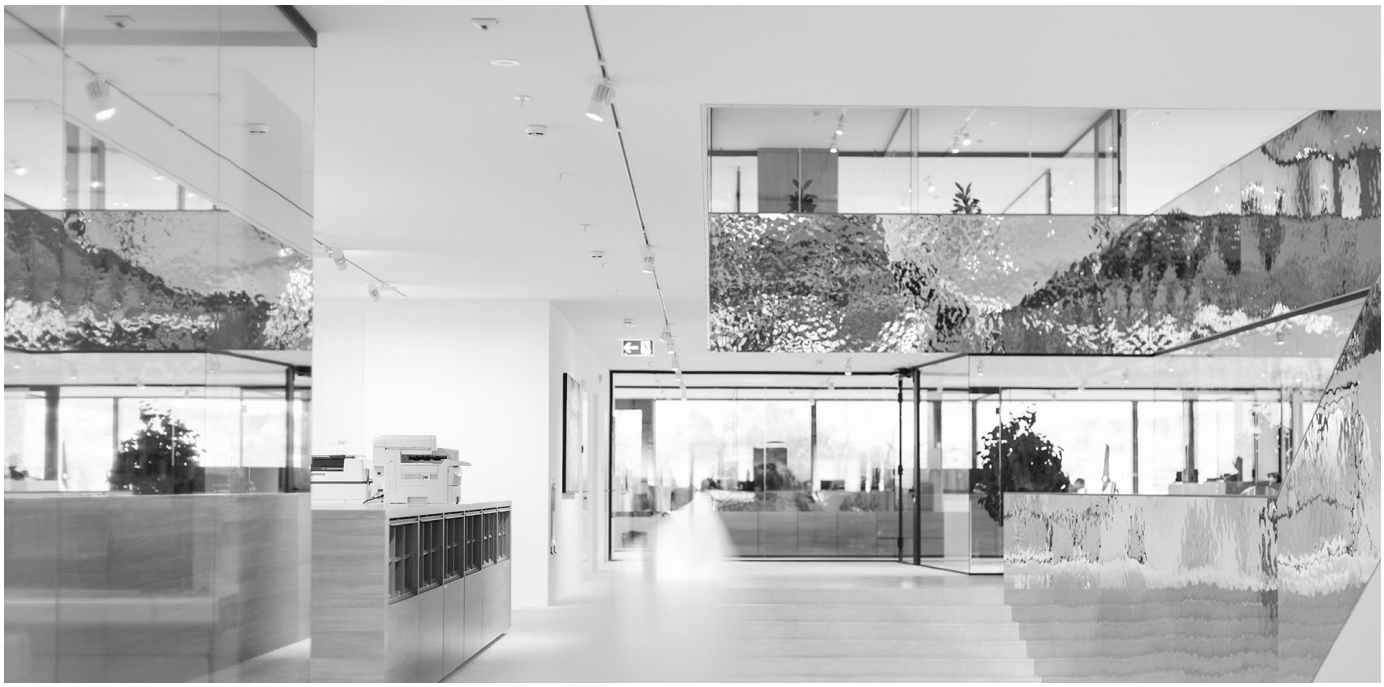
GASSER PARTNER

RECHTSANWÄLTE

Datenschutzgrundverordnung (DS-GVO)

Das Wichtigste für Liechtensteinische Unternehmen auf einen Blick



Einleitung

Mit 25. Mai 2018 tritt die Datenschutzgrundverordnung (DS-GVO) in Kraft und vereinheitlicht das materielle Datenschutzrecht innerhalb der Europäischen Union. Noch ist die DS-GVO in Liechtenstein nicht umgesetzt, dies wird aber unweigerlich durch Übernahme in den EWR Rechtsbestand geschehen. Die Übernahme in den EWR Rechtsbestand steht unmittelbar (spätestens im Juli 2018) bevor. Darüber hinaus, ist die DS-GVO, gemäss Art 3 Abs 2 lit a schon ab 25.5.2018 von jenen Unternehmen in Liechtenstein zu beachten, die Waren oder Dienstleistungen in der EU anbieten oder auch nur Daten von EU Bürgern verarbeiten. Neben Industrie- und Dienstleistungsunternehmen wird dies im Regelfall auch die Treuhänderbranche betreffen.
Es bleibt daher nur wenig Zeit, die Umsetzung der erheblichen Compliance-Anforderungen vorzubereiten, die mit oben genanntem Stichtag schlagend werden.

