# INDEX

Footnotes are indicated by n. after the page number, and figures by fig.


access right, 15, 38–40, 107–108, 158, 225–226, 266
accountability principle, 35, 60, 63, 151–152, 319–320
accuracy of data. *See* quality of data
adequacy findings, 61
administrative activities, data processing for, 28, 305
AI. *See* artificial intelligence
anonymization and pseudonymization
  for artificial intelligence use, 297, 301–302, 315
  before further processing, 24
  blockchain tools as pseudonymized personal data, 251–252, 261
  cash and voucher assistance beneficiaries' data, 139–140
  definitions, 18–20, 52n.12
  dimensionality problem, 85
  for drone-collected data processing, 105
  re-identification risk, 19–20, 71–72, 139–140, 297, 301–302
anonymous use of mobile messaging apps, 202–203
applicable law. *See also* international data sharing
applicable law, 20–21
artificial intelligence
  anonymized data, re-identification using, 297, 301–302
  benefits and applications, 219–220, 293, 294–295, 298
  bias problem, 296, 300–301, 309–311, 314, 316–318
    ethical assessment, 329–332
    HRIA (human rights impact assessment), 324–329
  data controller/data processor relationship, 299, 319–321
  data minimization principle, 295, 301, 312–314
  data protection by design and by default, 329
  data subjects' rights, 309–311, 316–319
  datasets used by applications, 296, 298–299, 320
  definition and functionality, 290–292
  DPIAs (data protection impact assessments) for, 296–297, 320, 322–324
  international data sharing, 320–322
  introduction to topic, 290
  legal bases for personal data processing, 302–305, 308–309, 318
  purpose limitation principle and further processing, 296–297, 304, 305–308, 322
  retention of data, 314–315
  risks and challenges, 292–303
  securitizing data, 315–316
  social media data analysis using, 232–233, 235, 237, 298, 303–306
  transparency principle, 304, 308–309, 311–312, 318
authenticating identities. *See* identity verification

backup procedures, 32
balancing of data rights and other interests
  confidentiality protection, 15, 39
  in emergency situations, 14–15, 17–18, 35, 44, 49
  historical record protection, 15, 26, 40–41
  human rights protection, 14–15, 54, 282
  proportionality principle, 14, 24–26, 122–123, 227–228, 264
bias problem of artificial intelligence. *See under* artificial intelligence
Big Brother Watch case, 177–178
biometrics. *See also* identity verification
  benefits and applications, 114–116
  data controller/data processor relationship, 126
  data minimization principle, 122–123, 227
  data subjects' rights, 124–125
  DPIAs (data protection impact assessments) for, 117–118, 120, 125–126
  fair and lawful use principle, 120–121
  generally, 114
  legal bases for biometric data processing, 118–120, 124
  purpose limitation principle and further processing, 121–122, 123
  retention of data, 123
  risks and challenges, 115, 116, 117–118
  securitizing data, 123–124
  sharing data, 125–126
  special protection requirements for data, 116–118, 124
  types, 115
blockchain
  applications in humanitarian sector, 219, 256–258, 267
  benefits, 250, 252–253, 255
  data controller/data processor relationship, 261–263
  data minimization principle, 263–264


Downloaded from https://www.cambridge.org/core. Berklee College Of Music, on 11 Feb 2025 at 12:30:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.025

blockchain (cont.)
data protection by design and by default, 260–261, 271–272
data subjects' rights, 265–268
decision-making framework for deployment, 269–272
definition and functionality, 250–253
DPIAs (data protection impact assessments) for, 258–260, 271
international data sharing, 268–269
proportionality principle, 264
retention of data, 264
risks and challenges, 255–256
securitizing data, 264–265
types, 253–255
'by design' approach. *See* data protection by design

