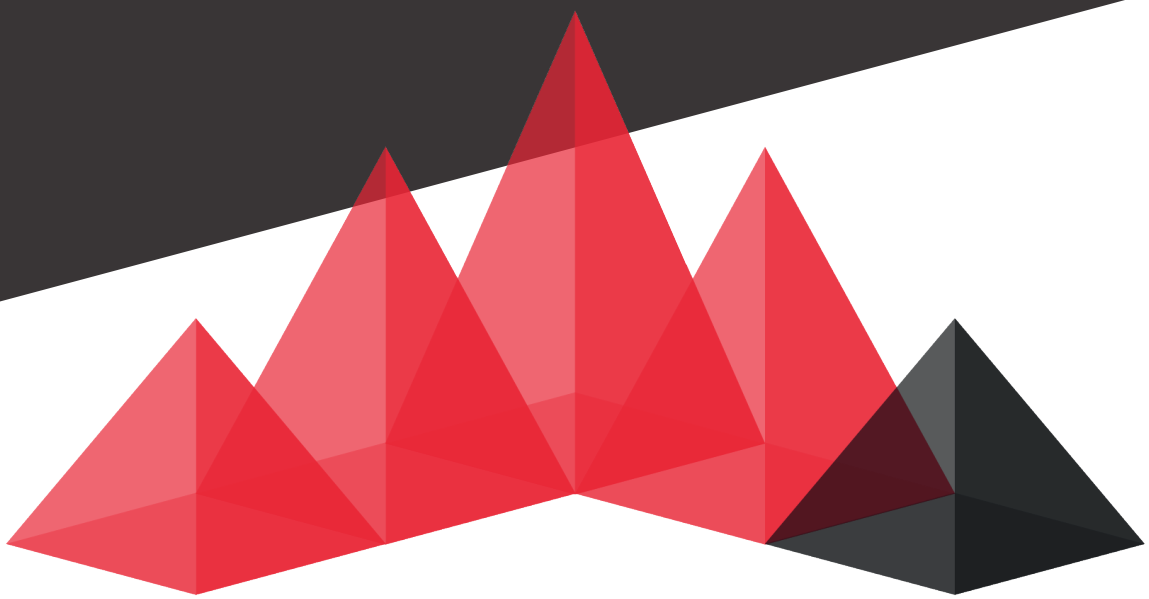
TALOS

Publikation



Die Datenschutzgrundverordnung («DSGVO») bei Banken und Finanzdienstleistern: Zeit für eine Bestandsaufnahme – wie steht es um die Implementierung?

von Matthias Greiller und Benedikt Aussems

Am 25. Mai 2018 ist die DSGVO europaweit in Kraft getreten. Bereits im Rahmen unserer letzten Publikation zum Thema haben wir festgestellt, dass die Umsetzung der Verordnung nicht nur aber sicherlich speziell auch Unternehmen des Banken- und Finanzdienstleistungssektors zum Teil vor große Herausforderungen stellt. Mit nunmehr über einem Jahr Abstand zum Inkrafttreten der DSGVO werfen wir erneut einen Blick auf den Implementierungsstand. Repräsentative Umfragen verdeutlichen, dass auch ein Jahr nach "go live" noch Handlungsbedarf besteht.

So wurden z.B. im Rahmen einer Studie im Auftrag des "Digitalverbandes Bitkom" 503 Datenschutzbeauftragte aus Unternehmen der digitalen Wirtschaft zum gegenwärtigen Stand der Umsetzung innerhalb ihres Betriebes befragt[1]:

- Lediglich rund ein Viertel sehen die Umsetzung der DSGVO als abgeschlossen an
- Rechnet man die Unternehmen hinzu, welche die Regelung zu großen Teilen – also nicht vollständig – umgesetzt haben, so kommt man auf 67 Prozent der Befragten
- Weitere 24 Prozent geben an die Regelungen lückenhaft umgesetzt zu haben und
- die verbleibenden 6 Prozent stehen erst am Anfang

Diese Ergebnisse decken sich mit einer weiteren Umfrage an der über 1000 Datenschutzbeauftragte zum Implementierungsstand befragt wurden[2]:

