Index

Page numbers followed by f refer to figures.

A
Access, right of, 201–203
and FB privacy policy, 400
and government use of data, 294–295, 297f
in Privacy Shield, 170
Accountability, 61–62
for big data operations, 158
early digital privacy laws on, 27
information on, 197–198
in Privacy Shield, 170
at technology firms, 385f
Accreditation, certification body, 110–111
Accuracy, data, 130, 204
Adequacy decisions, 162–166
Adherence, for Controller, 64
Adhesion contracts, 261
Administrative agreements, 176
Administrative fines, 275–279
Adult Friend Finder, 446
Advisory duties and powers, of SA, 246, 250
Affiliates, 328
Aggregation, 90
Alternate dispute resolution (ADR), 171, 258–265, 264f–265f
Amazon, 381f–385f
Ancestry.com, 455–456
Anonymization, 50, 89, 91
Anthem, 432–433
Antitrust regulations, German, 393–394
Apple Health, 450
Application security, 101
Appropriation, 25
Arbitration, 259–260, 262
Archiving activities, 156–157, 213, 223, 304–305
Arrest warrants, 40
Ashley Madison, 435–436
Associations, 108–109, 154
Audience identification, 349
Australian Department of Immigration, 432
Authenticity, of content, 366–367
Authority, exercising, 145–146
Authorization, 115, 175–177, 250
Automated cyber-security, 102
Automated decision making, 221–226
Availability breach, 95

B
Bank of Montreal (BMO), 463
Banner Health, 438–439
Bargaining mechanism, 141–142
Behavioral data, 150, 151
Betriebsrat (Works Council), 312–313
Big data operations, 75, 157–158
Big processing, 127
Binding corporate rules, 172–175, 173f–175f
Biometric data, 152
Blanket data policy, 325
Blockchain technology, 91–92
Blue Cross, 430–431
Blurring, 91
Bots, 49
Brand protection, 360–361
Breach Level Index (BLI), 97–99
Breach response plan, 101
British Airways, 431–432, 457
Budget independence, 243
Budgeting, for GDPR Compliance Team, 322–323
 Bundling of privacy policies, 138–139, 342
 Burden of proof, 143
 Business, risk to, 70
 Business competition, 218–219
 Business model, Facebook’s, 341
 Business plan, SA’s oversight of, 78–80

