Trust in, and value from, information systems

Nr. 02 | Juni 2017 | www.isaca.ch

Switzerland Chapter NEWSLETTER

xx

xx Seite @

xx

xx Seite @

ISACA-Training

Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder Seite @

GDPR – die neue Datenschutzverordnung der EU hat es in sich …

… und bleibt damit nicht ohne Folgen für Unternehmen in der Schweiz.

Von Martin Andenmatten, CISA, CRISK, CGEIT und ITIL-Master

Der Schutz der Privatsphäre ist ein hohes Gut, welches insbesondere im Zeitalter von Sozialen Medien, Big Data und «Everything as a Service» nicht selten zu kontroversen Diskussionen führt. Die Durchdringung der IT-Technologie, nicht nur im beruflichen sondern insbesondere auch im privaten Bereich, macht den Schutz der einzelnen Individualrechte von Bürgern zwingend nötig. Das Ausspionieren und die Profilierung von Web-Nutzern durch grosse Internet-Giganten wie beispielsweise Facebook, Google oder Amazon haben die Grenzen des Erträglichen schon lange überschritten. Jeder der versucht hat Einträge seine Person betreffend aus einem System zu löschen kann davon ein Lied singen.

Der Schutz auf personenbezogene Daten wird massiv erweitert

Am 28. Mai 2018 tritt nun eine neue Datenschutzverordnung der EU in Kraft: die General Data Protection Regulation (GDPR) 2016/679. Unternehmen können sich bereits seit letztem Jahr auf diese neuen Bestimmungen vorbereiten. Auch die Schweiz ist aktuell daran, ihr Datenschutzgesetz zu stärken und insbesondere auf die neue Europäische Verordnung auszurichten. Wie das schweizerische Datenschutzgesetz dann konkret aussieht, ist derzeit noch nicht definitiv entschieden. Die Vernehmlassung ist erst im April 2017 abgeschlossen worden und der Ball liegt nun wieder bei den Behörden.

Man könnte nun argumentieren, dass GDPR eine Europäische Gesetzgebung ist und uns dies in der Schweiz nicht wirklich kümmern muss. Das ist jedoch nicht der Fall. Es gilt für alle Unternehmen weltweit, welche Leistungen für die EU oder für EU-Bürger anbieten. Oder sei es nur, dass ein hiesiger Webshop-Betreiber Produkte an Personen in der EU anbietet oder Webstatistiken führt und damit Daten von natürlichen Personen bearbeitet. Alle Unternehmen in der Schweiz, welche Waren oder Dienstleistungen für

den Europäischen Raum anbieten oder Mitarbeiter aus dem Europäischen Raum einsetzen, werden nicht darum herumkommen, die GDPR-Anforderungen zu befolgen.

Für Unternehmen sind sämtliche Kunden und Kontakte in erster Linie individuelle, natürliche Personen, welche entsprechend der neuen Regulation umfassende Rechte haben. Sie sind daher gut beraten die neue Verordnung genau zu studieren und eine Reihe von Prozessen zu implementieren. Dass es der EU mit der Umsetzung ernst ist, liegt bereits an der grundlegenden Abschreckung durch Bussenandrohung: Verletzungen der Datenschutzprinzipien werden mit 4% des weltweiten Umsatzes und bis zu 20 Millionen Euro bestraft.

Neue Verantwortlichkeiten mit Auswirkungen auf die IT

Es fängt bereits damit an, dass eine vollständige Dokumentation der bestehenden Verarbeitungen, deren Zweck und Rechtsgrundlage sowie der beteiligten Provider vorhanden sein muss. Die Verarbeitungskette aller beteiligten internen und externen Service Provider muss vollständig dokumentiert und mit entsprechenden Verträgen bezüglich der neuen Verantwortlichkeiten abgesichert werden. Ohne die Transparenz des Ist-Zustandes wird es schwierig eine angepasste Soll-Lösung zu entwickeln. Es ist daher wichtig, dass sich nicht bloss die Unternehmensleitung, sondern alle Entscheidungsträger und Schlüsselpersonen mit den Anforderungen von GDPR vertraut machen.

Einzelpersonen haben nun umfassende Rechte was die Verarbeitung von Daten seine Person betreffend anbelangt. Nicht nur, dass er vollständiges Auskunftsrecht über Zweck und Rechtsgrundlage der Verarbeitung verlangen kann, er kann auch jederzeit die Löschung der Daten verlangen, wenn der legitime Zweck der Verarbeitung erfüllt ist. Beispielsweise nach Abschluss und Bezahlung der Transaktion eines Webshop-Einkaufs. Die Umsetzung muss innerhalb eines Monats erfolgen.

