bratschi
wiederkehr
& buob

Rolf H. Weber
Prof. Dr. iur., em. Professor an der Universität Zürich
Rechtsanwalt, Konsulent
Telefon +41 58 258 10 00
rolf.weber@bratschi-law.ch

Markus Näf
Master of Law, Rechtsanwalt
Certified Senior Project Manager IPMA B
Lehrbeauftragter für Informatikrecht und Projektmanagement an der FHS St. Gallen
Telefon +41 58 258 10 00
markus.naef@bratschi-law.ch

DSGVO-Assessment: Datenschutz Compliance mit Blick auf die EU-Datenschutzgrundverordnung

Die im April 2016 verabschiedete Datenschutzgrundverordnung (DSGVO) der Europäischen Union (EU) tritt am 25. Mai 2018 in Kraft. Ihre Bestimmungen sind in den EU-Ländern direkt anwendbar; aber auch Schweizer Unternehmen sind von den neuen Regulierungen betroffen, und zwar direkt, wenn Güter oder Dienstleistungen in der EU angeboten werden, und indirekt durch die Beeinflussung des Entwurfs für ein neues Schweizer Datenschutzgesetz (DSG), das der Bundesrat anfangs September 2017 dem Parlament zuleiten will.

1. Überblick und praktische Bedeutung der neuen Vorschriften

Dass die DSGVO Anwendung findet auf in der EU domizilierte Niederlassungen von Schweizer Unternehmen, war schon nach der bisherigen Richtlinie 95/46 der Fall und ist offensichtlich. Neu wird hingegen sein, dass deren Anwendbarkeit bereits durch das Angebot von Waren und Dienstleistungen in der EU, die Bearbeitung von Daten auf EU-Gebiet (Outsourcing) oder die Beobachtung des Verhaltens von Personen in der EU begründet wird (Art. 3 Abs. 2 DSGVO). Diese Vorschrift folgt dem sog. Auswirkungs- oder Marktortsprinzip, wie es aus anderen Bereichen (z.B. Wettbewerbsrecht) schon bekannt ist: Wer aus dem Ausland in einem bestimmten Markt tätig werden will, muss sich auch den inländischen Vorschriften unterwerfen. Was ein grenzüberschreitendes Angebot ist, lässt sich nicht immer leicht feststellen, v.a. bei Internet-Angeboten. Relevante Faktoren für die Auslegung sind insbesondere die Sprache oder die Währung eines EU-Landes, aber auch die Erwähnung von EU-Kunden oder EU-Nutzern. In der Tendenz dürfte der Anwendungsbereich der DSGVO vermutlich weit ausgelegt werden, d.h. die Wahrscheinlichkeit für Schweizer Unternehmen, die grenzüberschreitend tätig sind und nicht exklusiv den Schweizer Markt betreuen, dürfte gross sein, dass sie sich an die Vorgaben der DSGVO zu halten haben.

Die Einhaltung der DSGVO-Grundsätze ist in der Praxis deshalb sehr wichtig, weil im Falle ihrer Verletzung erhebliche Strafen drohen. Die Ansätze liegen je nach der betroffenen verletzten Bestimmung bei EUR 20‘000‘000 oder 4% des gesamten weltweit erzielten Umsatzes des Unterneh-

mens (höherer Betrag) bzw. bei EUR 10‘000‘000 oder 2% des gesamten weltweit erzielten Umsatzes des Unternehmens (höherer Betrag). Selbst wenn gerade zu Beginn kaum Höchstbussen ausgesprochen werden dürften, vermag die finanzielle Einbusse doch sehr spürbar zu sein.

