iGrafx

WHITE PAPER

General Data Protection Regulation (GDPR): Business Process Management für unternehmensweite Compliance

Oliver Schonschek
Technology Analyst, Insider Research

ABSTRACT

Die Umsetzung der Datenschutz-Grundverordnung bereitet vielen Unternehmen Schwierigkeiten. Obwohl nur noch bis 25. Mai 2018 Zeit dafür ist, kommen die meisten Unternehmen bislang über Insellösungen nicht hinaus.
Dieses White Paper zeigt, wie sich mit den Lösungen von iGrafx durch die Modellierung, Analyse, Optimierung und Automatisierung von Geschäftsprozessen durchgehend Compliance erreichen und die Datenschutz-Grundverordnung (GDPR) für alle Prozesse im Unternehmen lückenlos umsetzen lässt.

1. Datenschutz-Grundverordnung als neue Compliance-Anforderung

Ab 25. Mai 2018 gilt das neue europäische Datenschutzrecht, die Datenschutz-Grundverordnung auch General Data Protection Regulation, kurz GDPR genannt. Das bestehende Bundesdatenschutzgesetz (BDSG) in Deutschland wird ersetzt, GDPR gilt unmittelbar in allen Ländern der Europäischen Union (EU). Ein neues BDSG wird nationale Datenschutzregeln zur Ausgestaltung der GDPR mit sich bringen.

GDPR stellt nicht nur eine Anforderung an Unternehmen in der EU dar, sondern an alle Unternehmen, die Waren oder Dienstleistungen innerhalb der EU anbieten, auch wenn diese ihren Sitz außerhalb der EU haben (sogenanntes Marktort-Prinzip der GDPR).

Für die Unternehmen stehen weitreichende Änderungen in ihren Datenschutz-Prozessen an, die nun zeitnah umgesetzt werden müssen. Dazu gehören unter anderem:

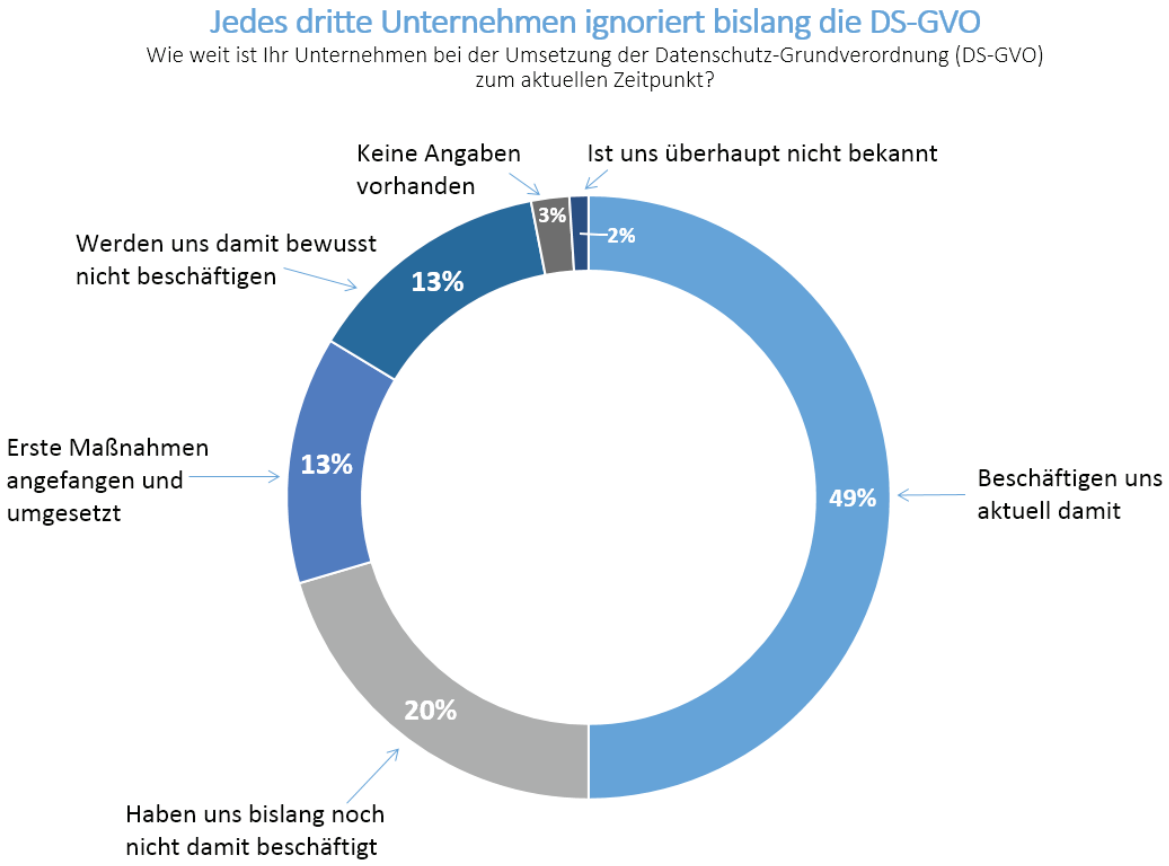
- erweiterte Löschpflichten (Recht auf Vergessenwerden),
- neue Betroffenenrechte (Recht auf Datenübertragbarkeit),
- verschärfte Meldepflichten bei Datenschutzverletzungen (72 Stunden Frist),
- neue Anforderungen an die Einwilligung zur Datenverarbeitung,
- das Instrument der Datenschutzfolgenabschätzung.

