scripted

Volume 22, Issue 1, September 2025

Book Review: *Data Protection, Privacy and Information Law: A Practical Guide*

Leo Davidson, John Fitzsimons and Ben Mitchell
The Law Society 2024. 306 pages.
ISBN 9781784461898. £110.
Available as paperback or e-book.

*Reviewed by Daniela Bincheva**

DOI: 10.2966/scrip.220125.110

* LL.M.; PhD Candidate at the European University Viadrina Frankfurt (Oder) and Assessor at GSK STOCKMANN, Daniela.bincheva@gsk.de.

'The world's most valuable resource is no longer oil, but data'

In this now classic phrase, *The Economist* captured a defining reality of the digital age.[1] Yet unlike oil, data is not finite, tangible, or buried deep in select geographic locations— it is omnipresent, generated with every online search, tap of a contactless card, or use of a smart device. It can be both personal and endlessly replicable, flowing invisibly across sectors and borders. And while oil reshaped geopolitics, data now reshapes law — resulting in rules that are increasingly complex and fragmented.

Against this backdrop of constant data flows, technological innovation, and regulatory flux — particularly in the UK's post-Brexit legal landscape — Leo Davidson, John Fritzsimons and Ben Mitchell provide a — one could argue — brief but comprehensive and highly structured account of UK data protection, privacy and information law. Their work unfolds across six parts and deftly navigates the intricate interplay between the UK General Data Protection Regulation (UK GDPR), the Data Protection Act (DPA) 2018, and the broad constellation of further legislation, including the Online Safety Act (OSA) 2023, the Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003, and freedom of information statutes.

What characterises this work is not merely its breadth (remarkable given its concise length of 250 pages), but its clarity of structure and commitment to practical relevance. The authors avoid the trap of abstraction, grounding their analysis in real-life duties, enforcement practice and authoritative regulatory guidance. The result is a legal map that guides the reader not only through the current law but also through its consequences — essential reading for

[1] The Economist, 'The world's most valuable resource is no longer oil, but data' (6 May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 19 May 2025.

practitioners seeking orientation in one of the most dynamic areas of contemporary law.

The present book review engages thoroughly with the main contents and key messages conveyed by the book. The first six sections follow its six parts, examining how the authors address core concepts, key rights and obligations, institutional structures, sectoral rules, and enforcement mechanisms. Each section draws attention to particularly insightful clarifications or practical contributions. The final section concludes with a brief assessment of the book's overall contribution.

1. Part I: Introduction

The opening chapter in Part I lays out the structure and scope of the book and provides a thoughtfully composed introduction to the work as a whole: The book does not attempt an encyclopaedic overview; instead, it focuses on the issues most likely to be encountered in practice, and the pitfalls most commonly misunderstood. Acknowledging the fast-moving nature of this legal terrain, the authors aim for a guide that is as accurate as possible up to November 2024, while pointing out cases where decisions are known to be subject to a pending appeal, or where proposed amendments to legislation are under consideration.

2. Part II: Data Protection

This part is the most extensive one, covering Chapters 2 to 8.

2.1. Chapter 2: Overview of the UK GDPR and the Data Protection Act 2018

The second chapter offers a robust overview of the UK GDPR and the DPA 2018, tracing their origins and interplay. The authors provide a brief but helpful historical retrospective, addressing the UK's exit from the EU and the

consequences for domestic data law. The reader is guided through the structure of the UK's post-Brexit data protection regime, including the relationship between UK GDPR and DPA 2018.

The concept of "adequacy" is lucidly explained, with the UK's approach to cross-border data transfers and current adequacy decisions clearly outlined. The chapter concludes by exploring proposed legislative reforms — offering readers a forward-looking sense of the evolving regulatory environment.

2.2. Chapter 3: Key terms, definitions and scope

This foundational chapter clarifies core definitions and principles that recur throughout the book. Key terms such as *personal data*, *processing*, *data subject*, *controller*, and *processor* are explained with reference to recitals, case law and current ICO guidance. Of particular value is the discussion on the distinction between anonymisation and pseudonymisation.