Die praktischen Auswirkungen, die sich durch DS-GVO und die sich daraus ergebende enorme Veränderung des datenschutzrechtlichen Umfeldes ergeben werden, können gar nicht überschätzt werden. Diese Einführung soll für die neuen datenschutzrechtlichen Verpflichtungen sensibilisieren und die massiven, vor allem finanziell drakonischen Strafen von bis zu **EUR 20‘000‘000.00** im Falle von Versäumnissen betroffener Unternehmen auf diesem Gebiet darstellen.

Datenschutz als Grundrecht

Ziel der DS-GVO ist es, das Recht auf Datenschutz als Grundrecht zu verankern und somit die Rechte der Betroffenen, deren Daten gesammelt werden, zu stärken. Auf die liechtensteinischen Unternehmen und Treuhänder rollt mit der DS-GVO eine Regulierungslawine zu, die zu einem immensen Mehraufwand an Bürokratie im Bereich der Compliance führen wird.
Der zentrale Regelungsinhalt der DS-GVO sind die Bestimmungen über das Verarbeiten von personenbezogenen Daten. Der Begriff „Verarbeiten" ist hier sehr weit gefasst und beinhaltet jegliche Erhebung, Bearbeitung, Speicherung, Anpassung, Veränderung, Abfrage, Verwendung, Übermittlung und Löschung von personenbezogenen Daten. Als „personenbezogen" werden Daten immer dann eingestuft, wenn sie dazu geeignet sind, eine Person zu identifizieren. Dies ist grundsätzlich bei fast allen persönlichen Daten der Fall, sei es der Name, das Geburtsdatum, die Sozialversicherungsnummer oder unter Umständen die IP-Adresse des Homepagebesuchers. Unter „sensiblen Daten" werden weiters personenbezogene Daten verstanden, die Rückschlüsse über Herkunft, politische Einstellungen, Gewerkschaftszugehörigkeit oder Religion geben. Auch Daten über Genetik, Biometrie, Gesundheit, Sexualleben und sexuelle Orientierung fallen darunter.

Grundsätze bei der Datenverarbeitung

Bei der Verarbeitung von personenbezogenen Daten ist zunächst zu beachten, jede Verarbeitung auf das unbedingt erforderliche Mass zu minimieren und das Speichern von Daten auch zeitlich zu beschränken. Ausserdem müssen personenbezogene Daten vertraulich behandelt und vor unbefugter Verarbeitung sowie vor Zerstörung, Verlust oder Schädigung geschützt werden.

Als weitere Voraussetzung für die zulässige Verarbeitung von personenbezogenen Daten muss zuvor entweder eine Einwilligung eingeholt worden sein oder die Verarbeitung für die Erfüllung eines Vertrages oder einer rechtlichen Verpflichtung erforderlich sein. Eine Datenverarbeitung kann aber auch zulässig sein, wenn dadurch berechtigte Interessen des Unternehmens oder eines Dritten gewahrt werden und die berechtigten Interessen von Personen, deren Daten verarbeitet werden, nicht schwerer wiegen. Dieser Erlaubnisgrund zur Verarbeitung von personenbezogenen Daten wird in der Praxis sehr bedeutsam sein, auch wenn er im Einzelfall konkretisiert werden muss.

Hinsichtlich der Einwilligung werden hohe Anforderungen an deren Wirksamkeit gestellt, die nach den Umständen des Einzelfalles zu beurteilen ist. Wird die Einwilligung in die Datenverarbeitung widerrufen, was jederzeit und ohne Angabe von Gründen möglich ist, sind grundsätzlich jegliche Verarbeitungsprozesse einzustellen, sofern sie sich nicht auf eine andere Rechtsgrundlage (zB ein berechtigtes Interesse des Verantwortlichen) stützen lassen.

