



TREUHAND|SUISSE SEKTION ZÜRICH

# EU-DATENSCHUTZ: AUSWIRKUNGEN AUF AARGAUER UNTERNEHMEN

Das Schweizer Datenschutzgesetz ist gegenwärtig in Revision. Die Europäische Union ist bereits einen Schritt weiter. Ihre neuen, strengeren Regeln sind dieses Frühjahr in Kraft getreten. Sie gelten auch für Schweizer Unternehmen, die grenzüberschreitend tätig sind. Welche Firmen sind genau betroffen und was müssen diese tun?

Personenbezogene Daten werden oft als «Rohstoff der Zukunft» bezeichnet. Tatsächlich, Unternehmen, Organisationen oder politische Parteien geben viel dafür, unsere persönliche Datenspur auszuwerten. Sie setzen alles daran herauszufinden, wie gut ihr Produkt, ihr Anliegen oder ihre Weltanschauung zu uns passt. Die meisten von uns reichern ihre persönliche Datenspur laufend an. Etwa wenn wir uns im Internet bewegen, via Social Media kommunizieren oder online eine Bestellung tätigen; aber auch wenn wir in einem Verkaufsgeschäft einen Wettbewerbsbogen ausfüllen oder an der Kasse unsere Kundenkarte vorweisen. Anders ausgedrückt: Sobald persönliche Daten in der einen oder anderen Art in Informationssysteme eingespeist werden, hinterlassen wir Informationen, über deren Verarbeitung und Verwendung wir nur noch bedingt bestimmen können. Die Folgen davon sind im harmloseren Fall, dass wir online mit Werbung für bestimmte Produkte belagert werden. Das grössere Problem



ist, wenn diese Daten intensiv genutzt werden oder in Umlauf kommen. Wenn sie also als Rohstoff gehandelt und von Dritten weiterverwendet werden. Dies ist der Grund, warum die Gesetzgebung rund um den Datenschutz derzeit überall in den Fokus rückt.

## Haben Sie Privatkunden in der EU?

Die Regelung der EU ist seit Mai 2018 in Kraft: die «Datenschutz-Grundverordnung der Europäischen Union (DSGVO)». Sie verbessert die Rechte von natürlichen Personen, wenn es um die Kontrolle über die eigenen Daten geht. Das bedeutet, dass die Unternehmen zusätzliche Massnahmen ergreifen müssen, um Personendaten zu schützen. Davon sind auch viele Unternehmen im Kanton Aargau betroffen, selbst wenn sie keine Niederlassung oder Tochterfirma in einem EU-Land haben. Vor allem zwei Kriterien sind

entscheidend. Erstens: Eine Firma mit Sitz in der Schweiz fällt dann unter die DSGVO, wenn sie natürlichen Personen, Produkte oder Dienstleistungen anbietet. Konkret betroffen sind also alle Unternehmen, die Waren oder Dienstleistungen in EU-Länder exportieren; dies umfasst auch Versandhändler und Betreiber von Internetplattformen, die Bestellungen aus dem EU-Raum erhalten. Zweitens: Auch Firmen, die diese personenbezogenen Daten beobachten und/oder analysieren, unterliegen der neuen, verschärften EU-Regelung. Dies betrifft also Unternehmen, die diesen «Rohstoff» bearbeiten oder beobachten (z.B. anhand von Cookies). Aber aufgepasst, zusätzlich sind Firmen bereits von der DSGVO betroffen, wenn sie auf ihrer Website Kommentar- und Formularfelder oder weitere Firmenapplikationen einsetzen. Auch die Anbindung von Software zur Datenanalyse, die Dritte zur Verfügung stellen (z.B. Google Analytics oder Facebook Pixel), fällt unter die Datenschutzverordnung – auch wenn die Online-Präsenz auf den ersten Blick statisch erscheint.

## Neue Pflichten

Eine Aargauer Firma, auf die eines der oben genannten Kriterien zutrifft, fällt unter die Datenschutz-Grundverordnung der EU und muss folglich eine Reihe von neuen Auflagen erfüllen. Nachfolgend die sechs wichtigsten:

**Informationspflicht:** Will eine Firma die Daten ihrer Privatkunden aus dem EU-Raum verarbeiten, muss sie die Betroffenen darüber informieren. Sie muss genau und gut erkennbar (in ihrer Datenschutzerklärung) darlegen, welche personenbezogenen Daten gespeichert werden. Zusätzlich muss sie die Einwilligung für die Datenverarbeitung einholen und explizit benennen, wofür diese genau gilt (z.B. den künftigen Erhalt eines Newsletters).

**Technische Gestaltung:** Jeglicher Online-Auftritt muss so gestaltet sein, dass der Schutz der Daten grundsätzlich eingehalten wird. Also zum Beispiel ohne gestalterische Elemente oder definierte Voreinstellungen, die automatisch auf die Sammlung und Speicherung der Daten hin-



auslaufen, solange der Kunde sie nicht entdeckt und deaktiviert. Man spricht hier von der Pflicht zu Privacy by Design und Privacy by Default. Deshalb ist es wichtig, die Frage der Datenverarbeitungsprozesse und des Datenschutzes schon bei der Konzeption einer Website oder einer App in den Anforderungskatalog aufzunehmen.

**Auskunftspflicht:** Das Unternehmen muss zu betroffenen Personendaten ein Verzeichnis erstellen, das über die Art der Datenverarbeitung Auskunft gibt. Dies ist vor allem deshalb relevant, weil das Unternehmen seinen Nutzern die drei folgenden Rechte einräumen muss: Das Recht auf Auskunft, das Recht auf Löschung und das Recht auf Berichtigung.