C
Cambridge Analytica scandal, 39
Castle privacy framework, 23–24
Censorship, 208, 371–372
Certification(s), 110–112
adherence to, 64
for data protection by design, 91
for GDPR Compliance Department, 331
mechanisms for, 111–112
purpose of, 107
Certification bodies, 110–111
Children:
consent given by, 134–135
information directed at, 28
Choice of law, 168, 261–262
Cloud computing, 158–159
Cloud security, 101
Coastal Credit Union, 449–450
Code of ethics, 378
Codes of conduct, 64, 107–109, 299, 338–339
Collective bargaining agreements (CBAs), 311–312
Comité d’entreprise (Works Council), 313
Commercial (economic) value, of individual data, 7, 27–31
Commonwealth of Nations, individual privacy in, 25–26
Community Health Systems, 424–425
Community payment terms, 338
Community Standards, 338, 361–369, 374–375
Community terms, 338
Compatibility test, 128–129, 148–149
Compensation for data subjects, 273–275
Competence of Supervisory Authorities, 244–246
Completeness, data, 204
Complicated information, 136
Conciliation, 259
Conditional consent, 133–134, 140, 141
Conduit (data handler), 54
Confidentiality:
in alternate dispute resolution, 262, 264
for data protection officer, 82
of processing operation, 131–132
for Processor, 114–115
revamping procedures on, 329
Confidentiality breaches, 95
Conflicts of interest, 83–84
Consent:
from children, 134–135
conditional, 133–134, 140, 141
defined, 132–134
explicit, 152–153, 166
freely given, 133–134, 140–141
hidden, 139–140
illusory, 140–142
for international data transfers, 166
for internet of things, 159–160
NYOB.eu case examples, 135–144
obtaining, with GDPR Team, 331
online, 140–141
processing based on, 132–144
withdrawal of, 133
Consequences, in compatibility test, 128, 129, 149
Consistency, 250–252, 263
Consumer assessments, 147
Consumers, risk to, 70–71
Content:
Community Standards on, 361–369
responsibility for, 359–360
Content moderation, 359–372
process for, 369–370
reasons for, 360–361
“Supreme Court” for, 370
Content removal requests, 368–370
Context of data collection, 128, 129, 148
Contracts:
clauses on international data transfers, 166–169, 176
data protection obligations in, 324–325
employment, 311
processing, 113–114
processing for formation/performance of, 144–145
Controller(s), 158
allocating liability to, 65–68, 271–273
in cloud computing, 158
communication of breach to data subjects by, 106–107
Controller-to-Controller SCC, 167
cooperation with SA for, 68–69
defined, 52
duties after personal data breach, 103–107
information and transparency obligations for, 194–197, 234–235
joint, 65–68, 147, 158
judicial action against, 253–254
notification by, 103–106
organizational requirements for, 62–69
outside of European Union, 67–68, 180–182, 297
relationship of Processor and, 112–113
responsibilities of, 63–64
selection of Processor by, 113–114
suits against data subjects by, 256–257
technical and organizational measures for, 69–73
territorial scope for, 55
Cooperation:
of Controllers with SAs, 68–69
of Facebook with regimes, 371
international, 183–184
between SAs, 247, 250–252
Coordinated attacks, 96
Corporate structure, 173f
Corporations, data for, 48–49
Corrective powers of SA, 249–250
Costs, of alternate dispute resolution, 263
Court of Justice of European Union (CJEU), 266
Cox Communications, 449
Criminal behavior or conviction data, 151–152, 292–293, 362–363
CrowdTangle, 337
Customization, 341, 399–400
CVS (Canada), data breach, 436–437
Cybercrime, 100
Cyber-espionage, 99
Cyberlibertarians, 12
Cyber-security, 99–103
Cyber-terrorism, 99
Cyber-warfare, 99

Data format, 217–218
Data handler (conduit), 54
Data importers, 167
Data mapping, 86
Data minimization, 86–87, 130–131
Data portability, right to, 216–220
business competition and, 218–219
and data format, 217–218
and FB privacy policy, 401
and government use, 295, 297f
intellectual property issues with, 219–220
restrictions on, 220
Data privacy:
defined, 5–6
doctrine of information privacy, 6–9
as extension of individual privacy, 37–39
future of, 407–412
in GDPR, 18–19
notice-and-choice model, 9–12
privacy-as-trust model, 9, 13–16
privacy practices at Facebook, 335–336
questions and challenges of, 2–3
with social robots, 16–18
and voluntary information, 3–4
Data processing, see Processing
Data Processor, see Processor
Data protection (data security):
determining needed level of, 86
Facebook settings for, 399–400
as fiduciary obligation, 355–356
hierarchy, 87f
implementing measures for, 90–91
maintaining level of, 69–71
safeguards for, 27
selecting measures for, 87–90
setting policies on, 64
Data protection and security requirement:
for big data operations, 157–158
in compatibility test, 128, 129, 149
for employee data, 309–313
at Facebook, 355–359
for international data transfers, 323–324
for internet of things, 160
and Privacy Shield, 170
during processing, 92–94, 93f, 328–329
technology firms’ compliance with, 384f
for telemadia, 302–303
Data protection by design (privacy by design), 84–92
applying principles of, 86–91
balancing amount of protection in, 85–86
and blockchain technology, 91–92
Index

Data protection by design (Continued)
- at Facebook, 398
- protection at outset, 84–85

Data protection impact assessments (DPIAs), 73–80
- and business plan oversight by SAs, 78–80
- at Facebook, 403–404
- general impact assessments vs., 297–298
- processing requiring, 74–75
- scope of, 75–78

Data protection management systems (DPMS), 94

Data protection officers (DPOs), 80–84
- appointment of, 319
- conflicts of interest for, 83–84
- defined, 53
- designation of, 80
- in DPIAs, 76–77
- liability of, 84
- and public interest rule, 298–299
- qualifications of, 81
- tasks of, 82–83

