BÄR & KARRER

**Briefing November 2016**

# Die neue EU-Datenschutz-Grundverordnung: Handlungsbedarf für Schweizer Unternehmen

Ab 25. Mai 2018 – in 18 Monaten – gilt die neue Datenschutz-Grundverordnung der EU. Sie bringt ein einheitliches Datenschutzrecht für alle Mitgliedsstaaten der EU. Das neue Recht ist global anwendbar und gilt für alle Unternehmen, die Personen in der EU Waren- oder Dienstleistungen anbieten oder das Verhalten von Personen in der EU analysieren, zum Beispiel auf ihrer Website oder App. Auch Schweizer Unternehmen sind deshalb davon betroffen.

Das neue Recht enthält verschiedene Neuerungen und Verschärfungen und sieht hohe Geldbussen von bis zu EUR 20 Mio. oder, falls höher, 4% des weltweiten Umsatzes des Unternehmens (nicht des Konzerns) vor. Die Umsetzung durch die betroffenen Unternehmen bedarf in vielen Fällen organisatorischer oder technischer Anpassungen. Auch Unternehmen in der Schweiz empfehlen wir deshalb, ihre Informationsverarbeitungsprozesse zu überprüfen und die erforderlichen Änderungen rechtzeitig vor dem 25. Mai 2018 zu implementieren.

## Neuerungen

Im Vergleich zum heutigen Schweizer Recht bringt die DSGV verschiedene wichtige Neuerungen.

**Information**
Neu sind die betroffenen Personen grundsätzlich über die Datenbearbeitung zu informieren. Die Information muss "in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" erfolgen. Der Umfang der Information wird vorgegeben, ist beträchtlich und umfasst u.a. den Zweck und die Rechtsgrundlage der Bearbeitung, berechtigte Interessen, auf welche sich der Verarbeiter stützt, die Empfänger der Daten, die angemessenen Garantien, auf welche sich ein internationaler Datentransfer stützt (inkl. dem Verweis auf die Möglichkeit, eine Kopie davon zu erhalten), die Dauer der Speicherung sowie eine ausdrückliche Information über die Rechte der betroffenen Personen.

Umfassende 'Privacy Notices' werden damit inskünftig unumgänglich.

**Einwilligung**
Dieselben Anforderungen geltend für die Form der Einwilligung, wenn die Bearbeitung auf einer Einwilligung beruht. Die Einwilligung hat "in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" zu erfolgen. Stillschweigen, bereits

angekreuzte Kästchen oder Untätigkeit stellen keine Einwilligung dar. Besondere Vorsicht ist geboten, wenn eine Dienstleistung von der Einwilligung zur Verarbeitung von Personendaten abhängig gemacht wird, welche für die Erbringung der Dienstleistung nicht erforderlich sind. Die Einwilligung ist zudem jederzeit widerrufbar.

Jugendliche ab dem Alter von 16 Jahren dürfen die Einwilligung bei Online-Angeboten selbst erteilten, doch können Mitgliedsstaaten das Mindestalter bis auf 13 Jahre reduzieren. Bei Kindern unter dem Mindestalter ist die Zustimmung der Eltern erforderlich, was soweit möglich auch technisch sicherzustellen ist.

**'Privacy by Design' und 'Privacy by Default'**
Das in der Schweiz bereits geltende Verhältnismässigkeitsprinzip wird durch die DSGV in zweierlei Hinsicht konkretisiert. Generell gebietet die DSGV ausdrücklich, Datenverarbeitungssysteme von Beginn weg datenschutzfreundlich auszugestalten ('Privacy by Design'), z.B. durch Minimierung der bearbeiteten Daten und Pseudonymisierung. Voreinstellungen (z.B. vorangekreuzte Kästchen) müssen grundsätzlich datenschutzfreundlich gewählt werden ('Privacy by Default'), d.h. so, dass keine für den Bearbeitungszweck nicht erforderlichen Daten bearbeitet werden.

Sinnvollerweise werden deshalb inskünftig interne Datenschutzspezialisten von Beginn weg bei der Entwicklung und Ausgestaltung von IT-Produkten, Diensten und Anwendungen zugezogen und ins Projektteam integriert.

**Privacy Breach**
Bei Sicherheitslücken muss inskünftig die zuständige Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden nach der Entdeckung der Sicherheitslücke benachrichtigt werden. Nur wenn kein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht, kann darauf verzichtet werden. Durch technische und organisatorische Massnahmen ist sicherzustellen, dass Sicherheitslücken sofort entdeckt werden.

Die betroffenen Personen selbst sind zu benachrichtigen, wenn voraussichtlich ein hohes Risiko für deren Rechte und Freiheiten besteht. Die Benachrichtigung hat unverzüglich und in einfacher und klarer Sprache zu erfolgen.

**Recht auf Vergessenwerden und Portability**
Den betroffenen Personen steht – ähnlich wie im Schweizer Recht – grundsätzlich das Recht zu, die Löschung ihrer Daten zu verlangen. Die Löschung hat unverzüglich zu erfolgen. Zudem haben die betroffenen Personen neu das Recht, Daten, die sie dem Verarbeiter selbst zur Verfügung gestellt haben, in einem gängigen maschinenlesbaren Format herauszuverlangen oder auf einen Nachfolger übertragen zu lassen (sog. data portability). Ob dieses auf Facebook und ähnliche soziale Netzwerke gemünzte 'Recht auf Datenübertragbarkeit' auch auf andere Fälle wie z.B. Banken, Versicherungen, Buchungsportale, Online-Shops oder ähnliches Anwendung findet, muss sich weisen. Die fristgerechte Erfüllung dieser Rechte bedarf in vielen Fällen technischer Anpassungen.