cash and voucher assistance
beneficiaries, identity verification, 115
benefits, 131
blockchain technology for, 256, 257, 258, 267
data controller/data processor relationship, 143
data minimization principle, 139–140
data subjects' rights, 141
DPIAs (data protection impact assessments) for, 139, 140, 141, 143–144
generally, 130–131
legal bases for beneficiaries' data processing, 136–137
personal data collected and generated via, 132–135
purpose limitation principle and further processing, 137–139
retention of data, 140
risks and challenges, 131–134, 256
securitizing data, 140–141
sharing data, 141–143
checklists for data protection compliance, 15–16, 26–27
children, 45–48, 294–295
CISCO Tactical Operations, 278
CLOUD Act (US), 178–181, 186
cloud services
benefits and applications, 148
blockchain applications supported by, 264
data controller/data processor relationship, 151–152, 154–158, 166–167
definition, service models and infrastructure, 148, 149–151
deletion of data, 150, 155–156, 157, 161
DPIAs (data protection impact assessments) for, 152, 153, 156, 165–166
fair and lawful use principle, 153
GDPR codes of conduct, 167–168
government access to data. *See* cloud-based data, government access
as international data sharing, 58, 165
legal bases for personal data processing, 152–153
privileges and immunities, implications for, 149, 152, 157, 160–161, 166–167, 186–189
purpose limitation principle and further processing, 153–154, 159
risks and challenges, 148–149
securitizing data. *See* cloud services, data security
transparency principle, 154–155
cloud services, data security
asset protection, 160–162
audits and procedures for, 164–165
data in transit protection, 160
data subjects' rights and, 158–160, 165
during development, 163
governance of, 162
identity verification, 164
operational security, 162–163
particular vulnerabilities, 164
privileged data, technical security measures, 167
responsibilities for, 156–158, 163–164
risks related to infrastructure types, 150–151
separation between users, 162
staff selection and training, 163, 164–165, 167
supply chain security, 163
cloud-based data, government access
criminal investigation grounds, 178–184
impacts on aid beneficiaries, 184
impacts on humanitarian organizations, 184–186
introduction to topic, 172–173
legal duties generally, 173–174
national security grounds, 174–178
risk mitigation, 186–189
community identifiable information, 8
compliance with legal obligation (legal basis), 53–57, 284
computer security measures. *See also* cloud services, data security
computer security measures, 31–32, 34, 51–52
confidentiality duties
cloud service providers, 157, 159, 181
contractual duties, 31, 32–33
data rights balanced against, 15, 39
in emergency situations, 17–18
health data processing, 27–28, 54, 89–90, 184
identity verification before information disclosure, 39–40, 216
levels of confidentiality, attribution of, 33
confirmation right, 39, 49
connectivity as aid programmes
data controller/data processor relationship, 282–283
DPIAs (data protection impact assessments) for, 279, 281–282

Downloaded from https://www.cambridge.org/core. Berklee College Of Music, on 11 Feb 2025 at 12:30:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.025

