BÜRGI NÄGELI Rechtsanwälte

Grossmünsterplatz 9
8001 Zürich
Tel. +41 (0)44 268 40 00
Fax +41 (0)44 268 40 05

info@bnlawywers.ch
www.bnlawyers.ch

Liebe Klienten
Liebe Geschäftsfreunde

MÖGLICHE REFLEXWIRKUNG DER EUROPÄISCHEN DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO) AUF UNTERNEHMEN UND PRIVATPERSONEN IN DER SCHWEIZ

I. Einleitung

Datenschutz wurde in vielen Unternehmen stiefmütterlich behandelt. Neue datenschutzrechtliche Bestimmungen in den Mitgliedstaaten der Europäischen Union (Europäische Datenschutz-Grundverordnung, kurz: DSGVO) zwingen alle Unternehmen dazu, diesem Thema mehr Beachtung zu schenken; denn am 25. Mai 2018 läuft die Frist zur Umsetzung der DSGVO ab.

II. Inhalt der DSGVO

Die DSGVO gilt für alle in der EU ansässigen Privatpersonen und Unternehmen. Unternehmen, die Daten von Personen erheben, speichern und/oder verarbeiten, über welche eine Person direkt oder indirekt identifiziert (sog. personenbezogene Daten) werden kann, werden mit der DSGVO künftig in Sachen Datenschutz stärker in die Verantwortung genommen. Betroffene Personen hingegen erhalten mehr Mitbestimmungsrechte über die von ihnen erhobenen Daten.

Wichtigste Bestimmungen:

A. Erweiterte Definition von personenbezogenen Daten (so auch: IP-Adressen und andere zur Identifikation führende Informationen im Internet, Einbezug von genetischen, biometrischen und gesund-heitsbezogenen Daten)

B. Datenbearbeitungsgrundsätze: Strenge Anforderungen an die Einwilligung zur Erhebung der Daten (aktive Handlung, Freiwilligkeit, beschränktes Koppelungsverbot)

C. Rechte des Datasubjektes:

1. Aktive und umfassende Information im Zeitpunkt der Datenerhebung
2. Recht auf Auskunft
3. Recht auf Berichtigung und Ergänzung
4. Recht auf Einschränkung der Bearbeitung
5. Recht auf Vergessen (Recht auf Löschung, auch bei Dritten, an welche Daten weitergegeben wurden)
6. Recht auf Widerspruch
7. Recht auf Datenportabilität: Personendaten sind Eigentum des Datasubjektes und nicht des Datenbearbeiters
8. Rechte bei automatisierten Datenbearbeitungen
9. Möglichkeit der Beschwerde bei der Datenschutzbehörde des Wohnsitzstaates

D. Pflichten des Datenbearbeiters

1. „Data Protection by Design" und „Data Protection by Default": Datenschutz durch Tech-nikgestaltung und datenschutzfreundliches Leistungsangebot
2. Bei Nicht-EU-Unternehmen: Pflicht zur Ernennung eines Vertreters in der EU
3. Dokumentationspflicht
4. Meldepflicht bei Datenschutzpannen
5. Pflicht zur Durchführung eines Data Protection Assessment (systematische Beschreibung der Datenbearbeitungsprozesse, Beurteilung Notwendigkeit und Verhältnismässigkeit, Beurteilung

BÜRGI NÄGELI Rechtsanwälte

Grossmünsterplatz 9
8001 Zürich
Tel. +41 (0)44 268 40 00
Fax +41 (0)44 268 40 05

info@bnlawywers.ch
www.bnlawyers.ch

Datenschutzrisiken, Massnahmen zur Reduktion der Risiken)

6. Ernennung eines Datenschutzverantwortlichen

E. Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen: Übermittlung nur gestützt auf internationale Abkommen

F. Folgen bei Nichteinhaltung: strenge administrative Sanktionen (z. B. hohe Bussen bis zu 4% des weltweiten Jahresumsatzes)

III. Anwendungsbereich

Die DSGVO gilt gemäss Art. 2 § 1 für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Davon erfasst werden alle personenbezogenen Daten, die sich auf identifizierte und identifizierbare natürliche Personen beziehen, unabhängig davon ob diese von einer natürlichen oder juristischen Person bearbeitet werden und unabhängig von der Staatsangehörigkeit oder des Wohnorts der Person (Beispiel: Wohnort Schweiz, Bearbeitung Daten EU-Raum).