Pflichten nach der DS-GVO

Aus der Verordnung ergibt sich eine Vielzahl von Pflichten, wobei sich aufgrund der neu eingeführten Rechenschaftspflicht des Verantwortlichen eine Beweislastumkehr ergibt. Das bedeutet, der Verantwortliche muss der Datenschutzbehörde nachweisen können, dass er sämtliche Pflichten erfüllt hat. Auf die wichtigsten Pflichten wird im Folgenden zusammengefasst eingegangen:

- ***Pflichten bei der Verarbeitung***

Wesentlich in diesem Zusammenhang ist jedenfalls die Pflicht, ein Verzeichnis von Verarbeitungstätigkeiten führen. Dieses Verarbeitungsverzeichnis muss unter anderem die Zwecke der Verarbeitungen, jegliche Information über betroffene Personen, Datenarten, Empfänger und Übermittlungen an Drittstaaten sowie eine allgemeine Beschreibung der getroffenen technischen und or-

ganisatorischen Massnahmen zum Schutz der Daten enthalten. Auf Anfrage der Aufsichtsbehörde ist ihr dieses Verarbeitungsverzeichnis vorzulegen.

Von der Pflicht, ein Verarbeitungsverzeichnis zu führen, sind allerdings Unternehmen befreit, die weniger als 250 Mitarbeiter beschäftigen, sofern ihre Verarbeitungsprozesse nicht risikogeneigt sind, nur gelegentlich erfolgen und keine „sensiblen" Daten betreffen. Im Zweifel über das Vorliegen dieser Befreiung ist zur Sicherheit ein derartiges Verzeichnis zu führen.
Des Weiteren muss der Verantwortliche Unternehmer eine objektive, risikobasierte Einschätzung über die Wahrscheinlichkeit und den Grad der Gefährdung der Rechte und Freiheiten der betroffenen Person vornehmen. Dies hat bereits zu Beginn der aufgenommenen Beziehung zu erfolgen. Das Risiko einer Verletzung von Rechten betroffener Personen ist voraussichtlich besonders gross bei Verarbeitungen, bei denen natürliche Personen betreffende Entscheidungen ausschliesslich automatisiert getroffen werden (Stichwort „profiling") oder „sensible" Daten im grossen Umfang verarbeitet werden. Sollte sich im konkreten Fall hierbei ein hohes Risiko ergeben, ist der Unternehmer zu einer „Datenschutz-Folgeabschätzung" verpflichtet, in der geplante Verarbeitungstätigkeiten genau dargestellt und der Zweck ihrer Verarbeitung genauer erläutert werden müssen. Falls sich dadurch ein tatsächliches hohes Risiko ergibt, ist eine Kontaktaufnahme mit der Datenschutzbehörde verpflichtend.

Die wahrscheinlich zur Umsetzung aufwändigste Pflicht ist die Einführung von geeigneten technischen und organisatorischen Massnahmen, die eine nach den datenschutzrechtlichen Vorschriften zulässige Datenverarbeitung garantieren. Dazu trifft das DS-GVO keine präzisen Vorgaben, weshalb anhand Art und Umfang der Verarbeitung selbst einzuschätzen ist, inwiefern und vor allem welche Massnahmen umgesetzt werden müssen Es ist jedenfalls zwischen „privacy by design" and „privacy by default" Massnahmen zu unterscheiden. Erstere zielen auf die Umsetzung der Grundsätze der Verarbeitung ab, wie z.B Datenminimierung, Speicherbegrenzung und Vertraulichkeit ab. Dafür eignet sich der verstärkte Einsatz von pseudonymisierten Daten. „Privacy by default" Massnahmen stellen Voreinstellungen dar, damit nur Daten für den jeweiligen Zweck verarbeitet werden und Daten nicht einer unbestimmten Zahl von Personen zugänglich gemacht werden.

