Datum: 10.04.2018

Swiss IT Magazine

Swiss IT Magazine
8800 Thalwil
044/ 723 50 00
www.swissitmagazine.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 8'106
Erscheinungsweise: 10x jährlich

Seite: 32
Fläche: 172'179 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 69180502
Ausschnitt Seite: 1/4

Die EU-DSGVO und die Schweiz

«Es ist nicht meine Aufgabe, EU-Recht durchzusetzen»

Interview Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte Adrian Lobsiger zum Datenschutz in der Schweiz im Hinblick auf die DSGVO und die Revision des Schweizer Datenschutzgesetzes.

Interview: Matthias Wintsch

Swiss IT Magazine»: Herr Datenschutzbeauftragter, waren Sie privat oder jemand aus Ihrem Umfeld schon einmal Opfer eines Data Breaches?

Adrian Lobsiger: Privat war ich bisher nie ein Opfer, auch mein privates Umfeld wurde bisher verschont. Geschäftlich habe ich aber natürlich mit solchen Fällen zu tun.

Dann hatten Sie bisher Glück, dass es Sie noch nie erwischt hat?

Mit Glück hat das nicht unbedingt zu tun, ich verfüge nur über eine überschaubare Anzahl Geräte. Neben meinem Geschäfts-Laptop und meinem Smartphone benutze ich selbst keinen Computer oder vergleichbare Geräte zuhause, auf denen ich meine Daten habe.

Könnten Sie für unsere Leser den Inhalt und Sinn der EU-Datenschutzgrundverordnung beschreiben?

Die Verordnung bestätigt die Prinzipien des bestehenden Schweizer Datenschutzgesetzes von 1993, aktualisiert und konkretisiert diese aber in Bezug auf unsere heutige digitale Realität und erweitert sie mit Sanktionsmöglichkeiten. Für mich stehen jedoch nicht die Sanktionen im Vordergrund, sondern die neuen Arbeitsinstrumente wie Risikofolgenabschätzungen, Meldepflichten oder Privacy by Design und Default, die dem betrieblichen wie auch dem behördlichen Datenschutz ermöglichen, effizienter arbeiten zu können. Das bestehende Zusammenspiel zwischen den Datenverantwortlichen, deren Compliance- und Datenschutzdiensten sowie dem behördlichen Datenschutz muss rationalisiert werden. Firmen, die viele Daten bearbeiten, sollen Ordnung halten, wissen wo die Daten liegen, Verzeichnisse anlegen, Massnahmen offenlegen sowie die Risiken kennen und analysieren, die mit Big Data einhergehen. Intelligentes und dokumentiertes Arbeiten sind der Sinn der Verordnung. Wenn es doch zu absichtlichen oder grobfahrlässigen Verstössen kommt, ist die Sanktion wichtig, zumal sie ein zusätzliches Reputationsrisiko für Unternehmen birgt. Heute sind die Sanktionsmöglichkeiten bei uns lächerlich, in welchem Masse diese verstärkt werden, muss nun der Gesetzgeber in der Schweiz entscheiden, das Thema ist in der Pipeline.

Dürfen wir das so verstehen, dass Sie die neue EU-Datenschutzgrundverordnung demnach begrüssen?

Die Datenschutzverordnung der EU beruht auf der Konvention 108 des Europarates, in der die Schweiz Mitglied ist. Die DSGVO übernimmt diese Grundsätze und auch wir werden die aktualisierte Konvention hoffentlich in der eigenen Gesetzgebung spiegeln. Diese Anpassungen sind eine Notwendigkeit, unabhängig, ob sie von der EU oder dem Europarat kommen. Wir sind unseren Usern schuldig, dass wir bald nicht mehr mit einem Erlass aus dem Jahre 1993 arbeiten. Bedenken Sie, dass das erste Smartphone 2005 vermarktet wurde.

Welche Rolle wird der EDÖB im Rahmen der Umsetzung der DSGVO in der Schweiz einnehmen?