In der heutigen Diskussion kommen meist die nachfolgend genauer zu betrachtenden Grundsätze der Datenbearbeitung gemäss DSGVO zur Sprache. Nicht ausser Acht gelassen werden darf aber, dass die EU parallel zur DSGVO die Richtlinie 2002/58 (Datenschutz in der elektronischen Kommunikation), deren Inhalt die Schweiz in der DSG-Revision von 2007 nicht übernahm, überarbeitet hat und eine Verabschiedung als künftig direkt anwendbare Verordnung kurz bevorsteht (Inkrafttreten ebenfalls Ende Mai 2018). Deren Anwendungsbereich wird für grenzüberschreitende Angebote identisch sein. Ziel der Neuregelung ist die Erfassung neuer elektronischer Dienste wie Internet of Things (IoT) und Over-the-Top-Dienste (z.B. Skype, WhatsApp). Überdies steht eine Vereinheitlichung der unterschiedlichen Vorschriften zu den Cookies und zur Rufnummernsperrung an. Schweizer Unternehmen, die grenzüberschreitend ein Direktmarketing betreiben, sind ebenfalls von der neuen Verordnung betroffen und müssen z.B. Allgemeine Geschäftsbedingungen (AGB) und den Bestellprozess anpassen.

2. Neue Grundsätze für die Datenbearbeitung

Bei der Bearbeitung personenbezogener Daten sind verschiedene materielle Grundsätze zu beachten, z.B. die Rechtmässigkeit und Richtigkeit der Datenprozesse, die Zweckbindung bei der Datensammlung, die Datenminimierung bei der Datenaufbewahrung, die Einhaltung des Verhältnismässigkeitsprinzips sowie der Grundsatz von Treu und Glauben. Diese Grundsätze haben in der DSGVO eine gewisse Verfeinerung erfahren, doch stimmen sie weitgehend mit den bisherigen Vorgaben der Richtlinie 95/46 sowie des Schweizer DSG überein. Eine Rechtfertigung der Datenbearbeitung lässt sich, abgesehen von höherrangigen privaten oder öffentlichen Interessen, insbesondere auf die Einwilligung des Betroffenen abstützen. Solche Einwilligungen erfolgen in der Realität meist „automatisch“ durch einen „Klick“, ohne dass die Allgemeinen Geschäftsbedingungen oder Datenschutzbestimmungen gelesen werden. Künftig muss die Einwilligung spezifischer sein, was ggf. die Installierung einer besonderen Software zur Abgabe der entsprechenden Erklärung notwendig macht.

Eine starke Erweiterung erfahren in der DSGVO die aktiven Informationspflichten und die (passiven) Auskunftspflichten. Dem Betroffenen steht neben dem Berichtigungs- auch ein umfassendes Löschungsrecht (inkl. ein sog. „Recht auf Vergessen“) zu. Besondere Regelungen betreffen die automatisierten Einzelfallentscheide und v.a. die sog. Data Breach Notification: Tritt im Unternehmen ein Problem bei der Datensicherheit oder ein Datenverlust ein, mit der Folge, dass Risiken für Personendaten eintreten könnten, besteht die Pflicht, die Aufsichtsbehörde und den Betroffenen (je nach Vorliegen bestimmter Voraussetzungen) zu informieren. Insoweit ergibt sich für Unternehmen ein Handlungsbedarf im Sinne der Vornahme von angemessenen Präventivmassnahmen.

Die grössten Neuerungen der DSGVO kommen auf Schweizer Unternehmen aber mit Blick auf die Einhaltung von technologieorientierten Datenschutzprinzipien zu. Ausgangspunkt dabei ist der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO). Weiter haben grössere Unternehmen eine Datenschutz-Folgeabschätzung (sog. „Data Protection Impact Assessment", Art. 35 DSGVO) einzurichten. Gemeint ist damit, dass eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (v.a. bei hohen Risiken) vorzunehmen ist. Die Folgenabschätzung muss eine systematische Beschreibung der geplanten Verarbeitungsvorgänge sowie Verarbeitungszwecke, eine Bewertung der Notwendigkeit sowie Verhältnismässigkeit der Verarbeitungsvorgänge, eine Bewertung der Risiken für die Rechte der betroffenen Personen und eine Vorbereitung der zur Bewältigung der Risiken geplanten Abhilfemassnahmen umfassen. In der Regel erweist es sich als sinnvoll, diese Datenschutz-Folgeabschätzung in das Compliance-Konzept des Unternehmens aufzunehmen.

