10 Fragen zur Umsetzung der EU-Datenschutz-Grundverordnung

Am 27. April 2016 wurde die neue EU-Datenschutzgrundverordnung (EU-DSGVO) erlassen. Sie gilt ab 25. Mai 2018, macht umfangreiche Dokumentationserfordernisse, Prüfungen und teilweise massive Umstellungen notwendig. In diesem Artikel werden in einer Art Betriebsanleitung 10 Fragen zur Umsetzung vorgestellt.

Einleitung

In den letzten Monaten sind zu dem Thema unzählige Artikel publiziert, Vorträge und Seminare gehalten worden. Das Thema tritt bei vielen Kunden in der Strukturierung von Informationsbeständen und der Gewährleistung einer korrekten Information Governance immer wieder auf. Es wird mehr oder minder dramatisch auf die möglichen extrem hohen Strafen von bis zu 4% des Umsatzes oder 20 Mio. EUR hingewiesen, um dem Thema Dringlichkeit und Aufmerksamkeit in der Akquise beschaffen. Oft werden spezifische Detailfragen behandelt und die Gesamtsicht geht verloren. Vieles geht so am Thema vorbei.

Es geht vielmehr um einen zukünftig bewussteren Umgang mit Unternehmensinformation als dem wesentlichen Wettbewerbsfaktor in einer zunehmend digitalisierten Gesellschaft. Die EU-DSGVO ist hier ein Teil einer von Unternehmen noch selten korrekt gelebten Information Governance als Teil der Corporate Governance.

Als Verordnung ist Sie direkt national anwendbares Recht, das noch um nationale Gesetze ergänzt wird. In Österreich gilt neben der EU-DSGVO das Datenschutzanpassungsgesetz 2018 (DSG2018), das in einem fragwürdigen Gesetzgebungs-Prozess ohne Berücksichtigung von Begutachtungskommentaren und den notwendigen Verfassungsbestimmungen Anfang Juli 2017 durch den Nationalrat gepeitscht wurde.

10 Fragen

Was sind die 10 wichtigsten Fragen, die sich umsetzungspflichtige Organisationen und ihre Leitungsorgane stellen sollten?

1. Projektorganisation aufsetzen?
2. Bestellung Datenschutzbeauftragter?
3. Awareness, Kommunikation, Schulung und Training?
4. Dokumentation Verarbeitungsvorgänge?
5. Datenschutz-Folgenabschätzung?
6. Erfüllung Informationspflichten & Betroffenenrechte?
7. Vorbereitung Meldung von Verstößen?
8. Privacy by design und by default erfüllt?
9. Prüfung / Überarbeitung rechtlich relevanter Dokumentation?
10. Periodische Überprüfung – Einführung DSMS?

Fragen im Detail

ad 1.) Aufsetzen Projektorganisation & Prozesse

Mittlere und große Organisation benötigen eine Projektorganisation mit Vertretern der verschiedenen Fachabteilungen. Die Projektleitung muss interdisziplinär rechtliche, technische, betriebswirtschaftliche und organisatorische Themen gleichsam behandeln und moderieren können, da es sich bei Datenschutzthemen um eine Querschnittsmaterie handelt. Ihr kommt eine wesentliche Brückenfunktion zu. Kritische Prozesse müssen identifiziert und angepasst werden.

ad 2.) Bestellung eines Datenschutzbeauftragten?

Art. 37 verpflichtet manche Verantwortliche, einen Datenschutzbeauftragten (kann extern wahrgenommen werden) zu ernennen. Die genaue rechtliche Abklärung sollte mit Hilfe eines Rechtsanwalts erfolgen. Es ist nicht empfehlenswert, ohne Notwendigkeit einen Beauftragten zu ernennen,

da diese Rolle diverse Pflichten und Qualifikationserfordernisse mit sich bringt.

ad 3.) Awareness, Kommunikation Schulung und Training

Bei Führungskräften abseits von Rechts-, Compliance oder IT-Abteilungen ist noch ein geringes Bewusstsein vorhanden. Entsprechende Kommunikationsmaßnahmen sind notwendig. Später sind diese durch Trainings und Schulungen aller Mitarbeiter zu begleiten.

ad4.) Dokumentation Verarbeitungsvorgänge

Art. 30 verpflichtet Verantwortliche zur Führung eines Verfahrensverzeichnisses. Letztendlich wird das eine Liste aller verwendeten SW-Anwendungen, der Informationsbestände / Informationsströme und eine genaue Darstellung der IT-Systemlandschaft sein.

ad 5.) Datenschutz-Folgenabschätzung

Art. 35 verpflichtet die Verantwortlichen für jede Verarbeitungsanwendung eine Abschätzung von Risiken und deren Eintrittswahrscheinlichkeit vorzunehmen. Abwägungen und notwendigen Maßnahmen zur Risikominimierung bzw. Compliance müssen beschrieben werden.

