# Accountability Obligations Under The Gdpr

This book contains selected papers presented at the 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School on Privacy and Identity Management, held in Ispra, Italy, in September 2017. The 12 revised full papers, 5 invited papers and 4 workshop papers included in this volume were carefully selected from a total of 48 submissions and were subject to a three-phase review process. The papers combine interdisciplinary approaches to bring together a host of perspectives: technical, legal, regulatory, socio-economic, social, societal, political, ethical, anthropological, philosophical, and psychological. They are organized in the following topical sections: privacy engineering; privacy in the era of the smart revolution; improving privacy and security in the era of smart environments; safeguarding personal data and mitigating risks; assistive robots; and mobility and privacy.

Part I Setting the scene -- Introduction: Individual rights, the public interest and biobank research 4000 (8) -- Genetic data and privacy protection -- Part II GDPR and European responses -- Biobank governance and the impact of the GDPR on the regulation of biobank research -- Controller' and processor's responsibilities in biobank research under GDPR -- Individual rights in biobank research under GDPR -- Safeguards and derogations relating to processing for archiving purposes in the scientific purposes: Article 89 analysis for biobank research -- A Pan-European analysis of Article 89 implementation and national biobank research regulations -- EEA, Switzerland analysis of GDPR requirements and national biobank research regulations -- Part III National insights in biobank regulatory frameworks -- Selected 10-15 countries for reports: Germany -- Greece -- France -- Finland -- Sweden -- United Kingdom -- Part IV Conclusions -- Reflections on individual rights, the public interest and biobank research, ramifications and ways forward. .

This book presents high-quality research on the concepts and developments in the field of information and communication technologies, and their applications. It features 134 rigorously selected papers (including 10 poster papers) from the Future of Information and Communication Conference 2020 (FICC 2020), held in San Francisco, USA, from March 5 to 6, 2020, addressing state-of-the-art intelligent methods and techniques for solving real-world problems along with a vision of future research Discussing various aspects of communication, data science, ambient intelligence, networking, computing, security and Internet of Things, the book offers researchers, scientists, industrial engineers and students valuable insights into the current research and next generation information science and communication technologies.

This book explores links and synergies between international trade and two of the most urgent challenges of the 21st century: achieving sustainable energy (i.e., energy that is affordable, secure, and clean) and mitigating climate change. It takes the unique approach of not only examining how international trade can help achieve energy and climate goals, but also the impact of emerging tools and technologies such as smart grids and demand response, and the potential role and impact of citizens and prosumers. The book analyzes energy- and trade-related regulations in a range of jurisdictions to assess how conducive the regulation is towards achieving sustainable energy, and identifies gaps and overlaps in the existing legal framework.

In order to ensure a consistent and high level of protection of the rights and freedoms of natural persons with regard to the processing of such data and to remove the obstacles to flows of personal data in all Member States of the EU, the “General Data Protection Regulation (GDPR)” was adopted in 2016. Today, the GDPR is the main legislation in the EU for the protection of personal data of the natural persons. Due to the increased value of personal data in EU Member States, the objective of the GDPR is to provide high level protection of the data while harmonizing data protection within the EU. Even though it aims at a high level of data protection, it is questionable whether it actually achieves this objective. Since the natural persons provide their personal data on Internet frequently in order to purchase a product, the protection of consumers’ personal data is a significant matter in practice. In order to throw light on this matter, this thesis inquires the protection of consumers’ data in the EU regarding electronic contracts with businesses. Within the context, the main point that is discussed in this work is whether the personal data protection provided under the GDPR is sufficient to protect consumers' data regarding electronic contracts with businesses and some possible solutions and proposals to reduce the deficiencies of the GDPR protection.

In the age of technological advancement, including the emergence of artificial intelligence, big data, and the internet of things, the need for privacy and protection has risen massively. This phenomenon has led to the enforcement of two major legal directives in the European Union (EU) that aim to provide vigorous protection of personal data. There is a need for research on the repercussions and developments that have materialized with these recent regulations and how the rest of the world has been affected. Personal Data Protection and Legal Developments in the European Union is an essential reference source that critically discusses different aspects of the GDPR and the Law Enforcement Directive as well as recent jurisprudential developments concerning data privacy in the EU and its member states. It also addresses relevant recent case law of the Court of Justice of the EU, the European Court of Human Rights, and national courts. Featuring research on topics such as public transparency, medical research data, and automated decision making, this book is ideally designed for law practitioners, data scientists, policymakers, IT professionals, politicians, researchers, analysts, academicians, and students working in the areas of privacy, data protection, big data, information technology, and human rights law.

