Datenschutzgrundverordnung – die wichtigsten Punkte

I. Allgemeines

Die DSGVO gilt ab dem **25. Mai 2018** unmittelbar in jedem EU-Mitgliedstaat. Die Verordnung
gewährt Schutz für die Verarbeitung der personenbezogenen Daten natürlicher Personen.
Die DSGVO gilt für die automatisierte Verarbeitung personenbezogener Daten und für nichtautomatisierte
Verarbeitung, die in einem Dateisystem gespeichert sind bzw. werden sollen.
Betroffen ist daher auch die manuelle Verarbeitung von personenbezogenen Daten, wie Akten oder Aktensammlungen, die nach bestimmten Kriterien geordnet sind.

II. Die wichtigsten Begriffsbestimmungen

- **personenbezogene Daten**

Darunter sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen zu verstehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

- **Verantwortlicher**

Ist jede 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. Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche bzw.
können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

- **Auftragsverarbeiter**

Ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

- **Empfänger**

Ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

- **Gesundheitsdaten**

Personenbezogen 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.

III. Grundsätze der Verarbeitung personenbezogender Daten

- **Rechtmäßigkeit :**

Daten dürfen nur entsprechend dem Gesetz verarbeitet werden.

- **Transparenz:**

Die Verarbeitung personenbezogener Daten muss für Betroffene nachvollziehbar sein. Erforderlich sind daher verständliche und vollständige Datenschutzerklärungen.

- **Zweckbindung:**

Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben worden sind.

- **Datenminimierung:**

Datenverarbeitungen müssen auf das notwendige Maß beschränkt werden. Eine Datenerhebung auf Vorrat ist verboten.

- **Integrität und Vertraulichkeit:**

Daten müssen durch technische und organisatorische Maßnahmen von unbefugter Verarbeitung, Zerstörung, Veränderung oder Verlust geschützt werden.

IV. Grundsatz der Rechtmäßigkeit der Verarbeitung nach Treu und Glauben

Die Verarbeitung personenbezogener Daten erfolgt demnach nur dann rechtmäßig, wenn

- entweder die betroffenen Person ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat
- oder die Verarbeitung für die **Erfüllung eines Vertrages**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist
- oder die Verarbeitung zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich ist
- oder die Verarbeitung erforderlich ist, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen
- oder die Verarbeitung zur **Wahrung der berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und
- Grundfreiheiten der betroffenen Person nicht überwiegen, insbesondere dann, wenn es
- sich bei der betroffenen Person um ein Kind handelt.

V. Verarbeitung von sensiblen Daten

Besondere Vorsicht ist bei der Verarbeitung von sensiblen Daten geboten. Hier sind strengere Voraussetzungen zu beachten. Zu den sensiblen Daten gehören:

- Daten über die rassische und ethnische Herkunft
- Daten betreffend die religiöse oder weltanschauliche Überzeugung
- Gewerkschaftszugehörigkeit
- genetische Daten
- biometrische Daten
- **Gesundheitsdaten**
- Daten zum Sexualleben oder der sexuellen Orientierung

Grundsätzlich ist die Verarbeitung von sensiblen personenbezogenen Daten untersagt. Damit die Verarbeitung zulässig ist, muss zumindest einer der im Gesetz genannten Erlaubnistatbestände vorliegen. In folgenden Fällen gilt das Verbot über die Verarbeitung sensibler Daten daher nicht:

1. Bei den sensiblen Daten handelt es sich um **bereits veröffentlichte Daten**. Die Daten müssen von der betroffenen Person offensichtlich öffentlich gemacht worden sein.

2. Die betroffene Person hat in die Verarbeitung **ausdrücklich eingewilligt**. Hier ist zu beachten, dass die ausdrückliche Einwilligung für einen oder mehrere festgelegte **Zwecke** erfolge muss.
3. Die Verarbeitung dient der Erfüllung von Rechten und Pflichten aus dem Arbeitsrecht oder dem Recht der sozialen Sicherheit.
4. Die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben.
5. Die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten. Die Verarbeitung darf sich in diesem Fall jedoch ausschließlich auf die Mitglieder oder ehemaligen Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten beziehen und dürfen die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Person nach außen offengelegt werden.
6. Die Verarbeitung dient der Durchsetzung oder Abwehr von Rechtsansprüchen.
7. Die Verarbeitung ist auf der Grundlage des Unionsrechts oder des nationalen Rechts, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblich öffentlichen Interesses erforderlich.
8. Die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialberich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaates oder aufgrund eines Vertrages mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich, dass diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaates oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.
9. Die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleitung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arbeitsmitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimbisses, vorsieht, erforderlich.
10. Die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaates, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person

vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich.