examples, 277–278
international data sharing, 287
introduction to topic, 276–277
legal bases for personal data processing, 283–284
operational context, 278–279
retention of data, 286
securitizing data, 284–286
stakeholder partnerships for, 279–281
transparency principle, 286–287
consent (legal basis). *See also* information right
for artificial intelligence use, 302–304, 308–309, 318
for biometric data processing, 118–120, 124
of cash and voucher assistance beneficiaries, 136–137, 258
of children, 45–48
of connectivity as aid beneficiaries, 283–284
for digital identity data processing, 225, 226–227
documentation of, 48
for drone-collected data processing, 102, 107
freely given, 46
information requirements for, 36–37, 46, 48
for international data sharing, 60
for mobile messaging app data processing, 203, 206
for social media data processing, 244–245
objection right, 40, 41, 44–45, 48–49, 107
timing of, 46
transmission methods and modes, 46, 48
of vulnerable adults, 45–47
when not required, 44, 45–46, 49
withdrawal of, 40, 49, 304
contact tracing apps. *See also* mobile messaging apps
data minimization principle, 93
DP3T protocol design, 81–82, 91–92
generally, 79–81
risks and challenges, 84–86, 88, 89–90, 92–93, 95
contingency planning, 33
contracts for data processing. *See* data controller/data processor relationship
contractual performance (legal basis), 52–53, 60, 284
correction right, 40, 207–208, 226, 266–267, 318
counter-terrorist legislation. *See* cloud-based data, government access
COVID-19 pandemic
combating misinformation during, 234
contact tracing apps used in. *See* contact tracing apps
criminal investigation legislation, 178–184
cross-border data sharing. *See* international data sharing
cross-functional needs assessments, 25
crowdsourcing, 108–109
data analytics. *See* artificial intelligence
data controller/data processor relationship
artificial intelligence use, 299, 319–321
biometric data processing, 126
blockchain use, 261–263
cash and voucher beneficiaries' data processing, 143
cloud services-held data processing, 151–152, 154–158, 166–167
connectivity as aid programmes, 282–283
digital identity management systems, 223–224
drone-collected data processing, 109–110
social media data processing, 243–244
data controllers
accountability of, 35, 60, 63, 151–152, 319–320
data processors, distinguished from, 18, 261
data processors, relationship with. *See* data controller/data processor relationship
data security obligations. *See* data security
data sharing by. *See* data sharing; international data sharing
data minimization principle. *See also* deletion of data; retention of data
artificial intelligence use, 295, 301, 312–314
biometric data, 122–123, 227
blockchain use, 263–264
cash and voucher assistance, 139–140
cloud-based data, 155
for data protection by design, 93–94
digital identity management systems, 216–217, 227–228
drone-collected data, 105–106
generally, 25, 26–27
mobile messaging app data, 207, 208–209
data processing principles
accountability, 35, 60, 63, 151–152, 319–320
data minimization. *See* data minimization principle
data quality. *See* quality of data
'do no harm' (precautionary principle), 24, 35, 69–70
fair and lawful use, 21–22, 120–121, 153, 308–311
proportionality, 14, 24–26, 122–123, 227, 264
purpose limitation. *See* purpose limitation principle
transparency. *See* information right
data processors
confidentiality duties. *See* confidentiality duties
data controllers, distinguished from, 18, 261
data controllers, relationship with. *See* data controller/data processor relationship
international data sharing by, 58, 63–65
sub-processors, 18, 124, 151, 157–158, 188

Downloaded from https://www.cambridge.org/core. Berklee College Of Music, on 11 Feb 2025 at 12:30:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.025