DSGVO Art. 2 § 2 sieht vier Fälle vor, bei denen die DSGVO nicht zur Anwendung gelangt:

- Tätigkeit ausserhalb des Unions-Rechts
- Tätigkeiten durch die Mitgliedstaaten der EU im Anwendungsbereich von EUV Titel V Kapitel 2
- Ausübung ausschliesslich persönlicher oder familiärer Tätigkeiten durch natürliche Personen
- Tätigkeiten von Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschliesslich dem Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

IV. Aussenwirkung der DSGVO auf die Schweiz

Auch wenn die Schweiz nicht Mitglied der EU ist, kann die DSGVO dennoch Auswirkungen auf Schweizer Unternehmen und Privatpersonen haben.

A Direkte Betroffenheit

- Niederlassung in der EU (Zweigniederlassung, Tochtergesellschaft, mit fester Einrichtung)
- Zielgruppe in der EU
- Bearbeitung von Daten in der EU von in der Schweiz wohnhaften Personen

bei

- Bearbeitung personenbezogener Daten im Rahmen der Tätigkeit in der EU,
- Bearbeitung personenbezogener Daten von Personen mit Wohnsitz in der EU durch das in der Schweiz ansässige Unternehmen, soweit diese Daten zum Zweck der Beobachtung des Verhaltens der betroffenen Personen innerhalb der EU genutzt werden (z. B. „Behavioural Targeting“)

BÜRGI NÄGELI Rechtsanwälte

Grossmünsterplatz 9
8001 Zürich
Tel. +41 (0)44 268 40 00
Fax +41 (0)44 268 40 05

info@bnlawywers.ch
www.bnlawyers.ch

- Absicht betroffenen Personen in Raum der EU Waren oder Dienstleistungen anzubieten.

Die DSGVO kommt unabhängig von der Staatsangehörigkeit auch zur Anwendung, wenn die Personen zwar in der Schweiz wohnen, deren Daten aber im EU-Raum bearbeitet werden.

B Indirekte Betroffenheit

Neben der direkten Betroffenheit gibt es zahlreiche Fälle, in denen Unternehmen indirekt von der DSG-VO betroffen sein können (z. B. Vertrag mit Unternehmen aus dem EU-Raum). Aus wirtschaftlicher Gründen kann es ratsam sein, sich umfassend an die DSGVO zu halten, auch wenn diese nicht direkt zur Anwendung käme oder nicht in allen Geschäftsbereichen effektiv von Belang ist. Ausschlaggebend ist nicht eine möglicherweise drohende Busse, sondern vielmehr ein allenfalls drohender Geschäftsrückgang, da EU-Unternehmen in vielen Bereichen darauf angewiesen sind, dass die Bestimmungen der DSGVO auch in Drittländern eingehalten werden; denn ein Ausweichen in Länder mit tieferen Datenschutz-Standards wird mit der DSGVO untersagt. Allgemein wird deshalb erwartet, dass viele Unternehmen weltweit die DSGVO materiell umsetzen und anwenden werden, auch wenn sie der Verordnung in formeller Hinsicht gar nicht unterstehen.

Die Schweiz ist nicht Mitglied der EU, weshalb die DSGVO hier nicht automatisch für sämtliche Unter-nehmen gilt. Die Frage der Betroffenheit bedarf der individuellen unternehmensinternen Bestandsaufnahme: Ergibt die Abklärung, dass ein Schweizer Unternehmen direkt oder indirekt der DSGVO untersteht, ist der allfällige Anpassungsbedarf der betroffenen Datenverarbeitungsprozesse zu eruieren.