Obwohl diese neuen Anforderungen an den Datenschutz und damit an die Compliance im Unternehmen bereits im Mai 2016 in Kraft getreten sind und für die Umsetzung eine Frist von zwei Jahren besteht, sind die meisten Unternehmen nicht über „Insellösungen“ hinausgekommen, die nur einzelne Forderungen der GDPR herausgreifen und deshalb keine durchgehende Compliance gewährleisten können.

Stand der Umsetzung der GDPR

Verschiedene Umfragen und Studien zur Umsetzung der GDPR zeigen, dass sich die Unternehmen - wenn überhaupt - nur mit Einzelmaßnahmen zur Umsetzung der GDPR befassen. So nehmen sie zum Beispiel die Umsetzung der Meldepflichten in den Blick oder die erweiterten Löschpflichten. Entsprechend suchen und implementieren sie lediglich Insellösungen, die nicht geeignet sind, die Gesamtheit der Anforderungen aus der GDPR zu berücksichtigen.

Eine Umfrage[ii] des Digitalverbandes Bitkom ergab, dass erst 13 Prozent der Unternehmen erste Maßnahmen zur Umsetzung der GDPR begonnen oder abgeschlossen haben. 49 Prozent beschäftigen sich derzeit mit dem Thema. Jedes dritte Unternehmen (33 Prozent) gibt an, sich bislang noch überhaupt nicht mit den Vorgaben der Verordnung beschäftigt zu haben. Von den Unternehmen, die sich bereits mit der GDPR beschäftigt haben, sagt rund die Hälfte (47 Prozent), dass sie bisher höchstens zehn Prozent aller notwendigen Arbeiten erledigt hat. Nur drei Prozent gehen davon aus, dass sie mehr als die Hälfte der Aufgaben abgearbeitet haben.



Eigene Darstellung. Datenquelle: Bitkom, https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/09-September/Privacy-Conference/Pressegrafik-Gallery.png

Eine Studie[iii] von Ingenium und iGrafx zu Risikomanagement und Business Process Management zeigt folgenden Stand des Risikomanagements und der Umsetzung der GDPR in Unternehmen:

- 50 Prozent der befragten Unternehmen sagten, dass sich ihre Prozesse und Systeme in den verschiedenen Abteilungen und Bereichen unterscheiden. Deshalb falle es ihnen schwer, eine vollständige Sicht auf die möglichen Risiken zu erlangen.
- Ein Viertel der Befragten hat gegenwärtig kein System für das Risiko-Monitoring im Einsatz.
- 62 Prozent der Unternehmen glauben nicht, dass sie die Auswirkungen der GDPR vollständig kennen und verstehen, und sie wissen auch nicht, welche Folgen die GDPR für ihr Risikomanagement haben wird.

Weitere Umfragen zur Umsetzung von GDPR zeigen zudem:

Den Unternehmen fehlt die Transparenz,

- wo die personenbezogenen Daten gespeichert, verarbeitet und genutzt werden,
- zu welchen Zwecken dies geschieht,
- wer auf die Daten Zugriff erhält,
- wer für den Schutz der Daten zuständig ist und
- wie schnell sie auf mögliche Datenschutzverletzungen oder aber Anfragen von Betroffenen reagieren können.

Ohne diese Transparenz aber ist es nicht möglich, Datenschutz-Anforderungen wie die Löschpflichten, die Datenübertragbarkeit, die Meldepflichten, die Sicherheitsstellung der Einwilligung oder die Datenschutzfolgenabschätzung zu gewährleisten.

