

EU-DSGVO

Eine Kurzanleitung

Alan Calder



EU-DSGVO

Eine Kurzanleitung

EU-DSGVO

Eine Kurzanleitung

ALAN CALDER



IT Governance Publishing

Es wurden alle möglichen Bemühungen unternommen, um sicherzustellen, dass die in diesem Buch enthaltenen Informationen zum Zeitpunkt der Drucklegung korrekt sind und der Herausgeber und der Autor keine Haftung für etwaige Fehler oder Auslassungen übernehmen. Jede wie immer geartete Meinung, die in diesem Buch zum Ausdruck gebracht wird, entspricht der des Autors und nicht des Herausgebers. Angegebene Webseiten dienen lediglich als Referenz und nicht als Bestätigung, jeder Webseiten-Besuch erfolgt auf eigene Gefahr des Lesers. Herausgeber oder Autor übernehmen keinerlei Haftung für allfällige Verluste oder Schäden, die durch Handlungen bzw. unterlassene Handlungen gegenüber anderen Personen als Folge des Materials in dieser Veröffentlichung entstehen.

Abgesehen von der ehrlichen Handlungsweise zum Zwecke der Forschung oder privaten Studie bzw. Kritik oder Rezensionen entsprechend den Vorgaben des Copyright, Designs und Patents Act 1998, darf diese Publikation nur mit vorheriger schriftlicher Genehmigung des Herausgebers oder im Falle der reprographischen Vervielfältigung gemäß den Lizenzbedingungen der Copyright Licensing Agency in jeder Form vervielfältigt, gespeichert oder übertragen werden. Anfragen in Bezug auf eine Vervielfältigung außerhalb der vorgenannten Bedingungen sind dem Herausgeber unter der hier folgenden Adresse zu übermitteln:

IT Governance Publishing
IT Governance Publishing
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom

www.itgovernance.co.uk

© Alan Calder 2017

Der Autor erklärt die Autorenrechte nach dem Urheberrecht, Designs and Patents Act, 1988, um als Autor dieser Arbeit identifiziert zu werden.

Zum ersten mal im Vereinigten Königreich 2017 von IT Governance Publishing veröffentlicht:

ISBN 978-1-84928-864-4

ÜBER DEN AUTOR

Alan Calder ist Gründer und Vorstandsvorsitzender der IT Governance Ltd (www.itgovernance.co.uk), ein Informations-, Analyse- und Beratungsunternehmen, das Betriebe bei der Verwaltung von IT-Governance-, Risikomanagement-, Compliance- und Informationssicherheitsfragen unterstützt. Er blickt auf eine langjährige Führungserfahrung im privaten wie öffentlichen Sektor.

Das Unternehmen betreibt auf der ganzen Welt Webseiten, die eine Reihe von Büchern, Werkzeugen und anderen Veröffentlichungen zu IT-Governance, Risikomanagement, Compliance und Informationssicherheit vertreiben.

INHALTE

Einführung	8
Kapitel 1: Kurzer geschichtlicher Überblick zum Datenschutz.....	11
Kapitel 2: Begriffe und Definitionen	20
Kapitel 3: Die Verordnung.....	33
Grundsätze	38
Anwendbarkeit.....	40
Rechte des Datensubjekts	42
Zustimmung	44
Recht vergessen zu werden	47
Datenportabilität.....	48
Rechtmäßige Verarbeitung	49
Aufbewahrung von Daten.....	51
Der “One-Stop Shop”	52
Aufzeichnungen der Datenverarbeitungsvorgänge	53
Datenschutzfolgenabschätzungen	54
Datenschutz durch Technik und Grundeinstellung.....	55
Verträge Datenverwalter/-verarbeiter	57
Der Datenschutzbeauftragte.....	58
Haftung und Vorstand.....	61
Datenverletzungen	62
Verschlüsselung.....	64
Internationale Transfers	66
Verbindliche Unternehmensregeln	67
Zusätzliche Überlegungen	69
Änderungen der Cookie-Gesetze.....	70
IP Adressen	72
EU-Netz und Informationssicherheitsrichtlinie (NIS)....	73

Inhalte

Kapitel 4: Einhaltung der Verordnung.....	75
Auswirkungen.....	75
Verständnis Ihrer Daten: wo und wie diese verwendet werden.....	78
Unterlagen	79
Geeignete technische und organisatorische Maßnahmen und ISO/IEC 27001.....	81
Standards, Systeme und Vertrauenssiegel.....	85
Sicherung der Lieferantenbeziehungen.....	86
Kapitel 5: Verzeichnis der Verordnung.....	88
Anhang 1: Nationale Datenschutzbehörden ...	97
Anhang 2: EU-DSGVO Quellen	98
ITG Ressourcen	102

EINFÜHRUNG

Im Laufe der letzten zehn Jahre entwickelte sich die Cyber-Sicherheit zu einem immer wichtigeren Thema für Unternehmen in der gesamten EU. Obwohl Cyber-Bedrohungen ein breites Spektrum von Zielen betreffen, von kritischen, nationalen Infrastrukturen und geistigem Eigentum, über Geschäftsgeheimnisse bis hin zu finanziellen Informationen, behalten Cyber-Kriminelle auch weiterhin vor allem persönlich identifizierbare Informationen oder PII im Auge.

