Chancen und Risiken der EU-DSGVO

WHITEPAPER

RA Mag. Andreas Schütz LL.M.

Dr. Lambert Gneisz MAS CMC SV

Zum Verständnis

Mit über 4.000 Änderungsanträgen war die EU-DSGVO das im Europäischen Parlament am intensivsten diskutierte Gesetz aller Zeiten. Diese Diskussionen setzen sich in Österreich – bei Juristen wie bei Managern fort wenn es darum geht, das Gesetz zweckmäßig anzuwenden und seine Folgen für die Wirtschaft zu verstehen.

Was bedeutet die EU-DSGVO in der betrieblichen Praxis? Wie können sich Unternehmen und Organisationen jetzt darauf vorbereiten, um nicht später mit den massiv formulierten Strafen bei Nichteinhaltung konfrontiert zu werden? Welche wirtschaftlichen Vorteile sind für Unternehmen bei intelligenter Erfüllung der neuen Rechtsvorschriften möglich?

Das vorliegende Whitepaper ist eine auszugsweise Darstellung einiger wesentlicher DSGVO-Anforderungen. Es soll für den Entscheidungsträger im Management eine Hilfe sein, Chancen und Risiken bei der Bewältigung der vom Gesetzgeber nicht immer glücklich formulierten neuen Datenschutzverpflichtungen zu verstehen und erfolgreich umzusetzen.

Die beiden Autoren bieten dem Leser dazu ihre Sicht als juristische und betriebswirtschaftliche Experten mit IT-Fokus und langjähriger Praxiserfahrung an.

Als Besonderheit des Textes kann gelten, dass **nicht** die Strafrisiken betont werden, wie das in Kommentaren zum Thema DSGVO-Einführung häufig zu finden ist. Vielmehr sollen (auch) die umfangreichen betrieblichen Vorteile sichtbar gemacht werden, die dem Unternehmer bei einer professionellen DSGVO-Einführung zur Verbesserung der Wettbewerbssituation möglich sind und daher auch genutzt werden sollten!

RA Mag. Andreas Schütz LL.M.

Taylor Wessing

e|n|w|c Natlacen Walderdorff Cancola Rechtsanwälte GmbH

1030 Wien, Schwarzenbergplatz 7

www.taylorwessing.com

Dr. Lambert Gneisz MAS CMC SV

Performer Management Instruments Dr. Gneisz GmbH

1080 Wien, Albertgasse 1 A

www.DSGVO-Performer.com

Wien, im Dezember 2017

TaylorWessing

DSGVO Performer®

Inhaltsverzeichnis

Zum Verständnis 1

Inhaltsverzeichnis 2

1. Wen die EU-DSGVO betrifft 3
2. Wie teuer sind IT-Risiken? 3
3. DSGVO-Risiken kalkulieren 4
4. Vorgehen zur Risikoerfassung und Risikobewertung 4
5. Die wichtigen Vorteile aus DSGVO-Aktivitäten 4
6. Die Gefahr der Wahrnehmungsschwelle 5
7. Projektablauf 6
8. DSGVO-Implementierung mit „Gap Analysis“ 6
9. Projektsteuerung und Ressourcen-/Budgetplanung 7
10. Im Überblick: Umsetzung einer Datenschutz-Struktur 7
11. Datenschutz-Management-System 8
12. Verfahren und Konzepte 9
13. Resümee 9
14. Vitae der Autoren 10
15. Literaturhinweise 11
16. Glossar (vgl. www.DSGVO-Performer.com) 12
17. Links zu Sicherheitsinformationen (vgl. www.DSGVO-Performer.com) 13

1. Wen die EU-DSGVO betrifft

Wie aus dem Wortbestandteil „Verordnung“ zu erkennen ist, hat die Europäische Datenschutzgrundverordnung zunächst direkte Auswirkungen auf Funktionsträger mit juristischem Fokus. Da sie die Regelung personenbezogener Daten zum Ziel hat, bringt sie auch Personalverantwortlichen und Organisationsabteilungen neue verpflichtende Aufgaben.

Wer sich dem Thema weiter nähert, den mag es überraschen, dass es eine dritte und eine vierte Betroffenenkategorie gibt, die der Bedeutung der beiden zuvor genannten, Recht und HR/ORGA als Risikotreiber sogar noch übertreffen können.