- Lediglich 28 Prozent gaben an, die DSGVO vollständig integriert zu haben
- Viele der Betriebe haben länger für die Implementierung der Verordnung gebraucht als ursprünglich angenommen
- Gründe für die Verzögerung im Implementierungsprozess sind insbesondere Unsicherheit hinsichtlich rechtlicher Anforderungen und unterschätzte Kosten

Bemerkenswert sind diese Erkenntnisse insbesondere vor dem Hintergrund bzw. der Diskrepanz, dass bei einer weiteren vor dem "go live" der DSGVO durchgeführten Studie 78 Prozent der Unternehmen angaben, für das Inkrafttreten der DSGVO vollumfänglich vorbereitet zu sein[3].

Dies verdeutlicht unserer Auffassung nach, dass die Anforderungen der Verordnung und der zur Implementierung nötige Aufwand unterschätzt oder Teile der Regulierung möglicherweise sogar falsch interpretiert wurden. Unsere Beobachtungen und Erkenntnisse bei von uns begleiteten Firmen haben gezeigt, dass vielfach zwar die "unmittelbaren Hausaufgaben" aus der DSGVO erledigt wurden; hierzu zählen beispielsweise DSGVO-bezogene Disclaimer auf Webseiten oder auch Datenschutzvereinbarungen mit Mitarbeitern und Bewerbern. Allerdings besteht noch Nachholbedarf in mehreren Bereichen, insbesondere bei tiefgehenden Aufgaben zu einer vollständigen, regelkonformen Implementierung der DSGVO:

- Mängel betreffend die Umsetzung prozessualer und interner Dokumentationselemente: Vielfach wurden elementare Bestandteile wie z.B. das Verfahrensverzeichnis nicht oder nur unvollständig angefertigt; die DSGVO besagt gem. Artikel 30 eindeutig, dass bereits mit "go live" ein vollumfängliches Verzeichnis existieren muss und dieses fortlaufend zu pflegen und zu aktualisieren ist
- Unterschätzen der Tragweite einzelner Maßnahmen und Anpassungen: es hat sich gezeigt, dass z.B. das "Recht auf Vergessenwerden" (Art. 17 DSGVO) vielfach hinsichtlich technischer und organisatorischer Komplexität unterschätzt wurde; seit 25. Mai 2018 haben natürliche Personen das Recht auf Löschung, wenn z.B.:
  - > die Speicherung ihrer Daten unter Verstoß gegen die DSGVO erfolgt ist
  - > sich die Zwecke, für die die Daten erhoben wurden, erübrigt haben
  - > die betroffenen Personen ihre Einwilligung in die Verarbeitung widerrufen oder Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten eingelegt haben
- Für alle oben aufgeführten Beispiele muss sichergestellt werden, dass entsprechende Daten im gesamten Unternehmen identifiziert und in jeder vorliegenden Form (physisch oder elektronisch) vernichtet bzw. gelöscht werden können; insbesondere Großbanken, die noch nicht über einen vollständigen Gesamtüberblick über eine Kundenbeziehung ("single client view") verfügen, laufen Gefahr bei der Datenhaltung z.B. in unterschiedlichen Geschäftsbereichen gegen die DSGVO zu verstoßen.
- Training der Mitarbeiter: Vielfach wurde oder wird ein solches Training gar nicht oder

Fussnote 1:
https://www.bitkom.org/Presse/Presseinformation/Zwei-Drittel-Unternehmen-DS-GVO-groesstenteils-umgesetzt

