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

```
access right, 15, 38-40, 107-108, 158,
                                                   purpose limitation principle and further
                                                        processing, 296-297, 304, 305-308,
       225-226, 266
accountability principle, 35, 60, 63, 151-152,
                                                        322
                                                   retention of data, 314-315
       319-320
accuracy of data. See quality of data
                                                   risks and challenges, 292-303
adequacy findings, 61
                                                   securitizing data, 315–316
                                                   social media data analysis using, 232-233,
administrative activities, data processing for,
       28, 305
                                                        235, 237, 298, 303–306
AI. See artificial intelligence
                                                   transparency principle, 304, 308-309,
anonymization and pseudonymization
                                                        311-312, 318
  for artificial intelligence use, 297, 301-302,
                                                 authenticating identities. See identity
                                                        verification
  before further processing, 24
  blockchain tools as pseudonymized
                                                 backup procedures, 32
       personal data, 251-252, 261
                                                 balancing of data rights and other interests
  cash and voucher assistance beneficiaries'
                                                   confidentiality protection, 15, 39
       data, 139-140
                                                   in emergency situations, 14-15, 17-18, 35,
  definitions, 18-20, 52n.12
                                                        44, 49
  dimensionality problem, 85
                                                   historical record protection, 15, 26, 40-41
                                                   human rights protection, 14-15, 54, 282
  for drone-collected data processing, 105
  re-identification risk, 19-20, 71-72,
                                                   proportionality principle, 14, 24-26,
       139-140, 297, 301-302
                                                        122-123, 227-228, 264
anonymous use of mobile messaging apps,
                                                 bias problem of artificial intelligence. See
       202-203
                                                        under artificial intelligence
applicable law. See also international data
                                                 Big Brother Watch case, 177-178
       sharing
                                                 biometrics. See also identity verification
applicable law, 20-21
                                                   benefits and applications, 114-116
                                                   data controller/data processor relationship,
artificial intelligence
  anonymized data, re-identification using,
       297, 301-302
                                                   data minimization principle, 122-123, 227
  benefits and applications, 219-220, 293,
                                                   data subjects' rights, 124-125
       294-295, 298
                                                   DPIAs (data protection impact assessments)
  bias problem, 296, 300-301, 309-311, 314,
                                                        for, 117-118, 120, 125-126
       316-318
                                                   fair and lawful use principle, 120-121
    ethical assessment, 329-332
                                                   generally, 114
    HRIA (human rights impact assessment),
                                                   legal bases for biometric data processing,
       324-329
                                                        118-120, 124
  data controller/data processor relationship,
                                                   purpose limitation principle and further
       299, 319-321
                                                        processing, 121-122, 123
  data minimization principle, 295, 301,
                                                   retention of data, 123
       312 - 314
                                                   risks and challenges, 115, 116, 117-118
  data protection by design and by default,
                                                   securitizing data, 123-124
                                                   sharing data, 125-126
  data subjects' rights, 309-311, 316-319
                                                   special protection requirements for data,
  datasets used by applications, 296,
                                                        116-118, 124
       298-299, 320
                                                   types, 115
  definition and functionality, 290-292
                                                 blockchain
  DPIAs (data protection impact assessments)
                                                   applications in humanitarian sector, 219,
       for, 296-297, 320, 322-324
                                                        256-258, 267
  international data sharing, 320-322
                                                   benefits, 250, 252-253, 255
  introduction to topic, 290
                                                   data controller/data processor relationship,
  legal bases for personal data processing,
                                                        261-263
       302-305, 308-309, 318
                                                   data minimization principle, 263-264
```