Etwa wenn man **als dritte Risikokategorie** die möglichen Auswirkungen der DSGVO auf das betriebliche Management von IT-Risiken bewertet. Seien das die höheren IT / Cyber-Sicherheitsanforderungen oder auch strengere vertragliche Anforderungen mit externen Service-Providern.

2. Wie teuer sind IT-Risiken?

Fast alle Geschäftsprozesse erfordern heute die IT-Nutzung. Risiken, die aus dem Einsatz der Informationstechnologie im Unternehmen stammen, verdienen daher besondere Betrachtung und besonderen Schutz. In der betrieblichen Praxis bietet dieser Punkt wertvolle Möglichkeiten, das Unternehmensrisiko abzusichern. Denn das typischerweise spontane Eintreten von IT-Risiken kann unerfreulich rasch zu wesentlichen - bis hin zu existenziellen - Problemen führen!

Ein risikoorientiertes Management der Informationstechnologie ist heute mehr denn je unabdingbar. Gemeint ist damit etwa ein IT-Betrieb mit zweckmäßiger Zuverlässigkeit, betreffend die technische Verfügbarkeit. Hervorzuheben ist auch die Compliance zu den durch die DSGVO neuen, wesentlich erweiterten und **in vielen Punkten verschärften gesetzlichen Normen.** Stark wachsend in ihrem Risikogehalt sind auch die Herausforderungen des Outsourcings und der Nutzung von IT-Services aus der Cloud. Ob im Gesundheitswesen, im bargeldlosen Zahlungsverkehr oder bei dem Betrieb von kritischer Infrastruktur.

Daher sind in DSGVO-Projekten, abgesehen von der Geschäftsführung, der Personalleitung und der Rechtsabteilung zwingend auch der Chief Information Officer (CIO) der IT-Services einzubinden. Zu beachten ist dabei, dass der CIO nicht zum Datenschutzbeauftragten – so ein solcher erforderlich ist – ernannt werden darf. Es würde sich daraus ein Rollenkonflikt ergeben, der vom DSGVO-Gesetzgeber nicht zugelassen wird.

3. DSGVO-Risiken kalkulieren

Es empfiehlt sich, die Risiken in kaufmännischen Größen, etwa in abgezinsten Barwerten zu kalkulieren und dafür in den zukünftigen Bilanzen ab dem Geschäftsjahr 2018 **kalkulatorisch einzuplanen.**

Dieses Vorgehen, das auch der Gesetzgeber durch dessen Auftrag zur unternehmerischen Sorgfalt erwartet, wird in jeder Organisation das Bewusstsein und die Aufmerksamkeit vieler Entscheidungsträger positiv beeinflussen.

4. Vorgehen zur Risikoerfassung und Risikobewertung

Es liegt in der Natur der unternehmerischen Sache, dass sich Risiken nicht ausschließen lassen und daher organisatorische Vorbereitungen für das Risikomanagement zu treffen sind. In Abstimmung auf die neuen Anforderungen der EU-DSGVO empfiehlt sich ein in Vorgehen in diesen fünf Schritten:

a. **Identifikation von Risiken** (Gap Analysis), z.B. in Zusammenarbeit mit externen Beratern
b. **Technische Bewertung von Risiken** (Risk Analysis), u.a. mit Benchmarks
c. **Unternehmerische Bewertung** von direkten Risiken (Business Impact Analysis)
d. **Bewertung von rechtlichen Haftungsrisiken** (Legal Impact Analysis)
e. **Bewertung von rechtlichen sonstigen Risiken** (Public Impact Analysis)

5. Die wichtigen Vorteile aus DSGVO-Aktivitäten

Es gibt **eine sehr wesentliche vierte Dimension** bei der Planung von Aktivitäten zur Erfüllung des DSGVO-Verpflichtungen. Bei einer anfänglichen Betrachtung der umfangreichen Verpflichtungen, die auf ein Unternehmen zur Einhaltung der DSGVO-Vorgaben zukommen, wird möglicherweise die Erwartung des Eintretens „des Scheiterns“ größer sein als jene, damit auch eine Reihe wirtschaftlich wirklich interessanter Vorteile für sein Unternehmen zu erschließen. Das ist aber damit ganz konkret möglich! **Diese positiven Effekte von DSGVO-Projekten müssen in die kaufmännische Gesamtbetrachtung integriert werden.** Sie sind vielfältig und natürlich von Fall zu Fall verschieden.