3. Umsetzung im Unternehmen

3.1 Überblick

Unternehmen müssen die Bearbeitung von Personendaten bis Mai 2018 konform mit den neuen Vorschriften gestalten. Dazu empfehlen wir ein DSGVO-Assessment mit folgenden Vorgehensschritten:

(i) Verantwortung für den Datenschutz im Betrieb festlegen;
(ii) Erhebung der aktuellen Datenbearbeitungen und Datenübermittlung innerhalb des Unternehmens;
(iii) Prüfen der Rechtfertigung (Rechtsgrund oder Erlaubnistatbestand) für die Datenbearbeitung (gesetzliche und/oder vertragliche Grundlagen in den Allgemeinen Geschäftsbedingungen und Vertragsdokumenten);
(iv) Prüfen der Zulässigkeit einer Datenübermittlung ins Ausland oder an Dritte auf der Basis der Datenschutzmassnahmen und des bestehenden Datenschutzniveaus;
(v) Evaluation der Instrumente zur Rechtfertigung der Datenbearbeitung sowie der Sicherstellung eines angemessenen Datenschutzes;
(vi) Umsetzung der Instrumente und Anpassung der Verträge zur Sicherstellung der Datenschutz-Compliance.

3.2 Verantwortlichkeit

Eine erste Aufgabe für Unternehmen besteht darin, eine für den Datenschutz verantwortliche Person im Unternehmen zu bestimmen. Diese Massnahme ist nicht zu verwechseln mit einer allfälligen Pflicht, einen Vertreter in der EU zu melden oder einen betrieblichen Datenschutzbeauftragten zu bestimmen, wofür zusätzlich auch nationale Vorgaben bestehen. Hier geht es vielmehr um die Zuordnung der innerbetrieblichen Verantwortung für die Einhaltung von Dokumentationspflichten und Datenbearbeitung. Wir empfehlen, dazu auch die Fragen der Datenaufbewahrung in Archiven,

die Auskunfts- und Löschungsverpflichtungen oder die Prüfung der Vertragsbestimmungen und Einwilligungen einzubeziehen.

3.3 Erhebung der Datenbearbeitungen

Damit festgestellt werden kann, ob ein Schweizer Unternehmen den Bestimmungen der DSGVO unterliegt oder die Datenbearbeitung mit derselben konform ist, muss als Grundlage festgestellt werden, welche Daten im Unternehmen bearbeitet und wohin diese übermittelt werden. Dabei geht es um folgende Punkte:

- **Datenkategorien**: Zu welchen Personengruppen liegen Daten vor (z.B. Mitarbeiter, Bewerber, Kunden, Interessenten, Webseiten-Besucher etc.) und um welche Informationen handelt es sich konkret (z.B. Name, Position, Gehalt von Mitarbeitern oder Name, Adresse und Bestellhistorie von Kunden)?
- **Datentransfer**: An welche Konzernunternehmen im In- oder Ausland werden die Daten übermittelt, bzw. von welchen Konzernunternehmen können Mitarbeiter auf die Daten zugreifen?
- **Bearbeitungszweck**: Zu welchen Zwecken erfolgt die Datenübermittlung (z.B. zentrale Lohnbuchhaltung, zentrales Kundenverwaltungsprogramm, Erbringung von Kundendienstleistungen etc.)?
- **Datenhoheit**: Wer entscheidet faktisch darüber, wofür die Daten genutzt werden (Zweck) und in welcher Weise?
- **Bekanntgabe an Dritte**: Werden die Daten Dritten zur Verfügung gestellt oder haben Dritte darauf Zugriff (z.B. Wartungsunternehmen, Softwareanbieter, externe Dienstleister, Lohnbuchhalter etc.)?
- **Dokumentation**: Unternehmen müssen die Zulässigkeit der Datenbearbeitung beweisen und unterliegen einer Dokumentationspflicht. Bei Risiken ist eine Datenschutzfolgeabschätzung (DSFA) vorzunehmen. Zudem haben Unternehmen bei der Auslagerung von Datenbearbeitungen an Dritte – sofern sie nicht unter die Ausnahmebestimmungen fallen – ein schriftliches Verzeichnis der Datenbearbeitungen zu führen und dieses auf Antrag den Aufsichtsbehörden offenzulegen (Art. 30 DSGVO).
- **Archivierung**: Die Konformität mit gesetzlichen Aufbewahrungs- und Archivierungspflichten ist sicherzustellen.