Am 25. Mai tritt die Verordnung in Kraft und wird auch auf gewissen Datenbearbeitungen in der Schweiz, welche in der EU Auswirkungen haben, anwendbar sein. In der Phase zwischen dem Inkraft-

Datum: 10.04.2018

Swiss IT Magazine

Swiss IT Magazine
8800 Thalwil
044/ 723 50 00
www.swissitmagazine.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 8'106
Erscheinungsweise: 10x jährlich

Seite: 32
Fläche: 172'179 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 69180502
Ausschnitt Seite: 2/4

treten der EU-Datenschutz-Grundverordnung und der Totalrevision unseres eigenen Datenschutzgesetzes muss die Wirtschaft die zuvor angesprochenen Instrumente anwenden, welche die DSGVO nun zur Verfügung stellt. Wir unterstützen die Wirtschaft bei der Einführung dieser Instrumente und beraten Unternehmen in Data-Breach-Situationen, die aktuell meistens freiwillig gemeldet werden. Bis der Gesetzgeber in der hoffentlich kurzen Übergangszeit ein neues Gesetz mit neuen Befugnissen, Mitteln und schärferen Sanktionen bringt, versuchen wir, mit den Partnerbehörden in der EU und der ganzen Welt pragmatisch zusammenzuarbeiten. Im Gegensatz zu den Datenschutzbehörden in der Europäischen Union arbeiten wir aber mit bescheidenen Mitteln und einem Gesetz von 1993. Das heisst, dass die Übergangsphase, bis das Schweizer Datenschutzgesetz nachziehen wird, für mich und meine kantonalen Kollegen eine sehr heikle Phase ist. Es ist wichtig für mich, nicht den Eindruck entstehen zu lassen, bis zur Schaffung des neuen Schweizer Gesetzes hilflos zu sein. Das wäre fatal. Der Eindruck eines Datenschutz-Vakuums in der Schweiz soll auf keinen Fall entstehen.

«Heute sind die Sanktionsmöglichkeiten bei uns lächerlich.»

Adrian Lobsiger, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Also ist es wirklich so, dass der EDÖB keine zusätzlichen Verpflichtungen, Rechte und Mittel im Rahmen der Einführung der DSGVO zugesprochen bekommt?

Der Bundesrat hat in einer Botschaft vom letzten September erhebliche zusätzliche Mittel in Aussicht gestellt. Man ging davon aus, dass die Revision des Schweizer Datenschutzgesetzes in der Frühlingssession durch den Erstrat geht. Nun kam es jedoch zu einer Aufsplittung und der Teil, der die Anpassung an die EU-Verordnung bringen sollte, wird nach hinten geschoben. Das heisst, dass die Übergangszeit länger und somit für uns Datenschützer umso anspruchsvoller wird, da wir mit den alten Mitteln und Befugnissen neue Herausforderungen stemmen müssen.

Viele Firmen in der Schweiz pflegen Kundenkarteien und bewegen sich auch ausserhalb des Binnenmarktes. Hat die DSGVO Auswirkungen auf alle diese Schweizer Firmen?

Es kursieren Schauergeschichten von Hotels, die einen eigenen Datenschützer anstellen oder horrend teure Beratungen einkaufen müssen. Das sind natürlich Übertreibungen. Grundsätzlich ist allerdings davon auszugehen, dass man keine Branche zum vornherein gänzlich ausschliessen kann. Die DSGVO ist kein Erlass, der sich gegen besonders grosse Firmen richtet und diesbezüglich einen Schwellenwert hätte. Innerhalb der Verordnung gibt es einige Bestimmungen, die in der Tat nur für grosse Firmen anwendbar sind, beispielsweise das Führen eines Verzeichnisses aller Verarbeitungstätigkeiten. Hier spielt die Grösse der Firma eine gewisse Rolle. Aber eigentlich geht es mehr um die Menge der gehaltenen Daten und die Intensität deren Bearbeitung. Wer die Daten von vielen Personen automatisiert bearbeitet und profilbildend auswertet, muss schon gute Gründe haben, um die Verordnung als irrelevant einzustufen. Wenn sich eine Online-Bearbeitung und Profilbildung massgeblich auf Personen in der EU auswirkt, ist davon auszugehen, dass die Verordnung anwendbar ist.