The General Data Protection Regulation (EU) 679/2016 (‘GDPR’)1 will be, as of 25 May 2018, the main data protection legal framework in the EU directly applicable in all Member States, repealing the Data Protection Directive 95/46/EC. The Regulation provides for a harmonization of the legal data protection regime throughout the EU, re-enforces

several principles and obligations of the Directive, it repeals and adds new provisions, including ones on data protection certification, seals and marks. Data protection certifications, seals and marks have the potential to play a significant role in enabling data controllers to achieve and demonstrate compliance of their processing operations with GDPR provisions. An additional function of certification, in the context of the GDPR, is to enhance transparency, since certifications, seals, and marks allow data subjects to “quickly assess the level of data protection of relevant products and services”. The objective of this report is to identify and analyse challenges and opportunities of data protection certification mechanisms, including seals and marks, as introduced by the GDPR, focusing also on existing initiatives and voluntary schemes. Certification, as a conformity assessment activity against specified requirements, is performed and attested by a third party. These requirements are derived from technical standards or legislation, as in the case of certification under GDPR, where the secondary EU legislation provides the normative framework as a basis for the assessment requirements. The outcome of a successful certification (process) is a certificate (thus a document), and/or a seal, that attests that the applicant organisation meets the requirements (substantive and procedural) specified in the certification scheme, and provided in technical standards or legislation. In the near future, it is also possible that such requirements, originating from GDPR provisions, are also provided in technical standards. Certification can be mandatory, when a relevant obligation for certification is established in legislation or voluntary when such obligation is not legally imposed, as in the case of GDPR certifications, which rely on the decision of a data controller or a processor to submit oneself to the certification procedure. Certification, under GDPR, is well linked to the newly introduced principle of accountability and appears to be limited to substantive requirements related only to GDPR provisions, must concern specific processing operations and can only be pursued only by data controllers or data processors, as they perform the personal data processing.

Going Digital in Latvia analyses recent developments in Latvia’s digital economy, reviews policies related to digitalisation and make recommendations to increase policy coherence in this area, based on the OECD Going Digital Integrated Policy Framework.

Are you planning to move from projects to products? Do you relish listening to your customers? Does the curiosity urge the creativity in you to solve real-world problems? Are you a number lover? If your reaction is yes, then it is a must-read for you. Get involve, delight, and excite about the entire journey of envisaging, creating, and managing a successful customer-oriented and value propositional product.

This book analyses the legal approach to personal data taken by different fields of law. An increasing number of business models in the digital economy rely on personal data as a key input. In exchange for sharing their data, online users benefit from personalized and innovative services. But companies’ collection and use of personal data raise questions about privacy and fundamental rights. Moreover, given the substantial commercial and strategic value of personal data, their accumulation, control and use may raise competition concerns and negatively affect consumers. To establish a legal framework that ensures an adequate level of protection of personal data while at the same time providing an open and level playing field for businesses to develop innovative data-based services is a challenging task.With this objective in mind and against the background of the uniform rules set by the EU General Data Protection Regulation, the contributions to this book examine the significance and legal treatment of personal data in competition law, consumer protection law, general civil law and intellectual property law. Instead of providing an isolated analysis of the different areas of law, the book focuses on both synergies and tensions between the different legal fields, exploring potential ways to develop an integrated legal approach to personal data.

This book provides a comparison and practical guide for academics, students, and the business community of the current data protection laws in selected Asia Pacific countries (Australia, India, Indonesia, Japan Malaysia, Singapore, Thailand) and the European Union. The book shows how over the past three decades the range of economic, political, and social activities that have moved to the internet has increased significantly. This technological transformation has resulted in the collection of personal data, its use and storage across international boundaries at a rate that governments have been unable to keep pace. The book highlights challenges and potential solutions related to data protection issues arising from cross-border problems in which personal data is being considered as intellectual property, within transnational contracts and in anti-trust law. The book also discusses the emerging challenges in protecting personal data and promoting cyber security. The book provides a deeper understanding of the legal risks and frameworks associated with data protection law for local, regional and global academics, students, businesses, industries, legal profession and individuals.

