



DATENSCHUTZ und DSGVO

Evaluieren | Planen | Einführen

Ihr Leitfaden für die Praxis

Status
Datenschutz
evaluieren

Datenschutz
organisation
aufsetzen

Projekt
DSGVO
planen

Budget
planen und
Ressourcen
freigeben

Projekt
DSGVO
umsetzen

Datenschutz
gem.
DSGVO
"leben"

Aufbau von Datenschutz gemäß EU DSGVO 2016/679

In diesem Buch werden Sie

- die Grundlagen der DSGVO (auch bekannt unter EU-GDPR) und ihre Prinzipien für die Umsetzung kennen lernen,
- Ihre Readiness für die DSGVO evaluieren, d.h. analysieren, bewerten und dokumentieren,
- herausfinden, wie Sie ein Projekt zum Einführen der DSGVO durchführen können und darüber hinaus
- zahlreiche nützliche Tipps für die Praxis erhalten, die Sie auf Ihrem Weg zur DSGVO-Compliance begleiten und Ihnen das Verständnis zum Datenschutz insgesamt erleichtern.

Über die Autoren:

Dr. Alfons Bridi

ist geschäftsführender Gesellschafter einer Unternehmensberatung für IT Strategie, IT Governance und IT Reorganisation, hat umfangreiche fachliche und organisatorische Erfahrungsschwerpunkte in den Bereichen Strategie und Organisationsentwicklung, IT Governance und war Leiter eines Softwareentwicklungslabors. Zum Thema Informationssicherheit und DSGVO hat er für Banken, Industrieunternehmen sowie im öffentlichen Sektor Projekte durchgeführt.

StB MMMag. Felix AIGNER, LL.M, BSc

ist als Steuer- und Unternehmensberater tätig. Einer der Schwerpunkte seiner Tätigkeit liegt in der Beratungstätigkeit zu betrieblichem Risikomanagement, Informationssicherheit und Datenschutz und ist als geprüfter Datenschutzexperte tätig.

Lesehinweis:

Aus Gründen der einfachen Lesbarkeit wird auf geschlechtsspezifische Unterscheidungen weitgehend verzichtet. Entsprechende Begriffe gelten daher grundsätzlich für beide Geschlechter.

Inhaltsverzeichnis

1. [Einleitung](#)
2. [Grundlegendes zum Datenschutz](#)
3. [DSGVO – Folgen für Ihr Unternehmen](#)
4. [Datenschutz Aufbauorganisation](#)
5. [Einführung der DSGVO](#)
6. [Kontinuierliche Verbesserung](#)
7. [Auditing](#)
8. [Toolbox Evaluieren](#)
9. [Toolbox Datenschutz-Organisation](#)
10. [Toolbox Projekt DSGVO](#)
11. [Toolbox Verarbeitungsverzeichnis](#)
12. [Toolbox Datenschutz - Folgeabschätzung](#)
13. [Toolbox Wahrung der Betroffenenrechte](#)
14. [Toolbox Verhalten bei Data Breach](#)
15. [Toolbox Datenschutzhandbuch](#)
16. [Toolbox Awareness Programm](#)
17. [Anhang](#)

1 Einleitung

1.1 Über dieses Buch: From “Know How” to “Do How”

Seit der Kundmachung der EU-Datenschutz-Grundverordnung (im Weiteren: DSGVO) im April 2016¹ wurden zahlreiche Bücher zum Thema Datenschutz veröffentlicht. Vielfach eröffnet diese Literatur dem interessierten Leser umfassende Einblicke in alle möglichen Facetten des Datenschutzes und trotzdem: Fragen zur alltäglichen Anwendung und praktischen Umsetzung des Datenschutzes bleiben häufig unbeantwortet.

An diesem Punkt setzt das vorliegende Buch an, in dem es den Leser vorrangig mit praktischen Fragen und Lösungsansätzen konfrontiert: rechtliche Grundlagen und theoretische Fragen der Informationssicherheit werden Ihnen daher bewusst nur in dem Umfang vorgestellt, als es zum Verständnis und dem Erkennen von Zusammenhängen notwendig ist, um Sie bei der praktischen Umsetzung zu begleiten.

Dementsprechend liegt der Schwerpunkt dieses Buches darin, Ihnen Anleitungen für die praktische Arbeit zur Hand zu geben, die Sie bei der Umsetzung der DSGVO rasch und zielführend unterstützen.

