

# Index

- access by employees in good faith 6.52, 6.101
- access by governments 1.17, 3.34–5, 6.21, 6.24–5, 6.76–81
- access by transfer 1.20–21, 3.18
- access controls 1.03
  - breach notifications 6.100–101
  - companies' privacy and security policies 4.10, 4.28–31, 6.139
  - compliance 2.02, 2.30
  - data collection methods 6.07, 6.72
  - security laws 1.05, 2.33, 2.43
- access rights
  - cloud computing 6.11, 6.19, 6.33–8, 6.41–2
  - company compliance 6.117
  - customer access 6.41–2
  - data handlers 1.23, 3.07, 6.11, 6.19, 6.33–8
  - employee databases 6.54
  - external vs. internal candidates 2.13
  - mergers and acquisitions 5.07
  - organization protocols 4.64
  - standard contractual clauses 3.46
- accountability 2.17, 6.85
- Ad Networks 4.26, 6.126
- Ad Servers 6.127
- advertising 6.02–5
  - cookies 6.124
  - direct marketing 6.130–36
  - location data 6.95
  - marketing consent 4.58, 6.133
  - ownership rights 6.111
  - terminology and content 4.13, 4.66, 6.70
- aggregation 1.13, 6.146
- agreements 4.56–63
  - Binding Corporate Rules 3.36–7
  - breaches 6.117
  - documentation categories 4.15
  - providers, qualified agreements from 6.12
  - standard contractual clauses 3.15–20, 3.27–8, 3.34–5, 3.37–8, 3.46, 6.31
  - template preparation 6.93–4
  - valid consent, obtaining 4.37–8
- alternative dispute resolution 3.47
- anonymity 1.19, 6.19, 6.67–9, 6.72, 6.115
- APEC (Asia-Pacific Economic Cooperation) 3.50
- Article 29 Working Party, EU 1.24, 3.29, *Resources*
- audits 2.02, 2.28, 5.01–10, 6.41–2, 6.137–8
- background checks 6.51
- beacons, web 6.124
- best practice 4.08, 6.86, 6.152
- big data 6.06–9
- Binding Corporate Rules (BCRs) 3.21, 3.27, 3.29, 3.48, *Table* 3.1
  - approval process 3.37, 3.39, 3.41
  - onward transfers 3.36
  - substantive compliance 3.32
- biometric data 6.145
- blocking statutes 6.76
- breaches 4.60, 6.98–108
  - agreements 6.117
  - checks when taking over existing program 5.03
  - and cloud computing 6.19
  - notification laws 2.44
  - record retention requirements 6.45
  - vendor's acceptance of unlimited liability 6.38–40

