Zahlreiche Unternehmen sind daran, sich auf die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) vorzubereiten – die Umsetzungsfrist für die DSGVO läuft bis zum 25. Mai 2018. Auch im Hinblick darauf, dass in der Schweiz das Datenschutzgesetz revidiert wird und sehr ähnliche Regelungen wie die DSGVO dereinst (voraussichtlich ab 2019) haben wird, ist dringender Handlungsbedarf gegeben.

DSGVO – HERAUSFORDERUNGEN UND ERKENNTNISSE

VON CARMEN DE LA CRUZ
UND BORIS INDERBITZIN

Unternehmen der IT-Branche sind von den Änderungen besonders betroffen; die Bearbeitung von Daten gehört für sie zum Kernbereich ihrer Geschäftstätigkeit. Die technischen Möglichkeiten erlauben oftmals weitreichende Bearbeitungen von Personendaten durch viele Mitarbeiter, intern oder extern, womit es von Anfang an wichtig ist, sich ein klares Bild von der eigenen System- und Datenbearbeitungslandschaft zu verschaffen. Im Rahmen der Projekte zur Umsetzung der DSGVO haben sich zahlreiche Themen und Herausforderungen in verschiedenen Unternehmen gestellt. Diese gesammelten Erfahrungen seien im nachfolgenden Artikel dargelegt.

Datenschutz ist ein Projekt

Es gibt sie nicht, die EINE Checkliste, das EINE Handbuch und DIE universale Lösung. Die Umsetzung datenschutzrechtlicher Vorschriften erfolgt individualisiert, massgeschneidert in Bezug auf die tatsächlichen Verhältnisse jedes Unternehmens; diese sind individuell, haben ihre eigenen Geschäftsprozesse, bearbeiten zahlreiche Daten auf ihre besondere Weise, haben einen besonderen Kundenstamm, spezifische Dienstleister und eine jeweils unterschiedliche geografische Ausbreitung.

Und so beginnt die Umsetzung der DSGVO mit einem strukturierten, eigenen Projekt, mit genügend Budget und Personal. Es bedarf von Anfang an einer breiten Analyse der eigenen Personendaten und Datenbearbeitungen zur darauffolgenden Beurteilung der geeigneten Massnahmen – kurz: eine umfassende und ehrliche Auseinandersetzung mit den internen (Datenbearbeitungs-) Prozessen. Diese anfängliche Investition an Zeit und Ressourcen ermöglicht es, vorab eine sorgfältige Planung inklusive Ressourcen zu machen sowie im späteren Projektverlauf gezielt und speditiv die notwendigen Prozessanpassungen vorzunehmen und die Umsetzung schnell und v.a. richtig abzuschliessen.

Ausgangspunkt der Umsetzung: Der Ist-Zustand

Die Darstellung des Ist-Zustands sämtlicher Datenbearbeitungen wird allzu häufig unterschätzt und birgt meistens Überraschungen – nicht selten pikante Details, welche die Einhaltung der DSGVO verkomplizieren. Die gute Nachricht ist: Es gibt verschiedene Tools, die es ermöglichen, sämtliche Bearbeitungsprozesse zu analysieren, darzustellen und den Lebenszyklus bestimmter Daten von ihrer Erhebung über ihre Bearbeitung bis zu ihrer Archivierung und/oder Löschung zu verfolgen. Solche Untersuchungen bringen oftmals Überraschendes zutage: Ausufernde Einsichtsrechte für Basisnutzer gewisser Systeme, systemübergreifende Zugriffe auf Stammdaten, externe Zugriffe über Wartungs- und Supportdienstleistungen oder gar systemisch eingebaute Datenübermittlung an Hersteller für den vordergründigen Zweck der Lizenzverwaltung – allesamt Bearbeitungen, bei denen sich die Unternehmensleitung überlegen muss, welche Massnahmen sie zur Einschränkung der Bearbeitung implementieren möchte, und nicht nur um des Datenschutzes willen!

Eine solche Analyse bildet nicht nur eine gute Grundlage für das Projektausmass sowie die Massnahmen zwecks Einhaltung datenschutzrechtlicher Vorgaben. Sie führt der Unternehmensleitung auch vor Augen, welche Bearbeitungen intern überhaupt erfolgen und generell wie die Vorgaben zukünftig aussehen.

Datenschutz-Folgeabschätzung

Die Datenschutz-Folgeabschätzung im Sinne des Datenschutzrechts ist oftmals ein Prozess, den Unternehmen neu aufsetzen müssen oder aber für welchen die bestehenden Produkte-Entwicklungszyklen anzupassen sind. Vor der Einführung neuer Produkte und Dienstleistungen, die die Bearbeitung von personenbezogener Daten beinhaltet, hat sich das Unternehmen die Frage zu stellen, ob sie eine Datenschutz-Folgeabschätzung durchzuführen hat. Die Datenschutz-Folgeabschätzung analysiert eine neu zu implementierende Bearbeitung personenbezogenen Daten aus der Sicht der betroffenen Personen. Je nach vorgesehener Bearbeitung personenbezogener Daten muss das Unternehmen entscheiden, ob es eine Datenschutz-Folgeabschätzung durchführen soll, sodann die Risiken der Bearbeitung den getroffenen Massnahmen gegenüberstellen und unter Umständen das Resultat der zuständigen Aufsichtsbehörde vorlegen.

Die Datenschutz-Folgeabschätzung hilft auch den datenschutzrechtlichen Grundprinzipien «privacy by design» und «privacy by default» gerecht zu werden. Auch für diese Prozesse gibt es verschiedene Tools, darunter eine mehrsprachige Open-Source-Lösung der Aufsichtsbehörde Frankreichs (CNIL, Commission Nationale de l'Informatique et des Libertés)[1].

Data Breach Notification

Kommt es zu einer Datenschutzverletzung, die zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, so muss diese den zuständigen Datenschutzbehör-

den binnen 72 Stunden seit Bekanntwerden der Datenschutzverletzung gemeldet werden – allenfalls sind auch sämtliche von der Datenschutzverletzung betroffenen Personen zu informieren. Die sogenannte Artikel-29-Datenschutzgruppe[2] (Vertreter der EU-Datenschutzbehörden) hat einen Leitfaden entworfen[3], in welchem diePflichten des Verantwortlichen und des Auftragsdatenverarbeiters beschrieben werden, angereichert mit Workflows und Fallbeispielen. Dieses Dokument ist eine wertvolle Denkstütze für das Aufsetzen eines Prozesses zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde. Einen solchen Prozess werden zahlreiche Unternehmen definieren müssen oder in ein bestehendes Business Continuity Management zu integrieren haben. Die Datenschutzverletzung und die damit verbundenen Folgen sind Hauptauslöser für Bussgelder und weitere Sanktionen der Behörden. Es kann deshalb nicht genug Wert auf den Prozess der Datenschutzverletzung gelegt werden. Von den rechtzeitigen Meldungen und professioneller Kommunikation wird schlussendlich abhängen, ob die Busse im oberen angedrohten Bereich (10 resp. 20 Mio. Euro) liegen oder eher im unteren.

Auch für die Meldung einer Datenverletzung innerhalb eines Unternehmens werden unterdessen zahlreiche Tools angeboten (Eingabeformulare im Intranet, Apps), die es intern ermöglichen, eine Datenschutzverletzung an die richtige Stelle zu adressieren und sämtliche benötigten Informationen bspw. mittels Fragebogen oder Eingabemaske mitzuteilen. Dies ist notwendig, da die gesetzliche Frist von 72 Stunden zur Meldung an die zuständige Aufsichtsbehörde sehr knapp ist. Zahlreiche Aufsichtsbehörden verfügen ihrerseits über Online-Meldeformulare, mittels welcher ihnen Meldungen von Datenschutzverletzungen zugesandt werden können.

Wichtig: Hersteller, Lieferanten und Dienstleister

Augen auf bei Herstellern, Lieferanten und Dienstleistern! Erst anlässlich der eingangs erwähnten eingehenden Analyse der internen Datenbearbeitungen ist vielen Unternehmen bewusst geworden, dass externe Dienstleister und Lieferanten Zugriff auf zahlreiche Datensätze haben. Während dies bei Support- und Wartungsarbeiten zumindest bekannt ist, überraschen öfters automatisierte Datenübermittlungen an Lieferanten zwecks Nutzungsstatistiken oder Lizenzpreisberechnungen. Es kann im Interesse des Unternehmens selbst liegen, die Einsicht in diese Daten (seien es personenbezogene Daten oder nicht) einzuschränken. Zudem erfolgen solche Dienstleistungen (gerade Support) nicht selten von ausserhalb der Schweiz, womit sich die Frage der grenzüberschreitenden Bekanntgabe von personenbezogenen Daten stellt. Werden Daten gar ausserhalb der Europäischen Union bearbeitet, sind unter Umständen besondere Massnahmen zu treffen – dies bereits unter geltendem, schweizerischem Datenschutzrecht.

Fazit

Ausgangspunkt zur Umsetzung der DSGVO (und des kommenden revidierten Datenschutzgesetzes) in einem Unternehmen ist eine umfassende Bestandesanalyse über der eigenen (Personen-)Daten sowie der Prozess- und Systemlandschaften. Erst danach können konkrete Massnahmen geplant und umgesetzt und neue Prozesse implementiert werden. Ein mit Zeit und Mittel ausreichend ausgestattetes Projektteam kann dem Unternehmen zur Einhaltung der DSGVO verhelfen – ein Unterfangen, das im Übrigen auch als Qualitätsmerkmal den Kunden gegenüber mitgeteilt werden kann. Die Einhaltung und erfolgreiche Umsetzung des Datenschutzes im Unternehmen kann als Vertrauensbasis für Kunden erachtet werden und somit als Chance für das Unternehmen.

1 www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
2 www.ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936
3 www.ec.europa.eu/newsroom/document.cfm?doc_id=47741

IHR DATENSCHUTZPROJEKT – WAS SIE BEACHTEN MÜSSEN

- **Datenklassifizierung:** Eine Datenklassifizierung nach verschiedenen Datenkategorien von Personendaten, Vertraulichkeitslevel etc. ist Basis für die weiteren Compliance-Aufgaben im Datenschutz.
- **Bestandsaufnahme der Datenbearbeitung:** Machen Sie sich von Ihrer eigenen Prozess-, System- und Datenbearbeitungslandschaft ein klares Bild
- **Verantwortlichkeiten definieren:** Weisen Sie Aufgaben zu und nennen Sie eine interne Anlaufstelle für Datenschutz. Bei Bedarf ernennen Sie diese Person zum Datenschutzbeauftragten.
- **Datenschutz-Folgeabschätzung:** Implementieren Sie die Datenschutz-Folgeabschätzung in jede angedachte Datenbearbeitung und überprüfen Sie mindestens jährlich, ob die Massnahmen den Risiken immer noch genügen.
- **Data Breach Notification:** Implementieren Sie einen Prozess zur internen und externen Bearbeitung von Datenschutzverletzungen.
- Ziehen Sie **Hersteller, Lieferanten und Dienstleister** in Ihr Datenschutzprojekt mit ein
- **Training & Awareness:** Schulen Sie Ihre Mitarbeiter – und kombinieren Sie Datenschutz mit Datensicherheit
- **Unterstützung:** Lassen Sie sich von Experten im Bereich IT-Security und Datenschutzrecht beraten – der Teufel liegt im Detail.

ÜBER DIE AUTOREN

Carmen de la Cruz, Mitglied der **Rechtskommission von swissICT**, Rechtsanwältin/Partnerin de la cruz beranek Rechtsanwälte AG

Boris Inderbizin, Rechtsanwalt de la cruz beranek Rechtsanwälte AG