtung gilt für die ***Menge der erhobenen personenbezogenen Daten***, den ***Umfang ihrer Verarbeitung***, ihre ***Speicherfrist*** und ihre ***Zugänglichkeit***. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten ***durch Voreinstellungen*** nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Sicherheit der Verarbeitung (Art. 32 DSGVO)

(1) Unter Berücksichtigung des ***Stands der Technik***, der ***Implementierungskosten*** und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der ***unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos*** für die Rechte und Freiheiten natürlicher Personen treffen der ***Verantwortliche*** und der ***Auftragsverarbeiter*** geeignete ***technische und organisatorische Maßnahmen***, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die ***Vertraulichkeit***, ***Integrität***, ***Verfügbarkeit*** und ***Belastbarkeit der Systeme*** und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die ***Verfügbarkeit*** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall ***rasch wiederherzustellen***;

d) ein Verfahren zur ***regelmäßigen Überprüfung***, ***Bewertung*** und ***Evaluierung*** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die ***Risiken*** zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — ***Vernichtung***, ***Verlust***, ***Veränderung*** oder ***unbefugte Offenlegung*** von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
(4) ***Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte***, um sicherzustellen, dass ihnen ***unterstellte natürliche Personen***, die Zugang zu personenbezogenen Daten haben, diese ***nur auf Anweisung*** des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

TIPP!

Erheben Sie nur die tatsächlich unbedingt notwendigen Daten, stellen Sie den Stand der Technik Ihrer Datensysteme sicher, legen Sie eine Löschfrist für die Daten fest und beschränken Sie den Zugang zu diesen Daten auch innerhalb Ihrer Belegschaft auf das notwendige Maß. Weiters arbeiten Sie nur mit Auftragsverarbeiter zusammen, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen derart durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet.

Meldepflicht bei Data-Breach (Datenpanne) (Art. 33 und 34 DSGVO)

Als Data-Breach wird ein Verlust, Diebstahl oder nicht autorisierter Zugriff auf personenbezogene Daten verstanden. Sobald Sie als Verantwortlicher Kenntnis über einen erfolgten Data-Breach (eine ***Verletzung des Schutzes personenbezogener Daten***) erlangen, haben Sie innerhalb von 72 Stunden Meldung an die Aufsichtsbehörde zu erteilen! (**Ausnahme**: wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ***nicht zu einem Risiko für die Rechte und Freiheiten*** natürlicher Personen führt).

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein ***hohes Risiko für die Rechte und Freiheiten*** natürlicher Personen zur Folge, so hat neben der Meldung an die Aufsichtsbehörde auch eine Meldung an die betroffenen Personen zu erfolgen!

Risikoanalyse und Folgeabschätzung

Sie, als Verantwortlicher, haben Risikoanalysen über Ihre Datenanwendungen durchzuführen und im Falle eines wahrscheinlich hohen Risikos auch eine entsprechende Folgenabschätzung vorzunehmen.

Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(3) Eine ***Datenschutz-Folgenabschätzung*** gemäß Absatz 1 ist insbesondere in folgenden Fällen ***erforderlich***:

a) ***systematische*** und ***umfassende Bewertung persönlicher Aspekte*** natürlicher Personen, die sich auf ***automatisierte Verarbeitung*** einschließlich ***Profiling*** gründet und die ihrerseits als ***Grundlage*** für ***Entscheidungen*** dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) ***umfangreiche Verarbeitung besonderer Kategorien*** von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) ***systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche***.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