data protection by design
artificial intelligence systems, 329
blockchain applications, 260–261, 271–272
case study. *See* contact tracing apps
cash and voucher assistance systems, 140–141
data collected centrally, 93–94, fig.6.1
data minimization principle, 93–94
design assessment process
potential risks identification, 88–90
risks assessment, 90–93
digital identity management systems, 222–223
generally, 78–79
mobile messaging apps, 210–211
purpose limitation principle
purposes determination, 87, 88
rationale, 82–87
technical challenges, 94–97
risks retention, 87–88, fig.6.2, 94–95
'system' definition, 79
data protection impact assessments. *See* DPIAs (data protection impact assessments)
data quality. *See* quality of data
data retention or deletion. *See* deletion of data; retention of data
data security
anonymization and pseudonymization. *See* anonymization and pseudonymization
artificial intelligence applications, 315–316
biometric data, 123–124
blockchain-stored data, 264–265
cash and voucher assistance beneficiaries' data, 140–141
cloud-based data. *See* cloud services, data security
for connectivity as aid programmes, 284–286
contingency planning, 33
data controllers' general duties, 29–31
deletion of data. *See* deletion of data
by design. *See* data protection by design
digital identity data, 228–229
drone-collected data, 106
internal organization measures, 34–35
international data sharing, risk mitigation, 61–63
IT security, 31–32, 34, 51–52
mobile messaging app data, 202–205
physical security, 31
social media data, 247
data security officers, 34–35
data sharing. *See also* international data sharing
anonymized or pseudonymized data, 18–20
biometric data, 125–126
cash and voucher assistance beneficiaries' data, 141–143
with cloud service providers, 159–160
digital identity data, 220–221
drone-collected data, 108–109
generally, 41–43
with government authorities. *See* government access to personal data
with humanitarian organizations without privileges or immunities, 54–57
information right, 42
mobile messaging app data, 199–200, 204–205
by social media platforms, 211, 236–238, 247
with third parties. *See* third parties
data subjects' rights. *See also* human rights
access, 15, 38–40, 107–108, 158, 225, 266
artificial intelligence use and, 309–311, 316–319
balanced against other interests. *See* balancing of data rights and other interests
blockchain applications and, 265–268
claims for breach of, 38
cloud services and, 158–160, 165
confidentiality. *See* confidentiality duties
correction, 40, 207–208, 226, 266, 318
digital identity management systems and, 224–226
erasure, 40–41, 155–156, 207–208, 226, 267, 318
information. *See* information right
objection, 40, 41, 44–45, 48–49, 107
deceased persons, 8, 39, 49
deletion of data. *See also* data minimization principle; retention of data
biometric data, 123
cash and voucher assistance beneficiaries' data, 140
cloud-based data, 150, 155–156, 157, 161
drone-collected data, 106
erasure right, 40–41, 155–156, 207–208, 226, 267, 318
inaccurate data, 27
mobile messaging app data, 201, 203–204, 207–208
paper records destruction, 33–34
from portable media equipment, 32, 34
social media data, 246
by third parties, 29, 32, 34, 140
demographically identifiable information, 8
designing systems for data protection. *See* data protection by design
detained persons, 51
differential privacy, 315–316
digital identity management systems. *See also* identity verification
adoption of, 214, 218–219, 221–222
data controller/data processor relationship, 223–224
data minimization principle, 216–217, 227–228
data subjects' rights, 224–226
design of, 216–220, 222–223
DPIAs (data protection impact assessments) for, 222

Downloaded from https://www.cambridge.org/core. Berklee College Of Music, on 11 Feb 2025 at 12:30:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.025

governance of, 218
international data sharing, 229
legal bases for personal data processing, 226–227
proportionality principle, 227
purpose limitation principle, 227
retention of data, 229
scenarios of use, 220–221
securitizing data, 228
terminology, 214n.4, 215, 217
digital systems for data protection. *See* data protection by design
digitization of paper records, 33–34
disasters. *See* emergency situations
discretion, duties of. *See* confidentiality duties
disease prevention, 234, 295
'do no harm' (precautionary principle), 24, 35, 69–70
DPIAs (data protection impact assessments)
for artificial intelligence use, 296–297, 320, 322–324
for biometric data processing, 117–118, 120, 125–126
for blockchain use, 258–260, 271
for cash and voucher assistance, 138–139, 140, 141, 143–144
for cloud services use, 152, 153, 156, 165–166
for connectivity as aid programmes, 279, 281–282
for digital identity management systems, 222
DPIA report template, 333–337
for drone operations, 110
for mobile messaging apps use, 196, 206
process. *See* DPIA process
for social media use, 239–241, 247
when appropriate, 45, 63, 66–67, 72–73
DPIA process
(1) determining necessity for DPIA, 67
(2) assembling DPIA team, 67–68
(3) describing the processing of personal data, 68
(4) consulting stakeholders, 68–69
(5) identifying risks, 69
(6) assessing risks, 69–70
(7) identifying solutions, 70–72
(8) proposing recommendations, 72
(9) implementing recommendations, 72–73
(10) providing expert review or audit of DPIA, 73
(11) updating the DPIA, 73
drones/UAVs and remote sensing
data collection and processing equipment, 98, 100
data minimization principle, 105–106
data subjects' rights, 106–108
DPIAs (data protection impact assessments) for, 110
generally, 100–101
humanitarian action uses, 98–99
legal bases for drone-collected data processing, 102–104, 107
outsourced operations, 101, 109–110
purpose limitation principle, 105
retention of data, 106
safety risks, 99–100, 101
securitizing data, 106
sharing of data, 108–109
transparency principle, 104–107