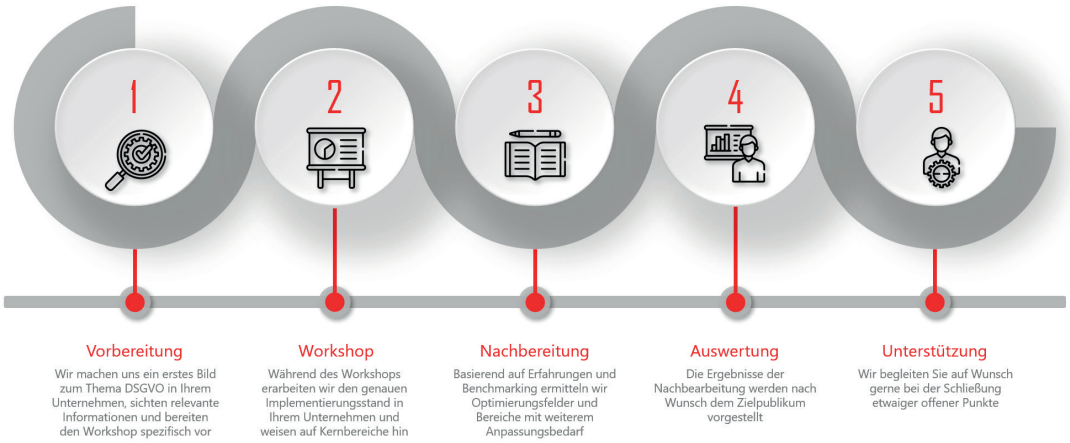
Fussnote 2:
https://www.compliance-junction.com/only-28-of-companies-gdpr-compliant-capgemini-research-institute-survey/

Fussnote 3:
https://www.capgemini.com/resources/seizing-the-gdpr-advantage/

nur unzureichend durchgeführt; Kern des Problems ist hier, dass oft ein Training im Sinne einer "juristischen Vorlesung" gehalten wird; dies ist oft wenig hilfreich, da der Bezug zum Tagesgeschäft nicht erkannt und somit Gelerntes nicht umgesetzt werden kann; Warnsignale und Stolpersteine hinsichtlich der DSGVO werden so nicht im Bewusstsein der Mitarbeiter verankert; wer klärt z.B. den betroffenen Mitarbeiter auf, der sich aktiv in den Rekrutierungsprozess einer Unternehmung einbringt und die ihm dazu überlassenen Bewerberdossiers (evtl. sogar ohne Datenschutzeinwilligungserklärung) bei sich auf dem PC sauber geordnet ablegt hat?

Dies sind nur drei Beispiele, wie aus einer unvollständigen oder nicht zielgerichteten Implementierung der DSGVO schnell Probleme mit u.U. massiven Folgen entstehen können. Die Dringlichkeit einer ordnungsgemäßen Umsetzung der Verordnung begründet sich immer stärker auch durch die Tatsache, dass etwaige Verstöße mit zunehmend härteren monetären Strafen seitens der nationalen Regulatoren belegt werden. Ein aktuelles Beispiel hierfür ist der Fall der Deutsche Wohnen, welche bedingt durch die Nichteinhaltung der DSGVO ein Bußgeld i. H. v. 14,5 Millionen Euro zu zahlen hat[4]. Wenn auch nicht finanziell messbar, aber sicherlich nicht minder von Bedeutung, ist die rufschädigende Wirkung für Unternehmen, Produkte und Marken, wenn es zu öffentlich bekannten Verstößen und Strafmaßnahmen bezüglich der Nichteinhaltung der DSGVO kommt.

Um Verstöße und daraus resultierende Strafmaßnahmen wann immer möglich zu vermeiden, leistet TALOS praxisnahe und lösungsorientierte Unterstützung bei der fortlaufenden Implementierung bzw. Einhaltung der DSGVO. Im vergangenen Jahr konnten wir während der Betreuung mehrerer Unternehmen im Banken- und Funds Management Bereich unseren eigens hierfür entwickelten 5-Stufen Ansatz validieren. Im Vordergrund steht hierbei die praxis- und prozessnahe Analyse des gegenwärtigen Implementierungsstandes der DSGVO. Wie erfolgreich wurde die Verordnung ins Tagesgeschäft integriert? Welche Berührungspunkte sind bereits aufgetreten, z.B. mit Kunden, Drittparteien und Regulatoren? Wie tiefgreifend wurde die Implementierung verankert – ist die DSGVO integraler Bestandteil des Geschäftsmodells geworden? Im Rahmen eines Workshops mit Vor- und Nachbereitung gehen wir anhand von genau definierten Arbeitspaketen alle von der DSGVO betroffenen Kernfunktionen und -bereiche eines Unternehmens durch und überprüfen gemeinsam mit dem Management, ob die getroffenen Maßnahmen und Veränderungen die Anforderungen