V. Prüfung der Betroffenheit von der DSGVO

Wer unter den räumlichen und sachlichen Anwendungsbereich fällt, hat spätestens ab dem 25. Mai 2018 eine Vielzahl von Pflichten zu beachten, was ein strukturiertes internes Vorgehen erforderlich macht.

A Definition internes Vorgehen (als Beispiel)

1. Ernennung verantwortliche Person für Prozess DSGVO

   Ernennungeines Projektverantwortlichen und/oder einer Projektgruppe bestehend aus Mitgliedern der Geschäftsleitung und - sofern vorhanden - Mitarbeitern aus den Bereichen IT, Legal, Buchhaltung und HR (die Geschäftsleitung weiss über eine Vielzahl von betrieblichen Prozessläufen oftmals nicht hinreichend Bescheid)

2. Analyse

3. Risikobewertung / kritische Hinterfragung Analyse

BÜRGI NÄGELI Rechtsanwälte

Grossmünsterplatz 9
8001 Zürich
Tel. +41 (0)44 268 40 00
Fax +41 (0)44 268 40 05
info@bnlawywers.ch
www.bnlawyers.ch

4. Entscheid zum Vorgehen (vgl. Lit. C nachfolgend)
   - Strukturierung Daten
   - Löschung nicht notwendiger Daten
   - Aktives Tätigwerden gegen aussen, u. U. unter Einbezug Dritter
5. Umsetzung unter Einhaltung sachlicher und terminlicher Vorgaben
6. Kontrolle der Umsetzung
7. Einführung sich wiederholender periodischer Erneuerungs- und Kontrollmechanismen

ja	nein	**Auswahl an Vorabklärungsfragen (nicht abschliessend)**
		Betroffenheit von der DSGVO (vgl. Ziffer IV lit. A und B)
		Antwort „nein“: erledigt Antwort „ja“: Vorabklärungsfragen
		Rechtmässigkeit: Vorhandensein einer hinreichenden Rechtfertigungsgrundlage für die Verarbeitung der erhobenen Daten (z.B. Einwilligung, Vertrag oder eine gesetzliche Bestimmung)?
		Treu und Glauben, Transparenz: Verarbeitung der Daten in redlicher, vertrauenswürdiger und nachvollziehbarer Weise
		Zweckbindung: Datenverarbeitung zum festgelegten und legitimen Zweck gemäss dem Erhebungsgrund
		Datenminimierung: Speicherung nur notwendiger Daten und Notwendigkeit der Daten
		Richtigkeit und Aktualität der Daten
		Zeitliche Begrenzung der Datenspeicherung
		Integrität und Vertraulichkeit, Einsehbarkeit und Zugriff
		Risikoeinschätzung: Objektive Beurteilung der Risiken und Gefährdungen der Rechten und Freiheiten
		Datenschutzfreundliche Grundeinstellungen: Privacy by Design und Privacy by Default
		Registerführungspflicht: Dokumentation der Verarbeitungstätigkeiten
		Sicherheit: Verschlüsselung und Schutz vor Zugriff unbefugter Dritter
		Melde- und Informationspflicht: Sicherstellung der Meldepflichten für Datenlecks innert Frist
		Ernennung eines Datenschutzverantwortlichen
		usw.

BÜRGI NÄGELI Rechtsanwälte

Grossmünsterplatz 9
8001 Zürich
Tel. +41 (0)44 268 40 00
Fax +41 (0)44 268 40 05

info@bnlawywers.ch
www.bnlawyers.ch

B Ergebnis: Betroffenheit (örtlicher und sachlicher Bezug zur EU gegeben)

Folgende Massnahmen sind – sofern nicht schon erfolgt bzw. vorhanden – vorzukehren:

- Bestimmung eines Vertreters in der EU;
- Bezeichnung eines Datenschutzbeauftragten bzw. eines betriebsinternen Verantwortlichen in Angelegenheiten betreffend Datenschutz;
- Einholung Einwilligungen zur Datenverarbeitung (sofern nicht schon vorhanden);
- Verbesserung des Schutzes der Daten vor unbefugtem Zugriff Dritter (technische und/ oder organisatorische Schutzmassnahmen);
- Erstellung einer internen Dokumentation mit Angabe der zuständigen Personen und deren Verantwortlichkeit in Bezug auf die Verarbeitung personenbezogener Daten;
- Anpassung der Datenschutzerklärungen (z.B. beim Betrieb einer Homepage oder eines Newsletters);
- Überprüfung und gegebenenfalls Anpassung von Verträgen mit Beauftragten, die personenbezogene Daten verarbeiten;
- Ausarbeitung oder Anpassung interner Prozesse zur Behandlung von Anfragen von betroffenen Personen, die ihre Informations- und Auskunftsrechte wahrnehmen wollen (entsprechende Gesuche sind unverzüglich und spätestens innerhalb eines Monats zu behandeln);
- Ausarbeitung oder Anpassung der internen Prozesse bei allfälligen Verletzungen des Datenschutzes (dies empfiehlt sich insbesondere deshalb, weil Datenlecks innerhalb von 72 Stunden der Aufsichts-behörde gemeldet werden müssen).

C Ergebnis: Keine Betroffenheit

Wird nach Prüfung aller relevanten Fragen auf „keine Betroffenheit" geschlossen, so wurden die Abklärungen nicht vergeblich vorgenommen. In jedem Unternehmen ist es angezeigt, das erlangte Wissen über Betriebsabläufe etc. aktuell zu halten. Ratsam sind etwa folgende Massnahmen:

- Behebung erkannter Schwachstellen mit Bezug auf Datensicherheit. Schwachstellen eines
  Schweizer Unternehmens können gegebenenfalls auch eine Verletzung des hierzulande geltenden Schweizerischen Datenschutzgesetzes darstellen.
- Ausarbeitung einer Datenschutzstrategie.
- Bezeichnung eines betriebsinternen Datenschutzverantwortlichen (Kompetenzzentrum; spätestens bei der Inkraftsetzung des revidierten Datenschutzgesetzes dürfte dies viel Zeitersparnis mit sich bringen).

BÜRGI NÄGELI Rechtsanwälte

Grossmünsterplatz 9
8001 Zürich
Tel. +41 (0)44 268 40 00
Fax +41 (0)44 268 40 05

info@bnlawywers.ch
www.bnlawyers.ch

VI. Fazit

Unternehmen sind grundsätzlich gut beraten, das Thema DSGVO ernst zu nehmen. Dies heisst allerdings nicht, dass sich für sämtliche Unternehmen in jedem Fall umfassende Änderungen betriebsinterner Abläufe aufdrängen. In der Schweiz werden auch nach dem 25. Mai 2018 in vielerlei Hinsicht, in erster Linie und einzig das Schweizer Datenschutzgesetz (DSG) und/oder die entsprechenden arbeitsrechtlichen Bestimmungen zur Anwendung gelangen.

Die DSGVO verfolgt und verlangt einen „risikobasierten" Ansatz. Nicht jedes Unternehmen muss sämtliche erdenklichen Massnahmen und Vorkehrungen ergreifen, um eine Verletzung um jeden Preis vorzubeugen. Die DSGVO sollte jedoch in jedem Fall als Chance genutzt werden, um sich mit der aktuellen Datenschutzproblematik innerhalb des Unternehmens auseinanderzusetzen und gegebenenfalls Massnahmen zu ergreifen. Entsprechende Bemühungen können sich selbst für Unternehmen lohnen, die beinahe ausschliesslich in der Schweiz aktiv sind. Dies gerade auch deshalb, weil die derzeit stattfindenden Revisionsbemühungen auf Bundesebene hinsichtlich des Datenschutzgesetzes in vielerlei Hinsicht eine wesentliche Annäherungen an die EU-Bestimmungen der DSGVO darstellen werden und somit entsprechende Aufwendungen keinesfalls als unnötig zu betrachten sind.