Zu den vier übergeordneten Nutzenkategorien:

- **Sicherheit**
- **Kosten**
- **Wettbewerb**
- **Compliance**

sollten diese zwölf möglichen Veränderungsvorteile für jedes DSGVO-Projekt initial erfasst und in ihrer Entwicklung dokumentiert werden:

1. Erhöhung der Sicherheit im IT-Betrieb
2. Vermeidung von Kosten durch Produktionsausfälle / vermeidbare unproduktive Zeiten
3. Qualitätssicherung durch Qualitätsmanagement
4. Kostensenkung durch Prozessoptimierungen
5. Erhöhung von Produktivität und Wertschöpfung
6. Ausbau des Vorsprungs gegenüber dem Mitbewerb
7. Positives Zeichen an Mitarbeitende für mehr Mitarbeitermotivation
8. Erhöhung der Rechtssicherheit im Allgemeinen
9. Anhebung des Compliance-Niveaus
10. Absicherung der Geschäftsführerhaftung
11. Verbesserung des Images am Markt, wie zB Employer Branding
12. Erhöhung des Vertrauens von Eigentümern, Kapitalgebern, Aufsichtsrat und auch insbesondere der nationalen Datenschutzbehörde.

6. Die Gefahr der Wahrnehmungsschwelle

Risiken sind für Unternehmer „das tägliche Brot“. Daher besteht die **latente Gefahr**, dass neue Risikothemen entweder übersehen oder unterschätzt werden, oder beides. Risiken werden oft nur als formal mögliche Abweichungen von geplanten Zielen verstanden, die je nach Branche und je nach Unternehmenssituation geradezu „natürlich erwartet“ werden. Zwar werden Risiken auch durch die beste vorausschauende Planung nicht zu vermeiden sein. Doch können und müssen ihre Auswirkungen durch vorbereitende Maßnahmen zur Risikosteuerung verringert werden. Die professionelle Umsetzung der DSGVO-Vorgaben ist dafür eine sehr gute Gelegenheit, mit hoher strategischer wie auch risikopolitischer Tragweite!

Sollte ein Schaden eintreten, so wird es bei der Beurteilung von Haftungsfragen wesentlich sei, belegen zu können, welche Aktivitäten zur Schadensvermeidung vorab getroffen wurden. Darin liegt die Verantwortung der Geschäftsführung. Fahrlässigkeit, grobe Fahrlässigkeit und Vorsatz sind Termini, die dann unerfreulich zur Diskussion stehen werden. Durch die professionelle Planung eines Datenschutzprojektes kann diesen, spätestens ab Mai 2018 gegebenen neuen Gefahren jetzt begegnet werden. Jede Organisation hat dabei die Möglichkeit, durch Vorbereitungsmaßnahmen in einem vom jeweiligen Unternehmen gewünschten Ausmaß, ein neues Sicherheitsniveau zu schaffen.

7. Projektablauf

Die vielfältigen Anforderungen der DSGVO können zumeist nicht zeitgleich und vollständig erfüllt werden. Das Unternehmen muss daher abschätzen und priorisieren, welche Verarbeitungen von personenbezogenen Daten das größte Risiko für den Geschäftsbetrieb des Unternehmens und/ oder die Rechte der betroffenen Personen darstellen sowie welche Risiken am wahrscheinlichsten zu hohen Geldbußen führen können.

Im Anschluss an diese Einschätzung sind die **Ressourcen entsprechend umfangreich und vor allem zeitnah bereitzustellen.** Denn die Strafbestimmungen wurden bekanntlich sehr massiv erhöht. Existenzgefährdende Geldbußen in jedem Einzelfall von bis zu 20 Mio. EUR bzw. 4 % des gesamten weltweit erzielten Jahresumsatzes einer Unternehmensgruppe können von der Aufsichtsbehörde verhängt werden. Dazu können als „Beugestrafen“ Verwaltungsstrafen von bis zu € 25.000,- zusätzlich und pro Übertretungsfall kommen.

Da die Vorbereitung auf die DSGVO eine gründliche Analyse, möglicherweise auch eine Restrukturierung sehr vieler interner Prozesse erfordert ist es höchst empfehlenswert, rasch auf die Anforderungen von technischen und organisatorischen Maßnahmen (TOM´s) zu reagieren.