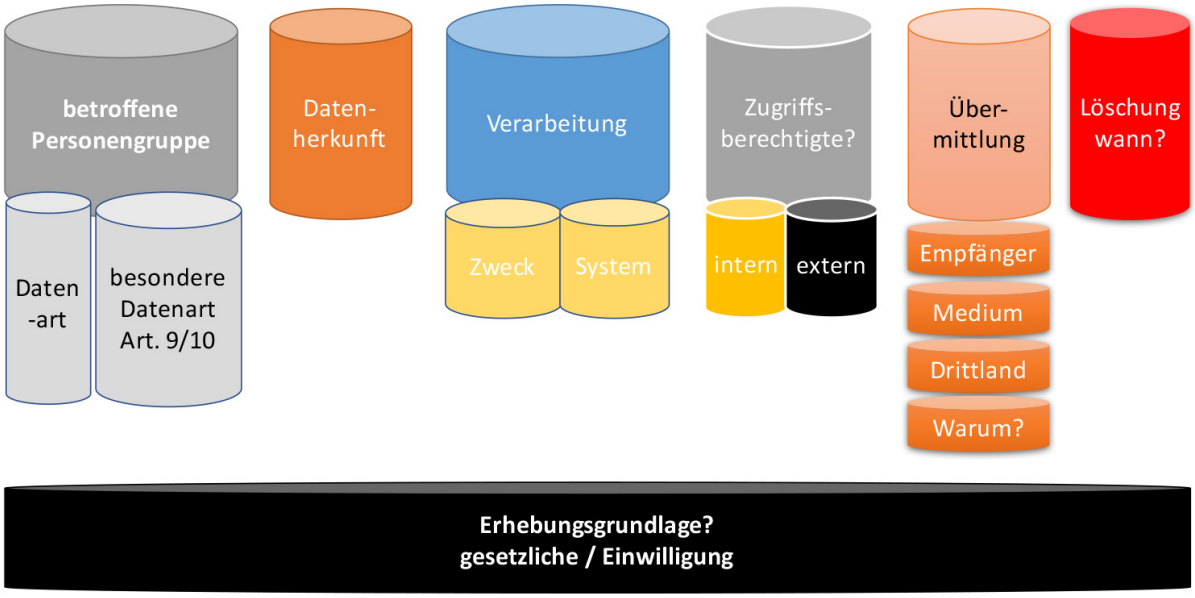
d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten

wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

(9) Der Verantwortliche holt gegebenenfalls den ***Standpunkt*** der ***betroffenen Personen*** oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

Dokumentationspflicht

Mit Gültigkeit der DSGVO ist keine Meldung mehr an das Datenverarbeitungsregister (DVR) zu erstatten und somit gehört auch die DVR-Nummer der Vergangenheit an. Stattdessen ist der Verantwortliche als auch der Auftragsverarbeiter verpflichtet, ein Verzeichnis über die Verarbeitungstätigkeiten (Verfahrensverzeichnis) zu führen.



Das Verfahrensverzeichnis des Verantwortlichen hat dabei grundlegend folgende Informationen zu beinhalten:

- Name und Kontaktdaten des Verantwortlichen und etwaigen Datenschutzbeauftragten
- Zweck der Verarbeitung (wir empfehlen auch die Rechtsgrundlage zu erfassen: Vorschrift, Einwilligung, ...)
- Beschreibung der Kategorien betroffener Personen (Kunden, Mitarbeiter, ...)
- Beschreibung der Kategorien personenbezogener Daten (Adressdaten, Geburtsdaten, ... -> wir empfehlen dies auf Basis der einzelnen Daten zu erstellen: Vorname, Nachname, Wohnstraße/Nr, PLZ, Ort, Geburtsdatum, ...)

- Kategorien der Empfänger (Steuerberater, Lohnverrechnung, Gebietskrankenkassen, Finanzamt, ...) inkl. Empfänger in Drittländern (Konzernmutter, ...) und Grund
- Etwaiger Übermittlungen an ein Drittland oder internationale Organisation (Dokumentierung geeigneter Garantien)
- Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen (gem. Art. 32, Abs. 1)
- Vorgesehene Löschfristen der verschiedenen Datenkategorien

Conclusio und Prüfung

Informieren Sie die betroffenen Personen über Ihre internen Abläufe und stellen Sie sicher, dass Sie geeignete Schutzmechanismen zum Schutze der Daten installiert haben. Erstellen Sie ein Verfahrensverzeichnis als Grundlage für sämtliche weiteren Schritte.

Prüfen Sie die folgenden Fragen:

Haben Sie die betroffenen Personen ordnungsgemäß über die Datenerhebung und Datenverarbeitung informiert? Haben Sie die betroffenen Personen über Ihre Rechte informiert? Ist die Sicherheit der Verarbeitung gewährleistet (Datenintegrität und Vertraulichkeit, Stand der Technik)? Haben Sie ein Löschkonzept? Haben Sie ein Backup-Konzept? Haben Sie die Risiken der Verarbeitung analysiert und etwaige daraus entstehenden Folgen abgeschätzt? Haben Sie ein vollständiges Verfahrensverzeichnis, das die Grundlage Ihrer Dokumentationspflicht darstellt?