- ***Pflichten in Bezug auf die betroffenen Personen***

Grundsätzlich ist der Verantwortliche dazu verpflichtet, der betroffenen Person mitzuteilen, dass ihre Daten bearbeitet werden. Neu geregelt werden die Auskunfts- und Berichtigungspflichten. Auch das „Recht auf Vergessenwerden" wird nun eingeführt. Demnach ist der Verantwortliche dazu verpflichtet, die personenbezogenen Daten unverzüglich zu löschen, sofern etwa der ursprüngliche Zweck für die Verarbeitung der Daten nicht mehr gegeben ist, die betroffene Person ihre Einwilligung widerruft oder der Verarbeitung grundsätzlich widerruft.

- ***Pflichten bei der Datensicherheit***

Wie bereits erwähnt, sind angemessene organisatorische und technische Massnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Mögliche Massnahmen sind beispielsweise die Pseudonymisierung, Verschlüsselung oder Zugriffsbeschränkungen. Darüber hinaus besteht nunmehr auch die Pflicht, der Datenschutzbehörde die Verletzung des Schutzes personenbezogener Daten anzuzeigen. Dies muss im Rahmen der so genannten „Data Breach Notification" immer dann gemacht werden, wenn aufgrund eines „Datenzwischenfalls" eine Gefährdung von personenbezogenen Daten eingetreten sein könnte. Auch bei der Übermittlung von Daten ins Ausland, beispielsweise an einen Subunternehmer gelten, sofern es sich um einen Drittstaat handelt, strenge Regeln.

Datenschutzbeauftragter

Sofern eine der folgenden beiden Bedingungen erfüllt ist, muss der Verarbeiter von Daten in seinem Unternehmen einen Datenschutzbeauftragten benennen:

- *sofern das Unternehmen Bearbeitungen durchführt, die eine umfangreiche regelmässige und systematische Überwachung der betroffenen Person erfordern, oder*

- *sofern das Unternehmen sensible Datenbearbeitungsvorgänge vornimmt.*

Es ist zu erwarten, dass beispielsweise neben Banken und Versicherungen auch Treuhänder, die aufgrund ihrer Kerntätigkeit notwendigerweise mit der Verarbeitung von sensiblen Daten befasst sind, einen Datenschutzbeauftragten bestellen werden müssen.

Die Bestellung eines Datenschutzbeauftragten kann auch freiwillig erfolgen. Voraussetzung für die Bestellung einer Person zum Datenschutzbeauftragten sind jedenfalls Fachkenntnisse im Datenschutzbereich. Der Datenschutzbeauftragte kann ein Mitarbeiter des Unternehmens oder eine externe hierzu befähigte Person – wie etwa ein Rechtsanwalt – sein. Die wichtigsten Aufgaben eines Datenschutzbeauftragten sind die Überwachung und fortlaufende Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften und deren Implementierung, insbesondere auch durch die Sensibilisierung von Mitarbeitern. Zur Erfüllung seiner Aufgaben muss dem Datenschutzbeauftragten Zugang zu allen datenschutzrelevanten Informationen und Unterlagen gewährt werden und es müssen ihm sämtliche notwendige Ressourcen zur Verfügung gestellt werden. Ansprechpartner (und gleichzeitig verantwortlich) für den Datenschutzbeauftragten ist die höchste Managementebene des Unternehmens.

Massnahmen und Sanktionen

Grundsätzlich kommen den Aufsichtsbehörden diverse Untersuchungs- und Abhilfebefugnisse zu. Darunter fallen etwa Hausdurchsuchungen, Verwarnungen, Anweisungen etc. Daneben haben Aufsichtsbehörden aber auch Strafbefugnisse. Je nach Art des Datenverstosses können die Aufsichtsbehörden Geldbussen von bis zu **EUR 20‘000‘000.00** (!) verhängen.