Data quality, 27

Data resources, of Facebook, 343

Data security, see Data protection

Data sharing:
- empowerment with, 6
- at Facebook, 353–354
- within FB Group, 337–338
- with social media services, 341
- at technology firms, 383f

Data subjects. See also Remedies for data subjects
- communicating breach to, 106–107
- Controller suits against, 256–257
- defined, 53
- DPO’s relationship with, 82
- incapacitated, 153–154
- providing information to, 195–196, 235
- representation for, 240–241
- as third-party beneficiaries, 168

Data subjects’ rights, 193–232. See also specific rights by name
- and automated decision making, 221–226
- as “digital Miranda” rights, 197–201
- and duty of transparency, 194–197
- and Facebook, 400–401
- legally mandated clauses on, 173f
- and processing in public interest, 294–297
- restrictions on, 226–228
- technology firms’ compliance with, 383f

Data transfers:
- international, see International data transfers
- intragroup, 147, 182–183
- Deceased individuals, 49
- Decision making, automated, 221–226
- Deloitte, 455
- Democratic National Committee, 448
- Denial of service attacks, 96
- Department of Homeland Security, 447–448
- Derogations, international data transfer, 177–179
- Destruction of data, 95
- Detriment, for declining service, 140, 141
- Developer payment terms, 338
- Differential privacy, 90
- Digital businesses, value of individual data for, 29–31
- Digital campaigning, 377
- Digital devices, 408–412
- Digital literacy, 378
- “Digital Miranda” rights, 197–201
- Digital public spaces, 7–8
- Digital rights activism, 241
- Digital service providers, 71–72, 301–302
- Digital services tax levy, 377
- Direct marketing, 147, 222–223, 347, 349–352
- Directory replacement, 91
- Disclosures, 200, 301–304
- Disinformation, 372–374, 378. See also “Fake” news
  “Disinformation and ‘Fake News’” (UK
  House of Commons), 372, 375–379
- Dispute resolution, 168, 239–240. See also
  Alternate dispute resolution (ADR)
- Distinguishability, 133, 139
- Doctrine of information privacy, 6–9
- Documented instructions for Processors, 114
- Domestic law:
  - compliance with, 323–324
  - in conflict with GDPR, 184–185
  - temporary injunctions under, 279–280
- Domestic representatives, 67–68
- Domino’s, 424
- Drivers licenses, 28
- Dunn & Bradstreet, 422–423

Ebay, 416–417
Economic (commercial) value, of individual data, 7, 27–31
Electronic breaches, 96
Eli Lilly and Company, 11
Employee data, 153, 309–313
Employment agreements, 311–312
Empowerment, 6, 410–412
Encrypted data:
  creating, 85, 89–90
  governmental use of, 308–309
Endorsements, 354–355, 398–399
Enforceability, of arbitral reward, 262
Equifax, 454–455
Erasure, right of, 205–214
  definition of erasure, 212
  development of, 205–206
  exceptions to, 212–214
  and FB privacy policy, 400
GDPR on circumstances for, 209–211
  and government use, 294–295, 297f
for personal data made public, 211–212
  resolving disputes related to, 206–209
EU Commission decisions, on international
data transfers, 166–167
EU Data Protection Authority (DPA), 171
EU Data Protection Board (DPB), 251, 252
EU Injunction Directive, 280–281
Europe, history of individual privacy in,
25–26
European Central Bank, 423–424
European Union (EU):
  Controllers outside, 67–68, 180–182, 297
  cooperation obligation in, 182–184
  EU–US Privacy Shield, 169–172
  GDPR for entities with physical presence
  in, 54–55
  GDPR for users based in, 56
  history of individual privacy in, 33–36
  international cooperation by bodies in,
  183–184
  international data transfers not authorized
  by, 179
  legislation on governmental data use by
  members of, 287–291
Excellus, 430
Exempted activities, GDPR, 51–52
Experian, 429–430
Explanation, right to, 223–224, 296, 297f
Explicit consent, 152–153, 166
Exporters, data, 167
Expression, freedom of, 26, 34–35, 306–308
External industry operators, on GDPR Team,
326–327
Eyewire, 446–447