Er kann aber auch verlangen, dass die verarbeiteten Daten über ihn zu einem anderen Unternehmen transferiert werden. Wenn er beispielsweise die Bank oder seinen Lieferanten wechselt. Ein weiteres Beispiel ist ein Spital, welches sein Patientendossier und seine Daten vollständig in ein anderes Spital transferieren soll. Er hat zudem auch das Recht auf Richtigstellung von Informationen welche ihn betreffen.

Diese aus Sicht der Einzelpersonen wichtigen und begrüssenswerte Rechte stellen Unternehmen vor grosse Hürden in der Umsetzung. Wie gut ist heute transparent ersichtlich, wo überall personenbezogene Daten abgelegt und von wem sie verarbeitet werden? Dies kann in den verschiedensten Systemen, wie beispielsweise in einem SAP, CRM, Web-Shop, Marketing & Sales etc., sei. Ebenso kann dies auf unterschiedlichen elektronischen Medien und sogar Papier-Dokumenten erfolgen.

Unternehmen, welche bereits erfolgreich Web-Cookies für Datenanalyse-Zwecke einsetzen und Nutzerprofile für Marketing-Aktionen nutzen, werden ihre Lösung ebenfalls überdenken müssen, denn diese Cookies gelten explizit als Verarbeitung von personenbezogenen Daten. Denn die Identifikation von Individuen kann mittels einer Kombination von anonymen Daten ermittelt werden (Pseudonymisierung).

Es ist bei weitem nicht mehr damit getan, neu formulierte Datenschutzbestimmungen den Nutzern von Websites anzubieten, welche diese dann genervt einfach wegklicken können. Dass in solchen Hinweisen implizit die Zustimmung zur Verarbeitung abgefragt wird, ist nur eine Seite der Medaille. Die dem Nutzer zustehenden Rechte müssen nicht nur klar offengelegt, sondern auch mit entsprechenden Verfahren intern sichergestellt werden. So reicht es nicht, automatisierte Verfahren einzurichten, welche die Anfragen der einzelnen Personen abwickeln. Es muss immer auch eine verantwortliche Person offengelegt werden, an welche sich die Berechtigten wenden können und ihm menschliches Gehör verschafft.

Die Unternehmen haben zudem auch erweiterte Sorgfaltspflichten, welche sie über alle beteiligten Provider garantieren müssen. Datenschutzverletzungen müssen binnen 72 Stunden an die Datenschutzbehörde gemeldet werden. Dabei

WEITERE INFORMATIONEN

Weitere Informationen zu den hängigen Datenschutzverordnungen finden sich unter folgenden Links:

- GDPR:
  https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/eu-richtlinie-d.pdf
- Vorentwurf Schweizerisches Datenschutzgesetz:
  https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vorentw-d.pdf

ist bei einem Verlust von Datenträgern, wie beispielsweise ein USB oder auch ein Cybersecurity-Vorfall, genauestens zu untersuchen ob personenbezogene Daten betroffen sind. Jeder interne oder externe Service Provider muss so einen Vorfall unverzüglich an das verantwortliche Unternehmen melden. Sollten sich grosse Risiken auf die Rechte der betroffenen Personen ergeben, sind auch diese sofort zu informieren. Zudem müssen all diese Vorfälle detailliert dokumentiert und ein Log darüber geführt werden.

Die Verarbeitung der Daten erfolgt über die Systeme der IT und der beteiligten Service Provider. Lösungen zur Ausübung der umfangreichen Rechte müssen daher auch zu einem Grossteil über entsprechende Prozesse und Verfahren innerhalb der IT sichergestellt werden.

Was ist zu tun?

Es bleibt noch knapp ein Jahr bis zur Umsetzung der neuen Anforderungen. Wer damit noch nicht begonnen hat, wird arg in Bedrängnis kommen den Nachweis zu erbringen, dass er GDPR-compliant ist. Es gibt zwar eine gewisse Übergangsfrist und in der Praxis wird sich zeigen müssen, wie heiss die Suppe tatsächlich gegessen wird. Aber man kann sich auch ein Szenario vorstellen, wo tausende von Personen nach in Krafttreten der neuen Datenschutzverordnung auf die Unternehmen zugehen und die Löschung ihrer Daten verlangen. Wie geht man damit um?