**Privacy Impact Assessment**
Neu muss eine Abschätzung der Folgen von Datenverarbeitungsvorgängen durchgeführt werden, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt. Eine solche Datenschutz-Folgeabschätzung (Privacy Impact Assessment, PIA) umfasst unter anderem eine Bewertung der Risiken nach Eintretenswahrscheinlichkeit und Schwere der Verletzung und die Darstellung und Bewertung geplanter Schutzmassnahmen. Falls ein Risiko nicht mit Schutzmassnahmen beschränkt werden kann, ist die Aufsichtsbehörde zu konsultieren. Unter Umständen sind sogar die betroffenen Personen zu involvieren.

**Accountability**
Bearbeiter von Personendaten sind für die Einhaltung der Datenbearbeitungsgrundsätze verantwortlich und müssen auch nachweisen können, dass sie diese einhalten. Dies erhöht den Compliance-Aufwand beträchtlich: Unternehmen werden in verstärktem Masse gezwungen, ihre Verarbeitungsvorgänge zu dokumentieren.

## Hohe Geldbussen

Die DSGV sieht – wie gesagt – hohe Geldbussen bis zu EUR 20 Mio. oder, für Unternehmen, von bis zu 4% des gesamten weltweit erzielten Jahresumsatz des vorangegangenen Geschäftsjahres vor (des Unternehmens, nicht des Konzerns), falls dieser Betrag höher ist. Diese Geldbussen gelten zum Beispiel für Verstösse gegen die (allgemeinen) Datenverarbeitungsgrundsätze und die Accountability, gegen die Rechtmässigkeit der Datenbearbeitung, die Vorschriften zur Information und Einwilligung oder gegen die Rechte der betroffenen Personen (inkl. Recht auf Vergessenwerden und Recht auf Datenübertragbarkeit).

Bei gewissen anderen Verstössen, z.B. Verstössen gegen die Vorschriften zur Einwilligung bei Kindern, zu Privacy by Design und Privacy by Default, zum Privacy Impact Assessment oder Verstössen gegen die Benachrichtigungspflicht bei Sicherheitslücken, drohen Bussen bis EUR 10 Mio. oder 2 % des Umsatzes.

Auch die zivilrechtliche Haftung für Schadenersatz dürfte in Zukunft strenger werden, da die DSGV ausdrücklich eine Haftung auch für "immateriellen Schaden" vorsieht.

## Anwendung auf Unternehmen in der Schweiz

Die DSGV gilt – wie gesagt – nicht nur für Unternehmen mit Niederlassung in der EU. Auch Unternehmen ohne Niederlassung in der EU sind davon betroffen, sofern sie Waren oder Dienstleistungen betroffenen Personen in der EU anbieten (mit oder ohne Bezahlung) oder das Verhalten von Personen in der EU beobachten, z.B. auf ihrer Website oder in einer App. Auch wer an der Datenverarbeitung für solche Zwecke als Verantwortlicher oder Auftragsverarbeiter mitwirkt, untersteht der DSGV.

## Empfehlungen

Wir empfehlen deshalb allen Unternehmen in der Schweiz, zu prüfen, ob sie von der DSGV betroffen sind und gegebenenfalls welche Massnahmen zur Umsetzung der DSGV erforderlich sind.

Ein solches Projekt umfasst typischerweise die folgenden Schritte:

– Projekt-Team: Einsetzen eines gemischten Projektteams (IT, HR, Legal, Compliance, Risk) mit einem professionellen Projektmanagement; Buyin des Topmanagements.

– Projektplanung: Definition der Ziele und des Scopes des Projekts (z.B. Beschränkung auf gewisse zentrale Informationsverarbeitungsprozesse des Unternehmens).

– Informationssammlung (Mapping): Zusammenstellung (durch Dokumente, Interviews, Workshops) und Dokumentation der heute bereits bestehenden Informationsverarbeitungsprozesse, Datenflüsse und Kontrollmechanismen.

– Status- und GAP-Analyse: Vergleich der existierenden Prozesse mit den Anforderungen der DSGV.

– Massnahmenplanung: Erstellung eines Massnahmenplans mit Zeitplan und Budget; Genehmigung durch Board/ Management.

– Implementierung der Massnahmen und operationellen Änderungen.

## … und das Schweizer Recht?

In der Schweiz wird das Datenschutzgesetz zurzeit revidiert. Es wird erwartet, dass der Bundesrat noch dieses Jahr eine Vernehmlassung zu einem Vorentwurf zur Revision des Datenschutzgesetzes eröffnet. Die Revision dient nicht nur der Umsetzung der revidierten Europarats-Konvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, sondern dürfte auch verschiedene Neuerungen der DSGV aufgreifen. Dies ist richtig und wichtig, damit die Schweiz von der EU als Staat mit angemessenem Datenschutzniveau anerkannt bleibt. Bis die Revision in Kraft tritt, wird es aber wohl noch zwei bis drei Jahre dauern.

Wir werden Sie nach Eröffnung der Vernehmlassung über die geplanten Änderungen informieren.

## Autor

**Dr. Corrado Rampini**
Partner

T: +41 58 261 52 83
corrado.rampini@baerkarrer.ch

**Bär & Karrer AG**
Brandschenkestrasse 90
CH-8027 Zürich

Telefon: +41 58 261 50 00
Fax: +41 58 261 50 01
zurich@baerkarrer.ch

baerkarrer.ch
Zürich, Genf, Lugano, Zug