F
Facebook, 335–405
  advertising and direct marketing at,
  346–352
  business model of, 341
  censorship of livestreaming services,
  371–372
  “code of conduct” policies at, 338–339
  consent complaint against, 135–144
  content moderation at, 359–372
  cooperation with regimes, 371
  customized data protection settings,
  399–400
  data abuse charges against, 336–337,
  402–403
  data breaches at, 356–358, 459–460
  data protection at, 355–359
  data sharing at, 337–338, 353–354
  and data subjects’ rights, 400–401
  disinformation and fake news on, 372–380
  fulfillment of information obligations,
  394–395
  GDPR for future projects at, 403–404
  GDPR violations by, 336
  German antitrust regulations, 393–394
  Lead Supervisory Authority at, 393
  mission of, 339–340
  notifications at, 352–353
  personal data collection mechanisms at,
  344–346
  privacy-as-trust model and, 15–16
  privacy by design at, 398
  privacy policies of, 342–343, 381f–385f
  privacy practices at, 335–336
  probable future investigations of, 402–403
  processing for legitimate corporate
  interests, 396–398
  processing for philanthropic purposes by,
  343–344
  public endorsement of personalized
  shopping on, 398–399
  purpose limitation obligation for, 395–396
  subsidiary companies of, 337
  uncompensated endorsement at, 354–355
  use of GDPR loophole at, 401–402
Facebook Payments Inc., 337
Facilitation of processing, 183
Fair processing, 126
  Fake profiles, 49
False light and publicity, 25
False news policy, Facebook, 374–375
FB brand resources, 338
FB Content Moderation Appeals Court, 370
FB Group:
ads based on data from partners in, 350
advertisers’ data collection from, 347–348
data protection and expansion of services by, 359
data sharing within, 337–338
German antitrust violations, 393–394
subsidies in, 337
FB platform policy, 338
Fees, for copies of personal data, 202–203
Fiduciary obligation, data protection as, 355–356
Fines, administrative, 275–279
Foreign laws in conflict with GDPR, 184–185
Forum selection clauses, 265–266
France, employee data protection in, 313
Freedom:
of expression, 26, 34–35, 306–308
of information, 306–308
of speech, 26, 34–35, 207
Freely given consent, 133–134, 140–141
Fruit of the poisonous tree doctrine, 40
Full compensation, 273–274

G
Gaming profiles, 49
GDPR Compliance Department (GDPR Team), 313–319
bringing affiliates into compliance, 328
bringing Processor partners into compliance, 327–328
budgeting for, 322–323
conducting internal data audit, 321–322
employee training by, 330
ensuring security of processing, 328–329
establishing human capital for, 326–327
establishing point person for compliance, 319–321
identifying level of compliance needed, 323–325
obtaining certification for, 331
providing oversight for, 325–326
record keeping by, 329–330
revamping confidentiality procedures, 329
setting privacy policies and getting user consent, 331
worst-case scenario planning, 331–332
GDPR-compliance enforcement, 233–270
alternate dispute resolution for, 258–265
and challenging existing GDPR provisions, 266
and data subject representation, 240–241
forum selection clauses for, 265–266
in-house mechanisms, 233–240
judicial remedies, 253–258
by Supervisory Authorities, 241–253
GDPR scope of application, 45–59
and exempted activities, 51–52
for instruments of public international law, 57
“personal data” definition, 47–51
“processing” definition, 46–47
and stakeholder types, 52–54
territorial scope, 54–57

General Data Protection Regulation (GDPR):
about, 18–19
on alternate dispute resolution, 260
and blockchain technology, 91–92
challenging existing provisions of, 266
on circumstances for erasure, 209–211
Facebook’s use of loophole in, 401–402
foreign law in conflict with, 184–185
for future projects at Facebook, 403–404
identifying needed level of compliance with, 323–325
legally mandated clauses on compliance with, 173f
opening clauses of, 288–289, 289f–290f, 310–311
violations of, by Facebook, 336
General impact assessments, 297–298
Generalization, 49, 89
Genetic data, 152
Germany, 25–26, 312–313, 393–394
Global Status Quo, on adequacy determinations, 164, 164f–165f
Google, 135–144
Google+, 458–459
Google Spain v. Costeja, 205–209
Governmental regimes, Facebook’s cooperation with, 371
Governmental use of data, 287–317
archiving activities, 304–305
disclosure of public documents and data, 301–304
employee data protection, 309–313
encrypted data, 308–309
and freedom of information and expression, 306–308
handling government subpoenas, 305
member state legislations on, 287–291
processing in the “public interest,” 291–300
public interest restrictions on GDPR, 305–306
Government subpoenas, 305
Gramm-Leach-Bliley Act (GLB Act), 28–29
Granularity, of services provided, 138–141
Grave infringements, 276
Guarantees, sufficient, 113
Gyft, 445