Ohne strukturierte Prozesse, ohne Risikoidentifizierung, -bewertung und -überwachung und ohne Transparenz über Datenhaltung, Datenverarbeitung, Datenzugriffe, Datenübermittlung, Systeme und Zuständigkeiten kann die Umsetzung der GDPR nicht gelingen, weder bis zum 25. Mai 2018 noch danach. Es besteht deshalb dringender Handlungsbedarf.

2. GDPR und Business Process Management

Mit Business Process Management Lösungen lassen sich Prozesse für das gesamte Unternehmen flexibel entwerfen, realisieren und optimieren. Für die notwendige unternehmensweite Umsetzung der GDPR eignen sich die Methoden des Business Process Management (BPM) und die Lösungen von iGrafx[iv] in besonderer Weise. Die GDPR kann als eine neue Compliance-Anforderung mittels BPM in die Unternehmensprozesse eingebracht werden. Die GDPR mit ihren spezifischen Vorgaben benötigt dazu keine Sonderlösung, sondern kann im BPM mit den gleichen Methoden der Modellierung, Analyse, Optimierung und Automatisierung wie alle anderen Compliance-Anforderungen systematisch umgesetzt werden.

Dabei leisten die Lösungen für die Umsetzung der GDPR unter anderem folgendes:

- Alle datenschutzrelevanten Abläufe und Aktivitäten im Unternehmen können modelliert und analysiert werden. Die Maßnahmen zum Schutz der Daten lassen sich modellieren als Kontrollen, wie personenbezogene Daten erhoben, verarbeitet und genutzt werden, als Aktivitäten, wie dem Einholen der Einwilligung, und in der Ermittlung von Abweichungen zwischen Ist- und Soll-Zustand, die als Datenschutzverletzung zu werten sind und Folgeaktion wie die Meldung an die Aufsichtsbehörden nach sich ziehen können.

- Alle datenschutzrelevanten Zuständigkeiten und Zugriffsmöglichkeiten auf personenbezogene Daten können dokumentiert und überprüft werden, fehlende Zuständigkeiten und unerlaubte Zugriffsmöglichkeiten werden aufgedeckt, eine Behebung kann angestoßen werden.

- Datenschutzrelevante Rollen wie Datenschutzbeauftragter (DSB) oder Data Protection Officer (DPO) können definiert und den Datenschutz-Prozessen zugeordnet werden.

- Datenschutz-Forderungen wie das Einholen und Dokumentieren der Einwilligung in die Datenverarbeitung lassen sich in den Prozessen abbilden und können bei Bedarf mit den Workflow-Funktionen automatisiert werden (Process Automation).

- Individuelle Aufgabenlisten mit schrittweisen und nach Priorität aufgelisteten Aufgabenzuweisungen sorgen dafür, dass datenschutzrelevante Aktionen wie die Antwort auf Anfragen von Betroffenen vorgabengetreu und effizient durchgeführt werden.

- Datenverarbeitungen ohne Einwilligung, fehlende Datenschutzerklärungen oder Datenübermittlungen ohne ausreichendes Datenschutzniveau lassen sich in den Prozessen aufdecken, als Abweichung des Ist-Zustandes von den Compliance-Forderungen.

- Regeln, wann und wie Prozesslücken und damit Datenschutzverletzungen an wen kommuniziert werden müssen, lassen sich abbilden und bei Bedarf automatisieren.

- So kann nicht nur der Ist-Zustand der Prozesse dargestellt werden, sondern es kann auch die Einhaltung der GDPR-Richtlinien mit Hilfe von Prozessautomatisierung strukturiert umgesetzt werden. Modellierte Datenschutz-Prozesse können automatisiert werden, um die Compliance dauerhaft zu gewährleisten.

Beispiel: Datenschutzfolgenabschätzung

Das Risikomanagement, die Identifizierung und Bewertung von Risiken mit den Lösungen von iGrafx hilft Unternehmen bei der Implementierung und regelmäßigen Durchführung einer Datenschutzfolgenabschätzung, wie sie in Artikel 35 GDPR gefordert wird. So können Nutzer zum Beispiel:

- Risiken benutzerdefiniert berechnen, um so die Abhängigkeiten eines Datenrisikos von Datenkategorien, genutzten IT-Systemen und nutzerabhängiger Parametern wie dem aktuellen Standort der Datenverarbeitung zu berücksichtigen,

- Risiken und Kontrollen einmal definieren und dann regelmäßig wiederverwenden, um reproduzierbare Datenschutzfolgenabschätzungen und Audits sicherzustellen.