Im Einzelnen stellt sich das Strafregime wie folgt dar:

Bei einem Verstoss gegen die Bestimmungen über die Führung eines Verzeichnisses von Verarbeitungstätigkeiten, die Bestimmungen zur Datenschutzfolgeabschätzung und dergleichen können Strafen von bis zu EUR 10‘000‘000.00 oder bis zu 2% des gesamten weltweit erzielten Jahresnettoumsatzes des vorangegangenen Geschäftsjahres verhängt werden.

Bei einem Verstoss gegen die Grundsätze der Verarbeitung, gegen Betroffenenrechte oder die Bestimmungen zur Datenübermittlung an Drittländer kommt hingegen ein Strafausmass von bis zu EUR 20‘000‘000.00 oder bis zu 4% des gesamten weltweit erzielten Jahresnettoumsatzes des vorangegangenen Geschäftsjahres in Frage.

Die konkrete Höhe der Geldbusse hängt etwa auch von der Schwere und Dauer des Datenverstosses und vom Verschulden ab.

Fazit

Es zeigt sich, dass die DSG-VO schon vor ihrer Umsetzung in Liechtenstein weitreichende Folgen für sämtliche im Land tätigen Unternehmen, insbesondere auch die Treuhandbranche, zeitigt. Das „Regulierungsmonster“ DS-GVO bringt einen enormen Mehraufwand im Bereich der Compliance mit sich. Vor diesem Hintergrund sollte mit dem Beginn der Implementierung der notwendigen Massnahmen nicht zugewartet werden.

Zur Haftungsbeschränkung empfiehlt es sich daher, anwaltliche Hilfe in Anspruch zu nehmen, um eine rasche und effiziente Implementierung der neuen datenschutzrechtlichen Verpflichtungen im Unternehmen zu gewährleisten.

Tipps für Unternehmen in Liechtenstein:

- Die Pflichten aus der DS-GVO treffen spätestens ab Juli 2018 jeden Unternehmer in Liechtenstein, der personenbezogenen Daten verarbeitet. Daraus ergeben sich erhebliche Compliance – Anforderungen. Wir können Sie dabei unterstützen, dass Sie rechtzeitig sämtliche Auflagen erfüllen.
- Wir empfehlen als ersten Schritt ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen, weil dadurch abgeschätzt werden kann, welche Pflichten das Unternehmen nach der DS-GVO treffen. Unter Umständen besteht sogar die Pflicht zu Erstellung eines solchen Verzeichnisses. Gerne können wir Ihnen ein Muster eines Verarbeitungsverzeichnisses übermitteln.
- Auch sollte umgehend geprüft werden, ob ein Datenschutzbeauftragter im Unternehmen zu bestellen ist. Für viele Unternehmen wird die Bestellung eines externen Datenschutzbeauftragten (z.B. ein Rechtsanwalt) sinnvoll sein.
- Die vorhandenen Vertragsvorlagen sind an die Bestimmungen der DS-GVO anzupassen. Insbesondere sind die Vertragspartner darüber zu informieren, welche Daten, zu welchen Zwecken und auf welcher Rechtsgrundlage gespeichert werden. Auch die bisher verwendeten Einwilligungserklärungen werden vielfach zu überarbeiten sein.
- Schliesslich sind eine Reihe von Prozessen (zB Data Breach Process) zu definieren, Konzepte (zB Löschkonzept) und Dokumente (zB Datenschutzfolgeabschätzung) zu erstellen und das Verhältnis mit Ihren Auftragsdatenverarbeitern (zB IT-Unternehmen) auf eine neue vertragliche Basis zu stellen. Auch dabei können wir Ihnen gerne behilflich sein.
- Nehmen Sie mit unseren Datenschutzexperten Michael Nueber und René Saurer Kontakt auf, um in einem persönlichen Treffen herausfinden, wie Gasser Partner Rechtsanwälte Sie bei der Umsetzung der DS-GVO unterstützen kann.

Mag. René Saurer MES

Dr. Michael Nueber, LL.M.

Kontakt:
michael.nueber@gasserpartner.com
rene.saurer@gasserpartner.com

www.gasserpartner.com

Gasser Partner Rechtsanwälte
Wuhrstrasse 6
9490 Vaduz
Fürstentum Liechtenstein