H
Hash function pseudonymizing, 90
Health insurance information, 28
Heathrow Airport, 453–454
Hidden advertisements, 351–352
Hidden consent, 139–140
Hilton Hotels, 429
Home Depot, 418
Human capital, for GDPR Team, 326–327
Human resources (HR) department, 320–321
Hyatt Hotels, 428

I
Identifiability, of personal data, 47–49
Identification, processing that does not require, 129–130
Illusory consent, 140–142
Importers, data, 167
Incapacitated data subjects, 153–154
Independence, 82, 243
Individual compliance, for entities in conglomerates, 182–183
Individual data, commercial value of, 27–31
Individual participation, 27
Individual privacy, 23–43
Cambridge Analytica scandal, 39
castle framework, 23–24
data privacy as extension of, 37–39
in digital age, 26–28
and economic value of data for businesses, 29–31
in Europe and Commonwealth, 25–26
in European Union, 33–36
Gramm-Leach-Bliley Act, 28–29
impending threats to, 37
in law enforcement context, 39–41
monetary value of, 7
tort law formation, 24–25
US legislative initiatives on, 31–32
Information:
facilitating requests for, 195
freedom of, 306–308
right to, 207–208, 306–308
voluntary, 3–4
Information and transparency requirements:
for Controller, 194–197
and digital Miranda rights, 197–201
Facebook’s fulfillment of, 394–395
and in-house enforcement, 234–235
technology firms’ compliance with, 381f
Information privacy, doctrine of, 6–9
Information technology (IT) department, 320
In-house employees, on GDPR Team, 326
In-house GDPR enforcement mechanisms, 233–240
implementing, 235–240
and information/transparency obligations, 234–235
at Privacy Shield Companies, 171
Injunctions, 279–282, 282f
Instagram, 135–144
Insurance, cyber-security, 102–103
Integrity, 131–132, 147, 366–367
Integrity breaches, 96
Intellectual property rights, 219–220, 367–368
Intermediary liability, 51
Internal data audit, 321–322
Internal responsibilities of SA, 248
Internal Revenue Service (IRS), 434
International agreements, 163
International company, 159
International data transfers, 161–182
adequacy decisions and “safe” countries, 162–166
binding corporate rules for, 172–175
data protection standards for, 323–324
derogations, 177–179
and EU–US Privacy Shield, 169–172
explicit consent for, 166
with non-EU Controllers, 180–182
SA authorization for, 175–177
standard contractual clauses, 166–169
third-country, and public interest rule, 299–300
International law, instruments of, 57
International legal standards for data protection, 324
Internet of things (IoT), 159–160
Internet rights, 34–36
Intragroup processing privileges, 147, 182–183
Intrusion against seclusion, 25
Inuvik Hospitals, 444–445
Investigative duties and powers, of SA, 247, 248–249

J
Joint and several liabilities, 65–66, 168, 272–273
Joint Controllers, 65–68, 147, 158
Journalism, 306–307
JPMorgan Chase, 417
Judicial remedies, 253–258, 264f–265f