VI. Pflichten des Verantwortlichen bzw. Auftragsverarbeiters und Rechte der betroffenen Person

1. Informationspflicht:
   Bereits zum Zeitpunkt der Datenerhebung soll die betroffene Person darüber informiert werden, welche sie betreffenden personenbezogenen Daten verarbeitet werden. Über folgende Punkte ist die betroffene Person zu informieren: Name und Kontaktdaten des Verantwortlichen, allenfalls Daten des Datenschutzbeauftragten, die Zwecke für die die Daten verarbeitet werden und die Rechtsgrundlage; allenfalls die berechtigten Interessen, auf welchen die Verarbeitung beruht; die Empfänger, die Speicherdauer, Belehrung über das Recht auf Auskunft, Berichtigung, Löschung, Widerspruch und Einschränkung; bei Einwilligungen ist über das Recht des jederzeitigen Widerrufs aufzuklären, Beschwerderecht.

2. Auskunftsrecht:
   Jede betroffene Person hat ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind. Die Auskunft muss in Form einer unentgeltlichen Kopie der verarbeiteten Daten zur Verfügung gestellt werden. Hier ist die Frist zur Auskunftserteilung von **einem Monat** zu beachten. Diese Frist kann jedoch begründet um weitere zwei Monate verlängert werden.

3. Recht auf Berichtigung:
   Jede betroffene Person kann die Berichtigung oder Vervollständigung der Daten begehren.

4. Recht auf Löschung und Vergessen:
   Dies kann begehrt werden, wenn die Daten für die Zwecke, für die sie erhoben bzw. verarbeitet wurden, nicht mehr notwendig sind. Oder wenn die Einwilligung widerrufen wird und eine anderweitige Rechtsgrundlage für die Verarbeitung nicht vorliegt. Weiters wenn Widerspruch eingelegt wird oder die Daten unrechtmäßig verarbeitet wurden.

5. Recht auf Einschränkung der Verarbeitung:
   Dies kann verlangt werden, wenn die Richtigkeit der personenbezogenen Daten bestritten wird oder wenn statt Löschung Einschränkung verlangt wird.

6. Mitteilungspflicht im Zusammenhang mit der Berichtigung, Löschung oder Einschränkung der Verarbeitung:
   Der Verantwortliche hat allen Empfängern einer Datenverarbeitung eine Berichtigung, Löschung und Einschränkung mitzuteilen, außer dies ist unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden.

7. Recht auf Datenübertragbarkeit:

   Dieses Recht besteht, wenn die Datenverarbeitung auf Einwilligung oder auf einem Vertrag beruht und die Verarbeitung mit Hile automatisierter Verfahren erfolgt.

8. Widerspruchsrecht
   Eine betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund einer Verarbeitung die zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder zur Wahrung

berechtigter Interessen erforderlich ist, Widerspruch einzulegen. Sollte es daher zu einem solchen Widerspruch kommen und dieser berechtigt sein, bedeutet dies die gänzliche Unzulässigkeit der weiteren Verarbeitung der Daten.

VII. Verzeichnis der Verarbeitungstätigkeit

Der Gesetzgeber möchte durch erhöhte Dokumentationspflichten, dass Unternehmen sich mehr Gedanken um den Datenschutz machen.

Es gibt zwar wenige Ausnahmen von der Verpflichtung zur Führung eines Verarbeitungsverzeichnisses. Wir empfehlen jedoch jedem, ein derartiges Verzeichnis zu führen.

Es bestehen inhaltliche Vorgaben für die Führung des Verzeichnisses, die Form wie das Verzeichnis geführt wird, kann jedoch frei gewählt werden.

Das Verzeichnis hat insbesondere folgende Angaben zu enthalten:
1. Grundangaben zum Unternehmen
2. die einzelnen Verarbeitungstätigkeiten
3. Dokumentation der einzelnen Verarbeitungstätigkeiten
4. technische und organisatorische Maßnahmen: Hier ist darzustellen, welche technischen und organisatorischen Maßnahmen ergriffen wurden, um die verarbeiteten personenbezogenen Daten vor Kenntnisnahme durch Unbefugte, Zerstörung oder Missbrauch zu schützen.