blockchain (cont.) data protection by design and by default,	legal bases for personal data processing, 152–153
260–261, 271–272	privileges and immunities, implications for
data subjects' rights, 265–268 decision-making framework for	149, 152, 157, 160–161, 166–167, 186–189
deployment, 269–272	purpose limitation principle and further
definition and functionality, 250–253	processing, 153–154, 159
DPIAs (data protection impact assessments) for, 258–260, 271	risks and challenges, 148–149 securitizing data. <i>See</i> cloud services, data
international data sharing, 268–269	security
proportionality principle, 264	transparency principle, 154–155
retention of data, 264	cloud services, data security
risks and challenges, 255–256 securitizing data, 264–265	asset protection, 160–162 audits and procedures for, 164–165
types, 253–255	data in transit protection, 160
'by design' approach. See data protection by	data subjects' rights and, 158-160, 165
design	during development, 163 governance of, 162
cash and voucher assistance	identity verification, 164
beneficiaries, identity verification, 115	operational security, 162-163
benefits, 131	particular vulnerabilities, 164
blockchain technology for, 256, 257, 258, 267	privileged data, technical security measures, 167
data controller/data processor relationship,	responsibilities for, 156–158, 163–164
143	risks related to infrastructure types,
data minimization principle, 139–140	150–151
data subjects' rights, 141 DPIAs (data protection impact assessments)	separation between users, 162 staff selection and training, 163, 164–165,
for, 139, 140, 141, 143–144	167
generally, 130–131	supply chain security, 163
legal bases for beneficiaries' data processing, 136–137	cloud-based data, government access criminal investigation grounds, 178–184
personal data collected and generated via,	impacts on aid beneficiaries, 184
132–135	impacts on humanitarian organizations,
purpose limitation principle and further	184-186
processing, 137–139 retention of data, 140	introduction to topic, 172–173 legal duties generally, 173–174
risks and challenges, 131–134, 256	national security grounds, 174–178
securitizing data, 140-141	risk mitigation, 186–189
sharing data, 141–143 checklists for data protection compliance,	community identifiable information, 8 compliance with legal obligation (legal basis)
15–16, 26–27	53–57, 284
children, 45–48, 294–295	computer security measures. See also cloud
CISCO Tactical Operations, 278	services, data security
CLOUD Act (US), 178–181, 186 cloud services	computer security measures, 31–32, 34, 51–52 confidentiality duties
benefits and applications, 148	cloud service providers, 157, 159, 181
blockchain applications supported by,	contractual duties, 31, 32–33
264	data rights balanced against, 15, 39
data controller/data processor relationship, 151-152, 154-158, 166-167	in emergency situations, 17–18 health data processing, 27–28, 54, 89–90,
definition, service models and	184
infrastructure, 148, 149–151	identity verification before information
deletion of data, 150, 155–156, 157, 161 DPIAs (data protection impact assessments)	disclosure, 39–40, 216 levels of confidentiality, attribution of, 33
for, 152, 153, 156, 165–166	confirmation right, 39, 49
fair and lawful use principle, 153	connectivity as aid programmes
GDPR codes of conduct, 167–168	data controller/data processor relationship
government access to data. <i>See</i> cloud-based data, government access	282–283 DPIAs (data protection impact assessments)
as international data sharing, 58, 165	for, 279, 281–282

