DSGVO – WAS IST ZU TUN?

Ab dem 25.5.2018 ist die Datenschutzgrundverordnung ("DSGVO") in allen Mitgliedstaaten der EU – praktisch über Nacht – anwendbar. Bis zu diesem Datum haben alle Unternehmen, die personenbezogene Daten verarbeiten, umfangreiche Umsetzungsmaßnahmen zu treffen, um nicht den hohen Strafdrohungen ausgesetzt zu sein. Für die Praxis lassen sich folgende wesentliche To Do's zusammenfassen:

1. **Prüfung sämtlicher Datenverarbeitungen**: Rechtzeitig alle Informationen über die aktuellen Datenverarbeitungen zusammentragen, um zu prüfen, ob diese zum eigenen Zweck oder im Auftrag eines Dritten durchgeführt werden und ob sie datenschutzrechtlich zulässig sind.

   Zulässig sind Datenverarbeitungen grundsätzlich in folgenden Fällen:

   > **Einwilligung**: Die betroffene Person hat ihre Einwilligung zur Verarbeitung abgegeben. Dabei sind die strengen Voraussetzungen der DSGVO einzuhalten. Diese Rechtsgrundlage ist insbesondere bei der Verarbeitung von Daten zu Marketingzwecken (zB Newsletter) relevant.
   > **Vertragserfüllung**: Die Datenverarbeitung ist zur Erfüllung des Vertrages mit dem Betroffenen erforderlich.
   > **Gesetzliche Ermächtigung/Verpflichtung**: Die Datenverarbeitung ist gesetzlich vorgeschrieben.
   > **Berechtigte Interessen:** Die Datenverarbeitung ist zur Wahrung der berechtigten Interessen des Datenverarbeiters erforderlich. Die österreichische Datenschutzbehörde und die Rechtsprechung sind in diesem Punkt allerdings sehr streng.

2. **Verarbeitungsverzeichnis** mit folgenden Informationen erstellen:

   > Name und Kontaktdaten des Datenverarbeiters (und des Vertreters sowie gegebenenfalls des Datenschutzbeauftragten);
   > Zwecke jeder einzelnen Datenverarbeitung;
   > Kategorien betroffener Personen;
   > Kategorien verarbeiteter Daten;
   > Empfänger oder Kategorien von Empfängern (am besten aufgeteilt in interne Zugriffsberechtigte, externe Verantwortliche und externe Auftragsverarbeiter);
   > Aufbewahrungsdauer der verschiedenen Datenkategorien;
   > allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen.

   Auftragsverarbeiter, die Daten lediglich im Auftrag eines Verantwortlichen verarbeiten, müssen folgende Informationen dokumentieren:

   > Name und Kontaktdaten (und des Vertreters sowie gegebenenfalls des Datenschutzbeauftragten);

> Name und Kontaktdaten jedes einzelnen Verantwortlichen, für den Daten verarbeitet werden;
> Kategorien der für jeden Verantwortlichen durchgeführten Verarbeitungen;
> allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen.

3. **Bestehende Einwilligungen überprüfen und aktualisieren**: Insbesondere muss genau geprüft werden, ob folgende Voraussetzungen erfüllt sind:

> Klare und einfache Sprache
> Umfassende Information des Betroffenen (also etwa des Empfängers eines Newsletters) über
    - die konkret verarbeiteten Daten (zB Name, Email Adresse),
    - den Zweck der Verarbeitung (zB detaillierte Beschreibung der zu erwartenden Werbeinhalte sowie die konkrete Art der Kontaktaufnahme – etwa per E-Mail)
    - etwaige dritte Datenempfänger (inkl Name und Anschrift) und
    - die jederzeitige Möglichkeit, die Einwilligung zu widerrufen.
> Freiwilligkeit: Insbesondere darf die Erfüllung eines Vertrages nicht von der Abgabe einer Einwilligungserklärung abhängig gemacht werden. Außerdem sind nach aktueller Auslegung der DSGVO Zustimmungen in AGB kritisch.
> Nachweisbarkeit: Die Einwilligungserklärung muss jederzeit nachweisbar sein.