- bring your own device (BYOD) programs
  - 6.61
- browser settings 6.125
- business associates 1.22–3, 2.33, 2.38, 4.63, 6.83, 6.139
- Canada
  - anti-spam legislation (CASL) 6.129
  - FOIPPA (British Columbia's public sector privacy law) 6.25
- CAPTCHA 6.07, *Abbreviations*
- CBPR, (cross-border privacy rules) 3.50
- certification, Safe Harbor 3.47, 3.50, 6.27, 6.29–31, *Table 3.1*
- checklists 3.47, 6.141, *Checklist*
- Chief Privacy Officer 2.07, 2.10, 2.19
- Children Online Privacy Protection Act (COPPA), USA 6.97
- cloud computing 4.20, 6.10–43
- cold calls 6.129–32
- colocation providers 1.23
- Communications Decency Act (CDA) 6.120
- computer fraud 6.07, 6.72
- Computer Fraud and Abuse Act (CFAA), USA 6.07, 6.72
- consent 3.45, 4.33–66
  - browser features 6.125
  - data subject 3.14
  - documentation 4.15
  - flexibility 3.24–6
  - from employees 6.53
  - implementation 6.133
  - parental 6.96
- contracts 1.10, 2.42, 3.13, 3.24–6, 4.38, 4.63, 6.93–4, 6.96–7
- contributory liability 4.66, 6.113, 6.115, 6.120, 6.150
- control (data controllers) 1.22–3, 3.17, 3.21, 4.20, 4.55, 4.59–62
- cookies 1.12, 4.33, 4.37, 6.97, 6.124–6
- COPPA (Children Online Privacy Protection Act), USA 6.97
- covered entity 2.33, 2.38, 4.63, 6.83, 6.139
- crawler, web 6.07
- cross-border privacy rules (CBPR) 3.50
- cybersecurity 6.09, 6.19, 6.23, 6.39, 6.113
- data brokers 6.08
- data controllers 1.22–3, 3.17, 3.21, 4.20, 4.55, 4.59–62
- data handlers 1.23
- data integrity 4.66
- data processors 1.21–3, 3.10, 3.17–18, 3.20–21, 4.55, 4.59–62, 6.27
- data protection authority 1.24–6, 6.31, 6.49
- Data Protection Directive, EU 1.03, 1.07, 6.119
- data protection laws 1.02–4, 1.13, 1.19, 1.22, 2.08–9, 2.33–8, 2.48–9
- data protection officer 1.25, 2.07–20
- data retention 6.44–9
- data room 5.07
- data security breach *see* breaches
- data transfer agreements 3.15–20, 3.27–8, 3.38–9, 3.46, 6.12
- Digital Millennium Copyright Act (DMCA), USA 6.07
- digital rights management (DRM) 6.128
- discovery 3.34, 6.79, 6.151
- DNT (do not track) signal 6.125
- 'do not call/email/fax' registers 6.130
- double opt-in process 4.40, 6.133
- drafting documentation 4.01–75
- DRM (digital rights management) 6.128
- due diligence 3.30, 5.05–10, 6.12, 6.42, 6.137–8
- employee data monitoring 6.50–73
- encryption 1.05, 1.13, 6.74, 6.100–102
- enforcement 6.90–92, 6.116–17
  - and facial recognition systems 6.06
  - international application 2.35, 4.26
  - personal and confidential information access 6.24, 6.105, 6.149
  - Standard Contractual Clauses 3.35, 3.37, 4.63
- EU
  - Article 29 Working Party 1.24, 3.29, *Resources*
  - Common Market 2.35
  - Data Protection Directive 1.03, 1.07, 6.119