The chapter also provides a well-structured account of both the material and territorial scope of the UK GDPR. It draws attention to important nuances — for instance, related to manual unstructured processing, processing by FOI public authorities, and the interpretation of 'inextricable link' in territorial scope analysis. The authors aptly weave in relevant CJEU and UK case law, as well as EDPB guidance, making this section an essential resource for practitioners seeking precise insight.

2.3. Chapter 4: Obligations on controllers and processors

In Chapter 4, the authors shift the focus to the architecture of responsibility underpinning the UK GDPR. This chapter outlines the obligations imposed on controllers, joint controllers, and processors — roles that are distinct yet interconnected.

Controllers remain the fulcrum of data protection obligations, and the authors unpack the six core principles of UK GDPR, art. 5 with an eye for both legal accuracy and practical relevance. Starting with the triad of lawfulness, fairness and transparency, they explore the conceptual and practical contours of 'lawful basis' under the UK GDPR.

This leads to an exploration of the lawful bases for processing under UK GDPR, art. 6(1). Particularly well-handled is the analysis of the consent under UK GDPR, art. 6(1)(a), with due attention to the often-contested criterion of 'freely given' — especially in contexts marked by power imbalances. Here, the authors unpack the ICO's guidance and highlight common pitfalls (e.g. bundling consent or making access to services conditional upon it).

Other lawful bases — necessity for the performance of the contract, legal obligation, vital interests, public interest task — are also explained clearly and efficiently. Notably, the treatment of legitimate interests (UK GDPR, art. 6(1)(f)) is framed through the 'three-stage test' (legitimate interest, necessity, balance), supported by examples relevant to practitioners. Special categories of data (UK GDPR, art. 9) receive similarly focused attention, with the authors emphasising the heightened sensitivity of such data. The commentary on criminal offence data (UK GDPR, art. 10) is clear and practical, noting the need for both a lawful basis and legal or official authority under DPA 2018.

The transparency obligations (UK GDPR, arts. 13–14) are also well-handled, with emphasis on the content of privacy notices (or fair processing notices).

Similarly, other principles—purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and the overarching principle of accountability—are discussed in a balanced and pragmatic way, with references to both case law and regulatory guidance.

The coverage of the obligations relating to the record of processing activities (UK GDPR, art. 30), data protection by design and default (UK GDPR, art. 25), data protection impact assessments (UK GDPR, art. 35) and data protection officers (UK GDPR, arts. 37–39) is equally robust. Each obligation is outlined with reference to thresholds, content, and good practice.

UK GDPR, art. 26 introduces the concept of joint controllership. Here, the authors keep their analysis focused, rightly emphasising the practical importance of a clear and transparent arrangement between the joint controllers.

The final section addresses processors, whose obligations under the UK GDPR are indeed extensive. The authors elucidate these systematically, with precise citations to the pertinent legal provisions.

What emerges from Chapter 4 is an accessible portrait of a system that demands clear role allocation, procedural discipline, and a strong culture of accountability — all of which are convincingly conveyed in this chapter.

2.4. Chapter 5: Rights of data subjects

In Chapter 5, attention is shifted to the rights of the individual — arguably the ethical nucleus of the data protection framework.

The authors provide a comprehensive and structured exposition of the seven core rights set out in the UK GDPR: access, rectification, erasure, restriction of processing, data portability, objection, and the right not to be subject solely to automated decision-making.

The analysis of the right of access (UK GDPR, art. 15), whose exercise often gives rise to significant practical challenges for controllers, is a standout. The authors stress its 'purpose-blind' nature while underscoring the real risks of inadvertent breaches, particularly in contexts involving third-party or mixed data. The lack of prescriptive detail in the UK GDPR concerning search scope and

methods is insightfully addressed, with the discussion enriched by overall practical guidance.

