ITMAGAZINE

Leserfragen zur DSGVO

7. April 2018 - *Von Reto C. Zbinden und Michèle Balthasar*

Michèle Balthasar und Reto C. Zbinden von Swiss Infosec beantworten die Fragen der Leser von "Swiss IT Magazine" zur DSGVO.

Wann ist die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung; DSGVO) in räumlicher Hinsicht anwendbar?
Nach Artikel 3 hängt die Anwendung der DSGVO von den beiden folgenden Kriterien ab:
1. dem Kriterium der Niederlassung: Das Unternehmen verarbeitet personenbezogene Daten im Rahmen der Tätigkeiten einer Niederlassung in der Europäischen Union (EU). In diesem Fall findet die DSGVO automatisch Anwendung, unabhängig davon, ob die Verarbeitung in der EU stattfindet oder nicht.
2. dem Kriterium des Zielmarktes: Das Unternehmen hat keine Niederlassung in der EU, aber die Datenverarbeitung steht im Zusammenhang damit
• betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist oder nicht;
• das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der EU erfolgt. Bei Letzterem bezieht sich die DSGVO vor allem auf die Beobachtung des Verhaltens von Internetnutzerinnen und -nutzern.

Fallen Unternehmen, die Grenzgänger beschäftigen, in den Anwendungsbereich der DSGVO?
Es gibt hierzu unterschiedliche Auffassungen. Unserer Meinung nach fällt die Verarbeitung von personenbezogenen Daten von Grenzgängern, also Personen, die in der Schweiz angestellt sind und im Ausland Wohnsitz haben, nicht in den Anwendungsbereich der DSGVO, sofern die personenbezogenen Daten in der Schweiz verarbeitet werden. Wenn das Unternehmen allerdings das Verhalten von Grenzgängern in der EU beobachtet (zum Beispiel durch GPS, VPN in Verbindung bei Homeoffice), sind diese Tätigkeiten vom Anwendungsbereich der DSGVO erfasst.

Artikel 13 DSGVO schreibt eine Informationspflicht vor. Muss ich jetzt jedem Kunden, der in meinem Online--Shop etwas bestellt, mitteilen, wer für die Datenverarbeitung verantwortlich ist, zu welchem Zweck die Daten gespeichert werden und auf welcher Rechtsgrundlage dies geschieht?
Ein elementarer Grundsatz der DSGVO ist die Transparenz. Betroffene Personen sollen in die Lage versetzt werden, die Datenerhebung, -verarbeitung bzw. -nutzung zu prüfen. Die DSGVO regelt die Informationspflichten in den Artikeln 13 und 14 in zwei sehr umfangreichen Artikeln. Werden personenbezogene Daten bei betroffenen Personen erhoben, muss das Unternehmen gemäss Artikel 13 f. unter anderem immer auch seine Identität, die Verarbeitungszwecke und die Rechtsgrundlage mitteilen.
Nach Artikel 12 DSGVO sind die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form zu erteilen. Dabei können sie schriftlich oder in elektronischer Form an die betroffene Person übermittelt werden. In elektronischer Form können sie beispielsweise auf einer Webseite bereitgestellt werden (Erwägungsgrund 30 der DSGVO). Empfehlenswert wäre unseres Erachtens, vor dem Abschicken der Bestellung in einem Online-Shop einen Link anzufügen, der direkt auf eine Datenschutzerklärung auf der Webseite des Unternehmens verweist.

Sind Webseitenbetreiber dazu verpflichtet, die Besucher über das Setzen von Cookies und die darin enthaltenen Daten zu informieren?
Die DSGVO findet auch auf die Verwendung von Cookies Anwendung, soweit sie personenbezogene Daten im Sinne der Artikel 4 Nr. 1 DSGVO enthalten, Anwendung. Der Besucher hinterlässt bei personenbezogenen Cookies auf der Webseite Identifikationsmerkmale wie zum Beispiel seine IP-Adresse. Diese Information kann durch den Cookie-Datensatz dem Benutzer zugeordnet werden (Erwägungsgrund 30 der DSGVO). Entsprechend gilt auch hier der Grundsatz der Transparenz und der Webseitenbetreiber, beziehungsweise das Unternehmen ist verpflichtet, den Besucher entsprechend darüber zu informieren.
Neben der DSGVO regelt auch die so genannte "Cookie-Richtlinie" (Richtlinie 2009/136/EG vom 25. November 2009) den Umgang mit Cookies. Diese Richtlinie soll in Zukunft durch die ePrivacy-Verordnung ersetzt werden. Wie genau der konkrete Inhalt dieser Verordnung aussehen wird und wann sie in Kraft treten wird, ist noch nicht klar.

In Artikel 32 DSVGO ist von der "Berücksichtigung des Stands der Technik" die Rede. Schliesst dies ein, dass etwa Kundendaten in einer Datenbank verschlüsselt gespeichert werden und dass auch der Verkehr über die Website nur via HTTPS läuft?

Nach Artikel 32 Absatz 1 DSGVO treffen Unternehmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Massnahmen, um ein dem Risiko angemessenes Schutzniveau der personenbezogenen Daten zu gewährleisten. Beispiele hierzu sind etwa die die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten.
Bei der Beurteilung des angemessenen Schutzniveaus sind nach Artikel 32 Absatz 2 DSGVO insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt, unrechtmässig oder unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
Die Verschlüsselung von Datenbanken sowie der Einsatz von HTTPS zur Übermittlung personenbezogener Daten entspricht der "good practice". Die Verschlüsselung der Daten einer Datenbank ist aus unserer Sicht bei der Verarbeitung besonderer Kategorien von personenbezogene Daten geboten.