K
KM.RU, 444
Knowledge promotion, by SA, 247
Korea Credit Bureau, 423

L
Law enforcement, individual privacy in, 39–41
Lawful processing, 126
Layered privacy notices, 127
L-diversity, 90
Lead Supervisory Authority (LSA), 245–246, 251, 393
Legal department, GDPR compliance by, 320
Legal grounds for data processing, 132–160
and changes in processing purpose, 148–149
consent-based processing, 132–144
legal sanction as basis for processing, 144–148
special categories of data, 149–160
Legal mandates, 145, 172, 173f–174f, 362
Legal purposes, processing special data for, 155
Legislation. See also Domestic law
in adequacy determination, 162–163
foreign laws in conflict with GDPR, 184–185
for governing social robots, 17–18
on government use of data, 287–291
on privacy, 31–32
on special data, 160
Legitimate corporate interests, 146–148, 159, 396–398
LexisNexis, 422–423
Liability(ies):
allocating, to Controller, 65–68, 271–273
allocating, to Processor, 271–273
of data protection officers, 84
intermediary, 51
joint and several, 65–66, 168, 272–273
moderating content to mitigate, 361
Linkage, in compatibility test, 128, 129, 148
Livestreaming services, 371–372
Local competence of SA, 246
Local legal standards, see Domestic law
Location data, 150, 151
Loss, data, 95

M
MacRumors forum, data breach, 422
Malware, 96
Manual cyber-security, 102
Manual processing, 46–47
Market dominance, 142–143
Marketing department, 320
Masking, 91
Masquerade, 337
Massachusetts General Hospital, 439
Master keys, 309
Material requisites for processing, 125–185
central principles of processing, 125–132
cooperation obligation on EU bodies, 183–184
with foreign law in conflict with GDPR, 184–185
for international data transfers, 161–182
intragroup processing privileges, 182–183
legal grounds for data processing, 132–160
Maximum financial value, 362
Mediation, 259
Medical Informatics Engineering, 427–428
Michaels, 421–422
Mobile devices, 407–408
Mozilla Firefox, 421
Multiple infringements, fines for, 277–278
Music guidelines, Facebook, 338
MyHeritage, 461–462

N
NASDAQ, 420–421
National Identification Numbers, 303–304
National Security Administration (NSA), 30–32
Natural Grocers, 427
Natural persons, defined, 47
Nature of data, 128, 129, 149
Necessity of processing, 136–138, 160
Negotiation, 259
Neiman Marcus, 420
Net neutrality, 35–36
Network integrity, 147
Network security, 101
9/11 attacks, privacy protection after, 29–31
Nival Networks, 444
Noise addition, 90
Not-for-profit bodies (NPO), 154, 240
Notice-and-choice model, 9–12
Notification obligation:
  after personal data breach, 103–106
  for Controllers, 196–197
  in Privacy Shield, 170
  of right to object, 223
Notifications, Facebook, 352–353
NYC Tax Company, data breach, 419–420
nyob.eu, 135–144

Object, right to, 221–223, 296, 297
Objectionable content, 365–366
Occasional processing, 68, 181
Oculus and Oculus Ireland Limited, 337
Office of Personnel Management (OPM), 434–435
Ombudsman, 171
Onavo, 337
Online consent, 140–141
Openness principle, 27
Operators of essential services, 71, 301
Opt-in and -out, in Privacy Shield, 170
Orbitz, 456–457
Organizational requirements under GDPR, 61–123, 239
  accountability-related, 61–62
  codes of conduct and certifications, 107–112
  for Controller, 62–69
  data protection by design, 84–92
  data-protection level maintenance, 69–71
  for data protection officers, 80–84
  data security during processing, 92–94
  DPIAs, 73–80
  at Facebook, 393–405
  in NIS Directive, 71–72
  and personal data breaches, 94–107
  and privacy policies of tech firms, 381f–385f
  processing-activity record maintenance, 72–73
  for Processor, 112–116
  and public interest rule, 297–300
Ownership, of online human interaction, 339