The chapter concludes by addressing several additional rights that serve to complement the core bundle, namely the right to be informed, to complain to the supervisory authority, to compensation, and to judicial remedy.

2.5. Chapter 6: Exemptions and derogations

Chapter 6 introduces another practically significant dimension of UK data protection law: the circumstances under which rights and obligations may be limited.

The authors begin with UK GDPR, art. 23, the legal anchor for exemptions enacted under national law. The chapter walks through how these exemptions are given effect in the DPA 2018, noting that their application typically requires nuanced, case-specific assessment. The discussion proceeds to derogations which are explored in light of the relevant UK GDPR provisions.

The focus is not on listing every exemption and derogation, but rather on cultivating an understanding of their underlying logic. Nevertheless, the authors identify commonly relied-upon exemptions and derogations and illustrate their application.

2.6. Chapter 7: Breaches and powers of the Commissioner to take regulatory action

A chapter that many readers will consult in crisis, the first section of which („Personal data breaches“) is a procedural lifeline for breach management.

The authors start with the definition of a personal data breach (UK GDPR, art. 4(12)) before walking through notification obligations (UK GDPR, art. 33): when must a breach be reported, how quickly, and with what content. The trigger point of controller awareness is particularly well explained. UK GDPR, art. 34

duties to notify individuals are clearly summarised, including exceptions, and the processor's role is woven throughout.

The chapter then shifts to the regulatory toolbox available to the ICO. These powers may be exercised on the Commissioner's own initiative or upon complaint, and are structured into investigative, corrective, and authorisation/advisory categories. Investigative powers include information and assessment notices, as well as powers of entry and inspection. The section on corrective powers is particularly instructive, commenting on enforcement notices, and providing a detailed treatment of monetary penalty notices, including the factors considered by the ICO, the statutory limits, and the relevance of the Commissioner's Guidance. Finally, the authors address the Commissioner's authorisation and advisory powers under the UK GDPR, completing a well-rounded overview of regulatory mechanisms.

2.7. Chapter 8: Privacy and electronic communication regulations

In the final chapter of Part I, the authors address a somewhat underappreciated but powerful piece of UK data protection law: the PECR 2003. While often overshadowed by the UK GDPR, PECR 2003 imposes sector-specific rules relating to public electronic communication services, including telephone calls, emails, and faxes.

The authors once again demonstrate their commitment to prioritising practical relevance by focusing on the regulatory framework for direct marketing. The conditions for lawful direct marketing are set out in detail, following a thorough discussion which carefully distinguishes direct marketing from other forms of communication, even including references to practices such as 'sugging'.

Finally, the authors address PECR 2003's security and data breach provisions, additional user rights, and its enforcement regime, which includes regulatory action by the ICO and civil litigation by individuals.

3. Part III: Misuse of private information and breach of confidence

3.1. Chapter 9: What is private information

Serving as a bridge to Chapter 10, this chapter unpacks the concept of 'private information'. It introduces the test of a 'reasonable expectation of privacy', referring to the Murray factors as helpful signposts. Through a comprehensive examination of case law and illustrative examples, the authors provide a detailed insight into where the boundaries of privacy lie.

3.2. Chapter 10: Misuse of private information

In Chapter 10, the authors present a clear and structured account of the tort of misuse of private information. They highlight that the tort requires a positive act by the defendant — unlike UK GDPR claims, which can arise from omissions — and that a threshold of seriousness must be met, a requirement courts are applying with increasing emphasis. Although outcomes are highly fact-specific, the authors provide readers with a framework for understanding how courts assess reasonable expectations of privacy and weigh these against justifications, typically involving competing rights such as freedom of expression under ECHR, art. 10. The discussion of this balancing exercise offers valuable insight into how the courts navigate these tensions in practice.