In diesem Buch werden Sie

- die Grundlagen der DSGVO und ihre Prinzipien für die Umsetzung kennen lernen,
- Ihre Readiness für die DSGVO evaluieren, d.h. analysieren, bewerten und dokumentieren,
- herausfinden, wie Sie ein Projekt zur Umsetzung der DSGVO durchführen können und darüber hinaus
- zahlreiche nützliche Tipps für die Praxis erhalten, die Sie auf Ihrem Weg zur DSGVO-Compliance begleiten.

Ab wann gilt die DSGVO?

Die DSGVO wurde am 04.05.2016 kundgemacht und ist mit 24.05.2016 in Kraft getreten. Ihre Geltung erlangt die DSGVO allerdings erst mit 25.05.2018. Praktisch bedeutet das, dass die Verordnung

- sich zunächst ausschließlich an die EU Mitgliedsstaaten richtet; und zwar in der Weise, dass bis zum 25.05.2018 alle notwendigen Schritte der Anpassung und Umsetzung auf nationaler Ebene zu erfolgen haben. Der österreichische Gesetzgeber ist dieser Verpflichtung bereits im Rahmen des Datenschutz-Anpassungsgesetzes 2018 nachgekommen.
- für uns Einzelne ab dem 25.05.2018 vollinhaltlich Geltung erlangt, d.h. ab diesem Zeitpunkt sämtliche Anforderungen des neuen Datenschutzrechts zu erfüllen sind.

Damit verfolgt die DSGVO im Wesentlichen folgende Ziele:

- einheitlichen Rechtsschutz für alle Betroffenen innerhalb der EU,
- einheitliche, gemeinsame Grundsätze und Standards für die Datenverarbeitung

- Gewährleistung eines forcierten Vollzuges, der Verstöße mit Bußgeldern bis zu 20 Millionen Euro oder im Fall eines Unternehmens von bis zu 4 % seines weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres sanktioniert².

Informationstechnologie, Informationssicherheit und Datenschutz

Das Zeitalter der Informationstechnologie schafft Möglichkeiten, die uns in die Lage versetzen, neue Kunden auf bisher nicht erschlossenen Märkten zu gewinnen. Dabei tätigen wir Transaktionen, die ohne die Möglichkeiten der modernen Internet-, Kommunikations- und Transaktionstechnologie vielfach überhaupt nicht möglich wären.

Hinter der Vielfalt und vermeintlichen Anonymität dieser Transaktionen steht eine zunehmende Flut an Daten. Wir speichern Daten zu unseren Geschäftspartnern oder fordern diese im Zuge der Geschäftsabwicklung ein. Umgekehrt geben wir Informationen oft genug auch selbst preis, selbstverständlich in der Erwartung, dass der Empfänger sicher und vertraulich damit umgeht. Überhaupt erfordert der Geschäfts- und Verwaltungsbetrieb ein umfangreiches Speichern und Verarbeiten von Daten, nicht zuletzt auch, um der Fülle an gesetzlichen und rechtlichen Anforderungen Rechnung zu tragen.

Vor diesem Hintergrund verlangen Informations- und Kommunikationsabläufe eine adäquate Sicherheit, die sich auf entsprechende Strategien und Vorsorgemaßnahmen stützt. Datenschutz ist daher von zentraler Bedeutung für sämtliche Belange der Informations- und Betriebssicherheit.

Daten und Informationen verkörpern gleichsam die Digitale Währung des Informationszeitalters, sie sind insbesondere

- der vierte, maßgebliche Produktionsfaktor des Unternehmens, der die konventionellen betriebswirtschaftlichen Ressourcen Personal, Kapital und Knowhow ergänzt,
- wertrelevantes Betriebsvermögen, dessen Verlust durchaus existenzbedrohende Folgen zeitigen kann und
- im Kontext der globalen Vernetzung und dem damit real einhergehenden Gefahrenpotenzial vor unberechtigttem Zugriff durch Dritte (insbesondere Konkurrenten und Cyberkriminelle) wirkungsvoll zu schützen.

Unter diesen Gesichtspunkten setzt sich der vorliegende Praxisleitfaden zum Ziel, systematische Wege zu beschreiben, die Sie bei der betrieblichen Umsetzung der Informationssicherheit, des Datenschutzes, der Risikofolgeabschätzung und abgeleiteten Maßnahmen einschlagen können. Dabei ist es den Autoren ein Anliegen, praktikable Lösungswege exemplarisch, an Hand von Musterlösungen, aufzuzeigen, die Sie im betrieblichen Alltag umsetzen und Ihren Bedürfnissen entsprechend weiterentwickeln können.

