© depositphotos, everythingposs

Es ist höchste Zeit zu handeln

Die schnelle Digitalisierung in Wirtschaft und Gesellschaft birgt grosse Gefahren und exponiert insbesondere sensible Unternehmensdaten. Das wertvolle Gut zu schützen ist eine grosse Herausforderung. Auch das Verhalten der Benutzer hat sich stark verändert: Geschäftsdaten überall, zur jeder Zeit und auf jedem Gerät.

Wolfgang Sidler

Die neue EU-Datenschutz-Grundverordnung (DSGVO) ist seit bald einem Jahr in Kraft; es handelt sich um eine neue Verordnung zum Schutz personenbezogener Daten. Sie soll die Datenschutzgesetzgebung im europäischen Binnenmarkt harmonisieren und Einzelpersonen die Kontrolle über ihre Daten zurückgeben. Die DSGVO wird internationale Geschäftsbeziehungen fördern und Verbrauchern die Gewissheit geben, dass ihre Daten sicher sind.

Erste DSGVO-Busse verhängt

Aufgrund der extraterritorialen Wirkung der DSGVO müssen zahlreiche Schweizer Unternehmen die Verarbeitung von Personendaten auf diese neuen Datenschutzbestimmungen ausrichten, wollen sie nicht Reputationsschäden sowie Sanktionen wie Schadenersatz und Bussen in der Höhe von bis zu 20 Mio. Euro oder vier Prozent des globalen Jahresumsatzes in Kauf nehmen. Neben der Vereinheitlichung des Datenschutzes in den EU-Mitgliedstaaten sollen mit der DSGVO die Datenschutzbestimmungen auch an die

«Datenschutz ist eine Compliance-Angelegenheit, die jedes Unternehmen beachten muss.»

digitale Welt angepasst werden. Letzteres ist – abgesehen von den internationalen Verpflichtungen der Schweiz – auch der Grund, weshalb zurzeit sowohl der Bund als auch die Kantone ihre eigenen Datenschutzgesetze revidieren. Neben diesen schweizerischen Datenschutzgrundlagen müssen jedoch viele Unternehmen in der Schweiz künftig auch die (strengere) DSGVO berücksichtigen, selbst wenn sie keine Niederlassung in der EU haben.

Beobachtete Verstösse gegen die DSGVO wurden wegen mangelnder Verschlüsselung (Webseite ohne SSL-Verschlüsselung), fehlende Datenschutzerklärung auf der Webseite, Nutzung von Google Analytics ohne IP-Anonymisierung und sauberes Opt-in und schlechte oder fehlende IT-Security (Benutzerberechtigungen) festgestellt.

Das erste bekannte Bussgeld auf Grundlage der DSGVO in Deutschland wurde gegen das soziale Netzwerk knuddels.de verhängt. Es beträgt 20 000 Euro. Der Verstoss bezieht sich auf das unverschlüsselte Speichern Hunderttausender Passwörter. Die niedrige Busse ist darauf zurückzuführen, dass sich das Unternehmen nach einem Hackerangriff selbst an die Behörde wandte und die Nutzer über das Datenleck informierte.

Wer ist betroffen?

Die DSGVO führt neu das sogenannte Marktortprinzip ein: Sobald ein Unternehmen aus der Schweiz oder einem anderen EU-Drittstaat Produkte und Dienstleistungen in der EU ansässigen Personen anbietet oder das Verhalten dieser Personen beobachtet (z.B. durch Web-Analysetools), greift die DSGVO; darunter fallen nur personenbezogene Daten. Dies umfasst alle Informationen, mit denen eine Person direkt oder indirekt identifiziert werden kann. Die Person, deren Daten verarbeitet werden, erhält mit der DSGVO weitreichende Rechte. So kann sie unter gewissen Umständen verlangen, dass ihre Daten gelöscht werden (Recht auf Vergessenwerden). Auch gibt es ein Recht auf Datenübertragbarkeit (Datenportabilität); dabei kann die betroffene Person die Herausgabe ihrer Daten in einem maschinenlesbaren Format sowie deren Übertragung an einen Dritten verlangen.