3.4 Rechtmässigkeit der Datenbearbeitung

Da der Grundsatz des „*Datenbearbeitungsverbots mit Erlaubnisvorbehalt*“ gilt, ist für jede Datenbearbeitung die Rechtmässigkeit zu prüfen. Diese kann aufgrund eines gesetzlichen Rechtfertigungsgrundes oder einer vertraglichen Einwilligung bestehen. Die weitaus häufigste Rechtfertigung wird die Einwilligung der betroffenen Person sein. Eine Einwilligung in die Datenbearbeitung kann jedoch nur erfolgen, wenn über die Datenbearbeitung korrekt informiert wird. Zudem bestehen für die Einwilligung von Allgemeinen Geschäftsbedingungen spezifische Formvorschriften.

Das Unternehmen hat überdies den Nachweis der Rechtmässigkeit und vor allem der Einwilligung zu erbringen.

3.5 Zulässigkeit der Datenübermittlung ins Ausland oder an Dritte

Eine Datenübermittlung von normalen Personendaten in Länder mit gleichwertigem Datenschutzniveau ist grundsätzlich zulässig. Bei besonderen Datenkategorien ist jedoch auch hier eine Einwilligung der informierten betroffenen Person notwendig.

Bei Datenübermittlungen in Länder ohne gleichwertigen Datenschutz sind zusätzliche Datenschutzvorkehrungen mittels vertraglicher Absprachen (d.h. mit individuellen Datentransfer-Vereinbarungen oder den Mustervereinbarungen der EU Datenschutzbehörden) nötig. Auch das Privacy Shield Abkommen mit den USA oder die Datenübermittlung innerhalb des Konzerns mit sogenannten Corporate Binding Rules fallen darunter. Bei diesen Vereinbarungen sind mögliche Notifikations- oder Genehmigungspflichten durch die Aufsichtsbehörden zu beachten. Selbstverständlich ist hier alternativ auch eine Einwilligung der betroffenen Person möglich.

Die Datenübermittlung an Dritte bedingt eine schriftliche Datenbearbeitungsvereinbarung. Zudem muss diese gegenüber der betroffenen Person offengelegt werden.

3.6 Evaluation der Konformität der Datenbearbeitung

In einem nächsten Schritt geht es um die Evaluation der Konformität der Datenbearbeitung mit allen relevanten Bestimmungen und der Ableitung der notwendigen Anpassungsmassnahmen. Massnahmen können in Form der Dokumentation von Datenbearbeitungen, der Anpassung von Vertragsunterlagen oder als Daten-Transfer-Verträge ergriffen werden.

Ebenfalls ist hier die Einhaltung der formalen Bestimmungen und Meldepflichten zu prüfen und zu dokumentieren.

3.7 Umsetzung der Massnahmen

Die Datenschutzmassnahmen und allfällige Vertragsanpassungen müssen bis zum 25. Mai 2018 umgesetzt sein. Ab diesem Datum können Unternehmen direkt sanktioniert werden.

Risiken für das Unternehmen bei Untätigkeit sind:

- Bussen bei Nichteinhaltung in der EU, später auch in der Schweiz.
- Risiken bei Lieferverträgen mit Compliance-Klauseln (Non-Compliance bei Nichteinhaltung der Datenschutzgesetze).
- Haftungsrisiken bei Datenschutzverletzungen.