Dieses Verzeichnis ist regelmäßig zu überprüfen und aktuell zu halten (Überprüfung mindestens einmal im Jahr!).

Die Pflicht zur Führung eines Verarbeitungsverzeichnisses trifft sowohl den Verantwortlichen als auch den Auftragsverarbeiter. Haben Sie daher einerseits Daten als Verantwortlicher und auch Daten, die sie von einem anderen Unternehmen zur Auftragserfüllung erhalten haben, sind Sie zur Führung von zwei Verzeichnissen verpflichtet.

VIII. Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung ist jedenfalls durchzuführen, wenn

- Profiling als Grundlage für schwerwiegende Entscheidungen, wie zum Beispiel Bonitätsbeurteilung, eingesetzt wird.
- im großen Umfang sensible Daten verarbeitet werden
- Videoüberwachung eingesetzt wird.

Umfangreich ist eine solche Verarbeitung, wenn eine Vielzahl von Personen betroffen ist und auch mehrere Personen (Mitarbeiter) auf diese Daten zugreifen können.

Hier sind die möglichen Risiken aufzuzählen und ist in einer Dokumentation darzulegen, wie

Sie diese abwenden können. Sollte eine Abwendung der Risiken nicht möglich sein, ist eine Meldung an die zuständige Datenschutzaufsichtsbehörde zu erstatten.

IX. Datenweitergabe

Zumeist werden Daten für eine weitere Auftragserfüllung weitergegeben. Das bedeutet, ein Unternehmen beauftragt ein anderes Unternehmen, personenbezogene Daten auf seine Anweisung hin zu verarbeiten (IT, Steuerberater, etc.). Auch hier sind gewisse Vorschriften zu beachten. Eine Weitergabe ist unter anderem zulässig, wenn:

- eine **gültige Einwilligung** der betroffenen Person vorliegt (kann jedoch jederzeit widerrufen werden und unterliegt strengen Anforderungen)
- die **Weitergabe zur Vertragserfüllung** erfolgt (zB Weitergabe der Daten an eine Bank zwecks Zahlung)
- ein berechtigtes Interesse an der Weitergabe von Daten vorliegt.

Die betroffene Person ist jedoch über die Weitergabe der Daten in Kenntnis zu setzen.

X. Erstellung eines Auftragsverarbeitungsvertrages bei der Datenweitergabe

Im Falle einer Datenweitergabe ist verpflichtend ein schriftlicher Vertrag zwischen den beiden Unternehmen abzuschließen.

In diesem Vertrag muss sich der Auftragnehmer dazu verpflichten, die Daten nur entsprechend dem Auftrag und nach Weisung zu verarbeiten. Weiters sind die Mitarbeiter zur Vertraulichkeit zu verpflichten und sind weitere Regelungen im Vertrag zu treffen. Diesbezüglich empfehlen wir jedenfalls die Erstellung durch einen Rechtsanwalt bzw. den Vertrag zumindest rechtlich überprüfen zu lassen.

XI. Mitarbeiter des Verantwortlichen

Jede einem Verantwortlichen oder einem Auftragsverarbeiter unterstellte Person (also Ihre Mitarbeiter), die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten.

Mitarbeiter dürfen personenbezogene Daten nur aufgrund einer **ausdrücklichen Anordnung** ihrer Arbeitgeber übermitteln, anderseits darf einem Mitarbeiter aus einer Verweigerung der Befolgung einer Anordnung zu einer unzulässigen Datenübermittlung kein Nachteil erwachsen. **Diese Verpflichtung muss vertraglich erfolgen**. Das Datengeheimnis ist auch nach Beendigung des Arbeitsverhältnisses zu wahren.

Hier ist daher der Abschluss einer schriftlichen Vereinbarung mit den Mitarbeitern erforderlich.

XII. Privacy by Design und Privacy by Default

Diese Bestimmungen legen fest, dass Datenschutzmaßnahmen nach dem Stand der Technik bereits in die konzeptionelle Entwicklung von Produkten und Verfahren einbezogen werden müssen.
Privacy by Default bedeutet, dass zum Beispiel bei Voreinstellungen bei Geräten oder bei Online-Plattformen standardmäßig die höchste Datenschutzstufe gewährleistet sein muss.

Der Verantwortliche hat zum Nachweis der Einhaltung der DSGVO eine interne Strategie festzulegen, die Maßnahmen zur Einhaltung der Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen umfassen.

Diesem Grundsatz kann zum Beispiel durch Pseudonymisierung der Daten, durch Datenminimierung und zeitliche Beschränkung der Speicherdauer etc. entsprochen werden.