DSGVO-Management

Das DSGVO-Managementsystem soll so aufgebaut sein, dass die Mitarbeitenden eines Unternehmens nur genau die Informationen bekommen (müssen), die sie zur korrekten Umsetzung des Datenschutzes benötigen. Daher besteht das DSGVO-Managementsystem aus vielen kleinen Weisungen, die nicht immer von allen Mitarbeitenden verpflichtend zu lesen sind, aber einen möglichst grossen Bereich der DSGVO abdecken und der Firma dabei den grösstmöglichen Nutzen zukommen lassen soll. Das DSGVO-Managementsystem basiert auf Basis von internationalen Standards wie ISO 27001. Das hat gute Gründe, denn ohne die Informationssicherheit kommt auch der heutige Datenschutz nicht aus, der zur Erreichung der Vertraulichkeit, Integrität und Verfügbarkeit eben genau diese Schutzmechanismen benötigt, die bereits in der Vergangenheit in Informationssicherheitsmanagementsystemen (ISMS) gefordert wurden. Sie haben also mit dem DSGVO-Managementsystem (vgl. auch Abb. 1) gleich mehrere Punkte erfüllt, nämlich:

- die nachweisliche Einhaltung des Datenschutzes auf Basis der DSGVO
- eine insgesamt reduzierte Risikosituation im Unternehmen und damit

Abb. 1: Gezeigt werden die notwendigen Richtlinien und Weisungen für ein erfolgreiches DSG-Managementsystem, kombiniert mit dem Sicherheitsstandard ISO 27001. Unter «externe Sicht» sind Aufgaben gemeint, die von aussen in Bezug auf die DSGVO sichtbar sind und von jedem betroffenen Unternehmen umgesetzt werden müssen.

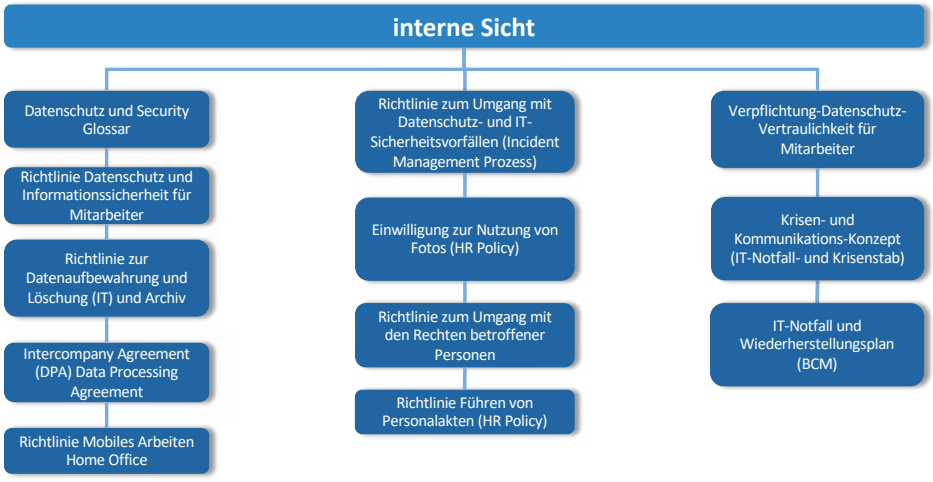

Abb. 2: DSGVO-Managementsystem Teil 2

verbunden auch weniger Haftungsrisiken für die Verantwortlichen (z.B. Geschäftsführung, Inhaber), da wesentliche Regelungen und Dokumentationen bereits vorliegen
- die nachweisliche Einhaltung zentraler Anforderungen aktueller Standards zur Informationssicherheit wie ISO 27001
- mehr Sicherheit für die Mitarbeitenden, da sie in allen wesentlichen Bereichen des Datenschutzes Regelungen und Vorgaben nachlesen können und sich nicht auf ihr Bauchgefühl verlassen müssen

Herausforderungen für den DPO

Der Data Protection Officer (DPO) im Unternehmen hat die folgenden Aufgaben:

- Durchführen einer GAP-Analyse, um den aktuellen Stand in Bezug auf den Datenschutz zu ermitteln
- Erstellen des DSGVO-Managementsystems inkl. der Übersicht der Verarbeitungstätigkeiten mit den Verantwortlichen (Art. 30 DSGVO)
- die neuen Rechte der betroffenen Personen erfüllen können (Auskunft, Löschung, etc.) (Art. 15 DSGVO)
- die Datenschutz-Folgenabschätzung in den Risiko-Prozess integrieren (Art. 35 DSGVO)
- innert 72 Std. einen Datenschutz-Vorfall melden können (PR, Juristen, technische Umsetzung) (Art. 33 DSGVO)
- Outsourcing-Verträge überprüfen und wenn nötig anpassen (Art. 28 DSGVO)
- Durchführen von Datenschutz-Schulungen

Beim Datenschutz ist die Einwilligung der betroffenen Person äussert wichtig, wenn es keine gesetzliche oder vertragliche Grundlage gibt. Dazu muss die Person transparent und verständlich über den Zweck der Datenverarbeitung informiert werden. Gründe für das Bearbeiten der Personendaten können auch vertraglicher Natur oder das Erfüllen einer Rechtspflicht (z.B. Geldwäschereigesetz etc.) sein. Hier gilt es eine Abwägung zu treffen.