Transparenz der Datensysteme

Die Transparenz Ihrer Datensysteme ist für Sie als Verantwortlicher die wesentliche Voraussetzung, die Rechte der betroffenen Personen wahrnehmen zu können. Denn, die Rechte der betroffenen Personen, sind Ihre Pflichten!

Im Prinzip müssen Sie zu jedem Zeitpunkt darüber Bescheid wissen (genau dazu dient auch das Verfahrensverzeichnis), wo genau welche Daten in Ihren Systemen verarbeitet und gespeichert werden. Sie haben sowohl die Auskunft darüber jederzeit erteilen, als auch die Korrektur dieser Daten uneingeschränkt gewährleisten zu können. Bei diesen Begehren der betroffenen Personen haben Sie 1 Monat Zeit für die Erledigung. Das klingt vielleicht nach ausreichend viel Handlungsspielraum, kann jedoch bei einigen parallelen Anfragen durchaus kritisch werden – vor allem dann, wenn Sie nicht genau wissen, wo und wie diese Begehren zu erfüllen sind.

Pflichten des Auftragsverarbeiters (Dienstleister)

Ihre Pflichten als Verantwortlicher haben Sie auch an Ihre Auftragsverarbeiter „weiter zu reichen“. Auch der Auftragsverarbeiter hat sich auf die Bestimmungen der DSGVO entsprechend vorzubereiten.

Dokumentationspflicht

Auch der Auftragsverarbeiter hat ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung (gem. Art. 30, Abs. 2 DSGVO) zu führen. Dieses Verzeichnis muss zumindest folgende Inhalte aufweisen:

- Name und Kontaktdaten des Auftragsverarbeiters und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, und eines etwaigen Datenschutzbeauftragten
- Kategorien der Verarbeitung, die im Auftrag des Verantwortlichen durchgeführt werden
- Etwaiger Übermittlungen an ein Drittland oder internationale Organisation (Dokumentierung geeigneter Garantien)
- Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen (gem. Art. 32, Abs. 1)

Datensicherheitsmaßnahmen

Entsprechende Maßnahmen zur Datensicherheit, sowie Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Privacy by Design, Privacy by Default) sind zu implementieren.

Die Sicherheit der Verarbeitung (Art. 32 DSGVO) gilt entsprechend auch für den Auftragsverarbeiter!

Warnpflicht und Meldepflicht

Der Auftragsverarbeiter unterliegt einer besonderen Warnpflicht. Er hat den Verantwortlichen unverzüglich zu informieren, falls eine Weisung nach eigener Auffassung gegen geltendes Datenschutzrecht verstößt.

Gemäß Art. 33, Abs. 2 DSGVO ist der Auftragsverarbeiter verpflichtet, dem Verantwortlichen unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten zu melden.

Risikoanalyse

Der Auftragsverarbeiter hat Risikoanalysen der Datenanwendungen durchzuführen und den Verantwortlichen bei der Erfüllung seiner Pflichten nach DSGVO zu unterstützen.

Sub-Auftragsverarbeiter

Der Auftragsarbeiter darf keinen weiteren Auftragsverarbeiter (Subunternehmen) ohne vorherige schriftliche Genehmigung des Verantwortlichen beauftragen! Über jegliche Veränderung in Bezug auf die Hinzuziehung oder Ersetzung anderer Auftragsverarbeiter ist bei Vorliegen einer allgemeinen schriftlichen Genehmigung der Verantwortliche zu informieren, wobei dieser seinerseits das Recht und die Möglichkeit hat, gegen jede Veränderung Einspruch zu erheben.

Vertragsbindung

Jegliche Zusammenarbeit bzw. Verarbeitung eines Auftragsverarbeiters erfolgt auf Grundlage eines Vertrages! Dieser hat folgende Bestandteile zu enthalten:

- Bindung an den Verantwortlichen
- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten
- Kategorien der betroffenen Personen
- Pflichten und Rechte des Verantwortlichen

Der Vertrag sieht insbesondere vor, dass der Auftragsverarbeiter

- personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeitet
- gewährleistet, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen
- alle erforderlichen Sicherheitsmaßnahmen ergreift
- vorherige schriftliche Genehmigung für Subunternehmen einholt
- den Verantwortlichen bei Beantwortung von Anträgen von Betroffenen unterstützt
- den Verantwortlichen bei Umsetzung und Einhaltung der Sicherheitsmaßnahmen und Meldepflichten unterstützt
- dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Pflichtgemäßheit zur Verfügung stellt und Überprüfungen durch den verantwortlichen ermöglicht

Etwaige Subunternehmen unterliegen denselben Datenschutzpflichten.

