THE SWISS
INFORMATION GOVERNANCE
COMPETENCE CENTER

Leistungsbeschrieb

DATENSCHUTZ.digital

MATRIO Methode®

Worum geht es?

Datenschutz wird 2018 ein zentrales Thema für viele Unternehmen weltweit. Obwohl Datenschutzgesetze seit über 25 Jahren existieren, hatte deren Umsetzung bei den meisten Organisationen wenig Priorität. Dies ändert sich nun mit der Einführung der Datenschutz-Grundverordnung (DSGVO) der EU. Deshalb müssen viele Organisationen ihre Datenschutz-Fähigkeiten verbessern und auf einen Stand bringen, welcher mit der Datenschutz-Grundverordnung im Einklang steht. Dies gilt auch für viele Schweizer Unternehmen.

Datenschutz und DSGVO: Situation Schweiz

Die Datenschutz-Grundverordnung der EU ist eine EU-weite Norm für die Verarbeitung personenbezogener Daten. Sie ersetzt de facto die nationalen Gesetze der EU-Mitgliedsstaaten, da sie nur noch wenig Spielraum für nationale Besonderheiten lässt. Durch die Anwendbarkeit auf Konzerne und damit deren Töchter betrifft die DSGVO u.a. auch Konzerne in der Schweiz und weltweit. Die Bedeutung der DSGVO geht damit über die EU-Mitgliedsstaaten hinaus. Wer Geschäfte mit Gesellschaften oder Behörden in der EU abwickelt oder Leistungen in der EU absetzen will, wird mit grösster Wahrscheinlichkeit die Anforderungen der DSGVO erfüllen müssen. Das trifft auch viele Unternehmen in der Schweiz, die vielfach stark exportorientiert sind.

Das schweizerische Datenschutzgesetz befindet sich in der Revision. Tatsächlich ist aber auch hier der Spielraum gering, denn die DSGVO wird zur Messlatte. Insofern ist es für Schweizer Unternehmen durchaus angebracht, die DSGVO Anforderungen direkt zu erfüllen und nicht auf die CH-Spezialnorm zu warten. Die DSGVO muss bis zum 25.5.18 umgesetzt sein.

Dem Unternehmen in der Schweiz wird deshalb empfohlen, den Datenschutz risikobasiert umzusetzen, d.h. bei der Umsetzung darauf zu achten, wo die grössten Risiken bestehen und entsprechend zu handeln.

Viele Themen wie Datenbeherrschbarkeit (Information Governance) oder Informationssicherheit sind nicht innert weniger Monate umsetzbar - hier bedarf es wesentlich grösserer Investitionen. Insbesondere wer seine Aufgaben im Bereich der Informationssicherheit noch nicht gemacht hat, der sollte das spätestens jetzt dringend tun.