Und wie sieht es mit den angesprochenen Hotels aus?

Geschäfte wie Friseursalons oder Hotels, die Kundendaten bearbeiten und Kundenkarteien haben, unter denen sich potentiell EU-Bürger befinden, können sich Folgendes sagen: Wenn sie die Grundsätze unseres eigenen Datenschutzgesetzes gewissenhaft anwenden, müssen sie sich keine Sorgen machen. Risikofolgenabschätzungen und ähnliche Instrumente,

Datum: 10.04.2018

Swiss IT Magazine
8800 Thalwil
044/ 723 50 00
www.swissitmagazine.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 8'106
Erscheinungsweise: 10x jährlich

Seite: 32
Fläche: 172'179 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 69180502
Ausschnitt Seite: 3/4

welche die Verordnung vorsieht, beziehen sich auf risikoreiche Bearbeitungen, die in solchen Betrieben in aller Regel nicht vorkommen. Hingegen kommt die Verordnung bei relativ kleinen Unternehmen, die sensible Personendaten von sehr vielen Menschen bearbeiten, sehr wohl zu Anwendung. Vor der Fusion mit Facebook wäre Whatsapp mit seinen ca. 50 Mitarbeitenden ein solcher Kandidat gewesen.

Unterscheidet sich die Anwendung des EU-Rechts für Schweizer Firmen von der bei EU-ansässigen Unternehmen?
Für EU-ansässige Unternehmen ersetzt die DSGVO das bisher geltende nationale Datenschutzgesetz und belässt für nationale Gesetze einzig noch kleine Spielräume. Die Schweiz ist demgegenüber kein Mitgliedstaat der EU. Hier gelten nach wie vor unser eigenes nationales Datenschutzgesetz und die kantonalen Regelungen. Nehmen wir das Beispiel eines Data Breach. Mit Inkrafttreten der DSGVO ist das Vorgehen für eine deutsche Firma ab dem 25. Mai 2018 klar, sie meldet ein entsprechendes Ereignis der deutschen Datenschutzaufsicht. Ein Schweizer Unternehmen sollte nach der Verordnung auch an eine Datenschutzaufsicht melden, im geltenden Schweizer Gesetz steht dazu jedoch nichts. Wenn das Unternehmen keine Meldung macht oder die betroffenen Kunden nicht informieren will, kann meine Behörde nichts erzwingen. Ich kann in diesem Fall nur beraten. Es ist nicht meine Aufgabe, EU-Recht durchzusetzen. Daher haben wir zurzeit keine richtige Rechtssicherheit. Ich möchte aber nicht dramatisieren, wir werden solche Fälle pragmatisch handhaben und die Zeit bis zur leider aufgeschobenen Totalrevision unseres Datenschutzgesetzes mit Improvisationstalent zu überbrücken wissen.

Sie sprachen gerade über den spezifischen Fall eines Data Breach und der resultierenden obligatorischen Meldepflicht. Wie verhält es sich umgekehrt, wenn ein Schweizer Unternehmen nun einen Verstoss gegen die Verordnung begehen würde? Wie würde eine Strafverfolgung aussehen?
In der Regel muss ein Vertreter in der EU zur Verfügung stehen, über den die behördlichen Kontakte laufen werden. Weiter wird das Vorgehen davon abhängen, ob es eine Niederlassung in der EU gibt. Gegenüber einem Unternehmen, das nur in der Schweiz ist, kann die EU weder Untersuchungshandlungen auf fremdem Boden noch Sanktionen durchsetzen. Da müsste also eine Amts- und Rechtshilfe laufen. Wenn das Unternehmen aber Vermögen und Niederlassungen in der EU hat, gibt es für die EU dort Angriffspunkte. Aber auch in der erwähnten Übergangszeit wird man sicher versuchen, mit der zuständigen EU-Behörde in Kontakt zu treten. Am Ende geht es um die Interessen der User und Geschädigten, das ist das gemeinsame Ziel aller Datenschutzbehörden.