Hier empfehlen wir die Überprüfung und Beratung durch einen IT-Experten.

XIII. Meldepflicht

Tritt der Fall ein, dass es beim Verantwortlichen zu einer Verletzung des Schutzes personenbezogener Daten gekommen ist, so hat der Verantwortliche unverzüglich zu reagieren.

Sollte der Verlust zu einem Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen führen, hat der Verantwortliche der Datenschutzbehörde unverzüglich, **binnen 72 Stunden**, eine Meldung zu erstatten.

Sofern ein **hohes Risiko** für die persönliche Rechte und Freiheiten der betroffenen Personen besteht, hat der Verantwortliche zusätzlich eine Meldung an die betroffenen Personen durchzuführen.

Eine Meldepflicht besteht sohin dann nicht, wenn die Verletzung des Schutzes personenbezogener Date voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

XIV. Datenschutzbeauftragte

Ein Datenschutzbeauftragter ist verpflichtend zu bestellen:

- von Behörden und öffentlichen Stellen
- von Verantwortlichen, deren Kerntätigkeit eine umfangreiche regelmäßige Überwachung betroffener Personen umfasst
- von Verantwortlichen, deren Kerntätigkeit eine umfangreiche Verarbeitung besonderer Kategorien von Daten umfasst.

Im Fall einer verpflichtenden Bestellung sind die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und ist dieser bei der Datenschutzbehörde zu melden.

Ein Datenschutzbeauftragter sollte über Fachwissen in Bezug auf

- nationales und europäisches Datenschutzrecht
- Kenntnisse in den Bereichen IT und Datensicherheit
- Branchenkenntnisse
- Fähigkeit, die Datenschutzstruktur im Unternehmen zu fördern
- Ressourcen

verfügen.

Zu den Aufgaben des Datenschutzbeauftragten zählen:

- Beratung des Verantwortlichen hinschlich der Datenschutzpflichten
- Beratung bei der Datenschutz-Folgenabschätzung
- Überwaschung der Bestimmungen der DSGVO
- Zusammenarbeit mit der Datenschutzbehörde

Stellung und Pflichten des Datenschutzbeauftragten:

- Der Datenschutzbeauftragte darf keine Aufgaben innerhalb des Unternehmens wahrnehmen, die es mit sich bringen, dass er Zwecke und Mittel für die Verarbeitung festgelegt.
- Der Datenschutzbeauftragte ist in alle mit dem Schutz personenbezogener Daten zusammenhänge Fragen einzubinden.
- Er muss unabhängig sein.
- Keine Abberufung und Benachteiligung eines Datenschutzbeauftragten wegen Erfüllung seiner Aufgaben.
- Geheimhaltungsverpflichtung.

XV. Geldbußen

Zuletzt möchte ich nochmal auf die Geldbußen der DSGVO hinweisen. Art 83 Abs 5 lit a DSGVO normiert eine Geldbuße in der Höhe von bis zu EUR 20.000.000,00 bzw. 4% des gesamten weltweit erzielten Jahresumsatzes, wenn die Grundsätze er Datenverarbeitung nicht beachtet werden. Bereits eine fehlende Dokumentation hinsichtlich der Eihaltung der Grundsätze der Datenverarbeitung kann daher für sich genommen zur Verhängung einer Geldbuße führen.

Ich ersuche daher die Umsetzung der DSGVO ernst zu nehmen und stehe Ihnen gerne für Fragen und eine weitere Beratung zur Verfügung.

XVI. Welche Maßnahmen sollten daher bis 25.05.2018 umgesetzt werden

- Die Datenverarbeitungsprozesse sollten auf ihre Zulässigkeit überprüft werden.
- Erstellung des Verfahrensverzeichnisses
- Überprüfung, ob die technische-organisatorische Sicherheit der Daten betroffener Personen erfüllt wird und gegebenenfalls eine Datenschutzfolgenabschätzung durchführen
- Prüfen, ob die Bestellung eines Datenschutzbeauftragten erforderlich ist
- Überprüfen ob allfällige Datenübermittlungsvorgänge zulässig sind
- Überprüfen, ob ein Beschwerdemanagement für die Fälle der Geltendmachung von Betroffenenrechten eingerichtet ist
- Datenschutzerklärungen aktualisieren
- Mitarbeiter schulen und falls nicht vorhanden Vertraulichkeitserklärungen unterschreiben lassen