This book provides expert advice on the practical implementation of the European Union’s General Data Protection Regulation (GDPR) and systematically analyses its various provisions. Examples, tables, a checklist etc. showcase the practical consequences of the new legislation. The handbook examines the GDPR’s scope of application, the organizational and material requirements for data protection, the rights of data subjects, the role of the Supervisory Authorities, enforcement and fines under the GDPR, and national particularities. In addition, it supplies a brief outlook on the legal consequences for seminal data processing areas, such as Cloud Computing, Big Data and the Internet of Things.Adopted in 2016, the General Data Protection Regulation will come into force in May 2018. It provides for numerous new and intensified data protection obligations, as well as a significant increase in fines (up to 20 million euros). As a result, not only companies located within the European Union will have to change their approach to data security; due to the GDPR’s broad, transnational scope of application, it will affect numerous companies worldwide.

This book on privacy and data protection offers readers conceptual analysis as well as thoughtful discussion of issues, practices, and solutions. It features results of the seventh annual International Conference on Computers, Privacy, and Data Protection, CPDP 2014, held in Brussels January 2014. The book first examines profiling, a persistent core

issue of data protection and privacy. It covers the emergence of profiling technologies, on-line behavioral tracking, and the impact of profiling on fundamental rights and values. Next, the book looks at preventing privacy risks and harms through impact assessments. It contains discussions on the tools and methodologies for impact assessments as well as case studies. The book then goes on to cover the purported trade-off between privacy and security, ways to support privacy and data protection, and the controversial right to be forgotten, which offers individuals a means to oppose the often persistent digital memory of the web. Written during the process of the fundamental revision of the current EU data protection law by the Data Protection Package proposed by the European Commission, this interdisciplinary book presents both daring and prospective approaches. It will serve as an insightful resource for readers with an interest in privacy and data protection.

This practical resource provides up-to-date coverage of how to structure and negotiate profitable corporate alliances, covering both the strategic benefits and potential risks involved in these complex arrangements. In clear and straightforward language, this handbook explains the proprietary rights issues involved and then walks the reader through the chronology of a deal, from the definition of objectives to the decision to seek an alliance, identification of potential partners, negotiations, and closing. Corporate Partnering: Structuring and Negotiating Domestic and International Strategic Alliances, Fifth Edition is full of practical forms covering all aspects of strategic alliances annotated with crisp, clear commentary that explains the real-world issues addressed by each provision and how alternative solutions may be used to accomplish different aims. These carefully crafted agreements cover the broad range of areas from supply and distribution agreements, product and technology licenses, and research and development agreements to investment and investment-related arrangements. Thoroughly revised and updated to reflect the latest developments, the Fourth Edition includes new sections on Spin-Out Transactions, virtual companies, and off-shoring arrangements plus updated transaction forms, intellectual property summary, and partnering transactions checklists.

Data Protection & Privacy, edited by Wim Nauwelaerts of Hunton & William, covers many of the most important data protection and data privacy laws in force or in preparation across 29 jurisdictions. As laws governing data protection become ever more significant whilst information becomes indispensable to commercial and public life, Data Protection & Privacy will guide you through the major issues. Topics covered include: breaches of data protection, exemptions, other affecting laws, PII formats, legitimate processing, notifications, accuracy, security obligations and breaches, registration formalities, penalties, transfers and internet use and electronic communications marketing. In an easy-to-use question and answer format, this book is-depth comparative study of the topic from the perspective of leading experts featuring additional editorial chapters on the EU as well as Safe Harbor and the Privacy Shield. &quote;The comprehensive range of guides produced by GTDT provides practitioners with an extremely useful resource when seeking an overview of key areas of law and policy in practice areas or jurisdictions which they may otherwise be unfamiliar with.&quote; Gareth Webster, Centrica Energy E&P

Social networks have created a plethora of problems regarding privacy and the protection of personal data. The use of social networks has become a key concern of legal scholars, policy-makers and the operators as well as users of those social networks. This pathbreaking book highlights the importance of privacy in the context of today's new electronic communication technologies as it presents conflicting claims to protect national and international security, the freedom of the Internet and economic considerations. Using the New Haven School of Jurisprudence's intellectual framework, the author presents the applicable law on privacy and social media in international and comparative perspective, focusing on the United States, the European Union and its General Data Protection Regulation of 2018 as well as Germany, the United Kingdom and Latin America. The book appraises the law in place, discusses alternatives and presents recommendations in pursuit of a public order of human dignity.