3.3. Chapter 11: Breach of confidence and breach of ECHR, article 8

Chapter 11 outlines the continuing relevance of the equitable action for breach of

confidence. While claims for breach of confidence often overlap with data protection and misuse of private information where the information at issue is personal, the authors highlight that breach of confidence retains an important and broader function. It remains a key legal tool for protecting confidential material that has no connection to an individual — such as commercial or technical information. The chapter clearly sets out the key elements of the cause of action, including the necessary quality of confidence, the circumstances giving rise to a duty of confidence, and the misuse or unauthorised use of the information. It also considers the defences available to defendants and the limits of the action's applicability to private information in light of more modern legal developments.

In addition, the chapter examines the 'vertical' dimension of privacy protection — namely, the use of ECHR, art. 8, as incorporated through the Human Rights Act (HRA) 1998, as a standalone basis for claims against public bodies. This includes a discussion of the scope of ECHR, art. 8, and how courts assess interference and its justification. Finally, the authors provide an overview of the remedies available for claims in this area, spanning misuse of private information, breach of confidence, and claims under HRA 1998, while referring to further details in Chapter 16.

4. Part IV: Freedom of information

4.1. Chapter 12: Access to information: Freedom of Information Act 2000

As the book pivots to public access to information, the Freedom of Information Act (FOIA) 2000 is placed front and centre. The chapter begins with a clear explanation of the role, structure and terminology of the FOIA 2000 before turning to the practical requirements of making a request. It outlines who is

entitled to request information, which public authorities are subject to its obligations, and what types of information may be requested. Detailed guidance is provided on how requests must be made and how public authorities should respond, including time limits and procedural rules.

A particularly thorough part of the chapter concerns the exemptions under FOIA 2000 — situations in which public authorities may withhold information. These are analysed in detail, with attention to the distinction between absolute exemptions and those subject to a public interest test. The authors offer careful commentary on how courts and the Information Commissioner interpret and apply these exemptions, underscoring the importance of balancing transparency with competing interests such as national security, defence, or health and safety.

4.2. Chapter 13: Access to information: other

This chapter examines three important access regimes that operate alongside the FOIA 2000, each with a distinct legal basis and scope: access to environmental information, access to court and tribunal documents, and public access under the Local Audit and Accountability Act (LAAA) 2014.

The Environmental Information Regulations (EIR) 2004 implement international and EU law obligations flowing from the Council Directive 2003/4/EC, and lastly the Aarhus Convention on Access to Information, Public Participation in Decision Making and Access to Justice in Environmental Matters. Now part of 'assimilated law' post-Brexit, EIR 2004 remain governed by principles that reflect their international roots. They offer a standalone access regime for environmental information, with a broader definition of 'public authority' than FOIA 2000 and a wide conception of 'environmental information', which the authors carefully examine. The chapter also details the regime's exceptions.

Access to information held by courts and tribunals is not governed by FOIA 2000 or EIR 2004, but is instead grounded in the principle of open justice and applicable procedure rules. The chapter clarifies which rules govern access to documents in civil litigation, and under what circumstances derogations from the principle of openness may be justified. The discussion highlights how courts balance transparency with privacy, confidentiality, or fair trial rights.

Lastly, the chapter outlines the LAAA 2014: The regime imposes requirements on local and some other public authorities regarding the preparation, maintenance, and audit of accounts. The authors describe how this access right functions within a system of local democratic accountability.

5. Part V: Data protection and access to information in context

5.1. Chapter 14: Other considerations: confidentiality, privilege, disclosure, defamation and the Online Safety Act 2023

In this expansive chapter, the authors explore a range of (regulatory) developments that intersect with, but extend beyond, the traditional boundaries of privacy law. Each topic is treated with just enough depth to equip readers with working knowledge, while signposting points of crossover with more specialised areas.

The discussion on confidentiality begins with a concise yet enlightening overview of how confidentiality is protected. It then moves on to provide practical illustrations of confidentiality clauses and best practices, which will be welcomed both by in-house counsel and lawyers dealing with this area of law.

Next, the chapter explores various forms of legal privilege, paying particular attention to legal professional privilege, but also touching on joint privilege, common interest privilege and without prejudice privilege.