8. DSGVO-Implementierung mit „Gap Analysis“

Zur Feststellung des datenschutzrechtlichen Handlungsbedarfs eines Unternehmens sollten zuerst rechtliche, organisatorische und IT-technische „Lückenanalysen“ durchgeführt werden. Dabei wäre die gegenwärtige Datenschutz-Compliance mit den Anforderungen der DSGVO abzustimmen. Hierbei sollte auch eine mögliche Non-Compliance im Hinblick auf die bereits bestehenden Vorgaben der europäischen Datenschutzrichtlinie 95/46/EG identifiziert werden.

Der nächste Schritt besteht in einer Risikoanalyse, mit bereichsübergreifenden und daher für Entscheidungsträger sehr relevanten **kaufmännischen Bewertung von juristischen, technischen und organisatorischen Risiken in einer Zusammenschau.** Unbedingt betrachtet werden müssen in dieser Phase auch die Risiken der persönlichen Haftung und in welchen denkbaren Schadensfällen diese wie schlagend werden könnten.

9. Projektsteuerung und Ressourcen-/Budgetplanung

Das Unternehmen muss die notwendigen Ressourcen zur Verfügung stellen. Die Budgetplanung sollte insbesondere interne Ressourcen, wie für die Umsetzung benötigtes internes Personal, rechtlichen Beratungsaufwand sowie IT-Kosten (z.B. für unterstützende Software; IT-Überprüfungen etc.) berücksichtigen.

Die Kosten eines DSGVO-Projekts können als Investition („Einzahlung“) in eine „Datenschutzrisiko-Versicherung“ verstanden werden.

Wie die betriebliche Praxis zeigt, sind zu Jahresende 2017 die wenigsten Organisationen auf die immerhin bereits seit April 2016 bekannten DSGVO-Anforderungen weder inhaltlich noch personell vorbereitet! Die erforderlichen Ressourcen können zweckmäßigerweise nur durch die Zusammenarbeit mit dafür qualifizierten externen Partnern (wie Rechtsanwälten, Unternehmensberatern, IT-Consultants) rasch und ergebnisorientiert beschafft werden. DSGVO-Schulungen und Kurse sind überbucht.

Zwei Gründe sprechen vor allem dagegen zu glauben, sich in dieser Situation, wie der berühmte Baron Münchhausen „am eigenen Schopf aus dem Schlamm ziehen“ zu können:

- Die Materie ist schlichtweg **zu komplex**, um sie in wenigen Tagen zu erlernen.
- Die möglichen operativen und strategischen Schäden sowie die **umfassenden Haftungsrisiken** sind zu massiv, um sie „auf die leichte Schulter“ zu nehmen.

10. Im Überblick: Umsetzung einer Datenschutz-Struktur

Die DSGVO enthält eine Reihe zusätzlicher wesentlicher Anforderungen im Verhältnis zum bisher geltenden Recht:

1. **Stärkere Rechte der betroffenen Personen** (z.B. auf Information, Auskunft und Berichtigung/Löschung; das Recht auf Datenübertragbarkeit; das Recht auf Widerspruch gegen bestimmte Datenverarbeitungstätigkeiten; das „Recht auf Vergessenwerden" – die Verpflichtung der Verantwortlichen, Auskunfts- oder Löschanträge an dritte Datenempfänger weiterzuleiten; strengere Anforderungen an Einwilligungserklärungen etc.).

2. **Strengere organisatorische Anforderungen** (z.B. die Verpflichtung, ein Verfahrensverzeichnis von internen Datenverarbeitungstätigkeiten zu erstellen und fortan zu führen; die Notwendigkeit, in verschiedenen Fällen eine Datenschutz-Folgenabschätzung durchzuführen ggf. und einen Datenschutzbeauftragten zu ernennen; Datenschutz durch Technik („privacy by design") und Datenschutz durch datenschutzrechtliche Voreinstellungen („privacy by default"); die Verpflichtung zur Verknüpfung personenbezogener Daten mit dem Zweck ihrer Erhebung und der Ermächtigungsgrundlage für ihre Verarbeitung; die Dokumentation von Datenübermittlungen; Erstellung diverser Löschungskonzepte etc.).