**Datenschutzbeauftragter:** Von der DSGVO betroffene Schweizer Firmen müssen einen Datenschutzbeauftragten benennen, der die Einhaltung der Pflichten, die mit der EU-Verordnung verknüpft sind, formell vorantreibt, koordiniert und überwacht.

**Meldepflicht:** Kommt es zu einer Verletzung des Datenschutzes, z.B. weil durch einen Diebstahl oder eine Computerpanne Daten entweichen, eigenen Firmen bisher dazu, dies unter den Teppich zu kehren. Neu be-

steht eine Meldepflicht. Betroffene Unternehmen müssen das Ereignis innert 72 Stunden an die Datenschutzbehörde melden.

**Vorgängige Risikoabschätzung:** Ein Unternehmen, dessen Datenverarbeitung die Datenschutzrechte der betroffenen Personen potenziell verletzen könnte, muss neu eine vorgängige interne Risikoüberprüfung vornehmen. Weil die Ausgangslage von Firma zu Firma sehr stark variiert, kommt man nicht darum herum, Spezialisten beizuziehen, die Unterstützung bei einer individuellen Analyse der technischen und rechtlichen Risiken bieten.

Hält sich ein Schweizer Unternehmen nicht an diese Auflagen und wird angezeigt (z.B. von einer betroffenen natürlichen Person im EU-Raum), drohen teils empfindliche Bussen. Für grössere Unternehmen kann das Strafmass bis 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes betragen.

## Nötige Anpassungen

Für betroffene Unternehmen, die sich noch nicht auf die DSGVO ausgerichtet haben, ist es höchste Zeit, die nötigen Anpassungen vorzunehmen. Ein erster Teil davon ist nach innen gerichtet. So müssen die Unternehmen in einem ersten Schritt einen strukturierten Überblick (Be-

standsaufnahme) schaffen, welche Personendaten im Unternehmen vorhanden sind. Gleichzeitig müssen sie festlegen, wie die Zugriffsrechte auf diese Personendaten verwaltet werden. Denn zum Schutz persönlicher Daten gehört, dass sie nur durch bestimmte Nutzer unter klar definierten Kriterien bearbeitet werden können. Begleitend zu diesen grundlegenden Arbeiten muss das Unternehmen auch seine Mitarbeitenden sensibilisieren und schulen. Es sollte den Mitarbeitenden klar sein, dass Verletzungen der EU-Datenschutzverordnung der Firma schaden können.

Auch die Informationsmittel und Kommunikationsprozesse für die Kunden müssen entsprechend angepasst werden. Es gilt, Verträge und die allgemeinen Geschäftsbedingungen mit den geforderten Datenschutzhinweisen zu ergänzen. Weiter müssen die Software und technische Abläufe (Website, Apps) angepasst werden. Die Datenschutzerklärung der Unternehmung muss in verständlicher, klarer und einfacher Sprache dem Kunden so leicht wie möglich zugänglich gemacht werden. Bei jeglichem Online-Auftritt – also bereits bei Anmeldung zu einem Newsletter oder bei Kontaktformularen – müssen explizite Einwilligungen eingefordert werden, z.B. mit einem Auswahlfeld, in das man als Nutzer ein Häkchen setzen kann.

Weiter ist bei der Nutzung von Cookies auf die entsprechenden Richtlinien der Unternehmung hinzuweisen.

## Individuelle Abklärung sinnvoll

Wie die obigen Ausführungen zeigen, ist die Umsetzung der Pflichten, die mit der europäischen Datenschutzgesetzgebung verbunden sind, recht anspruchsvoll. Die Rechtslage ist noch in vielen Punkten unklar. Über offene oder strittige Fragen werden in absehbarer Zeit die Gerichte zu befinden haben. Aargauer Unternehmen, die sich aufgrund der oben genannten Kriterien betroffen fühlen, tun gut daran, bei der Umsetzung der skizzierten Pflichten technische und rechtliche Unterstützung beizuziehen.



Boris Blaser\*

\* Dipl. Treuhandexperte und MAS in Treuhand und Unternehmensberatung FH. Vorstandsmitglied des Schweizerischen Treuhänderverbands TREUHAND|SUISSE, Sektion Zürich

## AGV-AGENDA / JAHRESPLANUNG

**Wichtige Termine – bitte in Ihren Kalendern, Outlook etc. vormerken.** Weitere Details (Einladungen) werden zur gegebenen Zeit auf [www.agv.ch](http://www.agv.ch) und in einer der nächsten Ausgaben der Mitgliederzeitung publiziert. Die Gewerbevereine und Berufsverbände werden gebeten, verschiedene Termine in ihre eigene Jahresplanung aufzunehmen und bei der Planung von eigenen Anlässen mitzubersichtigen.

### JAHRESPLANUNG 2018

**Oktober**  
Donnerstag 18.10.2018 Herbst-Delegiertenversammlung 2018

### JAHRESPLANUNG 2019

**Januar**  
Mittwoch 9.1.2019 Neujahrs-APéro 2019

**März**  
Dienstag 5.3.2019 Aargauer Berufsbildungstag 2019

**April**  
Donnerstag 25.4.2019 Frühlings-Delegiertenversammlung 2019  
Aargauer Wirtschaftstag 2019

**September**  
Di. bis So. 3.–8.9.2019 Aargauische Berufsschau ab'19