PII - Namen, Adressen, Sozialversicherungen oder Steueridentifizierungen, Zahlungskarteninformationen - sind wertvoll, weil sie den Weg zu zahlreichen Verbrechen, einschließlich Wirtschaftsdiebstahl und Identitätskriminalität, eröffnen können.

Die Besorgnis der Personen- welche das Datenschutzrecht in der Regel als Datensubjekt bezeichnet - reicht weit über die Cyber-Kriminalität hinaus. Nationalstaaten und große Unternehmen sind nun imstande, große Mengen an persönlichen Informationen zu erheben, die es ermöglichen, einzelne Aktivitäten im Cyberspace verfolgen. Digitale Marketing-Unternehmen entwickeln neue und immer effektivere Methoden zur Rückverfolgbarkeit der Verbraucheraktivitäten. Social-Media

Einführung

Unternehmen leben von der Veröffentlichung personenbezogener Daten. Zwar gibt es soziale Vorteile für all diese Aktivitäten, dennoch besteht eine potenzielle Untergrabung der individuellen Privatsphäre.

Die EU bemüht sich seit langer Zeit um den Schutz der Rechte von Einzelpersonen in Bezug auf ihre persönlichen Daten. Die inzwischen beschlossene und mit Mai 2018 in Kraft tretende Datenschutz-Grundverordnung (DSGVO) ist wohl weltweit ein Meilenstein in Bezug auf von gewählten Behörden ergriffenen Maßnahmen für angenehmen Schutz der Privatsphäre und persönlichen Daten der Bürger.

Die DSGVO sorgt dafür, dass gleiche Rahmenbedingungen für den Datenschutz in allen EU-Mitgliedstaaten gelten. Dies bedeutet, dass EU-BürgerInnen auf eine gleiche Behandlung in der EU vertrauen können und dass jene Unternehmen, welche die DSGVO-Anforderungen in einem Land einhalten, sicher sein können, dass diese auch mit allen anderen Mitgliedsstaaten vereinbar sind.

Unternehmen außerhalb der EU – und Dienstleistungen in die EU– unterliegen ebenso der DSGVO. Bestehende Vorkehrungen für den Datenexport aus der EU in andere Länder sind gezielt abgedeckt; vor allem aber werden Verstöße gegen die DSGVO mit Geldbußen geahndet, die “verhältnismäßig und abschreckend” sind, d.h. mit einer Höchststrafe von 20 Mio. € oder 4% der

Einführung

weltweiten Einnahmen, je nachdem, welche der beiden Einheiten größer ist.

Die Übergangsfrist für die Umsetzung der Vorgehensweisen für die Datenverarbeitung entsprechend den Vorgaben der DSGVO endet im Mai 2018. Von diesem Zeitpunkt an unterliegen Unternehmen, die gegen die Verordnungsvorschriften verstoßen, dem Risiko erheblicher Geldbußen.

Dieser Leitfaden soll Ihnen dabei helfen im Rahmen dieser neuen Bedingungen weiter zu wachsen, indem Sie ein Verständnis für die Verordnung, die Grundsätze des Datenschutzes und Bedeutung der Verordnung für Unternehmen in und außerhalb von Europa entwickeln.

Es gibt Schlüsselbegriffe in diesem Buch, die richtig verstanden werden müssen, um die neue Verordnung, die in Kapitel 2 - Begriffe und Definitionen definiert sind, richtig umzusetzen.

KAPITEL 1: KURZER GESCHICHTLICHER ÜBERBLICK ZUM DATENSCHUTZ

Das gemeinsame Konzept von Datenschutz ist ein sehr moderner Begriff. Wir denken an digital gespeicherte Datenbanken und Aufzeichnungen und verstehen, wie wichtig es ist, diese zu schützen. Es ist offensichtlich: digitale Aufzeichnungen haben kein physisches Gewicht und können verlegt oder gestohlen werden, ohne das Original zu berühren. Daher versteht es sich wie von selbst, dass ein derartiger Verlust eine enorme Menge an Informationen betreffen könnte. Das ist nicht so, wie es immer war, und auch heute noch müssen Informationen in anderen Formaten geschützt werden.

Möglicherweise kommen die frühesten Formen des Daten- und Datenschutzes eher von den Berufen als von der Gesetzgebung selbst. Das Vertrauensverhältnis Rechtsanwalt-Mandant (bzw. Anwaltsprivileg, wie es in Großbritannien genannt wird) wurde zum Beispiel als eine Art Vertrag zwischen einem Rechtsanwalt und seinem Mandanten über viele Jahrzehnte (und möglicherweise Jahrhunderte) gehandhabt, bevor es in das Gesetz selbst Eingang fand. Es wurde eingeführt, um zu garantieren, dass ein Rechtsanwalt die Interessen seiner Mandanten ohne der befürchteten rechtlichen Folgen angemessen vertreten kann.