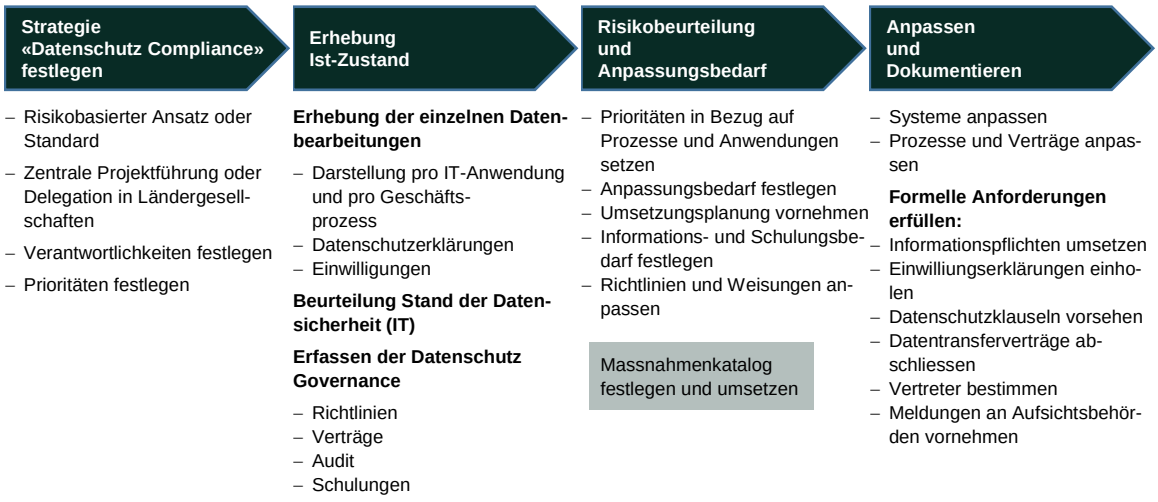
4. Information Governance

Mit der rasanten Entwicklung der Digitalisierung werden der Umfang und auch die Bearbeitung von Daten in Unternehmen weiter zunehmen. Es ist daher zu empfehlen, im Unternehmen den Schutz von Personendaten nicht als isoliertes Projekt, sondern eingebettet in das gesamte Informationsmanagement, zu betrachten. Personendaten, die von der aktuellen Datenschutzgesetzgebung betroffen sind, stellen nur eine Kategorie von Daten dar. Im Unternehmen sind aber oftmals technische Daten oder Forschungsdaten genauso oder gar wichtiger als Personendaten. Daher sollte eine ganzheitliche Datenstrategie bzw. Datengovernance definiert werden. Zudem sind die weiteren Regulierungsentwicklungen bereits heute zu berücksichtigen.

Wenn ein Unternehmen in mehreren Ländern tätig ist, sind die Regulierungen immer auch aus der Sicht des betroffenen Landes zu beurteilen. Es genügt also nicht, die Zulässigkeit einer Datenbearbeitung in der Schweiz abzuklären, sondern es sind auch die lokalen Bestimmungen am Ort der Bearbeitung einzubeziehen.

5. DSGVO-Assessment

Wir bieten ein standardisiertes DSGVO-Assessment für die Erhebung und Beurteilung der Konformität sowie der notwendigen Massnahmen an.



Basel
Lange Gasse 15
CH-4052 Basel
Telefon +41 58 258 19 00
Fax +41 58 258 19 99
basel@bratschi-law.ch

Bern
Bollwerk 15
Postfach 5576
CH-3001 Bern
Telefon +41 58 258 16 00
Fax +41 58 258 16 99
bern@bratschi-law.ch

Lausanne
Avenue Mon-Repos 14
Postfach 5507
CH-1002 Lausanne
Téléfone +41 58 258 17 00
Téléfax +41 58 258 17 99
lausanne@bratschi-law.ch

St. Gallen
Vadianstrasse 44
Postfach 262
CH-9001 St. Gallen
Telefon +41 58 258 14 00
Fax +41 58 258 14 99
stgallen@bratschi-law.ch

Zug
Industriestrasse 24
CH-6300 Zug
Telefon +41 58 258 18 00
Fax +41 58 258 18 99
zug@bratschi-law.ch

Zürich
Bahnhofstrasse 70
Postfach
CH-8021 Zürich
Telefon +41 58 258 10 00
Fax +41 58 258 10 99
zuerich@bratschi-law.ch