Fussnote 4: https://netzpolitik.org/2019/datenschutz-grundverordnung-deutsche-wohnen-erste-millionenstrafe/

der DSGVO umfassend genug abdecken. Dies erfolgt immer mit direktem Bezug zum Tagesgeschäft, ergänzt durch unsere spezifischen Erfahrungen. Sollten sich Lücken oder Anpassungsbedarf zeigen, so dokumentieren wir diese, nehmen gemeinsam eine Priorisierung vor und leisten Entscheidungshilfe, wie diese gegebenenfalls zu adressieren sind. Auf Wunsch begleiten wir unsere Kunden bis zur Schließung aller offenen Punkte.

Von Anfang an hat TALOS Erfahrung mit der DSGVO gesammelt und die Implementierung bei Banken und Finanzdienstleistern begleitet – von organisatorischen Anpassungen bis hin zur Überarbeitung von Prozessen und – in Zusammenarbeit mit namhaften Kanzleien – der Aktualisierung von Dokumenten[5]. Bereits unmittelbar vor und nach dem Implementierungsstichtag hat TALOS Interim- DPO Mandate übernommen und konnte nicht nur eigenes Wissen einbringen, sondern auch Erfahrung aus dem täglichen Umgang mit der DSGVO sammeln.

Für unsere Kunden ergibt sich die Möglichkeit, pragmatisch und zu überschaubaren Kosten einen Sicherheitscheck zum eigenen Implementierungsstand sowie z.B. zu Qualität und Umfang von Dokumentationen, Templates etc. zu erlangen. Auch wird durch diese Vorgehensweise nochmal das Verständnis zur DSGVO im eigenen Unternehmen geschärft – der Workshop hat auch einen Trainingseffekt für den Teilnehmerkreis, der sich bevorzugt aus Entscheidungsträgern DSGVO-betroffener Bereiche zusammensetzt.

Fussnote 5:
TALOS erteilt keine Rechtsberatung

TALOS

Publikation

Wer wir sind

TALOS definiert neue Standards in der Management Beratung. Als spezialisierte Boutique Beratung mit Schweizer Wurzeln und Büros in Zürich und Luxemburg beraten wir Kunden aus der Europäischen Finanzindustrie.

TALOS wurde 2008 von erfahrenen Management Beratern gegründet und ist seither zu einem etablierten Beratungsunternehmen für Finanzunternehmen gewachsen.

Als Experten für regulatorische Transformationslösungen decken wir die gesamte Bandbreite möglicher Fragestellungen ab, von der Analyse über die Strategie bis hin zur Umsetzung.

Zürich
TALOS Management Consultants
Bleicherweg 45
CH-8002 Zürich
Tel. +41 44 380 14 40

Luxemburg
TALOS Management Consultants
6, Rives de Clausen
L-2165 Luxembourg
Tel. +352 26 20 23 54

www.talos-consultants.com
www.shapenewstandards.com

Ihr Kontakt

Matthias kam vor 10 Jahren zu TALOS und leitet heute als Managing Partner das Luxemburger Office. Er ist seit mehr als 20 Jahren in der Financial Services Industrie tätig, unter anderem bei zwei Schweizer Großbanken im Private Banking und als Management Consultant bei der Mitchell Madison Group. Der Schwerpunkt seiner Arbeit liegt auf regulatorischen und Compliance Themen, sowie im Bereich Sales Management für Private Banking.

Matthias Greiller
Managing Partner
matthias.greiller@talos-consultants.lu

Benedikt ist seit Anfang 2018 Consultant bei TALOS. Zuvor war er über 2 Jahre im Audit tätig. Er hat sich auf die Asset Management Industrie spezialisiert und verfügt über weitreichende Kenntnisse des luxemburgischen Finanzsektors.

Benedikt Aussems
Consultant
benedikt.aussems@talos-consultants.lu