This book provides practical, business-orientated and accessible guidance on key aspects of German employment and labour law as well as adjoining fields. This second, completely revised edition presents the latest changes in German labour and employment law and jurisprudence. It covers, amongst other newer developments, the statutory minimum wage, changes in agency work, extensive changes in European and German employee data protection law, and includes a completely new chapter on compliance issues in the employment context. Specialised lawyers with many years of experience explain the legal basis of these aspects of German law, highlight typical practical problems and suggest solutions to those problems. In addition, examples are given on how to best manage legal pitfalls to minimise risks. This book translates employment and labour law for foreign in-house counsels and human resources managers at international companies and provides a clear understanding of the complex legal regulations in Germany.

This open access volume of the AIDA Europe Research Series on Insurance Law and Regulation offers the first comprehensive legal and regulatory analysis of the Insurance Distribution Directive (IDD). The IDD came into force on 1 October 2018 and regulates the distribution of insurance products in the EU. The book examines the main changes accompanying the IDD and analyses its impact on insurance distributors, i.e., insurance intermediaries and insurance undertakings, as well as the market. Drawing on interrelations between the rules of the Directive and other fields that are relevant to the distribution of insurance products, it explores various topics related to the interpretation of the IDD - e.g. the harmonization achieved under it; its role as a benchmark for national legislators; and its interplay with other regulations and sciences - while also providing an empirical analysis of the standardised pre-contractual information document. Accordingly, the book offers a wealth of valuable insights for academics, regulators, practitioners and students who are interested in issues concerning insurance distribution.--

The growth of Blockchain technology presents a number of legal questions for lawyers, regulators and industry participants alike. Primarily, regulators must allow Blockchain technology to develop whilst also ensuring it is not being abused. This book addresses the challenges posed by various applications of Blockchain technology, such as cryptocurrencies, smart contracts and initial coin offerings, across different fields of law. Contributors explore whether the problems posed by Blockchain and its applications can

be addressed within the present legal system or whether significant rethinking is required.

This book contains selected papers presented at the 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School on Privacy and Identity Management, held in Vienna, Austria, in August 2018. The 10 full papers included in this volume were carefully reviewed and selected from 27 submissions. Also included are reviewed papers summarizing the results of workshops and tutorials that were held at the Summer School as well as papers contributed by several of the invited speakers. The papers combine interdisciplinary approaches to bring together a host of perspectives: technical, legal, regulatory, socio-economic, social, societal, political, ethical, anthropological, philosophical, historical, and psychological.

The definitive guide for ensuring data privacy and GDPR compliance Privacy regulation is increasingly rigorous around the world and has become a serious concern for senior management of companies regardless of industry, size, scope, and geographic area. The Global Data Protection Regulation (GDPR) imposes complex, elaborate, and stringent requirements for any organization or individuals conducting business in the European Union (EU) and the European Economic Area (EEA)—while also addressing the export of personal data outside of the EU and EEA. This recently-enacted law allows the imposition of fines of up to 5% of global revenue for privacy and data protection violations. Despite the massive potential for steep fines and regulatory penalties, there is a distressing lack of awareness of the GDPR within the business community. A recent survey conducted in the UK suggests that only 40% of firms are even aware of the new law and their responsibilities to maintain compliance. The Data Privacy and GDPR Handbook helps organizations strictly adhere to data privacy laws in the EU, the USA, and governments around the world. This authoritative and comprehensive guide includes the history and foundation of data privacy, the framework for ensuring data privacy across major global jurisdictions, a detailed framework for complying with the GDPR, and perspectives on the future of data collection and privacy practices. Comply with the latest data privacy regulations in the EU, EEA, US, and others Avoid hefty fines, damage to your reputation, and losing your customers Keep pace with the latest privacy policies, guidelines, and legislation Understand the framework necessary to ensure data privacy today and gain insights on future privacy practices The Data Privacy and GDPR Handbook is an indispensable resource for Chief Data Officers, Chief Technology Officers, legal counsel, C-Level Executives, regulators and legislators, data privacy consultants, compliance officers, and audit managers.