Sind Verfahrensänderungen geplant, ermöglicht die Lösung die notwendige Übersicht über die Folgen und Risiken: Informationen zu den geplanten, simulierten Prozessen können mit vorhandenen Daten zu bestehenden Prozessen verglichen werden. Hierfür ermöglicht die Lösung einen visuellen Versionsvergleich von Diagrammen und Risikowerten, wodurch Änderungen auf einen Blick sichtbar werden. iGrafx bietet damit ein effektives Änderungsmanagement und unterstützt die Abschätzung der Datenschutz-Folgen.

Da eine Datenschutzfolgenabschätzung immer in Zusammenarbeit zwischen den Datenschutzbeauftragten und den Fachbereichen, in denen die neue oder geänderte Datenverarbeitung geplant ist, stattfinden sollte, hilft eine weitere Eigenschaft der Lösung: Sie unterstützt eine effektive Zusammenarbeit und Kommunikation, indem es allen Beteiligten die gleichen Informationen im Risikomanagement zur Verfügung stellt. Das zentrale Prozessarchiv der Lösung, in dem Prozesse sowie die dazugehörigen Informationen gespeichert und verwaltet werden, bildet eine entscheidende Voraussetzung für die Transparenz und Zusammenarbeit im Datenschutz und bei der Datenschutzfolgenabschätzung.

3. Empfehlungen zur Umsetzung der GDPR

Mit den BPM-Lösungen lassen sich die Lücken in der Umsetzung der GDPR planvoll, strukturiert und in der Zusammenarbeit aller beteiligten Stellen im Unternehmen schließen. Unternehmen, die die GDPR noch nicht durchgehend umgesetzt haben, sollten nun diese Schritte angehen, die sich mit iGrafx vollständig realisieren lassen:

1. Aufnahme der Ist-Situation im Unternehmen mit den IT-Systemen, Datenverarbeitungen (Anwendungen), (personenbezogenen) Daten und Speicherorten, Abläufen, Rollen und Zuständigkeiten (Prozess-und IT-Landschaft); vorhandene Informationen über die IT- und Datenstrukturen können nach Möglichkeit über Schnittstellen importiert werden.

2. Abbildung bzw. Import der GDPR-Anforderungen als neue Prozess- und Workflow-Regeln.

3. Analyse der modellierten Strukturen und Prozesse, Abgleich mit den GDPR-Regeln, Ermittlung von Lücken in den Prozessen, Zuständigkeiten und Rollen.

4. Bewertung der aufgedeckten Lücken als Datenschutz-Risiko.

5. Einleitung von Maßnahmen zur Behebung der Lücken, Dokumentation der Restrisiken.

6. Nutzung der dokumentierten Prozesse und Kontrollen für das von der GDPR geforderte Verzeichnis der Verarbeitungstätigkeiten.

7. Nutzung der dokumentierten Zuständigkeiten und Workflows für interne Schulungsmaßnahmen.

8. Risikobewertung bei Einführung neuer Prozesse und Verfahren durch Modellierung und Analyse des geplanten Zustandes (in der GDPR Datenschutzfolgenabschätzung genannt).

9. Implementierung regelmäßiger Kontrollen, um die Wirksamkeit der Datenschutzmaßnahmen zu überprüfen, mit der Möglichkeit der Automatisierung der entsprechenden Workflows und Datenschutz-Prozesse.

10. Generierung von Berichten für interne Datenschutz-Audits und auf Anfrage der Datenschutz-Aufsichtsbehörden.

Resümee

Anstatt nur Insellösungen zu implementieren, kann durch den Einsatz eines ganzheitlichen BPM-Tools eine durchgehende GDPR-Lösung realisiert werden, die sich nahtlos in eine Gesamtlösung für die Unternehmens-Compliance einfügt.

Sie möchten mehr erfahren?

Sie interessieren sich für das Konzept in diesem Artikel? Besuchen Sie www.igrafx.de oder kontaktieren Sie uns unter +49 8131.3175 0.

Quellen:

[i] https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf

[ii] https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/09-September/Privacy-Conference/Bitkom-Charts-PK-Privacy-Conference-19-09-2017-final.pdf

[iii] http://www.igrafx.com/landing/download.html?name=Risk%20Management%20and%20Business%20Process%20Management%20-%20Survey%20Findings&ao_f=027a&ao_d=d-0001&c_type=c

[iv] http://www.igrafx.com/de/solutions/business-challenges/compliance