- Markets in Financial Instruments
  - Directive 6.42
- export control compliance programs 1.17
- facial recognition systems 6.06, 6.128, 6.145
- Fair Credit Reporting Act (FCRA), USA 4.38
- filtering 6.58, 6.144
- financial data 2.33, 6.74
- fingerprints 6.145
- FIPs (Fair Information Practice Principals) 6.85
- FOIPPA (British Columbia's public sector privacy law) 6.25
- forgotten, right to be 1.03, 6.49
- France, CNIL (data protection) 3.28
- genetic information 6.146
- Germany, Hessen data protection law 1.03
- good faith access 6.52, 6.101
- government information requests 6.58, 6.78–9
- Gramm-Leach-Bliley Act (GLB), USA 2.38, 6.74
- health information 4.33, 6.82–4
- Health Insurance Portability and Accountability Act (HIPAA), USA 1.05, 1.22, 2.33, 2.38, 4.33, 6.83
- hotlines 6.67–9
- household activity 1.12, 2.33, 6.119
- human resources information system (HRIS) 6.22, 6.36, 6.38, 6.54
- internet of everything 6.06–9, 6.128
- interoperability 2.37, 3.50, 6.85
- investigations 2.02, 3.34, 5.05, 5.10, 6.64–6, 6.75–81, 6.104
- IP address 1.12, 6.115, 6.124, 6.153–4
- jurisdictions 2.18–20, 3.37, 6.87–92
- key concepts 1.01–26
- lawful access by governments 6.58, 6.78–9
- legitimate interest exception 2.37, 4.35, 6.07–8, 6.54, 6.85, 6.145
- litigation hold 6.44, 6.61
- location data 4.47, 6.95
- machine-to-machine (M2M) commerce 6.09
- maintenance challenge 5.01
- making data available (transfer) 1.20–21, 3.01–50, 6.12
- 'marketing fluff' in privacy policies 4.09, 4.16, 4.31
- Markets in Financial Instruments
  - Directive, EU 6.42
- mere conduit 1.23, 6.83
- mergers and acquisitions (M&A) 4.06, 5.03, 5.05–8
- minors 6.96–7
- mobiles 4.48–9, 6.95
- Model Clauses *see* Standard Contractual Clauses
- monitoring, employee data 6.50–73
- multi-tenant data 6.19, 6.41
- National Security Agency (NSA), USA 1.03, 1.25, 6.21, 6.23
- networking 1.04, 4.58, 6.08, 6.118–22
- notices 4.18–33, 4.50, 6.98–108
- notifications to data protection
  - authorities 2.16, 4.70–75, 6.98–9
- NSA (National Security Agency) 1.03, 1.25, 6.21, 6.23
- onward transfers 3.33–6
- opt-in/opt-out consent 4.39–46, 6.133
- outsourcing 3.25, 3.38, 4.36, 6.11, 6.25, 6.43
- ownership 6.109–11
- Pareto Principle (80–20 rule) 2.30
- Patriot Act, USA 6.21, 6.25
- Payment Card Industry (PCI) 6.12, 6.43, 6.74, 6.94
- permissions 4.15, 6.95
- personal data 1.03, 1.10–18, 6.24, 6.105, 6.149
- personal use 6.60–61, 6.73
- platforms *see* mobiles; social networking

- privacy by design 6.112–14, 6.128
- privacy officer 2.07–20
- privacy policy notices 3.45, 4.06, 4.14, 4.16, 4.57, 6.97, 6.151
- privacy protection, reasons for 6.147–52
- Privacyville game 4.48
- 'private cloud' arrangement 6.19
- private household activity 1.12, 2.33, 6.119
- protocol 2.29, 4.10, 4.15, 4.64–5, 6.46–7
- questionnaires 4.66, 6.115, 6.138
- redacted data 1.13, 5.07–8
- retention protocol 6.46–7
- RFID (radio-frequency identification) 4.24, 6.56, 6.58, 6.95, 6.128
- right to be forgotten 1.03, 6.49
- rights and remedies 3.46, 6.117
- robo calls 6.130
- robots 6.07
- Safe Harbor Certification 3.47, 3.50, 6.27, 6.29–31, *Table 3.1*
- SAS 70 *see* SSAE 16
- SCC *see* Standard Contractual Clauses
- scraping technologies 6.07
- search engine 6.07, 6.49
- secondments 3.10, 3.13
- self-assessment 3.30, 3.47, 4.15
- sensitive data 1.10–18, 6.68, 6.82, 6.95
- service providers 1.21–3, 4.20, 4.55, 6.10–43
- smartphones 4.47, 4.49, 6.61, 6.113
- SOC (Service Organization Controls) Report 6.43
- social networking 1.04, 4.58, 6.08, 6.118–22
- Song-Beverly Credit Card Act, USA 2.38, 4.34, 6.153
- spam 2.33, 6.115, 6.129–36
- spiders 6.07
- SSAE auditing standard 6.43
- Standard Contractual Clauses (SCC) 3.15–20, 3.24–9, 3.34–8, 3.46, 6.31
- subprocessor 3.17, 3.46
- tags 4.24, 6.56, 6.58, 6.95, 6.128
- task list 2.21–51
- telematics 6.128
- tracking 6.95, 6.123–8
- transfer (making data available) 1.20–21, 3.01–50, 6.12
- TRUSTe 3.47
- unsolicited communications 6.129–36
- updating notices 4.58, 4.66, 4.73–5
- USA
  - Children Online Privacy Protection Act (COPPA) 6.97
  - Communications Decency Act (CDA) 6.120
  - Computer Fraud and Abuse Act (CFAA) 6.07, 6.72
  - data security breach notification laws 1.05
  - Digital Millennium Copyright Act (DMCA) 6.07
  - Fair Credit Reporting Act (FCRA) 4.38
  - Gramm-Leach-Bliley Act (GLB) 2.38, 6.74
  - Health Insurance Portability and Accountability Act (HIPAA) 1.05, 1.22, 2.33, 2.38, 4.33, 6.83
  - National Security Agency (NSA) 1.03, 1.25, 6.21, 6.23
  - Patriot Act 6.21, 6.25
  - Song-Beverly Credit Card Act 2.38, 4.34, 6.153
- vendors 4.20, 5.09–10, 6.19, 6.38–40, 6.137–40
- virus filtering 6.58, 6.143
- web crawlers 6.07
- whistleblower hotlines 6.67–9
- wiretapping 6.142–4
- X-rays 6.145
- Zip codes 6.153–4

*'Lothar Determann is Silicon Valley's go-to data privacy expert. Determann's Field Guide to Data Privacy Law is a practical and accessible guide for non-experts. I use it any time I encounter a new data privacy issue.'*

**Josh Faddis**

Vice President, General Counsel, Veeva Systems Inc., USA

*'Determann's Field Guide to Data Privacy Law allows privacy professionals to see the light at the end of the tunnel. The overview, practical advice, methodical organization and thoroughness distill down the complex world of international privacy, while also providing the necessary context behind these requirements. A must-have.'*

**Jeremy Livianu, Esq.**

Healthcare Compliance Officer, Associate Director, Legal Affairs,  
Nevro Corp, USA

*'Understanding and navigating the complexities of data privacy is of paramount importance for companies. Many in-house practitioners, who graduated from law school before data privacy was taught, feel left behind on this trending area of law. Determann's Field Guide to Data Privacy Law demystifies data privacy by providing practical and sound advice in an easy to navigate format. A must-have reference book for all legal departments.'*

**David Tognotti**

Vice President and General Counsel, Monster Inc., USA

What readers have said about the first edition:

*'The proliferation of electronic commerce and the unprecedented volume of data stored by businesses have made data compliance programs for most businesses a priority. Therefore, the creation and regular audit of an efficient program intended to minimize data thefts and manipulations has become a need of the hour. Determann's Field Guide addresses all these issues in a comprehensive manner. Dr. Lothar has also taken a lot of effort to collate the concepts and practices of international data privacy law in a most lucid manner. The Field Guide is the reflection of Dr. Determann's finesse towards details and accuracy, which is associated with all of his works. Focusing on the global regulatory regime of data privacy norms compliance requirements, the Field Guide comes with startling clarity through concise and up to date checklists essential for data compliance audits. The Field Guide is thoroughly recommended for the lay and expert alike, especially for lawyers,*

*accountants and other professionals engaged in operations covering various jurisdictions.'*

**Anand Mehta**

Partner, Khaitan & Co., India

*'As the data stored by business entities globally increases at an exponential pace, the legal frameworks and regulations governing such data increase in complexity at nearly the same rate, creating an environment of conflicting requirements and unclear obligations. Determann's book Determann's Field Guide to Data Privacy Law offers a real-world, practical approach to dealing with the data privacy challenges that in-house counsel face on nearly a daily basis. In particular, I recommend it as a source of invaluable information for those of us operating in multiple jurisdictions.'*

**Scott Trainor**

VP and Regional General Counsel, APJ, SAP Asia Pte. Ltd.

*'With the proliferation and diversity of privacy risks and international regulatory controls, and the increasingly obvious intersection of data security and privacy, no company can afford to overlook the importance of an up to date and well-tailored global compliance program. For companies doing business in the cloud or transacting with consumers, a well-considered international data privacy compliance program is not only a critical legal and liability control – it is fundamental to earning and maintaining the trust of your customers. In this comprehensive yet concise "Field Guide", Professor Determann has managed to consolidate an enormous breadth of legal requirements and best practices knowledge into a single, definitive reference that should be quite accessible even to non-privacy professionals. As general counsel of a multinational public company, I consider Determann's Field Guide to Data Privacy Law to be a pragmatic and indispensable reference in improving our compliance program, and highly recommend it for anyone looking for clear, practical guidance on establishing or improving their data privacy program!'*

**Felix Sterling**

Senior Vice President and General Counsel at Trend Micro Inc.,  
Silicon Valley, USA

*'Lothar Determann has done a great service to the field of privacy by providing practical, workable advice for a dynamic and challenging issue. This Field Guide will certainly be a valuable and soon dog-eared, addition to any privacy professional's reference library.'*

**J. Trevor Hughes**

President and CEO, International Association of Privacy Professionals  
(IAPP)

*'Determann's Field Guide takes the complicated subject of international privacy and breaks it down into helpful topics, checklists and suggestions. The focus on practical advice in an easy-to-use format makes it an ideal reference tool for in-house privacy professionals.'*

**Rebecca Matthias**

Senior Corporate Counsel, Privacy and Data Protection, VMware,  
Inc., Palo Alto, USA

*'Determann's Field Guide to Data Privacy Law is an indispensable handbook for international privacy professionals. Written by a star lawyer, it explains how to develop and maintain a corporate privacy compliance program. The book manages both to explain the "big picture" of global privacy challenges and to point out relevant details in a clear and concise fashion.'*

**Paul M. Schwartz**

Berkeley Center for Law & Technology, University of California,  
Berkeley School of Law (Boalt Hall), USA

*'Determann's Field Guide is an insightful practical guide which should be on every privacy practitioner's desk.'*

**Daniel Blaettler**

Vice President and Associate General Counsel, Verisign, Geneva,  
Switzerland

*'Understanding and having an awareness of international data protection laws is becoming increasingly essential – not just for privacy professionals – but for everyone in our globally-networked and information-driven economy. True to its title, Determann's Field Guide is a smart, pragmatic, highly personal and often funny reference that makes short work of simplifying opaque concepts and obliterates legal jargon. In its eminently readable form, it will empower the uninitiated and deepen the understanding of the seasoned professional.'*

**Laura Hamady**

Senior Corporate Counsel, Regulatory and Privacy, Groupon Inc.,  
Chicago, USA

*'This book is a timely and welcome addition to the available literature, providing a well-structured introduction to the key facets of international data privacy compliance. The guide provides the reader with clear guidance on managing the regulatory risk associated with data privacy compliance, notably in both the EU and the US. The use of checklists and an A–Z chapter are particularly welcome, as is the solution focused approach adopted throughout the guide. I recommend this book as a useful tool for obtaining an understanding of the practical issues thrown up by international data protection compliance.'*

**Colin Rooney**

Partner, Technology Group, Arthur Cox, Dublin, Ireland

*'This is a blueprint for an enterprise-wide privacy program that will cover 99% of all situations your company might encounter worldwide. It moves beyond "what do I need to think about" to "what do I need to do". An excellent resource for anyone tasked with running a holistic privacy program, or for CEOs who are considering whether they need to implement such a program.'*

**Patrick Hagan**

JD, Privacy Consultant, San Francisco, USA

*'Recently published by Elgar, this book, in our view, is almost certain to become required reading for practitioners (on both sides of the Atlantic) involved with privacy issues. It contains a wealth of references and resources for further research and speaking of guidance, it is easy to navigate via a detailed table of contents and index at the back.'*

**Phillip Taylor MBE and Elizabeth Taylor**

*The Barrister Magazine*