P
Pages, groups, and event policy, 338
Partial control model, 238
Password attacks, 96
Personal data:
  definition under GDPR, 47–51
  erasure for, 211–212
  inaccurate, 204
  incomplete, 204
  level of protection needed for, 86
  right of access for, 201–202
Personal data breaches, 94–107
  case examples, 413–466
  characteristics and types of, 95–103
  communication with data subjects, 106–107
  Controller’s duties after, 103–107
  at Facebook, 356–358
  notification of Supervisory Authority, 103–106
Personal data collection:
  by advertisers, 347–348
  context of, 128, 129, 148
  early digital privacy laws on, 27
  at Facebook, 342–346
  mechanisms for, 344–346
  reasons for, 342–343
  superfluous, for a purpose, 127
Personalized anonymization, 91
Personalized shopping, 398–399
Philanthropy, processing for, 343–344
Phishing, 96
Physical breaches, 96
Physical privacy, 5
Point person for compliance, 319–321
Pop Sugar Inc., 463–464
Portability, see Data portability, right to
Power imbalance, 140, 141
Premara, 433–434
Prevention and occupational medicine,
  special data for, 156
Privacy-as-trust model, 9, 13–16
Privacy by design, see Data protection by design
Privacy policies:
  as enforcement mechanism, 236–237, 236f
  of Facebook, 342–343, 381f–385f
  setting, 331
Privacy Shield, 169–172
Privacy Shield Arbitral Panel, 171
Privacy Shield Company, 171
Private life, right to, 26
Probable cause, 40
Processing. See also Material requisites for processing
for advertisers on Facebook, 349–350
central principles of, 125–132, 126f
in context of activities, 55–56
of criminal record data, 292–293
data security during, 92–94
definition under GDPR, 46–47
DPIA as requirement for, 74–75
ensuring security of, 328–329
legal grounds for, 132–160
for legitimate corporate interests, 396–398
for philanthropic purposes, 343–344
in the “public interest,” 291–300
restraint of, by SA, 281–282, 282f
Processing-activity records, 72–73
Processing contracts, 113–114
Processor(s):
allocating liability to, 271–273
bringing, into compliance, 327–328
with cloud computing, 158–159
Controller’s selection of, 113–114
Controller-to-Processor SCC, 167
defined, 53
duties, 114–116
judicial action against, 253–254
organizational requirements for, 69–73,
112–116
relationship of Controller and, 112–113
territorial scope for, 55
Professional secrecy, 243–244
Profiling, 74–75, 224–225
Prosthetic & Orthodontic Care (P&O), 439–440
Pseudonymization, 50, 88
Public authority, processing by, 68
Public data, 154–155, 211–212, 301–304
Public disclosure of private facts, 25
Public documents, 301–304
Public electronic communication services, 303
Public endorsements, 398–399
Public figures, right to erase for, 210
Public health, special data for, 156
Public interest, 291–300
and criminal record data, 292–293
defined, 291–292
exemptions/responsibilities related to, 297–300
as legal basis for processing, 292
processing for, 145–146
restrictions on GDPR for, 305–306
and rights of data subject, 294–297
special data for, 155, 292–293
Public international law, instruments of, 57
Public networks, 302–303
Purpose, changing processing, 148–149
Purpose limitation obligation, 127–129
for big data operations, 158
for Facebook, 395–396
for internet of things, 159
in Privacy Shield, 170