Viele Schweizer Firmen scheinen schlecht informiert und unvorbereitet zu sein. Was raten Sie solchen Firmen aktuell zu unternehmen, was sind die wichtigsten Massnahmen?
Firmen, die grenzüberschreitende, breitflächige Online-Angebote verbunden mit Tracking und Profiling entfalten, müssen sich professionell beraten lassen und gegebenenfalls entsprechende interne Stellen einrichten. Unter Umständen müssen sie auch einen Datenschutzbeauftragten einstellen. Der firmeninterne Datenschützer muss die Rolle des Advocatus Diaboli einnehmen und die Interessen der User artikulieren. Auch wenn es unbequem sein mag, muss er gegenüber der Geschäftsleitung Risiken aufzeigen und notwendige Investitionen einfordern. Bei kleinen Unternehmen, bei denen einzelne Bestimmungen der DSGVO anwendbar werden könnten, rate ich vor allem, dass das Schweizer Datenschutzgesetz vorbildlich erfüllt wird. Was im geltenden Datenschutzgesetz als Transparenzprinzip bezeichnet wird, sollte ernstgenommen werden. Wenn sich mein Angebot an viele User richtet und ich transparent sein will, muss es auf meiner Website klar sein, wie ich welche Daten beschaffe, zu welchem Zweck ich sie bearbeite und an wen ich sie im In- oder Ausland weitergebe. Das alles muss in einer digitalisierungswürdigen, benutzerfreundlichen Art dargestellt werden. Wenn das Schweizer Recht in vorbildlicher Weise angewendet wird, auch in Bezug auf die digitale Umsetzung, ist die Wahrscheinlichkeit intakt, dass damit die Bedingungen der EU-DSGVO auch erfüllt sind. In allen Fällen taugt diese Faustregel freilich nicht: Gerade wenn es im Umgang mit sensiblen Daten zu Pannen kommt, wenn sich eine EU-Behörde bei einem Schweizer Unternehmen melden würde, muss externer Rat eingeholt werden. Unser Merkblatt kann hier weiterhelfen. Falls nicht, kann man uns auch anrufen.

Die höchste Priorität hat für Sie also die einfache Anwendung von gesundem Menschenverstand nach Schweizer Recht?
Ja, aber nicht mit dem Menschenverstand von 1993, sondern dem von 2018.

Von unseren Lesern hören wir teilweise, dass sie erst reagieren werden, falls ein Problem auftaucht oder eine Anfrage gestellt wird. In Ihren Augen ein blauäugiges oder durchaus legitimes Vorgehen?
Wenn jemand seine Firma im Griff hat, weiss wo die Daten liegen, und das Risiko

Datum: 10.04.2018

Swiss IT Magazine
8800 Thalwil
044/ 723 50 00
www.swissitmagazine.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 8'106
Erscheinungsweise: 10x jährlich