3. **Strengere Meldepflichten** (z.B. die Verpflichtung, im Falle einer Verletzung des Schutzes personenbezogener Daten binnen 72 Stunden die Datenschutzbehörde sowie ggf. die betroffenen Personen zu informieren).

4. **Höhere Cyber-Sicherheitsanforderungen** an die IT

5. **Strengere vertragliche Anforderungen** (mit externen Service-Providern, Auftragsverarbeitern und unter Umständen auch innerhalb der Unternehmensgruppe).

Um allen neuen Verpflichtungen nachzukommen, von denen massive kaufmännische Risiken ausgehen können, muss das Unternehmen eine robustere Datenschutzstruktur einführen.

11. Datenschutz-Management-System

Die DSGVO sieht eine Reihe von Anforderungen vor, die ohne ein umfassendes Datenschutz-Management-System schwierig zu bewältigen sind. Ein solches System sollte unternehmensweit eingeführt werden, da datenschutzrechtliche Verstöße selbst kleiner Niederlassungen zu hohen Geldbußen für eine gesamte Unternehmensgruppe führen können.

12. Verfahren und Konzepte

Viele der Verpflichtungen aus der DSGVO können in der Praxis nur implementiert werden, wenn entsprechende Konzepte, Richtlinien und Standardvorgehensweisen (kumulativ sog. „Standard Operating Procedures“, „SOP“) zur Qualitätssicherung eingeführt werden. Dies betrifft insbesondere die Rechte betroffener Personen, die Meldepflichten bei der Verletzung des Schutzes personenbezogener Daten und die Datenschutz-Folgenabschätzungen.

Darüber hinaus müssen Mitarbeiter in Bezug auf ihre sich aus der DSGVO ergebenden Verpflichtungen und Verantwortlichkeiten geschult werden. **Das Unternehmen hat angemessene Maßnahmen zu ergreifen, um die Einhaltung der Anforderungen der DSGVO nachzuweisen.** Diese Maßnahmen sollten regelmäßig überprüft und aktualisiert werden.

13. Resümee

Aufgrund der hohen Anzahl von Vereinbarungen, die unternehmensintern sowie mit Dritten geschlossen werden müssen, ist bis zum 25. 05. 2018 eine durchdachte **Strategie für das Management von Datenverarbeitungsverträgen zu definieren und umzusetzen.**

Dabei scheint eine externe professionelle Begleitung unumgänglich, um für die gegebenen großen Risiken das gewünschte Sicherheitsniveau etablieren und halten zu können. Insbesondere, **um die genannten mehrdimensionalen Wertschöpfungsvorteile aus professionell umgesetzten DSGVO-Projekten realisieren zu können.**

Diese Unterlage dient der allgemeinen Information. Sie ist keine Grundlage für konkrete Maßnahmen und ersetzt nicht die Beratung im Einzelfall. Gerne stehen wir Ihnen für die Erörterung von Fragen zu den hier behandelten Themen zur Verfügung!

RA Mag. Andreas Schütz LL.M.

Taylor Wessing
e|n|w|c Natlacen Walderdorff Cancola Rechtsanwälte GmbH
1030 Wien, Schwarzenbergplatz 7
www.taylorwessing.com

Dr. Lambert Gneisz MAS CMC SV

Performer Management Instruments Dr. Gneisz GmbH
1080 Wien, Albertgasse 1 A
www.DSGVO-Performer.com

14. Vitae der Autoren

RA Mag. Andreas Schütz LL.M. a.schuetz@taylorwessing.com

Andreas Schütz ist CEE Partner der internationalen Anwaltssozietät Taylor Wessing in den Teams IP/IT sowie Umwelt, Planung & Regulierung. Er ist anerkannter Experte in sämtlichen Bereichen des IT-Rechts. Über besonderes Know-how verfügt er im Technologiesektor sowie im Datenschutz, gleichzeitig ist er auf die Rechtsgebiete Software Lizenzen & Vertriebsrecht, E-Commerce, Werberecht und Unlauterer Wettbewerb spezialisiert. Er leitet zudem die Gruppe Logistics & Transport in CEE und ist Mitglied der Industriegruppe Consumer & Retail. Die Beratung im Vergabe- und Lebensmittelrecht ist ein weiterer Schwerpunkt seiner Tätigkeit.