1.2 Wer sollte dieses Buch lesen

Die Informationstechnologie (IT) hat sich rasant in der Wirtschaft und der öffentlichen Verwaltung verbreitet. Es liegt geradewegs auf der Hand, dass keine Maßnahmen in der Informationstechnologie bzw. keine Hard- und Softwareprojekte durchgeführt werden sollten, ohne zuvor die Informationssicherheit und Datenschutz berücksichtigt zu haben.

Insbesondere **Geschäftsführer, Informationssicherheits- und Datenschutzverantwortliche, IT-Manager, Organisations- und Personalentwickler, Projektleiter, Business-Analysten, System-Analytiker, Software-Entwickler und Berater** sehen sich mit der Tatsache konfrontiert, dass grundlegendes DSGVO-Knowhow für optimale Sicherheitslösungen unverzichtbar geworden ist.

Vor diesem Hintergrund zählen Kooperation, Kommunikation und Schnittstellenmanagement zwischen den betroffenen Fachabteilungen zu den maßgeblichen Komponenten, die für eine erfolgreiche Umsetzung von Datensicherheit unabdingbar sind.

→ *Belange des betrieblichen Datenschutzes und der DSGVO richten sich daher an alle Personen!*

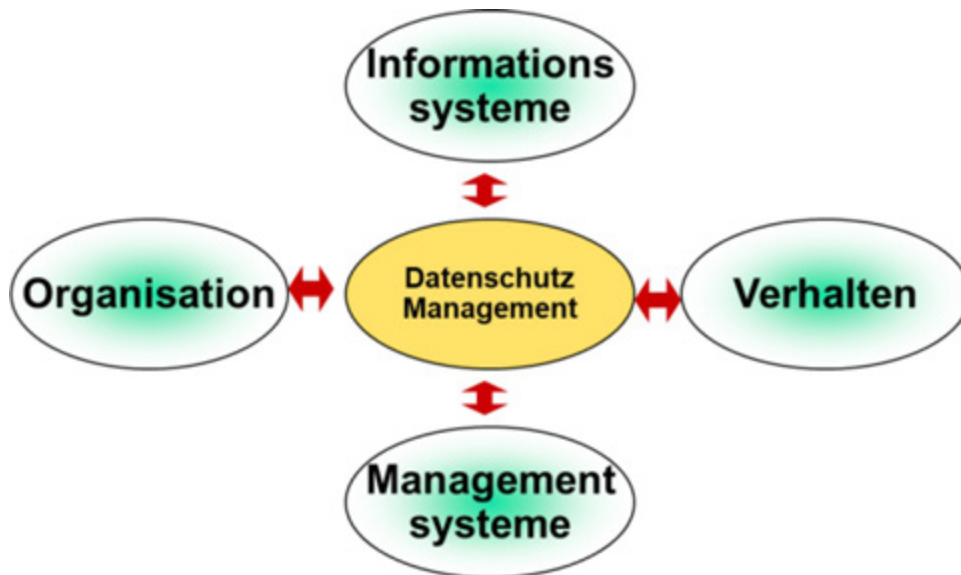
¹ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (*Datenschutz-Grundverordnung*). Diese Verordnung tritt am 25. Mai 2018 in Geltung. Die bisherige Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten wird damit abgelöst.

² Siehe Geldbußen: Art 83 DSGVO.

2 Grundlegendes zum Datenschutz

2.1 Eine Einführung

Durch den Einsatz von Informationstechnologie werden viele Arbeitsprozesse gesteuert und große Mengen von Informationen in digitaler Form gespeichert oder elektronisch verarbeitet. Die so bearbeiteten Daten werden dann im Netz übermittelt. Vielerorts ist die Wahrnehmung öffentlicher oder privatwirtschaftlicher Aufgaben deshalb ohne IT überhaupt nicht mehr möglich.



Daraus resultiert eine Abhängigkeit, die in ihrem Umfang vielerorts vielleicht gar nicht gewollt, ja bisweilen auch gar nicht erkannt wird. Dieser Umstand bewahrt Sie aber nicht davor, sich mit dem Thema Informationssicherheit und Datenschutz auseinanderzusetzen. Ebenso häufig wird der Aspekt vernachlässigt, dass Aufgaben der