R
Randomization, 49, 89
Ransomware, 96
Realistic choice, 140
Reasonable expectation of privacy, 40
Reasonable fees, 202–203
Reasonable suspicion, 40
Recipient, defined, 53
Record keeping, 147, 329–330
Rectification, right of, 203–205, 297f, 400
Redressability, 163
Regulatory compliance duties, of SA, 247–248
Regulatory infringements, 275–276
Regulatory standards on data protection, 324
Remedies for data subjects, 271–285. See also Judicial remedies
Administrative fines, 275–279
Allocation of liability, 271–273
Compensation, 273–275
Injunctions, 279–282
Specific performance, 283–284
Reporting duty, of DPO, 82
Request-based model, 238–239
Resource independence, 243
Restriction, right to, 214–215, 294–295, 297f, 401
Retention policies, 329–330
Revenue sources, Facebook, 346–347, 352–353
Revocation of adequacy decision, 165–166
Rights of data subjects, see Data subjects’ rights
Risk-based approach to data processing, 70–71, 75–76, 94
Safety threats, content related to, 363–365
Sales department, 320
Sanctions, 144–148, 277
Scottrade, 426–427
Scrambling, 91
Search warrants, 40
Secrecy, professional, 243–244
Self-certification, Privacy Shield, 170
Self-serve ad terms, 38
Shell companies, 377–378
Sing Health, 460–461
Slack, 426
Social actions, 351
Social media services:
  advertising/direct marketing for, 346–347
category of entity for, 376–377
code of ethics for, 378
data protection as obligation of, 355–356
ownership of online human interaction by, 339
privacy policies of, 381f–385f
sharing and customizability for, 341
social networking phenomenon, 335
Social networking, 335, 339–340
Social privacy, 5
Social protection, special data for, 153
Social robots, 16–18
Software, cyber-security, 100
Sony, 418–419
“Special” data:
  automated decision making and, 225–226
defined, 150, 151f
  DPIA for processing, 75
gleal grounds for processing, 149–161
level of protection needed for, 86
state use of, 292–293
Specific performance, 283–284
Speech, freedom of, 26, 34–35, 207
Spotify, 381f–385f
Stakeholders, GDPR, 52–54
Standard contractual clauses (SCCs), 166–169, 169f
Standing in court, 274–275, 274f
Starwood Hotels, 425–426
Storage of data, 131
Strategic analysis, 147
Streisand effect, 208–209
Submission agreements, 260
Subpoenas, 305
Subprocessors, 116, 159
Subpurposes, for processing, 127
Subsidiary companies, Facebook, 337
Substitution (permutation), 90
Superfluous data collection for a purpose, 127
Supervalu, 416
Supervisory Authorities (SAs), 241–253
  approval of rules by, 174–175
  authorization for data transfers, 175–177
  competence of, 244–246
  consultation with, prior to DPIA, 77–78
  cooperation and consistency for, 250–252
duty to cooperate with, 68–69
duty to notify, after data breach, 103–106
enforcement activities of, 252–254
independence of, 243
investigations by, 278–279
judicial action against, 254–256
members of, 242–243
monitoring code of conduct compliance, 109
oversight of business plan, 78–80
powers of, 248–250
processing restrained by, 281–282, 282f
professional secrecy for, 243–244
role of, 241–242
tasks of, 246–248
Surveillance, 30, 75
Suspension of proceedings, 257–258
Taobao, 443–444
Targeted advertising, 377–378
Taringa, 453
Tax levy, digital services, 377
TaxSlayer, 442–443
Technical measures, 69–72, 237–239
Technology:
  data use for advancement of, 344
  need for privacy and, 5–6, 24
  privacy policies of tech firms, 381f–385f
special data use by, 157–160
Telemedia data protection, 302–303
Telephonic consumer protection laws, 28
Termination of processing, 115, 168
Territorial scope for GDPR, 54–57
Third-country data transfers, 299–300
Third parties, 53, 71, 147, 383f
Third-party beneficiaries, data subjects as, 168
Ticketfly, 457–458
Time of stay standard, 57
Tokenization, 88–90
Tort laws on privacy, 24–25
Training, by GDPR Team, 330
Transparency. See also Information and transparency requirements
duty of, 194–197
information on, 198–200
of processing, 126
of terms of service, 133
Trespass theory of privacy, 40
Trump Hotels, 415–416
Trust, 17, 355–356
21st Century Oncology, 451
Twitch TV, 425
Twitter, 381f–385f

U
Uber, 381f–385f, 451–453
UCLA Hospitals, 437–438
UK House of Commons, 372, 375–379
Unauthorized derogations, data transfer, 178–179
Unauthorized processing, 95
Uncompensated endorsement, 354–355
Under Armour, 462–463
United States:
EU–US Privacy Shield, 169–172
legislative initiatives on privacy, 31–32
notice-and-choice model in, 9–11
US Center for Medicaid Services, 460
US Department of Commerce (DOC), 171
US Federal Trade Commission (FTC), 11, 14–16, 171
University of California, Berkeley, 442
University of Central Florida, 441–442
University of Maryland, 414
Unlawful processing, 95
UPS, 413–414

V
Vague information, 136
Violent content, 362–363
Virtual identifiers, 49
Vital interests, protection of, 145
Voluntary information, 3–4
VTech, 437

W
Walmart (Canada), 436–437
Warrants, 40
Weebly, 440–441
Wendy’s, 440
WhatsApp Inc. and WhatsApp Ireland Limited, 135–144, 337
Wire-tap warrant, 40
Works Councils, 312–313
World War II, personal data misuse in, 25–26
Worst-case scenario planning, 331–332

Y
YouTube, 381f–385f