This book presents state-of-the-art intelligent methods and techniques for solving real-world problemsand offers a vision of future research. Featuring 143 papers from the 4th Future Technologies Conference, held in San Francisco, USA, in 2019, it covers a wide range of important topics, including, but not limited to, computing, electronics, artificial intelligence, robotics, security and communications and their applications to the real world. As such, it is an interesting, exciting and inspiring read.

Blockchain is a much-discussed instrument that, according to some, promises to inaugurate a new era of data storage and code-execution, which could, in turn, stimulate new business models and markets. The precise impact of the technology is, of course, hard to anticipate with certainty, in particular as many remain sceptical of blockchain's potential impact. In recent times, there has been much discussion in policy circles, academia and the private sector regarding the tension between blockchain and the European Union's General Data Protection Regulation (GDPR). Indeed, many of the points of tension between blockchain and the GDPR are due to two overarching factors. First, the GDPR is based on an underlying assumption that in relation to each personal data point there is at least one natural or legal person – the data controller – whom data subjects can address to enforce their rights under EU data protection law. These data controllers must comply with the GDPR's obligations. Blockchains, however, are distributed databases that often seek to achieve decentralisation by replacing a unitary actor with many different players. The lack of consensus as to how (joint-) controllership ought to be defined hampers the allocation of responsibility and accountability. Second, the GDPR is based on the assumption that data can be modified or erased where necessary to comply with legal requirements, such as Articles 16 and 17 GDPR. Blockchains, however, render the unilateral modification of data purposefully onerous in order to ensure data integrity and to increase trust in the network. Furthermore, blockchains underline the challenges of adhering to the requirements of data minimisation and purpose limitation in the current form of the data economy. This study examines the European data protection framework and applies it to blockchain technologies so as to document these tensions. It also highlights the fact that blockchain may help further some of the GDPR's objectives. Concrete policy options are developed on the basis of this analysis.

FinTech has developed rapidly in recent years, and with these developments new challenges arise, particularly for regulators: how do you apply current law to these ever-changing concepts in a world of continual technological advancement?

As the power and sophistication of of "big data" and predictive analytics has continued to expand, so too has policy and public concern about the use of algorithms in contemporary life. This is hardly surprising given our increasing reliance on algorithms in daily life, touching policy sectorsfrom healthcare, transport, finance, consumer retail, manufacturing education, and employment through to public service provision and the operation of the criminal justice system. This has prompted concerns about the need and importance of holding algorithmic power to account, yet it is far fromclear that existing legal and other oversight mechanisms are up to the task.This collection of essays, edited by two leading regulatory governance scholars, offers a critical exploration of "algorithmic regulation", understood both as a means for co-ordinating and regulating social action and decision-making, as well as the need for institutional mechanisms through whichthe power of algorithms and algorithmic systems might themselves be regulated. It offers a unique perspective that is likely to become a significant reference point for the ever-growing debates about the power of algorithms in daily life in the worlds of research, policy and practice. The range ofcontributors are drawn from a broad range of disciplinary perspectives including law, public administration, applied philosophy, data science and artificial intelligence. Taken together, they highlight the rise of algorithmic power, the potential benefits and risks associated with this power, theway in which Sheila Jasanoff's long-standing claim that "technology is politics" has been thrown into sharp relief by the speed and scale at which algorithmic systems are proliferating, and the urgent need for wider public debate and engagement of their underlying values and value trade-offs, theway in which

they affect individual and collective decision-making and action, and effective and legitimate mechanisms by and through which algorithmic power is held to account.