Mag. Dr. Lambert Gneisz MAS CMC SV L.Gneisz@DSGVO-Performer.com

Lambert Gneisz ist Unternehmensberater, Gründer und Inhaber der Performer Management Instruments Dr. Gneisz GmbH in Wien. Als Gerichtssachverständiger für Unternehmensberatung ist er von der TÜV-Akademie zertifizierter Datenschutzbeauftragter nach ISO/IEC 17024 für die EU – DSGVO. Er ist vierfacher Preisträger des CONSTANTINUS Beratungs- und IT-Preises sowie ein „Hidden Champion“ des EU ISME-Wettbewerbs in der Kategorie Business Consulting International.
Mit www.DSGVO-Performer.com unterstützt er Mittelbetriebe bei der Umsetzung der DSGVO-Compliance-Anforderungen in der Praxis.

15. Literaturhinweise

Erhältlich über die Service-GmbH der Wirtschaftskammer Österreich https://webshop.wko.at

Datenschutz-Grundverordnung: Diese Publikation wird aktualisiert. Die - um das Anpassungsgesetz 2018 erweiterte Broschüre - ist ab Jänner 2018 verfügbar!

IT-Sicherheitshandbuch für KMU - 8. Auflage – 2017; IT-Sicherheitshandbuch für Mitarbeiter, 2017

Weitere Literaturhinweise (vgl www.manz.at):

Georg Beham; Reinhard Hübelbauer: EU-Datenschutz-Grundverordnung (EU-DSGVO), Praxiseinführung in 7 Schritten, Austrian Standards plus GmbH, 138 Seiten, 2017, ISBN: 9783854023555

Datenschutz in der Kundenbindung. Erstellung einer "Ticket-Card" im Rahmen der DSGVO, GRIN Verlag, E-Book Text, 14 Seiten, 1. Auflage, 2017, ISBN: 9783668574441

Die Einwilligung Minderjähriger und der Altersnachweis (Art.8 DSGVO), GRIN Verlag, E-Book Text (PDF sofort downloaden Downloads sind nur in Österreich möglich!), 14 Seiten, 1. Auflage, 2017, ISBN: 9783668579927

Die neue Datenschutzgrundverordnung (EU-DSGVO). Auswirkungen auf die Social Media Marketing Strategie von Unternehmen in Deutschland, Studylab, 100 Seiten, 1. Auflage, 2017, ISBN: 9783960951230

Walter Dohr; Hans J Pollirer; Ernst M Weiss; Rainer Knyrim, Kommentar Datenschutzrecht inkl. 21. Erg.-Lfg. + DSGVO (SonderEL 20a), Datenschutzgesetz 2000 samt Europarecht, Nebengesetzen, Verordnungen und Landesdatenschutz mit Prüflisten und Mustern für die Praxis ergänzt, MANZ Verlag Wien, Loseblatt-Sammlung, 3123 Seiten, 2. Auflage, 2017, ISBN: 9783214086596

Lukas Feiler; Nikolaus Forgó, EU-DSGVO, EU-Datenschutz-Grundverordnung, Verlag Österreich, 1. Auflage, 2016, ISBN: 9783704675804

Feiler Lukas, Gesetzbuch Datenschutzrecht Inklusive Guidelines der Artikel-29-Datenschutzgruppe, Stand: 1.10.2017, Verlag Österreich, VI, 744 Seiten, 2017. Auflage, 2017 ISBN: 9783704678386

Lukas Feiler; Bernhard Horn, Umsetzung der DSGVO in der Praxis, Fragen, Antworten, Muster, Verlag Österreich, 250 Seiten, 2018. Auflage, 201897837046. ISBN: 78591

Christoph Grabenwarter; Ferdinand Graf; Maria Mercedes Ritschl: Neuerungen im europäischen Datenschutzrecht für Unternehmen, MANZ Verlag Wien, XIV, 112 Seiten, 2017, ISBN: 9783214012397

Handbuch zum europäischen Datenschutzrecht, EU Publications, ISBN: 978-92-9239-329-8

Johanna Heberlein, Datenschutz im Social Web, Nomos, 319 Seiten, 1. Auflage, 2017, ISBN: 9783848746071

Susanne Kalss; Ulrich Torggler, Big Data, Informationen und Gesellschaftsrecht, MANZ Verlag Wien XX, 118 Seiten, Band 5, 2017, SIBN: 9783214032463