Folgende Schritte sind für eine Umsetzung der Anforderungen der neuen GDPR-Regelung zu berücksichtigen:

1. Seriöse Überprüfung, ob und in welchem Masse das Unternehmen von der neuen Verordnung betroffen ist. Dazu braucht es eine Transparenz, wo und zu welchem Zweck welche Daten verarbeitet werden und welche Websites ausgewertet werden.
2. Benennen eines internen Datenschutzverantwortlichen, welcher mit der Aufgabe betraut wird, die Koordination der Umsetzung innerhalb des Unternehmens sicherzustellen. Dazu gehören die Prozesse und Verfahren zur Information, Löschung, Berichtigung und Transfer der personenbezogenen Daten. Hier macht es wohl auch Sinn, rechtlichen Rat beizuziehen.
3. Dokumentation und Kategorisierung der verarbeiteten Daten. Dabei gilt insbesondere sicherzustellen, dass die Menge der verarbeiteten Daten explizit nur dem vereinbarten Zweck dient und nicht darüber hinausgeht. Personenbezogene Daten dürfen nicht um ihrer selbst willen erhoben werden, sondern nur dann, wenn es zur Erbringung eines Dienstes wirklich erforderlich ist.
4. Sicherstellen der rechtlichen Legitimierung der Verarbeitung von personenbezogenen Daten. Dazu braucht es eine Offenlegung des Zwecks der Verarbeitung, eine explizite Zustimmung der betroffenen Personen und letztlich eine Bewilligung der Datenschutzbehörde.
5. Sicherstellen, dass die Verantwortlichkeiten des Unternehmens mit entsprechenden Pflichten in den Verträgen mit externen Providern und Sublieferanten abgesichert sind. Wenn die verarbeitende Stelle in einem als nicht vertrauenswürdig deklarierten Land erfolgt, braucht es besondere Bestimmungen und Legitimationen. Dabei gilt auch hier: die Accountability bleibt beim Unternehmen bestehen.
6. Grundsätzliche Überarbeitung der technischen Architektur und Lösungsimplementierung. Systeme und Lösungen sind grundsätzlich so zu bauen, dass diese frei von Schwachstellen und robust gegen Angriffe geschützt sind. Zudem sind die Voreinstellungen von Applikationen so zu gestalten, dass Privilegien möglichst niedrig gewählt und selten genutzte Features grundsätzlich deaktiviert sind.

Die Vereinheitlichung des Datenschutzgesetzes auf europäischer Ebene bringt bestimmt sehr grosse Vorteile. Es darf davon ausgegangen werden, dass auch die schweizerische Verordnung in den Grundzügen ähnlich definiert wird, damit die Handelsbeziehungen nicht unnötig erschwert werden. Es bleibt jedoch noch viel zu tun – gerade jetzt in einer Zeit, in welcher IT-Systemgrenzen aufgebrochen und mit einer Multi-Cloud-Umgebung verschmelzt werden. Herr über Daten und Verarbeitung zu bleiben, lässt sich nicht völlig automatisieren. Es gilt insbesondere hier, die Kontrolle nicht zu verlieren.

Es ist wichtig sich mit GDPR genauer zu befassen, um beurteilen und entscheiden zu können wie diese Regelungen anzuwenden sind. Die Glenfis AG bietet ab Juni 2017 akkreditierte Schulungen an, welche die Grundlagen zu GDPR vermitteln und das erworbene Wissen mit einem international anerkannten Zertifikat besiegelt.

DER AUTOR

Martin Andenmatten ist seit 30 Jahren in unterschiedlichen Bereichen der Informatik tätig.

Certified Information System Auditor (CISA), Certified in the Governance of Enterprise IT (CGEIT), Certified in Risk and Information System Control (CRISC), COBIT® 5 Certified Assessor und akkreditierter COBIT® 5 Trainer für Foundation, Implementation und Assessor Ausbildungen. Zudem ist Martin Andenmatten zertifizierter ITIL® Master, ISO/IEC 20000 Auditor und Practitioner. Als diplomierter Wirtschaftsinformatiker II und diplomierter Betriebsökonom FH verfügt er über ein breit abgestütztes theoretisches Wissen. Seine Praxiserfahrungen hat er als Herausgeber und Autor in seinen Büchern «ISO 20000: Praxishandbuch für Servicemanagement und IT-Governance» sowie «Services managen mit ITIL®» und «COBIT 5 Grundlagen» beschrieben.