ad 6.) Erfüllung Informationspflichten / Betroffenenrechte

Art. 13 - 15 spezifizieren mannigfache Informationspflichten für Verantwortliche bzw. Auftragsverarbeiter und Rechte für Betroffene (z.B. Löschung, Änderung, Datenportabilität etc.). Diese Pflichten sind mit kurzen Fristen versehen. Vorab sind standardisierte Prozesse einzuführen und Information für Auskünfte zusammenzustellen, um das Tagesgeschäft nicht zu beinträchtigen.

ad 7.) Vorbereitung Meldung von Verstößen

Art. 33 verpflichtet Verantwortliche sofort nach Kenntnis eines Datenverlustes oder der Kompromittierung von Systemen eine Meldung an die Datenschutzbehörde zu erstatten. Für diesen Notfall sollten vorab ein Notfall-Team gebildet (kann extern sein) und notwendige Schritte in einem Prozess abgebildet sein. Sonst ist keine zeitnahe Reaktion gewährleistet und dann drohen sehr wahrscheinlich hohe Strafen. Basisinformation für die Meldung beinhalten die Punkte 4.) und 5.).

ad 8.) Privacy by design und by default erfüllt?

Art. 25 verlangt, dass Anwendungen vorab technisch so gestaltet und eingestellt sind, dass ein größtmögliches Maß an Datenschutz gewährleistet ist. Beispiele wären die Verschlüsselung sensibler Daten oder das Verbot auf Webseiten Checkboxes bei Zustimmungserklärungen vorab auszufüllen.

ad 9.) Prüfung / Überarbeitung rechtlich relevanter Dokumentation?

Vertragsmuster, AGBs, Standardvertragsklauseln, Betriebsvereinbarungen, Dienstverträge, Verträge mit Auftragsverarbeitern, Einwilligungserklärungen etc. müssen geprüft, aktualisiert und gegebenenfalls neu eingeholt werden. Das gleiche gilt für interne Richtlinien und Policies. Kurzum die gesamte betroffen Dokumentation muss identifiziert und mit Hilfe eines Rechtsanwalts geprüft und angepasst werden. Dabei ist für Betroffene eine einfache und verständliche Sprache zu verwenden.

ad 10.) Periodische Überprüfung – Einführung DSMS

Art. 24 verlangt eine periodische Überprüfung der getroffenen Maßnahmen. Mittel- und langfristig bedeutet das für mittlere und große Organisationen die Einführung eines (Datenschutz)managementsystems (DSMS) analog eines Information-Security Systems (ISMS) nach ISO 27001. Im Rahmen eines PDCA-Zyklus werden Anpassungen und Verbesserungen vorgenommen.

Umsetzung und Resultat

In einem ersten Schritt sollte man betreffend die Punkte 1.) – 3.) Überlegungen anstellen, Punkt 2.) sollte durch einen Rechtsanwalt abgeklärt werden. Die Punkte 4.) – 9.) sollten gemeinsam mit einem Berater bearbeitet werden. Danach ist die betroffene Dokumentation zu identifizieren und ein Rechtsanwalt mit der Anpassung zu beauftragen.

Mittel- und langfristig ist Punkt 10.) umzusetzen.

Hat man seine Umsetzungsmaßnahmen sorgfältig dokumentiert, so ist es unwahrscheinlich, dass die Datenschutzbehörde bei Mängeln eine Strafe aussprechen wird. Ist ein ernsthaftes Bemühen glaubhaft nachweisbar so wird sie es wohl bei einer Anordnung, Rüge oder eine Aufforderung zu Verbesserung belassen. Außerdem bewirkt die Vorbereitung, dass die Erfüllung von Informationspflichten und Auskunftsrechten ggü. Betroffenen und Behörden nicht zu einer massiven Behinderung des eigentlichen Tagesgeschäfts führt.

Als Nebeneffekt erlangen die Mitarbeiter ein besseres Verständnis für die verwendeten Informationsbestände und deren Wert.

Ein erster Start besteht meist in einer groben Beurteilung des Reifegrades der Organisation und der Bildung eines Projektteams bestehend aus Fachabteilungsleitungen unter Anleitung einer bereichsübergreifenden Projektleitung (eventuell der schon ernannte Datenschutzbeauftragte). Damit wird anfänglich ein Überblick für die Geschäftsführung gewonnen, wo Handlungsbedarf besteht und wo Umsetzungsmaßnahmen anstehen. Ein Zeit- und Ressourcenplan sollte das erste Ergebnis sein.

Abschließende Betrachtungen

Dieser Fachartikel ähnlich einer Betriebsanleitung kann keine detaillierte Abklärung betriebswirtschaftlicher, technischer oder organisatorischer Maßnahmen sowie die notwendige rechtliche Beratung ersetzen. Oft ist die Realität viel komplexer. Die gestellten Fragen stellen aber ein erstes Rahmenwerk dar, um sich mit dieser wichtigen Materie zu beschäftigen und sich Gedanken für die eigene Organisation zu machen.

Mag. Markus Lenotti, Juli 2017
Geschäftsführer
Lenotti Advisors GmbH