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

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

governance of, 218	legal bases for drone-collected data
international data sharing, 229	processing, 102–104, 107
legal bases for personal data processing,	outsourced operations, 101, 109–110
226–227	purpose limitation principle, 105
proportionality principle, 227	retention of data, 106
purpose limitation principle, 227	safety risks, 99-100, 101
retention of data, 229	securitizing data, 106
scenarios of use, 220–221	sharing of data, 108-109
securitizing data, 228	transparency principle, 104–107
terminology, 214n.4, 215, 217	
digital systems for data protection. See data	e-evidence legislation, 183-184
protection by design	email correspondence, 31
digitization of paper records, 33–34	emergency situations
disasters. See emergency situations	balancing of data rights and other interests
discretion, duties of. See confidentiality duties	in, 14–15, 17–18, 35, 44, 49
disease prevention, 234, 295	connectivity loss. See connectivity as aid
'do no harm' (precautionary principle), 24,	programmes
35, 69–70	drone-collected data processing in, 103
DPIAs (data protection impact assessments)	presumption of high risk in, 69–70
for artificial intelligence use, 296–297, 320,	social media use in, 233, 241
322–324	vital interests in. See vital interests (legal
for biometric data processing, 117-118,	basis)
120, 125–126	Emergency Telecommunications Cluster, 277
for blockchain use, 258-260, 271	erasure right, 40–41, 155–156, 207–208, 226,
for cash and voucher assistance, 138-139,	267, 318
140, 141, 143–144	EU law
for cloud services use, 152, 153, 156,	on data controllership, 243-244
165-166	GDPR (General Data Protection
for connectivity as aid programmes, 279,	Regulation), 6, 78n.1, 117, 167–168,
281–282	307
for digital identity management systems,	on government access to cloud-based data,
DDIA report template 222 227	176–177, 183
DPIA report template, 333–337	Facebook
for drone operations, 110	
for mobile messaging apps use, 196, 206	data collection and retention by, 236, 246
process. <i>See</i> DPIA process for social media use, 239–241, 247	as data controller, 243–244 data sharing by, 204, 237–238
when appropriate, 45, 63, 66–67, 72–73	Facebook Connectivity initiative, 278
DPIA process	Messenger and WhatsApp services. See
(1) determining necessity for DPIA, 67	mobile messaging apps
(2) assembling DPIA team, 67–68	facial recognition, 100, 105, 294–295, 299,
(3) describing the processing of personal	300–301, 315
data, 68	fair and lawful use principle, 21–22, 120–121,
(4) consulting stakeholders, 68–69	153, 308–311
(5) identifying risks, 69	family members, data access right, 39–40
(6) assessing risks, 69–70	fundamental rights. See human rights
(7) identifying solutions, 70–72	further processing. See also purpose limitation
(8) proposing recommendations, 72	principle
(9) implementing recommendations, 72–73	artificial intelligence use for, 304, 306–308
(10) providing expert review or audit of	of biometrics data, 121–122, 123
DPIA, 73	of cash and voucher assistance
(11) updating the DPIA, 73	beneficiaries' data, 138-139
drones/UAVs and remote sensing	of cloud-based data, 153-154, 159
data collection and processing equipment,	of drone-collected data, 105
98, 100	generally, 22–24
data minimization principle, 105-106	of mobile messaging app data, 193, 209, 210
data subjects' rights, 106-108	
DPIAs (data protection impact assessments)	GDPR (EU General Data Protection
for, 110	Regulation), 6, 78n.1, 117, 167–168,
generally, 100–101	307
9 , , ,	

Global Privacy Assembly, 4–5

humanitarian action uses, 98–99

government access to personal data impact assessments. See DPIAs (data cloud-based data. See cloud-based data, protection impact assessments) government access important grounds of public interest. See compliance with legal obligation (legal public interest (legal basis) basis), 53-55, 284 inaccurate data. See quality of data inferred data. See non-personal data, mobile messaging app data, 197, 200, 201-202, 204 inferences from smartphone surveillance, 284-285 information right social media data, 232-233, 238-239, 240, artificial intelligence use, 304, 308-309, 311-312, 318 balanced against other interests, 14-15, 35 health data processing, 27-28, 54, 89-90, 184 biometric data processing, 124 health promotion, 234, 295 of cash or voucher assistance beneficiaries, historical record-keeping, 15, 26, 40-41 human rights. See also data subjects' rights cloud-based data processing, 154 artificial intelligence, bias problem, 296, confirmation of data processing, 39, 49 300-301, 309-311, 314, 316-318 of connectivity as aid programme ethical assessment, 329-332 beneficiaries, 286-287 HRIA (human rights impact assessment), data sharing, right to be informed, 42, 60 324-329 digital identity data processing, 225 data protection as human right, 7 drone-collected data processing, 104, 106-107 data rights balanced against, 14-15, 54, personal data obtained from data subjects, 36-37, 46, 48 humanitarian emergencies. See emergency personal data obtained from third parties, situations humanitarian organizations. See also data social media data processing, 245-246 transmission methods and modes, 35, 39, controllers campaigning and fundraising by, 232, 49-50, 107 235-236, 244-245, 257 integrity of data. See quality of data compelled data disclosure, impacts on, International Committee of the Red Cross 184 - 186(ICRC), 6-7, 50n.8, 189n.52, 233, legitimate interests of. See legitimate 241n.46 interest (legal basis) international data protection standards, 5-7, 21, 58 NGOs (non-governmental organizations), 18, 20-21, 277-278 international data sharing. See also data staff of. See staff of humanitarian sharing organizations artificial intelligence use, 320-322 basic rules, 59-60 with privileges and immunities. See privileges and immunities biometric data, 125-126 blockchain-stored data, 268-269 ICRC (International Committee of the Red cash and voucher assistance beneficiaries' Cross), 7, 50n.8, 189n.52, 233, 241n.46 data, 142-143 ID2020 Alliance, 224 cloud services as, 58, 165 identity verification connectivity as aid programmes and, 287 biometrics. See biometrics contractual arrangements for, 61-65 cash and voucher assistance beneficiaries. definition and scenarios, 41–42, 59 digital identity data, 229 for cloud services access, 164 drone-collected data, 109 digital systems for. See digital identity entities engaging in, 58–59 management systems legal bases for, 60-61 facial recognition, 100, 105, 294-295, 299, mobile messaging app data, 211 300-301, 315 reasons for, 58 general duties of, 39–41, 216 risk mitigation, 61–63 KYC (know your customer) obligations, by social media platforms, 211, 236–238, 247 137, 142, 144, 221-222 US/UK agreement on electronic data 'legal identity' definition, 214n.4, 215 exchange, 180-183, 188 purpose creep risk, 86, 222 internet connectivity. See connectivity as aid for SIM card registration, 134, 137, 142, programmes 198, 221, 280 IT security measures. See also cloud services, social media data used for, 232-233 data security immunities. See privileges and immunities IT security measures, 31-32, 34, 51-52

KYC (know your customer) obligations, 137, mobile messaging apps. See also contact 142, 144, 221-222 tracing apps; social media benefits and applications, 192, 193, legal bases for international data sharing, 194-195 60 - 61data minimization principle, 207, 208-209 legal bases for personal data processing data protection by design, 210-211 alternatives to consent, when permitted, data subjects' rights, 207-208 44, 45-46, 49 data types collected and stored, 197-200 artificial intelligence use, 302-305, definition and functionality, 194, 197 308-309, 318 deletion of data, 201, 203, 207-208 biometric data processing, 118-120, 124 DPIAs (data protection impact assessments) for, 196, 206 cash and voucher assistance beneficiaries' data processing, 136-137 international data sharing, 211 cloud-based data processing, 152-153 legal bases for personal data processing, compliance with legal obligation, 53-57, 206-207 managing, analysing and verifying data, connectivity as aid programmes, 283-284 209-210 consent. See consent (legal basis) purpose limitation principle and further digital identity data processing, 226-227 processing, 193, 209, 210 drone-collected data processing, 102-104, risks and challenges, 192–194, 196–197 securitizing data, 202-205 legitimate interest. See legitimate interest third party data access routes, 199-202 (legal basis) Whiteflag Protocol, 257-258 list of, 36, 44 mobile network connectivity. See connectivity mobile messaging app data processing, as aid programmes 206-207 performance of a contract, 52-53, 60, 284 national security legislation, 174-178 'necessary' data processing, 25, 26-27, public interest, important grounds of. See public interest (legal basis) 50-53 social media data, 244-245 NGOs (non-governmental organizations), 18, vital interests of individuals. See vital 20-21, 277 interests (legal basis) non-personal data, inferences from legal risk assessment. See DPIAs (data anonymized data, re-identification risk, protection impact assessments) 19-20, 71-72, 139-140, 297, 301-302 generally, 17-18, 54, 297 legitimate interest (legal basis) for artificial intelligence use, 305 social media data, 235, 241-242, 305-306 for biometric data processing, 120 for cash and voucher assistance objection right, 40, 41, 44-45, 48-49, 107 beneficiaries' data processing, 137 once-only principle, 220 for connectivity as aid programmes, 284 outsourced data processing. See data for drone-collected data processing, 104 controller/data processor relationship generally, 51-52 overriding interests. See balancing of data for international data sharing, 60 rights and other interests machine learning. See artificial intelligence paper records destruction, 33-34 medical data processing, 27–28, 54, 89–90, passwords, 32 184 PATRIOT Act (US), 175-176, 177 performance of a contract (legal basis), 52-53, of cash and voucher assistance 60, 284 beneficiaries, 131-135, 136, 137, personal data processing 138-139, 142 anonymization and pseudonymization. See cloud-based metadata. See cloud-based anonymization and pseudonymization data, government access definition, 16-17 DPIA description of, 68 connectivity as aid programmes collecting, 280, 284-286 further processing. See further processing drone-collected, 100 for identity verification. See identity on mobile messaging apps, 193, 198-201, verification legal bases for. See legal bases for personal 203 on social media networks, 232, 240 data processing missing persons, 39-40, 49, 294-295, 298, parties engaged in. See data controllers; 299, 300-301

data processors

personal data processing (cont.)	digital identity data processing, 227
principles and rights. See data processing	drone-collected data processing, 105
principles; data subjects' rights	generally, 22
risk mitigation. See data security; DPIAs	mobile messaging app data processing, 209
(data protection impact assessments)	
sensitive data. See sensitive data	quality of data
sharing of data. See data sharing;	artificial intelligence, bias problem, 296,
international data sharing	300–301, 309–311, 314, 316–318
staff members' data, 28, 53	correction right, 40, 207–208, 226, 266, 318
perturbing/redacting data, 20, 39, 72	data quality principle, 27, 158–159
physical security of data, 31	data quality principle, 21, 130 139
portable media equipment, 32, 34	rape survivors, 184
precautionary principle ('do no harm'), 24,	rectification right, 40, 207–208, 226, 266, 318
35, 69–70	redacting/perturbing data, 20, 39, 72
principles of data protection. <i>See</i> data	re-identification risk, 19–20, 71–72, 139–140,
	297, 301–302
processing principles	
prisoners, 51	relatives, data access right, 39–40
privacy right. See also confidentiality duties	remote access to computer servers, 31–32
privacy right, 7	remotely piloted aircraft systems. See drones/
privacy-enhancing technologies. See data	UAVs and remote sensing
protection by design	retention of data. See also data minimization
privileges and immunities	principle; deletion of data
cash and voucher assistance provision and,	artificial intelligence use, 314–315
142, 143	biometric data, 123
cloud services use and, 149, 152, 157,	blockchain-stored data, 264
160–161, 166–167, 186–189	cash and voucher assistance beneficiaries'
data protection as human right	data, 140
transcending, 7–8	checklist for, 26–27
data sharing by protected organizations,	cloud-based data, 155–156
54–57	from connectivity as aid programmes, 286
data subjects' claims and, 38	digital identity data, 229
international data sharing and, 62	drone-collected data, 106
standards-setting permitted by, 21, 58	for historical record, 15, 26, 40–41
processing of personal data. See personal data	initial retention period, 28–29
processing	mobile messaging app data, 201, 203,
proportionality principle, 14, 24–26, 122–123,	207–208
227, 264	social media data, 246–247
pseudonymization. See anonymization and	by third parties, 34
pseudonymization	rights. See data subjects' rights; human rights
public interest (legal basis)	risk mitigation. See data security; DPIAs (data
for artificial intelligence use, 304–305, 318	protection impact assessments)
for biometric data processing, 120	
for cash and voucher assistance	securitizing data. See data security
beneficiaries' data processing, 137	sensitive data
for connectivity as aid programmes,	biometric data. See biometrics
283–284	definition, 17
for drone-collected data processing,	health data, 27–28, 54, 89–90, 184
103–104	inferred from non-personal data. See non-
generally, 44–45, 50–51	personal data, inferences from
for international data sharing, 60	on portable media equipment, 32
for mobile messaging app data processing,	sexual violence survivors, 184
206–207	sharing of data. See data sharing; international
purpose limitation principle. See also further	data sharing
processing	SIM card registration duties, 134, 137, 142,
artificial intelligence use, 296–297,	198, 221, 280
305–306, 322	social media. See also mobile messaging apps
biometric data processing, 121	artificial intelligence used to analyse,
by design. See data protection by design	232–233, 235, 237, 298, 303–306
cash and voucher beneficiaries' data	benefits and applications, 232, 233–234
processing, 137–138, 139	connectivity as aid programmes involving
cloud-based data processing, 153-154, 159	providers, 279

data controller/data processor relationship, sub-processors, 18, 124, 151, 157-158, 188 systems designers, 94 243-244 data sharing by platforms, 211, 236-238, unauthorized data access by. See data 247 security data types generated, 234-236, 240 TikTok, 234, 236, 238 DPIAs (data protection impact assessments) transborder data sharing. See international for, 239-241, 247 data sharing government access to data, 232-233, transparency principle. See information right 238-239, 240, 298 Twitter, 236, 238 legal bases for personal data processing, 244-245 UAVs (unmanned aerial vehicles). See retention of data, 246-247 drones/UAVs and remote sensing risks and challenges, 232–233, 241–243 UNHCR (UN High Commissioner for securitizing data, 247 Refugees), 7, 245-246, 277, 286-287 transparency principle, 245–246 United Kingdom sought persons, 39-40, 49, 294-295, 298, 299, interception of communications legislation, 300-301 176-178 staff of humanitarian organizations US/UK agreement on electronic data confidentiality duties. See confidentiality exchange, 180-183, 188 United Nations legal action, data processing for defence connectivity initiatives, 277 purposes, 52 data protection standards, 5-6, 7 personal data of, 28, 53 privileges and immunities of, 187 personal data processing by. See data United States processors CLOUD Act, 178-181, 186 remote access to computer servers, 31-32 US/UK agreement on electronic data security of, 39 exchange, 180-183, 188 USA PATRIOT Act, 175-176, 177 statistical disclosure control process, 71–72 sub-processors, 18, 124, 151, 157-158, 188 supply chain management, 163, 257 verifying identities. See identity verification Swiss Blocking Statute, 188 vital interests (legal basis) system design for data protection. See data for artificial intelligence use, 304 protection by design for biometric data processing, 119–120 for cash and voucher assistance tax administration, 53 beneficiaries' data processing, 137 telecommunications connectivity. See for cloud-based data processing, 153 connectivity as aid programmes for drone-collected data processing, 103 third parties generally, 44-45, 49-50, 51 cash and voucher assistance operatives. See for international data sharing, 60 cash and voucher assistance for mobile messaging app data processing, cloud service providers. See cloud services 206-207 connectivity as aid programmes in voucher assistance. See cash and voucher partnership with, 279-281 assistance deletion of data by, 29, 32, 34, 140 vulnerable adults, 45-47 drone operators, 101, 109–110 government authorities. See government WhatsApp. See mobile messaging apps access to personal data Whiteflag Protocol, 257-258 mobile messaging apps, third party data withdrawal of consent for data processing, 40, access, 199-202 49, 304 personal data obtained from, 37-38 World Medical Association International Code social media providers. See social media of Medical Ethics, 27