Rainer Knyrim, Datenschutz-Grundverordnung, Das neue Datenschutzrecht in Österreich und der EU, MANZ Verlag Wien, XXII, 418 Seiten, 2016, ISBN: 9783214100834

Hans-Jürgen Pollirer; Ernst M. Weiss; Rainer Knyrim; Viktoria Haidinger, DSGVO, Datenschutz-Grundverordnung, MANZ Verlag Wien, XII, 214 Seiten, 2017, ISBN: 9783214011673

16. Glossar (vgl. www.DSGVO-Performer.com)

Diese Begriffe sollten Sie kennen. Darauf sollte Ihre Organisation vorbereitet sein:

Auftragsverarbeiter
Auskunftspflicht des Verantwortlichen
Autovervollständigen
Bad Hotel
Backup
Betroffenenrechte
Besondere Kategorien von personenbezogenen Daten („sensible Daten“)
Niederlassung „Marktortprinzip“
Biometrische Daten
Brandschutz
Browserverlauf löschen
BOD-Bring Your Own Device
Bugs
Cloud Speicher
Data Breach Notification
Dateiverschlüsselung
Daten über Straftaten
Datenfolgenabschätzung
Datenimport
Datenschutz und -sicherheit durch Technik
Datenschutz und -sicherheit durch Voreinstellungen
Datenträgerproblematik
Datenschutzbeauftragte
Datenübertragbarkeit
Denial of Service (DoS)
Diebstahlschutz
Dokumentationspflicht
Dumpster-Diving
Einwilligung
Einwilligungserklärung
Entsorgung von Datenträgern
E-Mail Attacken
Exploits
Firewalls
Geldstrafen
Gelbes Schloss
Genetische Daten
Gesundheitsdaten
Grundsätze der Verarbeitung
Haftungsrisiko durch Cyberangriffe
Informationspflichten
Internationaler Datenverkehr
Internetwurm
IT-Notfallplan
IT-Risikomanagement
Katastrophen-Test (K-Test)
Kryptographie
Mailverschlüsselung
Maleware
Man-in-the-middle
Meldung von Datenschutzverletzungen
Notfallplan
Notfalldokumentation
Notfallkommunikation
Patch-Management
Passwörter
Personenbezogene Daten (pbD)
Pflicht zur Berichtigung
Pflicht zur Einschränkung
Pflicht zur Löschung
Pflichten des Auftragsverarbeiters
Pflicht zur Umsetzung eines Widerspruchs
Pflichten des Verantwortlichen
Pflichten gegenüber der Aufsichtsbehörde
Profiling
Pishing
Privacy by design
Privacy by default
Private E-Mails am Arbeitsplatz
Pseudonymisierung
Public Key Infrastructure (PKI)
RAID

Ransomware
„Recht auf Vergessenwerden“
Rechtmäßigkeit der Verarbeitung
Rechtsdurchsetzung und Strafen
Risikofolgenabschätzung
Safety-Checklist
Soziale Netzwerke
Spam
Spezielle Mitteilungspflichten
Sub-Auftragsverarbeiter
Verzeichnis von Verarbeitungstätigkeiten
Verantwortlicher
Videokameraattrappe
Videoüberwachung
Virus
Voraussetzungen für Weiterverarbeitung
Warnpflicht
Zero-Day-Attacken
Zutrittskontrolle

17. Links zu Sicherheitsinformationen (vgl. www.DSGVO-Performer.com)

- Heise Verlag: http://www.heise.de
- Hackerangriffe live verfolgen: http://www.sicherheitstacho.eu
- Onlinesicherheit Infoportal: http://onlinesicherheit.gv.at
- Rechtliche Pflichten für Unternehmer http://wko.at
- Passwortcheck: https://howsecureismypassword.net
- Kuratorium Sicheres Österreich: https://kuratorium-sicheres-oesterreich.at
- Bundesministerium für Inneres: http://www.bmi.gv.at/cms/BK/betrug/start.aspx
- SaferInternet: https://www.saferinternet.at/
- Sicherheit im Internet: http://virus-protect.org/
- Bundeskriminalamt: https://bka.de
- E-Day: http://www.eday.at
- TeleFIT Roadshow: http://www.telefit.at
- WKO-Sicherheitsseite: http://it-safe.at

(end).