DSGVO/DSG-Datenschutz-Audit

Was benötigt man, um einen DSGVO/DSG-Datenschutz-Audit zu bestehen?

- Können Sie den Nachweis erbringen, wie Sie sich als Unternehmen auf die DSGVO vorbereitet haben?
- Haben Sie ein Verzeichnis von den Verarbeitungstätigkeiten?
- Wie stellen Sie die Einhaltung der Betroffenenrechte (auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit) sicher?
- Wie stellen Sie sicher, dass Ihre technischen und organisatorischen Massnahmen bzw. die Ihrer Dienstleister ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten?
- Wie setzen Sie die Datenschutz-Folgenabschätzung um?
- Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern an die neuen Regelungen der DSGVO angepasst?
- Haben Sie einen Datenschutzbeauftragten (DPO)? Wie ist dieser in Ihre Organisation eingebunden?
- Können Sie die Meldepflichten einhalten?
- Können Sie die notwendigen Dokumente (Weisungen und Richtlinien) nachweisen?
- Wie haben Sie Ihre Mitarbeitenden inkl. C-Level geschult?

Wann kommt das neue CH-Datenschutzgesetz?

Weil die Bestimmungen über den Datenschutz in der Schweiz zurzeit viel weniger weit gehen als in der EU, könnten international tätige Firmen künftig Probleme bekommen. Die zuständige Nationalratskommission lässt sich Zeit bei der Beratung des neuen CH-Datenschutzgesetzes.

Das Ziel ist nun, das pendente Geschäft bis zur Frühlingssession 2019 fertig zu beraten, sagt beispielsweise Kurt Fluri (FDP, Solothurn). Plan ist nun, dass der Ständerat das neue Datenschutzgesetz diesen Sommer im Plenum besprechen kann. Das kann aber zeitlich eng werden für eine Inkraftsetzung auf Anfang 2020. Man kann nur hoffen, dass der Entwurf des Parlaments dem DSGVO in den Grundzügen angepasst wird. Die EU selbst erachtet die Einhaltung der Konvention 108 als zentral für die Anerkennung der Gleichwertigkeit. Eine rasche Revision des Datenschutzgesetzes würde für die Firmen bald Rechtssicherheit schaffen.

© depositphotos, axkabakov

«LUCERNE LAW & IT SUMMIT»

Am 28. Mai 2019 findet der dritte «Lucerne LAW & IT Summit 2019» unter dem Patronat der Uni Luzern mit hochkarätigen Speakers zum Thema «Ein Jahr EU-Datenschutz-Grundverordnung – Erste Erfahrungen und Ausblick auf weitere Entwicklungen» statt. Ziel der Tagung ist es, Recht und IT zusammenzubringen und einen praxisorientierten Dialog zwischen Juristen und IT-Fachleuten in Gang zu setzen, um aktuelle Themen sowie künftige Entwicklungen an der Schnittstelle von Recht und IT abzubilden. Nebst den DSGVO-Auswirkungen auf Schweizer Unternehmen und Behörden werden ferner Megatrends und neue technologische Herausforderungen präsentiert.

Anmeldung unter:
https://bit.ly/2VCXMbW

Fazit

Datenschutz ist eine Compliance-Angelegenheit und sollte bis 2020 in jedem Unternehmen eingeführt sein. Wer einen guten Datenschutz will, benötigt eine gute, angemessene und wirtschaftliche Cyber-Security (Art. 32 DSGVO). Spätestens jetzt ist es an der Zeit, im Unternehmen einen «Datenschutzverantwortlichen – DPO» zu benennen oder extern beizuziehen. ■

WOLFGANG SIDLER
Inhaber SIDLER Information Security GmbH, Stv. des Datenschutzbeauftragten des Kantons Luzern von 2009 bis 2018, Master of Advanced Studies in Information Security, Certified ISO 27001 Lead Auditor und Mitautor des «IT-Sicherheitshandbuches für die Praxis» (vgl. www.sihb.ch)