The Cyber Security Body of Knowledge
Law and Regulation Knowledge Tree

Version 1.0
31st October 2019
https://www.cybok.org/
COPYRIGHT

© Crown Copyright, The National Cyber Security Centre 2019. This information is licensed under the Open Government Licence v3.0. To view this licence, visit:

https://www.nationalarchives.gov.uk/doc/open-government-licence/ OGL

When you use this information under the Open Government Licence, you should include the following attribution: CyBOK Version 1.0 © Crown Copyright, The National Cyber Security Centre 2019, licensed under the Open Government Licence: https://www.nationalarchives.gov.uk/doc/open-government-licence/.

The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at contact@cybok.org to let the project know how they are using CyBOK.
The Cyber Security Body Of Knowledge

www.cybok.org

introductory principles of legal research
jurisdiction
privacy laws in general and electronic interception
data protection
computer crime
contract
intellectual property
internet intermediaries
dematerialisation of documents and electronic trust services
other regulatory matters
public international law
ethics

nature of law and legal analysis
applying law to cyberspace and information technologies
criminal law
civil law
liability and courts
evidence and proof
holistic approaches to legal risk analysis
legal terminology

prescriptive jurisdiction
enforcement jurisdiction
data sovereignty
prescriptive jurisdiction over online content
prescriptive jurisdiction over computer crime
prescriptive jurisdiction and data protection
GDPR
asset seizure and forfeiture
territorial location of the right to demand repayment of bank deposits
foreign recognition and enforcement of civil judgments
arrest of natural persons in state territory
extradition of natural persons
technological content filtering
orders to in-state persons directing production of data under their control whether held on domestic or foreign IT systems
international legal assistance
seizure and forfeiture of servers domain names and registries
international norms
interception by a state
interception by persons other than states
enforcement of privacy laws
metadata
human rights

subject matter and regulatory focus
core regulatory principles
investigation and prevention of crime
personal data breach notification
enforcement and penalties
data subject, personal data (and PII)
processing
controller and processor
definitions
dea-anonymisation
transfers pursuant to international mutual legal assistance treaty
derogations allowing transfers

crimes against information systems
de minimis exceptions to crimes against information systems
the enforcement of and penalties for crimes against information systems
warranted state activity
research and development activities conducted by non-state persons
self-help disfavoured: software locks and hack-back
improper access to a system
improper interference with data
improper interference with systems
improper interception of communication
undisclosed software locks
hack-back

online contracts
encouraging security standards via contract
parties and their exclusion
limitations of liability and exclusions of liability
breach of contract and remedies
effects of contract on non-contracting parties
conflict of law -- contracts
time of contract and receipt of contractual communication
supply chain
closed trading and payment systems
freedom of contract and its limitations
understanding intellectual property
catalogue of intellectual property rights
enforcement -- remedies
reverse engineering
international treatment and conflict of law
copyright
patents
trademarks
trade secrets
criminal liability
civil liability
circumventing copyright technological protection measures
testing a proprietary cryptographic algorithm
shields from liability
take-down procedures
admission into evidence of electronic documents
requirements of form and the threat of unenforceability
electronic signatures and identity trust services
conflict of law -- electronic signatures and trust services
industry-specific regulations
restrictions on exporting security technologies
matters classified as secret by a state
NIS directive
attributing action to a state under international law
state cyber operations in general
cyber espionage in peacetime
cross-border criminal investigation
the law of armed conflict
obligations owed to a client
codes of conduct
vulnerability testing
vulnerability disclosure
facilitating and acting on vulnerability disclosure