e-evidence legislation, 183–184
email correspondence, 31
emergency situations
balancing of data rights and other interests in, 14–15, 17–18, 35, 44, 49
connectivity loss. *See* connectivity as aid programmes
drone-collected data processing in, 103
presumption of high risk in, 69–70
social media use in, 233, 241
vital interests in. *See* vital interests (legal basis)
Emergency Telecommunications Cluster, 277
erasure right, 40–41, 155–156, 207–208, 226, 267, 318
EU law
on data controllership, 243–244
GDPR (General Data Protection Regulation), 6, 78n.1, 117, 167–168, 307
on government access to cloud-based data, 176–177, 183

Facebook
data collection and retention by, 236, 246
as data controller, 243–244
data sharing by, 204, 237–238
Facebook Connectivity initiative, 278
Messenger and WhatsApp services. *See* mobile messaging apps
facial recognition, 100, 105, 294–295, 299, 300–301, 315
fair and lawful use principle, 21–22, 120–121, 153, 308–311
family members, data access right, 39–40
fundamental rights. *See* human rights
further processing. *See also* purpose limitation principle
artificial intelligence use for, 304, 306–308
of biometrics data, 121–122, 123
of cash and voucher assistance beneficiaries' data, 138–139
of cloud-based data, 153–154, 159
of drone-collected data, 105
generally, 22–24
of mobile messaging app data, 193, 209, 210

GDPR (EU General Data Protection Regulation), 6, 78n.1, 117, 167–168, 307
Global Privacy Assembly, 4–5

Downloaded from https://www.cambridge.org/core. Berklee College Of Music, on 11 Feb 2025 at 12:30:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.025

government access to personal data
cloud-based data. *See* cloud-based data, government access
compliance with legal obligation (legal basis), 53–55, 284
mobile messaging app data, 197, 200, 201–202, 204
smartphone surveillance, 284–285
social media data, 232–233, 238–239, 240, 298

health data processing, 27–28, 54, 89–90, 184
health promotion, 234, 295
historical record-keeping, 15, 26, 40–41
human rights. *See also* data subjects' rights
artificial intelligence, bias problem, 296, 300–301, 309–311, 314, 316–318
ethical assessment, 329–332
HRIA (human rights impact assessment), 324–329
data protection as human right, 7
data rights balanced against, 14–15, 54, 282
humanitarian emergencies. *See* emergency situations
humanitarian organizations. *See also* data controllers
campaigning and fundraising by, 232, 235–236, 244–245, 257
compelled data disclosure, impacts on, 184–186
legitimate interests of. *See* legitimate interest (legal basis)
NGOs (non-governmental organizations), 18, 20–21, 277–278
staff of. *See* staff of humanitarian organizations
with privileges and immunities. *See* privileges and immunities

ICRC (International Committee of the Red Cross), 7, 50n.8, 189n.52, 233, 241n.46
ID2020 Alliance, 224
identity verification
biometrics. *See* biometrics
cash and voucher assistance beneficiaries, 115
for cloud services access, 164
digital systems for. *See* digital identity management systems
facial recognition, 100, 105, 294–295, 299, 300–301, 315
general duties of, 39–41, 216
KYC (know your customer) obligations, 137, 142, 144, 221–222
'legal identity' definition, 214n.4, 215
purpose creep risk, 86, 222
for SIM card registration, 134, 137, 142, 198, 221, 280
social media data used for, 232–233
immunities. *See* privileges and immunities
impact assessments. *See* DPIAs (data protection impact assessments)
important grounds of public interest. *See* public interest (legal basis)
inaccurate data. *See* quality of data
inferred data. *See* non-personal data, inferences from
information right
artificial intelligence use, 304, 308–309, 311–312, 318
balanced against other interests, 14–15, 35
biometric data processing, 124
of cash or voucher assistance beneficiaries, 141
cloud-based data processing, 154
confirmation of data processing, 39, 49
of connectivity as aid programme beneficiaries, 286–287
data sharing, right to be informed, 42, 60
digital identity data processing, 225
drone-collected data processing, 104, 106–107
personal data obtained from data subjects, 36–37, 46, 48
personal data obtained from third parties, 37–38
social media data processing, 245–246
transmission methods and modes, 35, 39, 49–50, 107
integrity of data. *See* quality of data
International Committee of the Red Cross (ICRC), 6–7, 50n.8, 189n.52, 233, 241n.46
international data protection standards, 5–7, 21, 58
international data sharing. *See also* data sharing
artificial intelligence use, 320–322
basic rules, 59–60
biometric data, 125–126
blockchain-stored data, 268–269
cash and voucher assistance beneficiaries' data, 142–143
cloud services as, 58, 165
connectivity as aid programmes and, 287
contractual arrangements for, 61–65
definition and scenarios, 41–42, 59
digital identity data, 229
drone-collected data, 109
entities engaging in, 58–59
legal bases for, 60–61
mobile messaging app data, 211
reasons for, 58
risk mitigation, 61–63
by social media platforms, 211, 236–238, 247
US/UK agreement on electronic data exchange, 180–183, 188
internet connectivity. *See* connectivity as aid programmes
IT security measures. *See also* cloud services, data security
IT security measures, 31–32, 34, 51–52

Downloaded from https://www.cambridge.org/core. Berklee College Of Music, on 11 Feb 2025 at 12:30:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.025

KYC (know your customer) obligations, 137, 142, 144, 221–222

legal bases for international data sharing, 60–61
legal bases for personal data processing
  alternatives to consent, when permitted, 44, 45–46, 49
  artificial intelligence use, 302–305, 308–309, 318
  biometric data processing, 118–120, 124
  cash and voucher assistance beneficiaries' data processing, 136–137
  cloud-based data processing, 152–153
  compliance with legal obligation, 53–57, 284
  connectivity as aid programmes, 283–284
  consent. *See* consent (legal basis)
  digital identity data processing, 226–227
  drone-collected data processing, 102–104, 107
  legitimate interest. *See* legitimate interest (legal basis)
  list of, 36, 44
  mobile messaging app data processing, 206–207
  performance of a contract, 52–53, 60, 284
  public interest, important grounds of. *See* public interest (legal basis)
  social media data, 244–245
  vital interests of individuals. *See* vital interests (legal basis)
legal risk assessment. *See* DPIAs (data protection impact assessments)
legitimate interest (legal basis)
  for artificial intelligence use, 305
  for biometric data processing, 120
  for cash and voucher assistance beneficiaries' data processing, 137
  for connectivity as aid programmes, 284
  for drone-collected data processing, 104
  generally, 51–52
  for international data sharing, 60

machine learning. *See* artificial intelligence
medical data processing, 27–28, 54, 89–90, 184
metadata
  of cash and voucher assistance beneficiaries, 131–135, 136, 137, 138–139, 142
  cloud-based metadata. *See* cloud-based data, government access
  connectivity as aid programmes collecting, 280, 284–286
  drone-collected, 100
  on mobile messaging apps, 193, 198–201, 203
  on social media networks, 232, 240
missing persons, 39–40, 49, 294–295, 298, 299, 300–301
mobile messaging apps. *See also* contact tracing apps; social media
  benefits and applications, 192, 193, 194–195
  data minimization principle, 207, 208–209
  data protection by design, 210–211
  data subjects' rights, 207–208
  data types collected and stored, 197–200
  definition and functionality, 194, 197
  deletion of data, 201, 203, 207–208
  DPIAs (data protection impact assessments) for, 196, 206
  international data sharing, 211
  legal bases for personal data processing, 206–207
  managing, analysing and verifying data, 209–210
  purpose limitation principle and further processing, 193, 209, 210
  risks and challenges, 192–194, 196–197
  securitizing data, 202–205
  third party data access routes, 199–202
  Whiteflag Protocol, 257–258
mobile network connectivity. *See* connectivity as aid programmes

national security legislation, 174–178
'necessary' data processing, 25, 26–27, 50–53
NGOs (non-governmental organizations), 18, 20–21, 277
non-personal data, inferences from
  anonymized data, re-identification risk, 19–20, 71–72, 139–140, 297, 301–302
  generally, 17–18, 54, 297
  social media data, 235, 241–242, 305–306

objection right, 40, 41, 44–45, 48–49, 107
once-only principle, 220
outsourced data processing. *See* data controller/data processor relationship
overriding interests. *See* balancing of data rights and other interests

paper records destruction, 33–34
passwords, 32
PATRIOT Act (US), 175–176, 177
performance of a contract (legal basis), 52–53, 60, 284
personal data processing
  anonymization and pseudonymization. *See* anonymization and pseudonymization
  definition, 16–17
  DPIA description of, 68
  further processing. *See* further processing
  for identity verification. *See* identity verification
  legal bases for. *See* legal bases for personal data processing
  parties engaged in. *See* data controllers; data processors

Downloaded from https://www.cambridge.org/core. Berklee College Of Music, on 11 Feb 2025 at 12:30:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.025

personal data processing (cont.)
principles and rights. *See* data processing principles; data subjects' rights
risk mitigation. *See* data security; DPIAs (data protection impact assessments)
sensitive data. *See* sensitive data
sharing of data. *See* data sharing; international data sharing
staff members' data, 28, 53
perturbing/redacting data, 20, 39, 72
physical security of data, 31
portable media equipment, 32, 34
precautionary principle ('do no harm'), 24, 35, 69–70
principles of data protection. *See* data processing principles
prisoners, 51
privacy right. *See also* confidentiality duties
privacy right, 7
privacy-enhancing technologies. *See* data protection by design
privileges and immunities
cash and voucher assistance provision and, 142, 143
cloud services use and, 149, 152, 157, 160–161, 166–167, 186–189
data protection as human right transcending, 7–8
data sharing by protected organizations, 54–57
data subjects' claims and, 38
international data sharing and, 62
standards-setting permitted by, 21, 58
processing of personal data. *See* personal data processing
proportionality principle, 14, 24–26, 122–123, 227, 264
pseudonymization. *See* anonymization and pseudonymization
public interest (legal basis)
for artificial intelligence use, 304–305, 318
for biometric data processing, 120
for cash and voucher assistance beneficiaries' data processing, 137
for connectivity as aid programmes, 283–284
for drone-collected data processing, 103–104
generally, 44–45, 50–51
for international data sharing, 60
for mobile messaging app data processing, 206–207
purpose limitation principle. *See also* further processing
artificial intelligence use, 296–297, 305–306, 322
biometric data processing, 121
by design. *See* data protection by design
cash and voucher beneficiaries' data processing, 137–138, 139
cloud-based data processing, 153–154, 159
digital identity data processing, 227
drone-collected data processing, 105
generally, 22
mobile messaging app data processing, 209

quality of data
artificial intelligence, bias problem, 296, 300–301, 309–311, 314, 316–318
correction right, 40, 207–208, 226, 266, 318
data quality principle, 27, 158–159

rape survivors, 184
rectification right, 40, 207–208, 226, 266, 318
redacting/perturbing data, 20, 39, 72
re-identification risk, 19–20, 71–72, 139–140, 297, 301–302
relatives, data access right, 39–40
remote access to computer servers, 31–32
remotely piloted aircraft systems. *See* drones/UAVs and remote sensing
retention of data. *See also* data minimization principle; deletion of data
artificial intelligence use, 314–315
biometric data, 123
blockchain-stored data, 264
cash and voucher assistance beneficiaries' data, 140
checklist for, 26–27
cloud-based data, 155–156
from connectivity as aid programmes, 286
digital identity data, 229
drone-collected data, 106
for historical record, 15, 26, 40–41
initial retention period, 28–29
mobile messaging app data, 201, 203, 207–208
social media data, 246–247
by third parties, 34
rights. *See* data subjects' rights; human rights
risk mitigation. *See* data security; DPIAs (data protection impact assessments)

securitizing data. *See* data security
sensitive data
biometric data. *See* biometrics
definition, 17
health data, 27–28, 54, 89–90, 184
inferred from non-personal data. *See* non-personal data, inferences from
on portable media equipment, 32
sexual violence survivors, 184
sharing of data. *See* data sharing; international data sharing
SIM card registration duties, 134, 137, 142, 198, 221, 280
social media. *See also* mobile messaging apps
artificial intelligence used to analyse, 232–233, 235, 237, 298, 303–306
benefits and applications, 232, 233–234
connectivity as aid programmes involving providers, 279

Downloaded from https://www.cambridge.org/core. Berklee College Of Music, on 11 Feb 2025 at 12:30:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.025

data controller/data processor relationship, 243–244
data sharing by platforms, 211, 236–238, 247
data types generated, 234–236, 240
DPIAs (data protection impact assessments) for, 239–241, 247
government access to data, 232–233, 238–239, 240, 298
legal bases for personal data processing, 244–245
retention of data, 246–247
risks and challenges, 232–233, 241–243
securitizing data, 247
transparency principle, 245–246
sought persons, 39–40, 49, 294–295, 298, 299, 300–301
staff of humanitarian organizations
confidentiality duties. *See* confidentiality duties
legal action, data processing for defence purposes, 52
personal data of, 28, 53
personal data processing by. *See* data processors
remote access to computer servers, 31–32
security of, 39
statistical disclosure control process, 71–72
sub-processors, 18, 124, 151, 157–158, 188
supply chain management, 163, 257
Swiss Blocking Statute, 188
system design for data protection. *See* data protection by design

tax administration, 53
telecommunications connectivity. *See* connectivity as aid programmes
third parties
cash and voucher assistance operatives. *See* cash and voucher assistance
cloud service providers. *See* cloud services
connectivity as aid programmes in partnership with, 279–281
deletion of data by, 29, 32, 34, 140
drone operators, 101, 109–110
government authorities. *See* government access to personal data
mobile messaging apps, third party data access, 199–202
personal data obtained from, 37–38
social media providers. *See* social media
sub-processors, 18, 124, 151, 157–158, 188
systems designers, 94
unauthorized data access by. *See* data security
TikTok, 234, 236, 238
transborder data sharing. *See* international data sharing
transparency principle. *See* information right
Twitter, 236, 238

UAVs (unmanned aerial vehicles). *See* drones/UAVs and remote sensing
UNHCR (UN High Commissioner for Refugees), 7, 245–246, 277, 286–287
United Kingdom
interception of communications legislation, 176–178
US/UK agreement on electronic data exchange, 180–183, 188
United Nations
connectivity initiatives, 277
data protection standards, 5–6, 7
privileges and immunities of, 187
United States
CLOUD Act, 178–181, 186
US/UK agreement on electronic data exchange, 180–183, 188
USA PATRIOT Act, 175–176, 177

verifying identities. *See* identity verification
vital interests (legal basis)
for artificial intelligence use, 304
for biometric data processing, 119–120
for cash and voucher assistance beneficiaries' data processing, 137
for cloud-based data processing, 153
for drone-collected data processing, 103
generally, 44–45, 49–50, 51
for international data sharing, 60
for mobile messaging app data processing, 206–207
voucher assistance. *See* cash and voucher assistance
vulnerable adults, 45–47

WhatsApp. *See* mobile messaging apps
Whiteflag Protocol, 257–258
withdrawal of consent for data processing, 40, 49, 304
World Medical Association International Code of Medical Ethics, 27

Downloaded from https://www.cambridge.org/core. Berklee College Of Music, on 11 Feb 2025 at 12:30:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.025

Downloaded from https://www.cambridge.org/core. Berklee College Of Music, on 11 Feb 2025 at 12:30:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.025