Dürfen Unternehmen Werbe- oder News-E-Mail mit öffentlich ersichtlichen Adressen versenden (d.h. alle Empfängeradressen sind ersichtlich)?

Auch E-Mail-Adressen sind personenbezogene Daten im Sinne von Artikel 4 DSGVO. Personenbezogene Daten dürfen an Dritte nur dann offengelegt werden, wenn ein Rechtfertigungsgrund gemäss Artikel 6 DSGVO vorliegt (Einwilligung, gesetzliche Grundlage, Vertrag, berechtigtes Interesses etc.). Ein solcher Rechtfertigungsgrund dürfte in der Regel hier nicht vorliegen, weshalb dieses Vorgehen unzulässig ist.

Wie kann ich gegen ein Unternehmen vorgehen, wenn sie mit einem Versand von Werbe- oder News-E-Mails meine E-Mail-Adresse öffentlich ersichtlich machen und sie dadurch kopiert und missbraucht werden könnte?

Jede betroffene Person hat nach Artikel 77 Absatz 1 DSGVO unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde. Daneben hat die betroffene Person gemäss Artikel 17 DSGVO das Recht, von Unternehmen zu verlangen, dass betreffende personenbezogene Daten unverzüglich gelöscht werden, und das Unternehmen ist verpflichtet, personenbezogene Daten unverzüglich zu löschen.

Welche Schweizer Unternehmen müssen einen Datenschutzbeauftragten in der EU benennen?

Sofern die DSGVO auf das Schweizer Unternehmen anwendbar ist, ist gemäss Artikel 37 Absatz 1 ein Datenschutzbeauftragter zu benennen, sofern:
• die Kerntätigkeit des Unternehmens in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmässige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
• die Kerntätigkeit des Unternehmens in der umfangsreichen Verarbeitung besonderer Kategorien von Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten besteht.
Darüber hinaus gibt die DSGVO den EU-Mitgliedstaaten die Möglichkeit, strengere Regelungen in Bezug auf die Bestellung eines betrieblichen Datenschutzbeauftragten zu schaffen (so zum Beispiel in Deutschland).
Mittels der am 13. Dezember 2016 veröffentlichten Stellungnahme der Artikel-29-Datenschutzgruppe (unabhängiges Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes) gibt es erste Klarstellungen was unter "Kerntätigkeit" im Sinne des Artikel 37 Absatz 1 b DSGVO zu verstehen ist. Demnach ist im Zusammenhang mit Erwägungsgrund 97 der DSGVO hierunter jede Tätigkeit zu verstehen, die essentiell für die Erreichung der Ziele des Unternehmens sind. Massgeblich für das Merkmal "umfangreiche Verarbeitung" sind die Anzahl der Betroffenen, die Menge der betroffenen Daten und/oder die Vielzahl der verschiedenen Datensätze und/oder die Dauer der Datenverarbeitung sowie die geographische Reichweite der Datenverarbeitung. Als Beispiel wird die Verarbeitung von personenbezogenen Daten für Werbezwecke durch Suchmaschinen für verhaltensbedingte Werbevorschläge genannt. Unter Berücksichtigung von Erwägungsgrund 24 der DSGVO können unter das Merkmal "umfangreiche regelmässige und systematische Überwachung" grundsätzlich alle Arten des Internet-Trackings und Profilings fallen.

Welche Behörde ist für uns als betroffenes Unternehmen (Belieferung von EU-Kunden) die federführende Aufsichtsbehörde?

Sofern das Unternehmen eine Hauptniederlassung oder eine einzige Niederlassung in der EU hat, ist nach Artikel 56 DSGVO die dortige zuständige Aufsichtsbehörde die federführende Aufsichtsbehörde für die von Ihrem Unternehmen durchgeführten grenzüberschreitende Verarbeitung personenbezogener Daten. Abweichend von diesem Grundsatz ist jede Aufsichtsbehörde dafür zuständig, sich mit einer bei ihr eingereichten Beschwerde oder einem etwaigen Verstoss gegen die DSGVO zu befassen, wenn der Gegenstand nur mit einer Niederlassung in ihrem Mitgliedstaat zusammenhängt oder betroffene Personen nur ihres

Mitgliedstaats erheblich beein-trächtigt.
Für Unternehmen, die keine Niederlassung in der EU haben, auf die aber die DSGVO dennoch anwendbar ist, ist unklar, welche Aufsichtsbehörde zuständig sein wird. Es könnte argumentiert werden, dass die zuständige Aufsichtsbehörde diejenige ist, in welchem ein EU-Vertreter nach Artikel 27 DSGVO zu benennen ist. Klarheit hierzu werden künftige Entscheidungen der Aufsichtsbehörden und Gerichte bringen.

Die Autoren

Reto C. Zbinden, Rechtsanwalt/CEO
Reto C. Zbinden, Rechtsanwalt, ist Gründer und Inhaber von Swiss Infosec und ausgewiesener Spezialist in den Bereichen Informationssicherheit, Datenschutz und IT-Sicherheit. Seine Fachgebiete sind Sicherheit und Organisation, Zertifizierung im Bereich der Informationssicherheit und die rechtlichen Aspekte der Informationssicherheit.

Michèle Balthasar, Rechtsanwältin, Head Legal & Privacy Consulting
Dr. iur. Michèle Balthasar, Rechtsanwältin, Member of the Executive Board, leitet als Head Legal & Privacy Consulting das Kompetenzzentrum für Datenschutz und Informatikrecht bei Swiss Infosec. Sie doziert an der Universität Freiburg und hat dort mit einer Masterthesis zum Thema IT-Sicherheit und Datenschutz einen EMBA in Utility Management abgeschlossen.