As the title of the book suggests, the section on disclosure obligations focuses on two questions: how personal data and private information contained within disclosable documents should be handled, and the prohibition on the collateral use of disclosed information. Appropriate reference is also made to the duty of candour here.

The defamation segment is brief but serviceable: The authors provide a clear and concise overview of defamation as a private law cause of action, tracing its development from common law origins to its modern statutory form under the Defamation Acts of 1996 and 2013. They outline the essential elements of a defamation claim, clarify legal definitions, and explain the distinction between libel and slander. Furthermore, they set out the principal defences available to defendants and summarise the four key remedies, offering a practical and accessible introduction to this area.

The chapter concludes with a topical overview of the Online Safety Act (OSA) 2023. The authors set out the main features of the OSA 2023, noting its parallels with the EU's Digital Services Act. The discussion effectively highlights the OSA 2023's conceptual shift: away from a purely harm-based model to one rooted in duties of care. Additional obligations for larger services, which the Act divides into three categories, as well as the enforcement regime are also covered.

6. Part VI: Appeals, remedies and regulatory enforcement

6.1. Chapter 15: Introduction to the enforcement of information law

In this introductory chapter to Part VI, the authors turn to the enforcement of information law, outlining the legal mechanisms available to address and remedy breaches. They emphasise that the rights and obligations explored throughout the book gain practical significance only through effective enforcement, setting the stage for the last two chapters.

6.2. Chapter 16: Civil courts — a practical guide

The chapter opens with a compact overview of the Civil Procedure Rules, before drilling down into those procedural aspects most pertinent to privacy claims. Venue allocation between the High Court and County Court is explained with reference to claim type and value. The authors then detail the four tracks (small claims, fast, intermediate, multi-track) and how assignment decisions are made.

Particularly valuable is also the section on abusive and unmeritorious claims — including the mechanisms of strike-out, summary judgment, and civil restraint orders. The commentary on SLAPPs (Strategic Litigation Against Public Participation) is especially timely, reflecting a growing concern among courts and legislators alike.

The following section on case management reveals the authors' fluency with litigation strategy.

The treatment of remedies is thorough: from damages and injunctions to compliance orders and declarations/statements in court. Costs, as ever, are a focal point — and the authors provide a digestible account of current trends and judicial discretion in cost assessments.

The chapter rounds off with a concise overview of judicial review as a means of challenging acts or omissions of the Information Commissioner or other public authorities with a privacy or data protection angle; it also outlines the appeals process, offering guidance on time limits and the requirement for permission to appeal.

6.3. Chapter 17: The tribunals - a procedural overview

The last chapter explores the role played by the First-tier and Upper Tribunals in adjudicating disputes central to the book's subject matter. The authors outline the First-tier Tribunal's full merits jurisdiction over matters such as decision notices issued under the FOIA 2000 and EIR 2004, explaining who may appeal

and under what conditions a claim may be struck out.

The procedural framework is clearly set out, including the handling of open and closed proceedings and the limited circumstances in which the principle of open justice may be derogated from. The chapter also examines the tribunal's powers to enforce decisions and review regulatory notices, such as enforcement and penalty notices issued by the Information Commissioner. Finally, the authors explain the route of appeal to the Upper Tribunal, which is confined to errors of law, and discuss the conditions under which permission to appeal is granted.

7. Conclusion

Undoubtedly, a work spanning just 250 pages cannot aim to exhaustively cover every aspect of data protection, privacy, and information law — nor do the authors claim to do so. Rather, their goal is more pragmatic and arguably more valuable: to equip readers with a solid foundational understanding of the UK data protection, privacy and information law, and to provide a practical guide for navigating its most critical and frequently encountered issues. By striking a balance between clear structure, precise language, and a consistent focus on real-world applicability, the authors succeed in making a dense and evolving field remarkably accessible. As such, this book serves not only as an entry point for newcomers but also as a dependable reference for practitioners working at the intersection of data and law.