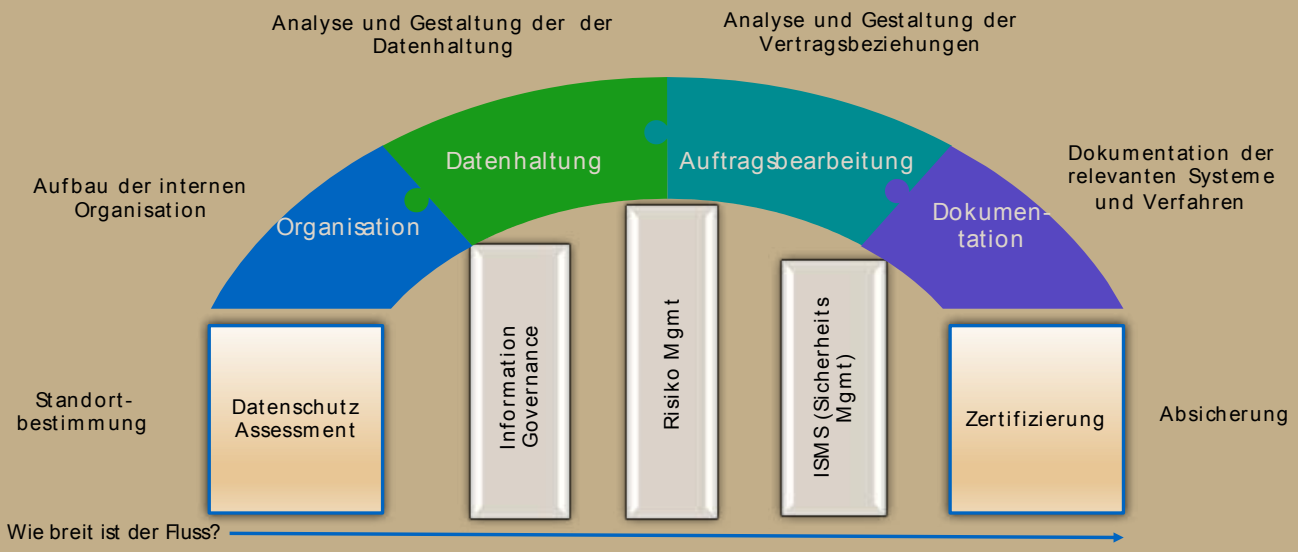
Methode

Der Aufbau der notwendigen Datenschutz-Fähigkeiten ist ein Prozess, welcher je nach Stand der aktuellen Fähigkeiten unterschiedlich lange dauert. Das KRM hat zu diesem Zweck eine Methode entwickelt, welche sich «DATENSCHUTZ.digital» nennt. Sie erlaubt ein kundenangepasstes Vorgehen und übernimmt die Grundprinzipien der MATRIO® Methode[1]. Diese bestehen in einem gezielten Vorgehen bei akutem Handlungsbedarf („Red Flags"), gekoppelt mit mittel- bis langfristigen Tätigkeiten, welche der Verbesserung der Performance wie auch der Conformance dienen.

Wir vergleichen den Aufbau der Datenschutz-Fähigkeiten mit dem Aufbau einer Brücke. Die Breite des zu überquerenden Gewässers hängt von der Exposition des Kunden sowie dem Anteil der zu verarbeitenden Personendaten wie auch den aktuellen Prozessen und Systemen ab.

[1] http://www.matrio.swiss/

Die Methode basiert auf einer modularen Vorgehensweise, in welcher die folgenden Themenblöcke bearbeitet werden:



Die Brückenelemente stellen die wichtigsten Anforderungen dar, die erfüllt werden müssen. Einige davon kann man sehr schnell erfüllen, andere benötigen einen längeren Aufbau. Letztere sind deshalb als Säulen dargestellt.

Unser Datenschutz-Assessment bildet die Basis für die weiteren Aktivitäten und zur Aufwandschätzung. Es beschreibt die vorhandenen Fähigkeiten, den dringendsten Handlungsbedarf sowie die längerfristigen Aufbauarbeiten.

Datenschutz-Assessment

In der Anfangsphase besteht der wichtigste Teil aus dem Datenschutz-Assessment für die Standortbestimmung. Dieses erlaubt die Identifikation der Hauptrisiken. Gleichzeitig wird der Handlungsbedarf bei den anderen Brückenelementen und Brückenpfeilern identifiziert und beschrieben.

Um die Reife und den Ist-Zustand beim Kunden zu erfassen, führen wir ein mehrstufiges Assessment durch:

1. **Kurz-Assessment** (webbasiert)
2. **Intensiv-Assessment** (Workshop mit Bericht)
3. **Penetration Testing** (bei vorhandenen Strukturen)

Das Kurz-Assessment ist selbsterklärend und kann über die KRM-Website zugegriffen werden: https://information-governance.ch/services/beratungsleistungen/dsgvo-kurz-assessment/.

Die Hauptarbeit besteht in der Durchführung des **Intensiv-Assessments**. Beim Kunden werden die notwendigen Fähigkeiten für den Datenschutz erfasst. Inhaltlich werden dabei die folgenden Themen untersucht:

- Datenschutz Organisation: Welche Rollen und Prozesse existieren?
- Datenhaltung: Wie werden Personendaten verarbeitet und wo werden sie gespeichert?
- Verträge: Wer verarbeitet Personendaten im Auftrag und ist dies geregelt?
- Dokumentation: Wie gut sind die Verfahren dokumentiert?

