

1. Record Nr.	UNINA9910819585203321
Autore	Room Stewart
Titolo	Data protection and compliance // Stewart Room
Pubbl/distr/stampa	Swindon : , : BCS Learning & Development Limited, , 2021 ©2021
ISBN	1-78017-526-4
Edizione	[2nd ed.]
Descrizione fisica	1 online resource (543 pages) : illustrations
Altri autori (Persone)	RoomStewart Maher O'BrienNiall PanagiotopoulosAdam NahidShervin HallRichard ThuraisingamTughan Drury-SmithJames DavisSimon
Disciplina	342.4
Soggetti	Data protection - Law and legislation - Great Britain Privacy, Right of - Great Britain Records - Law and legislation - Great Britain
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Front Cover -- Half-Title Page -- BCS, THE CHARTERED INSTITUTE FOR IT -- Title Page -- Copyright Page -- Contents -- List of figures and tables -- Contributors -- Copyright notices -- Abbreviations -- Preface -- PART I THE BIG PICTURE -- 1. INTRODUCTION TO DATA PROTECTION -- What is data protection? -- Does data protection mean privacy? -- What is privacy? -- Are there exceptions to the right to privacy? -- What else should be protected? -- Protecting fundamental rights and freedoms ('human rights') -- Protecting the free movement of personal data (data flows, transfers and shares) -- The protected activities -- Protecting processing -- Protecting personal data undergoing processing -- Special category data (or 'sensitive personal data') -- Thematic priorities of data protection, trends and hot topics -

supporting a risk-based approach -- AdTech and cookies -- Advanced technology and data processing techniques -- Advanced surveillance -- Artificial intelligence -- Automated facial recognition -- Connected vehicles -- Children -- Cybersecurity -- Data subject rights - timetable breaches -- Democracy -- HR problems -- International transfers -- Privacy and electronic communications ('ePrivacy') -- Profiling -- Virtual voice assistants -- Core law -- The UK Data Protection Act and its relationship to the GDPR and other EU law -- The Data Protection Convention -- Regulatory guidance and decisions -- Court judgments -- Related law -- Data protection penalties and litigation -- The regulatory bear market -- Summary -- 2. INTRODUCTION TO THE GDPR -- Brexit: the impacts for data protection and the impacts for this book -- The land mass in Europe to which the GDPR applies -- Recitals and articles of the GDPR -- Jurisdiction of the GDPR -- Nationality and location of people -- A.3.1 - processing in the context of EU establishments.

A.3.2 - targeting people in the EU -- Material scope of the GDPR -- The building blocks of the GDPR -- The actors -- Compliance framework - the standards of protection -- Data protection principles -- Lawful bases of processing -- Necessity -- Consent for processing -- Compliance framework - controls -- Appropriate technical and organisational measures -- Appropriate safeguards -- Prescribed controls -- Anonymisation and pseudonymisation -- Accountability -- Assessing appropriateness of controls -- Critical outcomes to be achieved -- Transparency -- Clarity of the lawful basis of processing -- Control -- Compensatory mechanisms to remedy non-compliance -- Regulator's enforcement powers -- Data subjects' enforcement powers -- Where the GDPR does not apply - exceptions and restrictions -- Domestic processing -- Restrictions and the UK DPA -- Brexit - the UK, Frozen and EU GDPR -- UK GDPR -- Frozen GDPR -- Brexit - international transfers of data -- Summary -- 3.

INTRODUCTION TO EPRIVACY -- Regulating the electronic communications sector -- The relationship between data protection and ePrivacy -- The actors and protected parties -- Confidentiality of communications -- Exceptions to confidentiality -- Consent for storing or accessing information in terminal equipment -- Consent, transparency and the use of cookie notices and consent tools -- Types of cookies -- Cookies, behavioural advertising and real-time bidding -- Cookies and legal risk -- Direct marketing -- The position under PECR -- Postal direct marketing -- Opt-out, as a matter of law -- Financial penalties for direct marketing contraventions -- Processing of traffic data, location data and value added services -- Security and personal data breach notification -- Personal data breaches -- Expanded rules for breach notifications -- Interplay with the breach notification rules in the GDPR.

Calling line ID and directories of subscribers -- Law reform underway -- Summary -- 4. INTRODUCTION TO OPERATIONAL DATA PROTECTION -- Operational adequacy schemes - implementing data protection (operationalisation) -- Focus on operational adequacy schemes -- The three layers of an organisation -- Implementing data protection in the people layer -- Governance structures -- Steering committee -- Recruitment and onboarding -- Education and training -- Access rights and privileges -- Monitoring -- Worker discipline -- Flowing requirements to data processors -- Implementing data protection in the paper layer -- Data Protection by Design and Default (DPbDD, or PbD) -- Governance structures -- Records of processing activities -- Risk registers and assessment tools and methodologies -- Legitimate interests assessments -- Transfer assessments --

Transparency notices -- Contracts and similar documents -- Policies, procedures and controls frameworks -- Records of significant events -- Programme and project plans -- Technology architecture -- Assurance records -- Other mechanisms for assurance -- Implementing data protection in the technology and data layer -- Privacy Enhancing Technologies -- Regulatory sandboxes -- 'The Journey to Code' -- Risk management - implementing measures to assess risks to rights and freedoms and the appropriateness of controls -- The adequacy test -- The impact of the 'consensus of professional opinion' - what are the risks and what should be done about them? -- Risk management - dealing with adverse scrutiny -- Globalisation - implementing data protection on an international stage -- International transfers - adequacy, appropriate safeguards and derogations -- Meaning of 'adequacy' for the purposes of international transfers -- Adequacy of the UK -- Appropriate safeguards -- Derogations. Wider operational challenges of international activities -- Impacts for micro, small and medium-sized enterprises -- Size of enterprise and size of risk -- Financial resources, cost and risk -- Security and connection to wider legal and operational frameworks -- Summary -- PART II CORE LAW -- 5. THE PRINCIPLES OF DATA PROTECTION -- A constant presence in data protection law -- The duty of compliance (accountability) -- Lawfulness, fairness and transparency - the first principle -- Lawfulness -- Fairness -- Transparency -- Purpose limitation - the second principle -- Expanded purposes - archiving in the public interest -- Expanded purposes - scientific and historical research -- Expanded purposes - statistics -- Compatibility -- Data minimisation - the third principle -- Accuracy - the fourth principle -- Storage limitation - the fifth principle -- Integrity and confidentiality (including security) - the sixth principle -- Accountability - the seventh principle -- Lawfulness of processing of personal data (Article 6) -- Categorising the lawful bases of processing -- Consent -- Contract -- Legal obligation -- Vital interests -- Public task -- Legitimate interests -- Lawfulness of processing - special category personal data and criminal convictions and offences -- The ban on processing special category personal data - enhanced sensitivity, risks and legal requirement -- Summary -- 6. THE RIGHTS OF DATA SUBJECTS -- Informing and empowering the protected party -- Transparency and information rights -- General obligation of transparency - GDPR A. -- Obtaining transparency - GDPR A.13 and -- The right of access to information - A. -- Personal data breaches - Article -- Rights over data processing -- Right to rectification - A. -- Right to erasure, or 'the right to be forgotten' - A. -- Right to restriction of processing - A. -- Right to data portability - A. -- Right to object - A. -- Right not to be subject to automated decision making, including profiling - A. -- Remedies and rights of redress -- Summary -- PART III OPERATING INTERNATIONALLY -- 7. NATIONAL SUPERVISION WITHIN AN INTERNATIONAL FRAMEWORK -- National regulatory systems and divergences -- GDPR solution for international processing -- Establishment of supervisory authorities -- General conditions for members of supervisory authorities -- Independence -- Interference -- Supervisory authority competence -- Member competence -- Tasks -- Monitoring -- Promotion and awareness -- Advice and administration -- Rights, complaints and enforcement -- Powers -- Lead supervisory authorities -- Cross-border processing -- Cooperation and mutual assistance -- Choosing a lead supervisory authority -- Appointing an EU Representative -- Summary -- 8. TRANSFERRING DATA BETWEEN THE GDPR LAND MASS AND THIRD COUNTRIES -- Why regulate international transfers? -- What is a transfer? -- General principles for

transfers -- Transfers on the basis of an adequacy decision -- Elements considered in assessing adequacy -- Adequacy decisions issued -- UK adequacy -- Partial adequacy decisions -- Ongoing monitoring of adequacy decisions -- Transfers subject to appropriate safeguards -- Standard contractual clauses -- Derogations for specific situations -- Relying on the derogations in practice -- Compelling legitimate interests -- Litigation on international data transfers -- Schrems I - Safe Harbor decision declared invalid -- Schrems II - Privacy Shield declared invalid and SCCs declared valid subject to certain conditions -- Navigating international data transfers -- EDPB's six-step recommendations -- Supplementary measures -- A practical approach to international transfers -- Getting to know your 'special characteristics' -- Understanding the 'zone of precedent'.

---

**Sommario/riassunto**

This comprehensive guide for those with little or no legal knowledge provides detailed analysis of current data protection laws. It enables the reader to operationalise a truly risk-based approach to data protection and compliance, beyond just emphasis on regulatory frameworks and legalistic compliance.

---