Seite: 32
Fläche: 172'179 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 69180502
Ausschnitt Seite: 4/4

eines Data Breach nicht verdrängt, dann ist er vielleicht schon sehr nahe an der Verordnung. Wenn sich aber jemand sagt «wir wurden nie gehackt, werden auch später nicht gehackt und benachrichtigen Kunden sowieso nicht», dann ist er nicht in der digitalen Welt angekommen und nicht nur inkompatibel mit der DSGVO, sondern auch mit dem Schweizer Recht. Anders gesagt, wenn die Firma nicht in das offensichtlich betroffene Segment fällt, sollten zumindest unsere verfügbaren Merkblätter gelesen und dann gesunder Menschenverstand angewendet werden. Bei vielen Bestimmungen sieht man sehr schnell, wenn man nicht betroffen ist, beispielsweise an den Schlagworten «hohes Risiko» oder «grosse Datenmengen». Abstraktere Begriffe wie «Privacy by Design» finden vor allem Anwendung, wenn etwas neu kreiert wird. Die Frage «fällt unsere Firma unter die Verordnung?» ist eigentlich zu generell. Richtiger Weise müsste sie für jede bestehende und neue App oder Online-Dienstleistung separat gestellt werden. Der Hauptteil der Firmen, die lediglich einfache Kundenkarteien führen, brauchen aber wie erwähnt keine kostspielige Beratung einer Anwaltskanzlei oder Beratungsfirma.

Sie erwähnten unser eigenes neues Datenschutzgesetz, welches in Arbeit ist. Gibt es relevante Punkte, in denen sich DSGVO und das revidierte Schweizer DSG widersprechen?

Wir haben die vom Bundesrat vorgeschlagene Totalrevision des DSG auf unserer Homepage bewertet und mit der DSGVO verglichen. Der bundesrätliche Vorschlag ist gut gemacht und geschrieben, sieht aber bei den Instrumenten, welche auch das EU-Recht vorsieht, stellenweise unnötige Abweichungen vor. Es gibt auch in Bezug auf die Kompetenzen unserer Behörde einige Abweichungen, die wenig geglückt sind. Beispielsweise müssen in der EU die Best Practices der Datenschutzbehörde vorgelegt werden, was der bundesrätliche Vorschlag nicht verlangt. Und bei Risikofolgenabschätzungen soll es Erleichterungen in der Schweiz geben, die in der DSGVO nicht vorhanden sind. Ich sage nicht, dass wir das EU-Recht einfach integral abschreiben sollten, aber da, wo man die gleichen Instrumente einsetzen will, sollte man Abweichungen vermeiden. Sonst wird das für die Bürger und die Wirtschaft zu kompliziert. Diese Punkte kann man im Gesetzgebungsprozess aber ohne weiteres korrigieren. Beim Vorschlag fehlt auch das Recht auf Portabilität, also das Recht, seine Daten in gesammelter und maschinenlesbarer Form von einem Anbieter zu einem anderen zu bewegen. Ab dem 25. Mai haben wir alle einen Anspruch auf Portabilität gegenüber Anbietern in der EU, aber nicht gegenüber unseren eigenen in der Schweiz. Ich gehe aber davon aus, dass unsere Wirtschaft begriffen hat, dass es bei grossen Projekten wie SwissID oder Swisssign Sinn macht, den Portabilitätsanspruch gegenüber EU-Bürgern auch für Schweizer User anzubieten. Auch diese unverständliche Abweichung von der DSGVO kann vom Parlament im Gesetzgebungsverfahren ohne Weiteres nachgeholt werden.

Wie wird man in der Schweiz die Sanktionen handhaben?

Die Sanktionen sind ein Problem. Aufgrund systemischer Unterschiede der Rechtsordnungen können wir die Verwaltungssanktionen der EU-Lösung schwerlich direkt übernehmen. Die neu vorgesehene Maximalbusse von 250'000 Franken ist für Mitarbeitende eines Rechtsdienstes hoch, für grosse kapitalkräftige Firmen indessen nicht abschreckend. Hier hat der Bundesrat das Ei des Kolumbus nicht gefunden. Ich setzte mich in den parlamentarischen Beratungen dafür ein, dass eine geeignete Lösung gefunden werden kann, die nicht auf die Mitarbeitenden des mittleren Kaders zielt. ■

«Der firmeninterne Datenschützer muss die Rolle des Advocatus Diaboli einnehmen.»

Adrian Lobsiger, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter