Index

access
  actual access 83–4
  assumptions, underlying 130
  customers, access by 140
  distributed storage 137–8
  encryption 137–41
  intelligible access 134–42
  intervenability, and 135–6
  physical possession 103, 134–6, 149
  providers, access by 140–41
  third parties, access by 141
  authorities, by 303–4, 330
  access, compelled 304–7
  access, direct 309–13
  data location, and 311–13
  interception 309–11
  jurisdictional conflicts and problems 313–15
  Pirate Bay, avoiding authorities’ effective access 307–9
  proportionality 313
  third country access 311–13
  availability, and 103–4
  backdoors 128, 140–41, 287–8
  closed circle/ restricted access 83–4
  compelled access 304–7
  controls 26, 103–4, 263–7, 270–72, 288–9
  data location, as proxy 143–4, 323
  exclusive access 142
  indirect access 83–4
  intelligible access (see intelligible access)
  intention to provide 84–6, 120–21, 127–8
  logical access 103–4, 264, 274–5
  physical access 103, 275–6
  policy objectives 26–7

privileged user access 271
  recklessness, and 85, 120
  remote access (see remote access)
  third countries 128–9
  unauthorized access 141, 268, 275–6, 289–92, 330
  account management 271
  accountability
    approach 29, 328
    interpretation 13
    onward transfers 175
    principle 221–2
  ad hoc agreements 209–10, 230, 234
  adequate protection 40
  adequacy decisions 158–9
  blacklisting 158–9
  challenges 161–1
  comitology procedure 160–61
  consultation requirement 160–61
  essential equivalence 158, 160
  GDPR, under 159–62
  Privacy Shield 161
  Safe Harbour 46, 158–9, 162–6
  whitelisting 21, 158–9, 161–2
  assessment
    who assesses – Commission or transferor 153–4
    mechanisms 154
    risk assessment 155
    assumptions, underlying 57–8, 147–9, 325
    core WP29 principles 156–8
    content 156–7
    procedure 157–8
  data controller obligations (see data controllers)
  data recipients 61–2, 64–5, 67–8
GDPR, under 22, 67, 156–7, 159–62, 221
individual vs. sets of transfers 154–5
national law adoption 25
non-participants, of 61–2
onward transfers 185–6, 216–19, 327–8
third countries 57–60, 64–5, 154, 156–9, 185–6
adequate safeguards 60–61, 152, 157
(see also ad hoc agreements; appropriate safeguards under GDPR; binding corporate rules)
DPD, under 21–2, 187
GDPR, under 22, 187
non-compliant transfers 230–32, 234 problems 187–212
SCC(S) (standard contractual clauses), and 190–92, 197–8, 230
airspace, as data location 111, 123
algorithm security lifetime 286
Amazon xv, 174, 177, 274 (see also AWS)
anonymization, anonymous data 10–11, 57, 125–6, 233, 280, 283,
anti-FISA clause 55, 314–15
anticircumvention objective of data export restrictions
Convention 108 44–5
DPD provisions 46–56
GDPR provisions 54–5
non-EEA countries, and 46–54
OECD Guidelines 44–5
onward transfers, and 46–54
policy objectives, generally 25, 29, 102–3, 321–2
APEC
Cross Border Privacy Rules (CBPR) 39–40, 206
Privacy Framework 29, 39–40, 221–2, 262
Apple 5, 26, 40, 170, 174, 255, 293
applicable law
DPA jurisdiction, and 47–8
purpose 28
uncertainty 6, 34
appropriate safeguards under GDPR 14, 22, 60–61, 67, 152, 188–9, 196 see also adequate safeguards
GDPR codes and certifications 188–9, 210–12, 327
Asia Cloud Computing Association (ACCA) 27
assumptions underlying data protection laws
access to data 130, 134–42
encryption, and 137–41
exclusive access 142
intelligible access, and 134–42
intervenability, and 135–6
physical possession, and 103, 134–6, 142, 149
adequate protection 57–8, 147–9, 325
data location (see data location)
data protection responsibilities 130
effective jurisdiction 130, 141, 143–7, 323
export restrictions 130–31, 149–50
generally 32, 150–51
intelligible access 70, 85, 91, 101–4, 116–17, 120, 123, 125–9, 264, 267
physical access, with 137–40, 142, 316, 323–4
physical access, without 140–42
physical possession, and 134–6
jurisdiction 32, 56–7
pre-Internet 131–4
processor use 126–9, 145–7
security responsibilities 57–8
validity 134, 147, 323–5
audits
audit powers 252
audit rights 16, 157, 191, 201–2, 205, 207, 253
audit trails 116
automated auditing 273
implications 242–3
third party audits 211
Australia 25, 28, 39, 118, 135–6, 158–9, 222, 262
Austria 29, 56, 164, 166, 195, 227, 231, 233–5, 245, 274
authentication 271
Index

authorization 271, 293
authorized access see access;
unauthorized access; unauthorized use
authorized persons, definition 293
availability
access, and 103–4
breach, definition 266–7
AWS xv, 4–5, 26, 102, 107–10, 170, 177, 181, 208, 273–4, 281, 306
Azure 2, 7, 26, 99, 108–9, 211, 274, 278, 291, 296, 300 see also Microsoft
backdoors 128, 140–41, 287–8
backups 62, 105, 266, 273, 276, 289
barriers to trade 113–14
Belgium xvi, 57, 89–90, 92, 98, 116, 146, 171, 246–7, 251, 320
binding corporate rules (BCRs) 40 see also adequate safeguards
availability and applicability 207
breach of transfer mechanisms, and 230–32, 253–4
challenges of 205–6
cloud computing, and 206–8
DPA enforcement 230–32, 253–4
GDPR, and 208–9
notification obligations 231–2, 234
onward transfers 207–8
principles 205, 207
Privacy Shield, and 178
purpose 204–5
Safe Harbour principles, and 166
blacklisting 158–9
border controls 104, 323

data protection law assumptions, and 130–31, 149–50
Box 40
Brazil 70, 141, 295, 305, 306, 310, 311–12
breach of transfer mechanisms
enforcement 236–7, 253
BCRs 230–32, 253–4
data subjects complaints 237–9
DPAs, by 230, 254–5
FTC, by 255–6
non-compliant transfer trends 229–32
Privacy Shield 168
regulatory 259–60
Safe Harbour 230, 254–6
SCCs 253
breach of transfer restrictions
authorization requirements 233–4
deliberate non-compliance 234–6
enforcement 236–7
approaches 248–9
cases 245–7
data subject complaints 237–9
DPA role 240–52
ICO powers 241–2
mandatory notifications 244
non-action, reasons for 247–50, 328–9
sanctions and penalties 15, 240–44, 252
trends 247–50
US transfers, post Schrems 250–52, 331
ignorance, and 233, 237–8
reasons for 232–6, 259
Brexit 13
Bulgaria 232
business continuity 112–13
cable tapping 309–11, 330
cached personal data 106–7
Canada, OPC xviii, xix, 29, 87, 114, 140, 147–8, 158, 169, 197, 218, 222, 258, 314)
adequate protection under PIPEDA 218
data residency 281
onward transfers 218
PIPEDA xix, 38–40, 98–9, 148, 158–9, 218, 262, 281, 286, 327
Quebec 158, 218
regulatory approach 147, 222
standard contractual clauses 197
CBPR see APEC Cross Border Privacy Rules
certification  
cloud certification schemes 211  
datacentres 139  
GDPR codes and 188–9, 210–12  
Safe Harbour, trends 230  
China 26, 259  
CipherCloud 281  
Cloud Certification Schemes  
Metaframework (CCSM) 211  
cloud computing  
barriers to 6–7  
benefits and potential 5  
binding corporate rules, and 206–8  
certification schemes 211  
cloud bursting 3  
cloud co-tenants 273–4  
cloud contracts 3  
cloud models 2–3  
cloud service providers, definition 12  
codes of conduct 211–12  
community cloud  
layered cloud services 3–4, 101, 111  
service models 2–5, 105  
compliance responsibilities 102–4  
data segregation 291–2  
definition 2–3  
EEA-established providers, and  
91–2, 95–100, 190–91  
encryption, and 277–9, 285  
information security (see information security)  
Infrastructure as a Service (IaaS) 2, 105  
information cloud services 4–5  
information location 95–101, 324–5  
transportation barriers 85, 91, 101–4, 116–17, 120, 123, 125–9  
intervenability 135–6  
layered services 3–4, 101, 111, 176–7, 200–201  
logistical access risks 274–5  
outsourcing 4, 126–9  
personal data location 91–2  
physical access risks 275–6  
Platform as a Service (PaaS) 2  
Privacy Shield, and 176–7  
private cloud service 3, 8  
public cloud services 3  
regional clouds 6–7  
service models 2–5  
shared resources, challenges of 289–92  
Software as a Service (SaaS) 2  
standard contractual clauses, and 190–92, 200–204  
subcontractors/subprocessors 102–3, 111, 128–9  
supply chain risks 102–4, 123  
WP 29 99–100  
Cloud Select Industry Group (C-SIG) 211  
Codes and certifications see appropriate safeguards under GDPR  
collateral damage 140  
Community Institutions’ Data Protection Regulation (CIDPR) 35–6, 62  
compliance see also enforcement mechanisms  
need for 259–60  
notifications 230–32, 244  
standard contractual clauses 191–2  
non-compliant transfers  
adequate safeguards, and 230–32, 234  
deliberate non-compliance 234–6  
identification 231–2  
reasons for 232–6, 259  
Safe Harbour certification, and 230  
sanctions and penalties 15, 240–44, 252  
trends 226  
whitelisted countries, to 229  
obligations  
cloud computing, generally 102–4  
data recipients 61–2  
datacentres 102–4  
information security (see information security)  
intermediaries/subprocessors 102–3, 128–9
<table>
<thead>
<tr>
<th>confidentiality</th>
<th>data controller obligations 18</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>data sovereignty, and 27</td>
</tr>
<tr>
<td></td>
<td>definition 265</td>
</tr>
<tr>
<td></td>
<td>DPD provisions 265, 267–8</td>
</tr>
<tr>
<td></td>
<td>hardware seizure, and 139, 324</td>
</tr>
<tr>
<td></td>
<td>information security 265, 270–71</td>
</tr>
<tr>
<td></td>
<td>295–6, 306, 329</td>
</tr>
<tr>
<td></td>
<td>intelligible access, and 295–6</td>
</tr>
<tr>
<td></td>
<td>conflict of laws 62, 147</td>
</tr>
<tr>
<td></td>
<td>consent</td>
</tr>
<tr>
<td></td>
<td>blanket consents 202–3</td>
</tr>
<tr>
<td></td>
<td>challenges 214–15</td>
</tr>
<tr>
<td></td>
<td>derogations 213–15</td>
</tr>
<tr>
<td></td>
<td>DPD rules 213–15</td>
</tr>
<tr>
<td></td>
<td>export data, to 29</td>
</tr>
<tr>
<td></td>
<td>GDPR rules 215–16</td>
</tr>
<tr>
<td></td>
<td>informed consent 214</td>
</tr>
<tr>
<td></td>
<td>personal data processing 17–18, 122</td>
</tr>
<tr>
<td></td>
<td>repeated or structural transfers 214–16</td>
</tr>
<tr>
<td></td>
<td>contract law 110 see also standard contractual clauses</td>
</tr>
<tr>
<td></td>
<td>control of data see also access; data controllers</td>
</tr>
<tr>
<td></td>
<td>logical control 103–4, 264</td>
</tr>
<tr>
<td></td>
<td>through security 26</td>
</tr>
<tr>
<td></td>
<td>controllers see data controllers</td>
</tr>
<tr>
<td></td>
<td>cooperation, cross-border 256–8</td>
</tr>
<tr>
<td></td>
<td>Convention 108 24, 132</td>
</tr>
<tr>
<td></td>
<td>Additional Protocol 36–8</td>
</tr>
<tr>
<td></td>
<td>adoption 29, 32</td>
</tr>
<tr>
<td></td>
<td>anticircumvention objectives 44–5</td>
</tr>
<tr>
<td></td>
<td>background 24, 32</td>
</tr>
<tr>
<td></td>
<td>data controllers concept 60</td>
</tr>
<tr>
<td></td>
<td>distributed processing 50</td>
</tr>
<tr>
<td></td>
<td>harmonization 42–3, 67</td>
</tr>
<tr>
<td></td>
<td>jurisdiction 42–3, 65–6</td>
</tr>
<tr>
<td></td>
<td>limitations 34, 68, 157</td>
</tr>
<tr>
<td></td>
<td>non-participants 62</td>
</tr>
<tr>
<td></td>
<td>purpose 32–4</td>
</tr>
<tr>
<td></td>
<td>cross-border data transfers see transborder data flows</td>
</tr>
<tr>
<td></td>
<td>customers encryption by 177</td>
</tr>
<tr>
<td></td>
<td>intelligible access by 140</td>
</tr>
<tr>
<td></td>
<td>Cyprus 246</td>
</tr>
<tr>
<td></td>
<td>Czech Republic 99, 232</td>
</tr>
<tr>
<td></td>
<td>data controllers</td>
</tr>
<tr>
<td></td>
<td>adequate safeguards 60–61</td>
</tr>
<tr>
<td></td>
<td>confidentiality 18</td>
</tr>
<tr>
<td></td>
<td>data in transit, and 74–6</td>
</tr>
<tr>
<td></td>
<td>definition 12, 174</td>
</tr>
<tr>
<td></td>
<td>EEA-established providers 51</td>
</tr>
<tr>
<td></td>
<td>cloud computing 91–2, 95–100, 190–91</td>
</tr>
<tr>
<td></td>
<td>interpretation 86–9</td>
</tr>
<tr>
<td></td>
<td>jurisdiction 86–9</td>
</tr>
<tr>
<td></td>
<td>location fixation, and 91–2, 320</td>
</tr>
<tr>
<td></td>
<td>obligations 184–6</td>
</tr>
<tr>
<td></td>
<td>uploading to 86–9</td>
</tr>
<tr>
<td></td>
<td>using non-EEA servers 89–90</td>
</tr>
<tr>
<td></td>
<td>hidden processing 4–5, 9</td>
</tr>
<tr>
<td></td>
<td>limitations 186</td>
</tr>
<tr>
<td></td>
<td>obligations 13–14, 17–18, 60, 102–4, 266–7</td>
</tr>
<tr>
<td></td>
<td>compliance 102–4</td>
</tr>
<tr>
<td></td>
<td>EEA-established providers 184–6</td>
</tr>
<tr>
<td></td>
<td>information security 266–7</td>
</tr>
<tr>
<td></td>
<td>onward transfers, and 174–81, 192–3, 195–6</td>
</tr>
<tr>
<td></td>
<td>physical location vs. jurisdiction 116–17</td>
</tr>
<tr>
<td></td>
<td>policy development 60</td>
</tr>
<tr>
<td></td>
<td>third countries 51–2, 64–5</td>
</tr>
<tr>
<td></td>
<td>transfer to 64, 184–6</td>
</tr>
<tr>
<td></td>
<td>unauthorized use threats 294–5</td>
</tr>
<tr>
<td></td>
<td>data deletion</td>
</tr>
<tr>
<td></td>
<td>appropriate deletion 272</td>
</tr>
<tr>
<td></td>
<td>automatic filing systems 301</td>
</tr>
<tr>
<td></td>
<td>blocking 300–301</td>
</tr>
<tr>
<td></td>
<td>consent 202–3</td>
</tr>
<tr>
<td></td>
<td>definition 301–2</td>
</tr>
<tr>
<td></td>
<td>intelligible access, and 299–302, 324, 330</td>
</tr>
<tr>
<td></td>
<td>processing restrictions 301–2</td>
</tr>
<tr>
<td></td>
<td>remote deletion 302, 306–7, 324</td>
</tr>
<tr>
<td></td>
<td>temporary removal 301</td>
</tr>
<tr>
<td></td>
<td>unauthorized use, and 299–302</td>
</tr>
<tr>
<td></td>
<td>data fragments 137–8</td>
</tr>
<tr>
<td></td>
<td>data havens 29–30, 144</td>
</tr>
</tbody>
</table>
Data localization

costs 112
data protectionism, as 114
definition 73–4
disadvantages 112–15, 331
global trade, and 113–15
independence, and 113
need, reasons for 6–7
policy limitations 116–17
Privacy Shield, and 170, 175–6
regional locations 108–9
resilience and business continuity,
and 112–13
third countries 116–17
data location
airspace 111
assumptions, underlying 130–34
data havens 144

effective jurisdiction 143–7, 323
limitations 134
location fixation 91–2
mainframe model 131–4, 323
proxy for access 143–4, 323
audit trails 116
cloud computing
contractual commitments 110
country risk, and 92–3
extraterritorial jurisdiction 93–5
influences on 6–7
knowledge, lack of 115–16
location-centricity 7–8, 88–9,
91–2, 104, 111, 115–16,
119–20, 321–2
location fixation 91–2, 320
regional localization 108–9
service type, and 108–9
colocation risks 139–40
data sovereignty, and 26–8
datacentres 26–7, 92
hardware 26–7, 92
information security, and 316–17
infrastructure legal personality, and
96–7
intelligible access, and 7
international waters 111, 123
jurisdiction, and 34, 48, 51–3, 70, 81,
116–17, 306
conflicts 117, 147, 314–15, 319
extraterritoriality 93–5
locations outside country’s
jurisdiction 111
location-independence 113
multiple locations 65–6, 68, 70–71,
89, 93–5, 104–5, 332
cached personal data 106
data storage/processing 105–7,
109
effective jurisdiction 145–7
outer space 111, 123
physical location 28, 34, 48, 70,
116–17, 150
uploading/downloading, and 81,
86–9
verification challenges 134
websites 77
data processing
confidentiality 18
consent 17–18, 122
data controller obligations 17–18
data use, and 262
definition 11, 55
disclosure, as 92–3, 262, 267, 322
distributed processing 50
exemptions 15, 165
fair processing 17
hidden processing 4–5, 9
processor regulation 13–14
purpose limitation 17
quality and accuracy 17
sensitive data obligations 18
storage limitation 17
transparency 17
data processors
adequate protection, and 148–9
definition 174, 192
DPD obligations 13–14, 17–18,
184–5
EEA-established providers 51
cloud computing 91–2, 95–100,
190–91
interpretation 86–9
jurisdiction 86–9
location fixation, and 91–2, 320
obligations 184–6
uploading to 86–9
using non-EEA servers 89–90
Index

exemptions 15
GDPR obligations 14, 184–5, 269–70
intelligible access, by 140–41
liability 184–5
limitations 186
Privacy Shield, and 184–6
record-keeping obligations 14
Safe Harbour principles, and 184–6
security compliance obligations 302–3
subprocessors
access and availability of data 103–4
compliance responsibilities 102–3, 128–9
effective jurisdiction 145–6
group procurement, and 201–2
identification and approval 128–9
layered services 111, 176–7, 200–201
onward transfers 176–7, 180–81, 192–3
standard contractual clauses 192–3, 200–203
transfers to 184–6
unauthorized use threats 295–6
Data protection authorities
appointment 16
cross-border cooperation 256–8
drafts 34–5
evaluation 23, 76–7, 220
GDPR, comparative table of provisions 335–63
implementation 15
enforcement, transfer restriction 240–52
exemptions 47, 123
GDPR, under 252
GDPR, under Schrems
mainframe model, and 133–4, 323
non-compliance penalties 15, 240–42
non-action, reasons for 247–50, 328–9
onward transfers 184–6
personal data, definition 10–11
principles 261–3
purpose 12, 35, 54–5, 125, 261–3, 318–19
security compliance obligations 302–3
supervision requirements 16
transfer, interpretation 75–6
data protection laws, generally
country vs. recipient approaches
GDPR development 66–7
pre-DPD methods 56–7
definitions 11
disadvantages 6
enforcement trends 239–44
harmonization 15
historical development 28–9
human right, as 58
implementation challenges 239–44
national laws, categorization 29
purpose 9
sanctions and penalties 15, 240–41
data protection officers 14
data recipients
adequate protection 61–2, 64–5, 67–8
appropriate safeguards 60–61, 67, 152, 188–9
compliance obligations 61–2
definition 33, 36–8, 61, 120, 264
ejurisdiction 33, 36–8, 41, 62–6
non-participants, and 61–2, 89
third countries 62–3
data residency 27, 281
data retention principle 168, 246
data security see information security
data sovereignty 26–8, 27
data storage
data transfers, and 105
distributed storage 134, 137–8
duration 106
limitations 17
data subject rights 17–18
data trustees 296
data use, definition 262
datacentres
certification 139
compliance responsibilities 102–4
data location 26–7, 92
effective jurisdiction 145
floating datacentres 111
intelligible access 85, 91, 101–4
SCCs, and 96–7, 101
whitelisting 159
defective product liability 103
deletion see data deletion
denial of service attacks 266
derogations see also adequate protection; adequate safeguards, appropriate safeguards
anticircumvention objective 44–5
case-by-case basis 59
Convention 108 37, 43–5
DPD 213–15
GDPR 160–61, 165, 215–16
legitimate interests 216, 328
public interest restrictions 161–2, 216
self-assessment 160–61, 165
disclosure
compelled access 304–7
data processing, as 92–3, 262, 267, 322
data transfer, definition 118–20, 322
data use, and 262
government agencies, to 182–3
onward transfers, and 175–6
standard contractual clauses, and 196–7
unauthorized purposes, for 127
unintelligible data 125–6, 280
distributed storage 134, 137–8
downloading, whether transfer 77–81
Lindqvist case 82–90, 320, 322
receipt criteria 83–4
Dropbox 5, 121–2, 138, 141, 170, 174, 177, 181, 211, 277–9, 295
E-Commerce Directive 332
EDPB see European Data Protection Board
EDPS see European Data Protection Supervisors
EEA see also non-EEA countries
EEA-established providers
cloud computing 91–2, 95–100, 190–91
interpretation 86–9
jurisdiction 86–9
liability 246
location fixation, and 91–2, 320
obligations 184–6
using non-EEA servers 89–90
email encryption 278–9
traffic trends and statistics 227–8
embassies, data transfer to 73
encryption 62
access assumptions 137–41
authorization 272
backups 273, 289
certification 285–6
cloud computing, and 277–9, 285
costs 283
customers, by 177
data processor/controller obligations 277–84, 279–84
data recipients, and 282–3
data residency, and 281
data transfer, interpretation 70
decryption keys 272, 282
gateways 281–3
implementation 286–7
intelligible access, and 277–84, 330
key management 272
key residency 277
limitations 101–2, 137–8, 284–9, 326–7, 330
national security decryption resources 287–8
operation implications 283–4
perfect forward secrecy 278
personal data 282–3
physical access, and 138–9
pre-upload 141
purpose 277–9
security lifetime 286
shielded execution, and 285
strong encryption 272, 286–7
sufficient means 282
tokenization 279, 282–4, 288, 330
unencrypted data, access 138–9
enforcement see also breach of transfer mechanisms; breach of transfer restrictions
conciliatory approach 243–4
cooperation, cross-border 256–8
data protection law, generally 239–44
data subject complaints 237–9
DPA role 230, 240–55
approaches 248–9
cases 245–7
non-action, reasons for 247–50, 328–9
FTC role 255–6
ICO powers 241–2
minimum levels, need for 259–60
notification requirements 244
Privacy Shield, and 168
regulatory 259–60
Safe Harbour 230, 245–6, 257
sanctions and penalties 15, 240–44, 252
SSCs mechanisms 253
obligations 196–7
US transfers, post Schrems 250–52, 331
ENISA 211
equipment
hardware seizures 139, 324
location 47–8, 51–2, 74, 88, 123–4, 306
physical movement, as data transfer 104
essential equivalence 158, 160
Estonia 73, 113
European Data Protection Board 16, 212
European Data Protection Seal 210
European Data Protection Supervisors 16, 35–6
EuroPriSe 212
export restrictions assumptions, underlying 130–31, 149–50
extraterritoriality Microsoft warrant case 93–5, 111, 117, 295, 320, 322
transfer restrictions 14, 219
Data localization laws and policy

Facebook 2, 5, 7, 115, 164, 170, 174, 198, 240, 251–2, 255, 278, 306

fairness principle 156, 246

Federal Trade Commission (FTC) xvii, 40, 162 (see also United States)

Safe Harbour enforcement 250, 255–8

file-sharing

Pirate Bay, The 307–9

Finland 29, 254

France, CNIL xvi, 57, 96, 99–100, 123, 135–6, 160, 203, 205, 207–8, 212, 230, 231–2, 239, 249–52, 254, 258, 288, 305, 310, 313, 331

Frankenrule, restrictions as 123–4, 152, 170–74, 199, 326, 332

gateways

encryption, and 281–3
tokenization, and 282–4

General Agreement on Trade in Services 1994 (GATS) 114

General Data Protection Regulation (GDPR)

adequate protection 22, 67, 159–62, 221
comitology procedure 160–61
consolation requirement 160–61
essential equivalence 158, 160
limitations 161–2
security measures 160–61
adequate safeguards 22, 187
applicability 13
appropriate safeguards 22, 67, 187–9, 196
BCRs 208–9
codes and certifications 188–9, 210–12, 327
data processors
exemptions 15, 165
obligations 14, 184–6, 269–70
derogations 215–16
consent 213–15
legitimate interests 216, 328

DPA powers 16–17, 252

DPD, comparative table of provisions 335–63

enforcement

mandatory notifications 244
sanctions and penalties 242, 252, 269–70
evaluation 20–21, 23, 220–22
harmonization 43, 220–21
implementation 16
jurisdiction 14, 219
onward transfers 184–6, 218–19, 327–8

policy objectives 66, 129

anticircumvention 54–5
country focus 66–7

principles 22–3

purpose 12–13, 220

reform opportunities 332–3

security measures 160–61

security requirements 269–70

supervision requirements 16–17

transfer, definition 76, 119

transit, definition 76

transparency 22–3
globagination 113–15, 220


Cloud Security Scanner 274

data deletion 299
data location 96–9, 101, 108–9, 126–8

encryption 278

standard contractual clauses 202–3

unauthorized use controls 294
Index

Greece 231–2, 245

hackers 141, 292

Hague Conference on Private International Law 2010 66, 258, 315

hardware
  data location, and 26–7, 92, 306
  seizures 139, 324

harm prevention principle 262

harmonization
  Convention 108 reforms 42–3, 67
  reasons for 35, 67–8, 220–21, 223

Hewlett Packard Enterprise 40

Hong Kong xix, 26, 222

HP 40

HTTP 288

human rights 58

Hungary 172, 215, 247

IBM 5, 40, 174, 208, 268

Iceland 1, 72

identity management 270–71

Information commissioners (ICOs)
  241–2

information flow controls 288

information security
  access controls 26, 103–4, 263–7, 270–72, 288–9
  algorithm security lifetime 286
  authentication 271
  authorization 270–74, 293
    backups 273, 289
    breach 272–3
    breach notification 279–8
    cloud co-tenants 273–4
    confidentiality 270–71
    encryption 272
    availability 266–8, 270, 276, 295, 306–7, 329
    backups 62, 105, 266, 273, 276, 289
    breach detection 272–3
    breach notifications 14, 279–80, 298
    certification schemes 211–12
    cloud computing, and 273–4
    compliance obligations 302–3
  confidentiality 265, 270–71, 295–6, 306, 329
  data location, and 316–17
  deletion controls 272, 299–302
  DPD provisions 266–8
  encryption (see encryption)
  failovers 273
  GDPR provisions 269–70
  identity management 270–71
  importance 315–16
  information flow controls 288
  insider threats
    controllers 294–5
    processors 295–6
    risk mitigation 296–8
  integrity 266–8, 276, 290–91, 295, 306–7, 329
  logical security 274–5, 303, 324, 329
  logs and logging 272–3, 294, 303
  natural disasters, and 273
  obscurity, by 137
  physical security 275–6, 303, 329
  access controls 272
  Pirate Bay approach 307–9
  purpose 264–5
  recruitment challenges 289–90
  risk assessment 275–6
  risk mitigation 275–6, 306
  service level agreements (SLAs)
    270–74
  shared responsibility 127, 273–4
  transparency, by 137
  unauthorized access 141, 268, 275–6, 289–92, 330
  unauthorized use 264, 268, 292–3
  compliance obligations 292, 302–3
  controller risks 294–5
  data deletion, and 299–302
  insider threats 294–5
  processor risks 295–303
  risk mitigation 296–8, 306

infrastructure
  definition 12
  effective jurisdiction, and 145–6
  transparency, by 137
  unauthorized access 141, 268, 275–6, 289–92, 330
  unauthorized use 264, 268, 292–3
  compliance obligations 292, 302–3
  controller risks 294–5
  data deletion, and 299–302
  insider threats 294–5
  processor risks 295–303
  risk mitigation 296–8, 306

infrastructure
  definition 12
  effective jurisdiction, and 145–6
  transparency, by 137
  unauthorized access 141, 268, 275–6, 289–92, 330
  unauthorized use 264, 268, 292–3
  compliance obligations 292, 302–3
  controller risks 294–5
  data deletion, and 299–302
  insider threats 294–5
  processor risks 295–303
  risk mitigation 296–8, 306

infrastructure
  definition 12
  effective jurisdiction, and 145–6
  transparency, by 137
  unauthorized access 141, 268, 275–6, 289–92, 330
  unauthorized use 264, 268, 292–3
  compliance obligations 292, 302–3
  controller risks 294–5
  data deletion, and 299–302
  insider threats 294–5
  processor risks 295–303
  risk mitigation 296–8, 306

infrastructure
  definition 12
  effective jurisdiction, and 145–6
  transparency, by 137
  unauthorized access 141, 268, 275–6, 289–92, 330
  unauthorized use 264, 268, 292–3
  compliance obligations 292, 302–3
  controller risks 294–5
  data deletion, and 299–302
  insider threats 294–5
  processor risks 295–303
  risk mitigation 296–8, 306

infrastructure
  definition 12
  effective jurisdiction, and 145–6
  transparency, by 137
  unauthorized access 141, 268, 275–6, 289–92, 330
  unauthorized use 264, 268, 292–3
  compliance obligations 292, 302–3
  controller risks 294–5
  data deletion, and 299–302
  insider threats 294–5
  processor risks 295–303
  risk mitigation 296–8, 306
shared risks 140
Infrastructure as a Service (IaaS) models 2, 105
infrastructure cloud services
background processing 4–5
certification schemes 211
SSCs, and 200–201
integrity 27, 266, 276, 295, 306–7, 329
Privacy Shield, and 168
resource-sharing, and 290–91
intelligible access 70, 85, 91, 101–4,
116–17, 120, 123, 125–9, 142,
264, 267
assumptions, underlying 134–42,
140–42
customers, by 140
data deletion, and 299–302, 324,
330
encryption, and 277–84, 330
hackers 141, 292
intervenability, and 135–6
logical access 274–5
physical access, with 137–40, 142,
316, 323–4
physical access, without 140–42
physical possession, and 134–6
prevention 127
Privacy Shield 176
providers, by 140–41
risk mitigation 296–8, 306
third parties, by 141
unauthorized access 141, 289–92
intelligible data 304–7
interception of transmissions 46
airspace, above 111
authorities, by 309–11, 330
cable tapping 309–11, 330
satellite transmitted data 311
intermediaries 102–3
international waters, as data location
111, 123
Internet routing 74
intervenability 17–18
intra-group agreements (IGAs) 209–10
Ireland 29, 93–4, 96, 99–100, 108–9,
111, 136, 164, 169, 172, 197–8,
200, 234, 240, 251, 262, 313
ISO 27017/27018 211–12
Israel 57
Italy xvii, 52, 99, 160, 231–2, 234, 247,
303, 313
Japan 39
jurisdiction
adequate protection 64–5
anticircumvention, and 46–54
assumptions about 32, 56–7, 144
underlying data protection law
143–7
availability of 32, 56–7
cloud computing 95–100
compelled access 305–7
conflicts 28, 62, 65–6, 68, 147,
314–15
data location, and 34, 48, 51–3, 70,
81, 116–17, 306
conflicts 117, 147, 314–15, 319
location outside country’s jurisdiction 111
proxy for access, as 143–4, 323
data recipients 33, 36–8, 41, 62–6
DPAs, of 28, 47–8
EEA-established providers 86–9
effective jurisdiction 7–8, 28, 70–71,
103, 110, 123, 130, 305–6, 321,
330
assumptions, underlying 130, 141,
143–7, 323
datacentres 145–6
multiple locations 145–7
SWIFT 92–3, 146–7, 171–2
equipment location 51–2, 74, 88,
123–4
extraterritoriality 93–5, 111, 117,
295, 320, 322
GDPR transfer restrictions 14, 219
infrastructure location 95–100,
145–6, 324–5
Microsoft warrant case 93–5, 111,
117, 295, 320, 322
multiple jurisdictions 65–6, 68,
70–71, 89, 93–5, 332
multiple locations 95, 104–5, 145–6
onward transfers, and 179, 327–8
Index

physical location, and 34, 116–17, 150
standard contractual clauses 192
third countries 51–2, 64–5

Kazakhstan 25
key management 272
key residency 277

Latvia 232
layered services 3–4, 101, 111, 176–7
group procurement, and 201–2
standard contractual clauses, and 200–201
legitimate interests 216, 328
legitimate public objectives 114
Liechtenstein 1
Lindqvist case 82–90, 92, 116, 123, 320
location see data location; equipment; infrastructure
logical security 274–5, 303, 324, 329
logs and logging 272–3, 294, 303

mainframe model 131–4, 323
Malaysia 145
metadata 107, 109
Mexico 39
Microsoft warrant case
encryption 278, 285–6
Customer Lockbox 141, 285, 296
Deutsche Telekom/T-Systems
German partnership 296
Privacy Shield adoption 252
standard contractual clauses 195–6, 200–203

Microsoft warrant case xviii, 70, 93–5, 109–11, 117, 141, 295, 305, 312, 320, 322
MLAT (mutual legal assistance treaty) 93–4, 110–1, 116, 119
model clauses see standard contractual clauses (SCCs)
money laundering, Art.16 objective of fighting 304–5

national laws, generally
adequate protection 25
categorization 29
definition variations 117–18
due diligence requirement 222
onward transfer rule variations 195–6

national security
data processing restriction
exemptions 15, 165, 182–4
decryption resources 287–8
jurisdictional conflicts 314–15
Privacy Shield, and 182–4
Safe Harbour principles 182–4

Netherlands, CBP xv, 79, 83–5, 99, 118, 171–2, 211, 234, 245, 251, 258, 313
Network File System (NFS) 132–3
New Zealand 25, 28, 39, 217, 327
non-EEA countries
adequate protection 40, 61–2
anticircumvention, and 46–54
APEC Privacy Framework 39–40
due diligence requirement 222
EEA providers using non-EEA servers 89–90
non-participants 61–2, 88–9
uploading to non-EEA providers 86–9
non-participants see participants
Norway 1, 12, 97, 99–100, 106–7, 122, 128, 182, 196, 211, 228, 247, 291–2, 299–300

OECD Explanatory Memorandum 28
Data localization laws and policy

OECD Guidelines 113
2013 update 41
adoption 29–30
anticircumvention objectives 44–5
data transfer, definition 31–2
limitations 32
permitted flows 31–2
Privacy Framework 18–19
purpose 30–31
onward transfers
accountability 175
adequate protection 185–6, 216–19, 327–8
anticircumvention objectives, and 46–54
binding corporate rules, and 207–8
contracts for 177–8
disclosure, and 175–6
extensions 157
GDPR 184–6, 218–19
interpretation 85
jurisdiction, and 179, 327–8
limitations 217–19
national rule variations 195–6
Privacy Shield, and 168, 174–81
restrictions 156–7
Safe Harbour, and 174–81
standard contractual clauses, and 181, 192–3, 216–17
subprocessors, and 176–7, 180–81, 192–3
Oracle 5, 7, 166, 174
organizational approach 29
outer space, as data location 111, 123
outsourcing 246
cloud layering 3–4, 101, 111
processor use assumptions, and 126–9
shared responsibility 127
traditional models 126–9
participants
adequate protection 61–2
data recipients, and 61–2, 89
definition 37–8
non-participants 61–2, 89
personal data
cached personal data 106–7
consent, and 17–18, 122
definition 10–11
encrypted data 282–3
intervenability 17–18
metadata 107, 109
security breach notifications 14, 279–80, 298
sensitive data obligations 18
stored personal data 105
transfer trends and statistics 227–9
working personal data 105, 107
Pirate Bay, The 307–9
Poland, GIODO 232, 246
policy objectives
access 26–7
anticircumvention 25, 29, 44–56, 102–3, 321–2
data location 26–8
data sovereignty 26–8
generally 24–7, 261–3
state surveillance 26
Portugal 212, 231, 234, 310–11
Privacy Shield
adequate safeguards, and 198
amendment 169
annual reviews 168
applicability 169
background 167–8
Choice principles 177
cloud computing, and 170, 176–7
correspondence, cross-border 257
criticisms 173–5
data localization, and 170, 175–6
data retention principle 168
decision 13, 161, 167–8, 176–9, 198
disclosures vs. transfers 175–6
DPA concerns 168–9
escape clause 182–4
intelligible access 176
limitations 170, 175
national security exclusions 182–4
onward transfers 174–81
Index

participants 174
revocation 169–70
rights and obligations 168
Safe Harbour, differences from 167–9, 173–81
self-assessment 168
standard contractual clauses, and 22, 199–200
transfer contracts 177–8
transfers to processors 184–6
private cloud services 3, 8
privileged user access 271
processing see data processing
processors see data processors
proportionality 17
providers, definition 12
proxy formulation 143–4, 323
pseudonymous data 282
public cloud services 3
public interest restrictions 161–2, 216
push vs. pull transfers 76, 78–81, 120
Quebec see Canada
recklessness 85, 120
regional clouds 6–7
remedies
data subject complaints 237–9
remote access 52–3, 70, 72, 103, 126–7, 321, 324
backdoors 128, 140–41
remote deletion 302, 306–7
threats from 139, 324–5, 329
responsibility, shared 127, 273–4
risk assessment
colocation risks 139–40
country risk 92–3
logical access 275, 329
physical access 276, 329
remote access 139, 324–5, 329
risky transfers, definition 155
risk mitigation
logical access 275
national security surveillance/decryption 287–8
physical access 276
unauthorized use 296–8, 306, 329
Russian Federation 26, 39, 42, 68, 113, 228, 311, 313
Safe Harbour decision
Frankenrule, as 171–4, 326
generally 97, 159
SCCs, and 96–7, 166, 197–8
Schrems case 46, 158–9, 162–6, 169, 183, 189–90, 192, 197–8, 250–52, 331
Safe Harbour principles
authorizations and notifications 163
background 162–3
benefits and limitations 98–9
certification trends 230
cloud computing, and 170
coordination, cross-border 257
criticisms 163, 171–4, 180, 325, 326
DPA enforcement 230
breach of transfer mechanism 254–6
breach of transfer restriction 230, 245–6
post-Schrems 250–52, 331
trends 254–5
escape clause 182–4
FTC enforcement 255–6
invalidation 46, 158–9, 162–6
national security exclusions 182–4
obligations 97–8
onward transfers 174–81
permissible transfers 96–7
Privacy Shield, differences from 167–9, 173–81
transfers to processors 184–6
safeguards see adequate safeguards; appropriate safeguards; specific safeguards
Salesforce 2, 5, 7, 115, 166, 200, 208, 271, 281, 293
sanctions
breach of transfer restrictions, for 15, 240–44
fines 16–17
GDPR 242, 252, 269–70
suspension 16
Schrems case 46, 158–9, 162–6, 169, 183, 189–90, 192, 197–8, 250–52, 331
security see information security
self-assessment 153–5, 327–8
abolition 153, 160–61, 165
Privacy Shield, under 168
sensitive data 18
service level agreements (SLAs) 270–74
shadow cloud models 3, 115
shared resources
integrity, and 290–91
Pirate Bay, The 307–9
unauthorized intelligible access 289–92
shielded execution 285
Singapore xiv, 26–7, 40, 75–6, 262–3, 283, 291–2
Slovakia 232
Slovenia 86, 99–100, 232, 247
SMTP Strict Transport Security (STS) standard 279
Software as a Service (SaaS) models 2, 200–201
South Africa 25
South America 25 see also Brazil
Spain, AEPD xv, 9, 47, 52, 57, 88, 99–100, 143, 146, 215, 230–31, 245–6, 251, 253, 310, 313
specific safeguards 61–2
standard contractual clauses (SCCs)
adequate safeguards, and 190–92, 197–8, 230
advance controller consent 202–3
amendment 198
audit rights 16, 157, 191, 201–2, 205, 207, 253
authorized transfer 231–2
availability and applicability 192–5, 198–200
background 190–92
bipartite vs. multipartite arrangements 192–5
blanket consents 202–3
challenges of 181, 194–6, 204
cloud computing, and 190–92, 200–204
compliance mechanisms 191–2
datacentres, with 96–7, 101–3
enforcement 196–7, 253
group procurement 201–2
infrastructure legal personality, and 96–7
jurisdiction 192
limitations 196–200, 203–4, 325–6
national procedural variations 195–6
need for 102–3, 199
obligations
disclosure 196–7
importer-processors, of 191–2
notification 204, 231–2
onward transfers, and 181, 192–3, 216–17
opt-ins 200–201
Privacy Shield, and 199–200
Safe Harbour decisions 96–7, 166, 197–8
subprocessors 192–3, 200–201
use trends 233–4
validity 192, 198–200
state responsibilities
adequate protection 147–9
assumptions 147–9
subprocessors
access and availability of data 103–4
compliance responsibilities 102–3, 128–9
definition 192
effective jurisdiction 145–6
group procurement, and 201–2
identification and approval 128–9
layered services 111, 176–7, 200–201
onward transfers 176–7, 180–81, 192–3
standard contractual clauses 192–3, 200–203
transfer restrictions 22
Index

surveillance 165, 183–4, 288, 317, 330
  bulk / mass 183–4, 288, 317, 330
  cable tapping 309–11, 330
  national security decryption resources 287–8
  national security exemption 15, 165, 182–4
  policy objectives 26
  Privacy Shield 182–4
  Safe Harbour principles 182–4
  effective jurisdiction 92–3, 146–7
  effective jurisdiction 92–3, 146–7
  Switzerland 113, 118, 217, 228, 251, 254
  technology neutrality 60, 181, 268
  data deletion 301–2, 324
  jurisdiction, and 65, 321
  temporary data movement 48, 50–51
  temporary data removal/ deletion 301
  third countries
  adequate protection 57–9, 57–60, 64–5, 154, 156–9, 185–6
  authorities, data access by 311–13, 330
  comity, and 51–2
  data localization 116–17
  data location 48
  data recipients 62–3
  data security 150
  data subject complaints 238–9
  data transfer to
    embassies 73
    trends 228–9
  encryption 150
  enforcement of breaches 238–9
  intelligible access 128–9
  intention to provide access 84–6, 120–21
  jurisdiction 51–2, 64–5

subprocessors/ intermediaries
  compliance obligations 103–4, 128–9
  uploading/ downloading 78–81
  Lindqvist case 82–90, 320
  to non-EEA provider 86–9
  webhosting 78–81
  whitelisting 21, 158, 161–2
  third parties
    beneficiary rights 191
    definition 174
  TJX 286
  tokenization 279, 282–4, 288, 330
  Trade in Services Agreement (TISA) (draft) 113–14
  trade statistics
    data transfer trends 227–9, 235
    information availability 230–32
  Transatlantic Trade and Investment Partnership (TTIP) 114
  transborder data flows
    data subject complaints 238–9
    definition 11–12, 31–2, 41, 63
    trends 227–9, 235
    volume, challenges of 235–6
  transfer mechanisms see also Privacy Shield; Safe Harbour
    additional measures 326
    adequate protection 153–62
    breach (see also breach of transfer mechanisms)
    derogations (see derogations)
    ex ante controls 224–5
    generally 222–3, 325–6
    harmonization 223–5
    limitations 152–4, 222–5, 235–6, 326–7
    transfer restrictions
      anticircumvention, and 44–56, 321–2

also see
  Trade in Services Agreement; Transatlantic Trade and Investment Partnership
  Trade in Services Agreement (TISA) (draft) 113–14
  trade statistics
    data transfer trends 227–9, 235
    information availability 230–32
  Transatlantic Trade and Investment Partnership (TTIP) 114
  transborder data flows
    data subject complaints 238–9
    definition 11–12, 31–2, 41, 63
    trends 227–9, 235
    volume, challenges of 235–6
  transfer mechanisms see also Privacy Shield; Safe Harbour
    additional measures 326
    adequate protection 153–62
    breach (see also breach of transfer mechanisms)
    derogations (see derogations)
    ex ante controls 224–5
    generally 222–3, 325–6
    harmonization 223–5
    limitations 152–4, 222–5, 235–6, 326–7
    transfer restrictions
      anticircumvention, and 44–56, 321–2

also see
  Trade in Services Agreement; Transatlantic Trade and Investment Partnership
  Trade in Services Agreement (TISA) (draft) 113–14
  trade statistics
    data transfer trends 227–9, 235
    information availability 230–32
  Transatlantic Trade and Investment Partnership (TTIP) 114
  transborder data flows
    data subject complaints 238–9
    definition 11–12, 31–2, 41, 63
    trends 227–9, 235
    volume, challenges of 235–6
  transfer mechanisms see also Privacy Shield; Safe Harbour
    additional measures 326
    adequate protection 153–62
    breach (see also breach of transfer mechanisms)
    derogations (see derogations)
    ex ante controls 224–5
    generally 222–3, 325–6
    harmonization 223–5
    limitations 152–4, 222–5, 235–6, 326–7
    transfer restrictions
      anticircumvention, and 44–56, 321–2

also see
  Trade in Services Agreement; Transatlantic Trade and Investment Partnership
  Trade in Services Agreement (TISA) (draft) 113–14
  trade statistics
    data transfer trends 227–9, 235
    information availability 230–32
  Transatlantic Trade and Investment Partnership (TTIP) 114
  transborder data flows
    data subject complaints 238–9
    definition 11–12, 31–2, 41, 63
    trends 227–9, 235
    volume, challenges of 235–6
  transfer mechanisms see also Privacy Shield; Safe Harbour
    additional measures 326
    adequate protection 153–62
    breach (see also breach of transfer mechanisms)
    derogations (see derogations)
    ex ante controls 224–5
    generally 222–3, 325–6
    harmonization 223–5
    limitations 152–4, 222–5, 235–6, 326–7
    transfer restrictions
      anticircumvention, and 44–56, 321–2

also see
  Trade in Services Agreement; Transatlantic Trade and Investment Partnership
  Trade in Services Agreement (TISA) (draft) 113–14
  trade statistics
    data transfer trends 227–9, 235
    information availability 230–32
  Transatlantic Trade and Investment Partnership (TTIP) 114
  transborder data flows
    data subject complaints 238–9
    definition 11–12, 31–2, 41, 63
    trends 227–9, 235
    volume, challenges of 235–6
  transfer mechanisms see also Privacy Shield; Safe Harbour
    additional measures 326
    adequate protection 153–62
    breach (see also breach of transfer mechanisms)
    derogations (see derogations)
    ex ante controls 224–5
    generally 222–3, 325–6
    harmonization 223–5
    limitations 152–4, 222–5, 235–6, 326–7
    transfer restrictions
      anticircumvention, and 44–56, 321–2

also see
  Trade in Services Agreement; Transatlantic Trade and Investment Partnership
  Trade in Services Agreement (TISA) (draft) 113–14
  trade statistics
    data transfer trends 227–9, 235
    information availability 230–32
  Transatlantic Trade and Investment Partnership (TTIP) 114
  transborder data flows
    data subject complaints 238–9
    definition 11–12, 31–2, 41, 63
    trends 227–9, 235
    volume, challenges of 235–6
  transfer mechanisms see also Privacy Shield; Safe Harbour
    additional measures 326
    adequate protection 153–62
    breach (see also breach of transfer mechanisms)
    derogations (see derogations)
    ex ante controls 224–5
    generally 222–3, 325–6
    harmonization 223–5
    limitations 152–4, 222–5, 235–6, 326–7
    transfer restrictions
      anticircumvention, and 44–56, 321–2
appropriate safeguards 14, 22, 60–61, 67, 152, 188–9, 196, 327
border controls, and 104, 130–31, 149–50
breach (see breach of transfer restrictions)
data localization, and 6–7
EEA controller interpretation 1
effective jurisdiction 7–8, 28, 70–71, 103, 110, 123, 321, 330
assumptions, underlying 130, 141, 143–7, 323
extraterritorial reach 14
Frankenrule, as 123–4, 152, 170–74, 199, 326, 332
limitations 7–8, 223–5
location centricity 7–8, 88–9, 91–2, 104, 119–20, 321–2
need for 120–22, 325
purpose 8, 54–6, 172
qualifying transfers 14
subproviders, use of 22
temporary movement 48, 50–51
transfers, generally see also onward transfers
actual access 83–4
asymmetric treatment by size and frequency 216
authorization
no need for 233–4
notification 230–32, 244
data processing, as 19
definition 11–12, 31–2, 76, 117, 119, 320
disclosure, and 118–20, 322
national variations 117–18
disclosure, and 73, 118–20, 322
duration of storage/processing 106
encryption, and 70
equipment location 47–8, 51–2, 74, 88, 123–4
guarantee clauses 114
historical evolution 227–8
trends and statistics 227–9
ubiquity 227–9
interpretation 69, 71–4, 322
closed/restricted access 83–4
communication, and 72–3, 85–6
data manipulation requirement 75
data movement 71–2
directed communications 85–6
examples 71–2
intention to transfer 72, 84–6, 120–21, 127–8
Lindqvist case 69, 78–90, 116, 123, 320, 322
physical transportation 70–72
remote access, and 72, 321, 324
transfer types 73
transfer vs. transmission 75
transit 45, 74–6, 122, 322
uploading/downloading 69, 78–90, 116, 123, 320, 322
via Internet 72, 74
joint responsibility for 85
non-compliant transfer trends 226, 229
purpose 325
push vs. pull 76, 78–81, 120
qualifying transfers 14
receipt criteria 83–4
suspension powers 16–17
uploading/downloading 77–81
judicial interpretation 82–90, 320, 322
transit
definition 45, 74–6, 122, 322
exclusions 74–6
privacy implications 75–6
transparency 17, 156
Turkey 228
Twitter 5, 174, 278, 306
unauthorized access 141, 268, 275–6, 289–92, 330
unauthorized use 264, 268, 292–3
compliance obligations 292, 302–3
controller risks 294–5
data deletion, and 299–302
insider threats 294–5
processor risks 295–303
risk mitigation 296–8, 306
unintelligible data 125–6, 280
Index 447


Electronic Communications Privacy Act 1986 94

enforcement penalties 243

Fair Information Practice Principles 19

Federal Information Processing Standards (FIPS 199) 265–6


Federal Information Security Modernization Act 2014 266

Foreign Intelligence Surveillance Act 1978 (FISA) 55, 119, 314–15

Federal Trade Commission (FTC) xvii, 40, 162

Safe Harbour enforcement 250, 255–8

Freedom Act 2015 117

International Communications Privacy Act 2016 (ICPA) 94

International Traffic In Arms Regulations (ITAR) 282

Law Enforcement Access to Data Stored Abroad Act 2015 (LEADS Act) 94

PATRIOT Act 2001 117, 141, 182–3, 320

rule of law 117

whitelisting 159, 162

uploading, whether transfer 77–81

Lindqvist case 82–90, 320, 322
to non-EEA provider 86–9

receipt criteria 83–4

verification 271

virtual data embassies 73

virtual machines 105–7

Webex 5

webhosting/ website publication

data access 77

data location 77

data storage functions 77

data transfer restriction implications 77–8

DPD limitations 76–7

Lindqvist case 69, 78–90, 320

Principles, applicability 120–22

push vs. pull transfers 76–81, 120

self-hosting 77

status, processors vs. controllers 88

uploading/downloading 77–81

judicial interpretation 82–90, 320
to non-EEA provider 86–9

whitelisting
datacentres 159

decisions 21, 158–9, 161
grandfathering 161

non-compliant transfers 229

US 162

Workday 40, 174

Working Party 12 (WP12)
core principles 157–8

Working Party 29 (WP29)

adequacy decisions 158–9, 162–6

adequate protection 154–7

adequate safeguards 187–8

availability 266

BCR checklists 40
cloud certification schemes 211
<table>
<thead>
<tr>
<th>confidentiality 265</th>
<th>Privacy Shield 168–9</th>
</tr>
</thead>
<tbody>
<tr>
<td>cooperation, cross-border 257</td>
<td>procedural mechanisms 157–8</td>
</tr>
<tr>
<td>functions 16</td>
<td>reform proposals 331</td>
</tr>
<tr>
<td>individual vs. sets of transfers 154–5</td>
<td>Safe Harbour reforms 163–5, 180</td>
</tr>
<tr>
<td>integrity 266</td>
<td>working personal data 105, 107</td>
</tr>
<tr>
<td>jurisdiction, importance of 64</td>
<td></td>
</tr>
<tr>
<td>onward transfers 156–7, 216–19</td>
<td>Yahoo 310–11</td>
</tr>
</tbody>
</table>