4. **Datenschutzbestimmungen überarbeiten bzw. erstellen**: Alle Betroffenen sind nach der DSGVO umfassend über die jeweiligen Datenverarbeitungen zu informieren. In der Praxis werden diese Informationen üblicherweise über Datenschutzbestimmungen oder Datenschutzerklärungen (Privacy Policies) zur Verfügung gestellt. Die Details dieser Datenschutzerklärungen müssen jeder Person, deren Daten verarbeitet werden (zB Kunden oder auch Mitarbeiter), in klarer und einfacher Sprache zur Verfügung gestellt werden. Insbesondere muss jeder Betroffene über (i) den Zweck der Verarbeitung, (ii) die Rechtsgrundlage, (iii) etwaige Empfänger der Daten, (iv) die Speicherdauer und (v) Betroffenenrechte informiert werden.

5. **Schriftliche Vereinbarungen mit externen Auftragsverarbeitern** nach den Vorgaben der DSGVO abschließen: Verarbeiten Dritte als Auftragsverarbeiter personenbezogene Daten für einen anderen (zB IT Provider oder Softwarehersteller), muss eine schriftliche Vereinbarung mit bestimmten Mindestanforderungen abgeschlossen werden. In diesem Vertrag sind etwa die konkreten Datenverarbeitungen genau zu beschreiben und die wesentlichen Pflichten der Parteien festzulegen.

6. **Prüfung, ob ein Datenschutzbeauftragter zu bestellen ist** und Dokumentation der Entscheidungsfindung: Unabhängig von der Größe eines Unternehmens ist ein Datenschutzbeauftragter zu bestellen, wenn die Kerntätigkeit

> eine umfangreiche regelmäßige und systematische Überwachung der Betroffenen darstellt; oder
> in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten (sensible oder strafrechtlich relevante Daten) liegt.

7. Überprüfen, ob für bestimmte Verarbeitungen eine **Datenschutz-Folgenabschätzung** durchzuführen ist: Werden Datenverarbeitungen durchgeführt, die (voraussichtlich) besonders riskant sind, ist vorab eine Folgenabschätzung durchzuführen. Damit werden in einen ersten Schritt die potentiellen Risiken identifiziert und bewertet. Daran anschließend sind für jedes identifizierte Risiko die getroffenen Sicherheitsmaßnahmen zu beschrieben.

8. Implementierung eines Standardprozesses, wie **Betroffenenrechte** (fristgerecht) gewahrt werden können und Vorbereitung entsprechender Vorlagen für die Erledigung:

   Alle Betroffenen haben nach der DSGVO insbesondere folgende Rechte:

   > Recht auf Auskunft: Jeder Betroffene kann jederzeit und ohne Begründung Auskunft über die verarbeiteten Datenkategorien, die Zwecke der Verarbeitung, etwaige Empfänger, die Speicherdauer sowie die Herkunft der Daten verlangen.
   > Recht auf Berichtigung: Unrichtige Daten sind auf Antrag des Betroffenen zu berichtigen; unvollständig Daten sind zu vervollständigen.
   > Recht auf Löschung ("Vergessenwerden"): Auf Antrag des Betroffenen müssen seine Daten dauerhaft gelöscht werden. Dies gilt allerdings nur, sofern die Daten nicht mehr erforderlich sind, der Betroffene seine Einwilligung widerrufen hat oder die Daten unrechtmäßig verarbeitet werden. Betroffene Personen haben daher kein unbegründetes oder grenzenloses Recht auf Löschung.

   Neben diesen in der Praxis wichtigsten Betroffenenrechten sieht die DSGVO zusätzlich ein Recht auf Einschränkung der Verarbeitung sowie auf Datenübertragbarkeit und ein Widerspruchsrecht vor.

9. Überprüfen, ob und welche **Datensicherheitsmaßnahmen** bereits implementiert wurden und gegebenenfalls nachjustieren: Bei der Datenverarbeitung sind angemessene technische und organisatorische Datensicherheitsmaßnahmen zu treffen. Die DSGVO nennt hier etwa die Pseudonymisierung und Verschlüsselung oder die Fähigkeit, Daten nach einem Zwischenfall rasch wiederherzustellen. Im Detail ist auf die best practice abzustellen. Relevant sind hier insbesondere ISO Normen (vor allem die ISO 27000-Familie) sowie das österreichische Informationssicherheitshandbuch (abrufbar unter https://www.sicherheitshandbuch.gv.at/).