Gemäß Art. 28, Abs. 10 DSGVO (Auftragsverarbeiter) „... ***gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt,***

in Bezug auf diese Verarbeitung als Verantwortlicher." Damit ist das entsprechend hohe Strafmaß auch für Auftragsverarbeiter evident!

Notwendige Prozesse

Alle diese Pflichten aus der Datenschutz-Grundverordnung und dem Österreichischen Datenschutz-Anpassungsgesetz bedürfen klar definierter interner (und etwaiger externer) Prozesse, damit im Falle eines Begehrens seitens betroffener Personen oder auch eines Datenverlustes in Ihrem Unternehmen klar definiert ist, wer – was – wann – wie zu tun hat. Viele Unternehmen bereiten sich sogar mit Textbausteinen vor, die somit auch ein einheitliches Wording garantieren und sicherstellen, dass alle notwendigen Informationen bereitgestellt werden. Weiters sind alle Beteiligten der Verarbeitungskette entsprechend einzubinden!

Spezialthema: Bildverarbeitung (Bild und Video)

Bilddaten entsprechen der im Art. 9 der DSGVO genannten biometrischen Daten und sind sohin sensibel. Derartige sensible Daten (= besondere Kategorien personenbezogener Daten) dürfen nur unter eng eingegrenzten Voraussetzungen erhoben und verarbeitet werden. Das Datenschutz-Anpassungsgesetz 2018 erweitert hierbei den legitimen Anwendungsbereich ein wenig, da im 3. Abschnitt in den §§12 und 13 die Verwendung von Bild- oder Videoaufzeichnung unter besonderen Bedingungen für private Zwecke erlaubt wird.

§12 DSG2018: Zulässigkeit der Bildaufnahme

(1) Eine Bildaufnahme im Sinne dieses Abschnittes bezeichnet die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu ***privaten Zwecken***. Zur Bildaufnahme gehören auch dabei mitverarbeitete akustische Informationen. Für eine derartige Bildaufnahme gilt dieser Abschnitt, soweit nicht durch andere Gesetze Besonderes bestimmt ist.

(2) Eine Bildaufnahme ist unter Berücksichtigung der Vorgaben gemäß § 13 zulässig, wenn

1. sie im lebenswichtigen Interesse einer Person erforderlich ist,

2. die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat,

3. sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt ist, oder

4. im ***Einzelfall überwiegende berechtigte Interessen des Verantwortlichen*** oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist.

(3) Eine Bildaufnahme ist gemäß Abs. 2 Z 4 insbesondere dann zulässig, wenn

1. sie dem ***vorbeugenden Schutz von Personen oder Sachen auf privaten Liegenschaften***, die ***ausschließlich vom Verantwortlichen genutzt*** werden, dient, und räumlich nicht über die Liegenschaft hinausreicht, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen,

2. sie für den ***vorbeugenden Schutz von Personen oder Sachen an öffentlich zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen***, aufgrund ***bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotenzials*** erforderlich ist und ***kein gelinderes geeignetes Mittel*** zur Verfügung steht, oder

3. sie ein privates Dokumentationsinteresse verfolgt, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist.

(4) Unzulässig ist

1. eine Bildaufnahme ohne ausdrückliche Einwilligung der betroffenen Person in deren höchstpersönlichen Lebensbereich,

2. eine Bildaufnahme zum Zweck der Kontrolle von Arbeitnehmern,

3. der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten mit anderen personenbezogenen Daten oder

4. die Auswertung von mittels Bildaufnahmen gewonnenen personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) als Auswahlkriterium.

§13 DSG2018: Besondere Datensicherheitsmaßnahmen und Kennzeichnung

(1) Der Verantwortliche hat dem ***Risiko des Eingriffs angepasste geeignete Datensicherheitsmaßnahmen*** zu ergreifen und dafür zu sorgen, dass der Zugang zur Bildaufnahme und eine nachträgliche Veränderung derselben durch Unbefugte ausgeschlossen ist.

