

## EU-Datenschutzgrundverordnung (DSGVO):

# Handlungsbedarf für Schweizer Firmen und Organisationen

Am 25. Mai 2018 tritt die neue EU-Datenschutzgrundverordnung (DSGVO) in Kraft. Damit werden die Regeln für die Verarbeitung personenbezogener Daten, die Rechte der Betroffenen und die Pflichten der Verantwortlichen EU-weit vereinheitlicht. Die Panik im Vorfeld der DSGVO ist beachtlich, nicht zuletzt wegen des drastischen Bussenkatalogs von bis zu 20 Millionen Euro bzw. 4% des weltweiten Jahresumsatzes. Die DSGVO betrifft nicht nur in der EU ansässige Unternehmen, sondern auch sämtliche Schweizer Unternehmen und Organisationen, die Leistungen an Kunden in der EU anbieten oder in der EU eine Niederlassung oder Tochtergesellschaft haben. Der schweizerische Gesetzgeber hinkt mit dem hiesigen Datenschutzgesetz noch etwas hinterher. Es ist jedoch zu erwarten, dass wesentliche Teile der DSGVO übernommen werden, damit das schweizerische DSG durch die EU als gleichwertig anerkannt wird.

Es soll hier nicht näher auf die DSGVO und deren Auswirkungen eingegangen werden. Diese werden im Beitrag von Christoph Zimmerli (Seite 5/6 in diesem Magazin) ausführlich dargestellt. Wir konzentrieren uns den nachfolgenden Ausführungen auf die konkreten Massnahmen, die von Firmen und Organisationen in der Schweiz getroffen werden müssen. Einerseits ist bei praktisch allen die Wahrscheinlichkeit gross, dass in irgend einem Bereich ein EU-Bezug besteht (EU-Bürger als Mitarbeiter, Kunden oder Lieferanten mit Adresse im EU-Raum), und andererseits ist zu erwarten, dass sich die neue schweizerische Datenschutzgesetzgebung weitgehend der DSGVO angleichen wird. Deshalb empfehlen wir den Unternehmen und Organisationen in der Schweiz, sich künftig grundsätzlich DSGVO-konform zu

verhalten. Ein wesentlicher Punkt dabei ist, dass es sich hier nicht um ein reines IT-Thema handelt. Die Firmenleitung (Verwaltungsrat, Geschäftsleitung) ist in der Verantwortung und tut gut daran, diese wahrzunehmen.

Welche Schritte müssen Sie vornehmen, damit auch Ihr Unternehmen den Anforderungen der neuen Datenschutzvorgaben genügen wird? Wir unterscheiden verschiedene Handlungsfelder, welche parallel anzugehen sind:

### Organisatorische Massnahmen

Als Erstes gilt es, ein Inventar zu erstellen von allen Datenbeständen natürlicher Personen (auf juristische Personen ist die DSGVO nicht anwendbar). Dabei sollte geprüft werden, welche dieser Daten wirklich gebraucht werden, und welche Daten als besonders schutzwürdig gelten. Anschliessend müssen Prozesse einführt, dokumentiert und dann auch regelmässig kontrolliert werden für deren Erfassung, Bewirtschaftung, sowie Archivierung und Löschung. Dabei ist der Grundsatz zu berücksichtigen, dass von den Betroffenen grundsätzlich die Zustimmung zu einer Datenschutzerklärung (s. unten) vorliegen muss. Ausserdem ist ein/e Datenschutzverantwortliche/r zu bestimmen.

### Massnahmen im Bereich Marketing

Die Zustellung von Newsletters ist beispielsweise neu nur bei vorhandener Einwilligung des Empfängers erlaubt. Mit dieser Bestimmung wird unter Umständen das Marketing-Konzept eines Unternehmens in Frage gestellt. Das bestehende CRM (Customer Relation Management) muss ebenfalls den neuen Bestimmungen entsprechen. Es gilt deshalb, die Auswir-

kung der DSGVO auch mit den Marketingverantwortlichen genau zu analysieren und bei Bedarf die notwendigen Anpassungen vorzunehmen.

### Technische Massnahmen

Mit der Umsetzung der technischen Massnahmen wird die IT beauftragt, allenfalls unterstützt von weiteren Experten. Hier geht es um verschiedene, ganz unterschiedliche Aspekte:

- Organisation der Datenbestände und Zugriffsberechtigungen
- Ort (bzw. Land) der Datenspeicherung
- Zugriffsschutz auf die IT-Infrastruktur (Systeme, Netzwerk)
- Allfällige Verschlüsselung besonders schützenswerter Daten
- Schutzmassnahmen im Bereich Cyber Security (Firewall, DMZ, usw.)
- Unterhaltmassnahmen, Service Level Agreements
- Datensicherung und –archivierung
- Physischer Schutz der IT-Systeme gegen Diebstahl und Zerstörung
- Notfallkonzept
- Controlling-Prozess und periodische Audits

### Juristische Massnahmen

Für diese Aufgaben ist die Unterstützung durch Fachjuristen sinnvoll. Minimal sollte eine Datenschutzerklärung zur Datenhaltung der Firma verfasst werden, welche separat von den Allgemeinen Geschäftsbedingungen publiziert wird. Je nach Art der bewirtschafteten Datenbestände braucht es weitere Massnahmen, wie beispielsweise eine Datenschutzfolgeabschätzung bei besonders schützenswerten Daten.

Je nach Branche und Art der Geschäftstätigkeit können die erforderlichen Mass-

nahmen sehr unterschiedlich sein. Wir empfehlen allen Verwaltungsräten von Firmen und Vorständen von Organisationen, umgehend eine verantwortliche Person aus ihrem Kreis zu bestimmen, welche mit der Umsetzung der notwendigen Massnahmen beauftragt wird. Dazu wird diese mit Fachleuten aus den jeweiligen Bereichen zusammenarbeiten müssen. Sofern intern das notwendige KnowHow fehlt (was bei den meistens KMU der Fall sein dürfte), sollten sie sich von externen Fachleuten beraten und begleiten lassen.

**Autor**

*Daniel Stucki*  
DS Management Consulting GmbH  
VR-Präsident Keller Informatik AG  
mail@dsmc.ch / 079 334 55 67

Weitere Informationen:  
[www.dsmc.ch](http://www.dsmc.ch)  
[www.kellerinfo.ch/dsgvo](http://www.kellerinfo.ch/dsgvo)  
[www.e-forum.ch/dsgvo](http://www.e-forum.ch/dsgvo)

*Lassen Sie uns an Ihren  
IT-Problemen kauen.*

**Unsere Leistungen:**

Umfassende Beratung in Informatikfragen | IT-Planung und -Budgetierung | Entwickeln von Lösungskonzepten  
IT-Lösungen für KMU | Projektleitung | IT-Sicherheit  
Support und HelpDesk | Systemunterhalt, Service Level Agreements

*Keller Informatik AG*  
*– seit 25 Jahren professionelle*  
*IT-Lösungen für KMU.*

[www.kellerinfo.ch](http://www.kellerinfo.ch)

**Keller Informatik®**

Keller Informatik AG | Worbstrasse 201 | 3073 Gümligen/Bern | Tel 031 950 41 41 | E-Mail [info@kellerinfo.ch](mailto:info@kellerinfo.ch)