Aus den Aktivitäten erstellen wir einen Bericht, welcher eine Zusammenfassung der wichtigsten Feststellungen und Empfehlungen für das weitere Vorgehen enthält. Der Schwerpunkt liegt in der Priorisierung nach Bausteinen und Themen sowie Angaben, in welchen Bereichen weitere Analysen notwendig sind. Der Bericht wird risikobasiert erstellt und fokussiert auf die Hauptrisiken im Kontext Datenschutz. Das Penetration Testing ist ein optionales Modul, welches sich vor allem für die Beübung der Organisation und die Nachprüfung eignet.

Sofortmassnahmen

Nach dem Assessment werden die identifizierten Themen mit hoher Priorität abgearbeitet. Hier werden kurzfristig erste Organisationsentscheidungen getroffen (wer ist für den Datenschutz zuständig?) und kurzfristige Massnahmen beschlossen, die unmittelbare Abhilfe schaffen (z.B. Anpassung von Verträgen mit Verarbeitern). In dieser Phase muss das Risiko-Management System soweit aufgebaut werden, dass die Datenschutz-Risiken durch die Organisation erkannt werden können. Im nächsten Schritt werden diese Hauptrisiken identifiziert und behandelt. Transparenz in allen Verarbeitungsschritten ist eine zentrale Anforderung des Datenschutzes. Wir unterstützen Sie beim Aufbau der notwendigen Dokumentation (Verarbeitungsverzeichnis, Verfahrensdokumentation).

Wie geht es weiter?

Die Resultate des Assessments dienen als Grundlage für die weitere Planung. Information Governance, Risko Management oder Informationssicherheit werden in gesonderten Projekten und Vorhaben umgesetzt. Gerne unterstützen wir Sie beim Aufbau dieser wichtigen Fähigkeiten.

Zertifizierung

Als Anbieter einer Lösung bietet die DSGVO eine neue Möglichkeit der Profilierung. In der Zukunft können Produkte nun auch nach der DSGVO für die ganze EU zertifiziert werden, womit sich einfach neue Märkte erschliessen lassen. Wir unterstützen Sie bei der Zertifizierung Ihrer Produkte durch die DQSBIT[2].

Aufwand und Kosten

Das Datenschutz-Assessment wird von uns zu einem fixen Preis angeboten. Dieser hängt vom Untersuchungsumfang, der Komplexität der Datenhaltung und der Organisation ab. In der Regel benötigen wir für die beschriebenen Lieferergebnisse insgesamt 3-5 Personentage Aufwand.

Alle Folgeaktivitäten sind individuell zu planen und werden mit dem Kunden vereinbart. Viele der aufzubauenden Fähigkeiten sind Teil anderer Initiativen und können vielfach kombiniert werden.

[2] https://www.dqsbit.de/

Weitere Informationen:

Wer ist das KRM?

Das Kompetenzzentrum Records Management (KRM) fokussiert sich auf Information Governance. Wir steigern den Wert von Information für unsere Kunden und minimieren die Risiken. Wir haben Erfahrung mit nationalen wie auch internationalen Kunden. Wir verfügen über Experten aus den Fachbereichen Recht, Organisation, IT, IT Security und Risko Management. Gerne vermitteln wir Referenzen auf Anfrage.

Wir verknüpfen dabei die klassischen Mittel der Informationstechnik, des Rechts und der Informationswissenschaft mit der neuen digitalen Welt. Wir betreiben dazu das erste Kompetenzzentrum in Europa. Mit unserem amerikanischen Partner Doculabs bieten wir auch ein Portfolio zum Thema Global Information Governance (GIG).

Alles Weitere finden Sie auf unserer Website: www.informationgovernance.ch

Materialien zum Datenschutz

Auch zum Datenschutz finden Sie umfangreiches Informationsmaterial auf unserer Website: https://information-governance.ch/services/datenschutz-und-dsgvo/

Was ist die MATRIO Methode®

Die MATRIO Methode® adressiert Information Governance neu: Strategisches Denken kombiniert mit direkter Lösungsfindung/Implementierung. Die Methode orientiert sich an international anerkannten und etablierten Corporate Governance Grundsätzen. Sie adressiert alle Ebenen der Unternehmensführung und stellt eine durchgängige und transparente Implementierung sicher.

Weitere Informationen auf http://www.matrio.swiss/

Kompetenzzentrum
Records Management
Rotfluhstrasse 91
8702 Zollikon
info@informationgovernance.ch
www.informationgovernance.ch