(2) Der ***Verantwortliche*** hat – außer in den Fällen einer Echtzeitüberwachung – ***jeden Verarbeitungsvorgang zu protokollieren***.

(3) Aufgenommene personenbezogene ***Daten sind vom Verantwortlichen zu löschen***, wenn sie für den Zweck, für den sie ermittelt wurden, nicht mehr benötigt werden und keine andere gesetzlich vorgesehene Aufbewahrungspflicht besteht. ***Eine länger als 72 Stunden andauernde Aufbewahrung muss verhältnismäßig sein und ist gesondert zu protokollieren und zu begründen***.

(4) Die Abs. 1 bis 3 finden keine Anwendung auf Bildaufnahmen nach § 12 Abs. 3 Z 3.

(5) Der Verantwortliche einer Bildaufnahme hat diese geeignet zu kennzeichnen. Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen, es sei denn, dieser ist den betroffenen Personen nach den Umständen des Falles bereits bekannt.

(6) Die Kennzeichnungspflicht gilt nicht in den Fällen des § 12 Abs. 3 Z 3 und für zeitlich strikt zu begrenzende Verarbeitungen im Einzelfall, deren Zweck ausschließlich mittels einer verdeckten Ermittlung erreicht werden kann, unter der Bedingung, dass der Verantwortliche ausreichende Garantien zur Wahrung der Betroffeneninteressen vorsieht, insbesondere durch eine nachträgliche Information der betroffenen Personen.

(7) Werden entgegen Abs. 5 keine ausreichenden Informationen bereitgestellt, kann jeder von einer Verarbeitung potenziell Betroffene vom Eigentümer oder Nutzungsberechtigten einer Liegenschaft oder eines Gebäudes oder sonstigen Objekts, von dem aus eine solche Verarbeitung augenscheinlich ausgeht, Auskunft über die Identität des Verantwortlichen begehren. Die unbegründete Nichterteilung einer derartigen Auskunft ist einer Verweigerung der Auskunft nach Art. 15 DSGVO gleichzuhalten.

Conclusio

Video-Überwachung ist möglich

Die Video-Überwachung von eigenen Geschäftsräumen (die dem Hausrecht des Verantwortlichen unterliegen!) ist somit in Bezug auf Erkennung von und Prävention gegen Strafrechtsdelikten unter der Voraussetzung geeigneter Datensicherheitsmaßnahmen, entsprechender Protokollierung, aktiver Löschung nicht benötigter Daten und Kennzeichnung der Bilddaten möglich.

Ausblick auf Kapitel 3 und Live-Event

Die Hälfte des Bildungsthemas ist erreicht, die Probleme und deren Auswirkungen haben wir durchgearbeitet. Es wird nun Zeit, sich an den Lösungen und Umsetzungsempfehlungen zu orientieren.

Kapitel 3: Umsetzungsbereiche und Lösungen

„Hier werden Sie geholfen“, wir gehen in die praktikable Umsetzung mit Lösungen, die Sie nicht wieder vor neue Probleme stellt. Wie gehen Sie konkret vor, um zu Ihrem Verarbeitungsverzeichnis zu gelangen, wie erstellen Sie Ihr Lösch- und Backupkonzept? Wie entscheiden Sie, welche Daten Sie in Zukunft noch erheben werden, wie genau bereiten Sie Zustimmungserklärungen vor? Welche Vertragsbestandteile sind für Sie wichtig, damit Sie Ihre externen IT-Dienstleister entsprechend mit in die Verantwortung nehmen? Welche Textbausteine können Sie in Auskunftsbegehren verpacken und welche Entscheidungsgrundlagen sind zu erarbeiten?

Live-Event

„Hands-on“ am Live-Event: In Kleingruppen erarbeiten Sie sich Ihre Grundlagen und werden von Experten bei Ihren Fragen und ersten Schritten begleitet. Sie werden nach dem Live-Event alle notwendigen Informationen und Anleitungen haben, um in Ihrem Unternehmen die DSGVO richtig umsetzen zu können.

Vielleicht kommen Sie bereits mit Ihren vorbereiteten Unterlagen zum Live-Event und gehen diese gemeinsam mit uns durch? Ihre konkreten Fragen sind dabei herzlich willkommen!