This book constitutes the refereed proceedings of the 1st International Congress on Blockchain and Applications 2020, BLOCKCHAIN'20, held in L'Aquila, Italy, in October 2020. Among the scientific community, blockchain and artificial intelligence are a promising combination that will transform the production and manufacturing industry, media, finance, insurance, e-government, etc. Nevertheless, there is no consensus with schemes or best practices that would specify how blockchain and artificial intelligence should be used together. The 21 full papers presented were carefully reviewed and selected from over 40 submissions. They contain the latest advances on blockchain and artificial intelligence and on their application domains, exploring innovative ideas, guidelines, theories, models, technologies, and tools, and identifying critical issues and challenges that researchers and practitioners must deal with in future research.

Examines the interplay between artificial intelligence and international economic law, and its effects on global economic order. This title is also available as Open Access.

Don't be afraid of the GDPR wolf! How can your business easily comply with the new data protection and privacy laws and avoid fines of up to $27M? GDPR For Dummies sets out in simple steps how small business owners can comply with the complex General Data Protection Regulations (GDPR). These regulations apply to all businesses established in the EU and to businesses established outside of the EU insofar as they process personal data about people within the EU. Inside, you'll discover how GDPR applies to your business in the context of marketing, employment, providing your services, and using service providers. Learn how to avoid fines, regulatory investigations, customer complaints, and brand damage, while gaining a competitive advantage and increasing customer loyalty by putting privacy at the heart of your business. Find out what constitutes personal data and special category data Gain consent for online and offline marketing Put your Privacy Policy in place Report a data breach before being fined 79% of U.S. businesses haven't figured out how they'll report breaches in a timely fashion, provide customers the right to be forgotten, conduct privacy impact assessments, and more. If you are one of those businesses that hasn't put a plan in place, then GDPR For Dummies is for you.

Corporate Compliance has changedand—stricter guidelines now impose criminal penalties for activities that were previously considered legal. The and"business judgmentand" rule that protected the decisions of officers and directors has been severely eroded. The Corporate Federal Sentencing Guidelines of the U.S. Sentencing Commission require an effective compliance program, but even if you follow their requirements to the letter, you wonand't really know if your compliance program works or if you have created a corporate culture that supports compliance. Now, with the completely updated Second Edition of Corporate Legal Compliance Handbook, youand'll have help in creating a complete compliance system that complies with federal regulations and meets your specific corporate needs. Unlike the complicated or incomplete resources available today, Corporate Legal Compliance Handbook, Second Edition provides explanatory text and background material in two convenient formats: print and electronic. The accompanying CD-ROM contains reference materials, forms, sample training materials and other items to support program development. Corporate Legal Compliance Handbook, Second Edition gives you a unique combination: the essentials of the key laws your corporation must address, specific compliance regulations, and practical insights into designing, implementing, and managing an effectiveand—and efficientand—legal compliance program. It will help you identify the risks your company faces, and devise a system to address those risks. It will help you create a targeted compliance program by examining the risks attached to job descriptions, creating the appropriate corporate policies, establishing control programs, communicating effectively, and testing the effectiveness of your program. Corporate Legal Compliance Handbook, Second Edition will show you: How to ensure that your company establishes an effective compliance program How to master practical risk assessment tools How to identify any special risks posed by you clientand's type of business How to make sure that each employee involved in a business process understands his or her individual responsibility in the companyand's legal compliance program

Companies, lawyers, privacy officers, compliance managers, as well as human resources, marketing and IT professionals are increasingly facing privacy issues. While information on privacy topics is freely available, it can be diffcult to grasp a problem quickly, without getting lost in details and advocacy. This is where Determann's Field Guide to Data Privacy Law comes into its own – identifying key issues and providing concise practical guidance for an increasingly complex field shaped by rapid change in international laws, technology and society.

The concept of a risk-based approach to data protection came to the fore during the overhaul process of the EU's General Data Protection Regulation (GDPR). At its core, it consists of endowing the regulated organizations that process personal data with increased responsibility for complying with data protection mandates. Such increased compliance duties are performed through risk management tools. This book provides a comprehensive analysis of this legal and policy development, which considers a legal, historical, and theoretical perspective. By framing the risk-based approach as a sui generis implementation of a specific regulation model known as meta regulation, this book provides a recollection of the policy developments that led to the adoption of the risk-based approach in light of regulation theory and debates. It also discusses a number of salient issues pertaining to the risk-based approach, such as its rationale, scope, and meaning; the role for regulators; and its potential and limits. The book also looks at they way it has been undertaken in major statutes with a focus on key provisions, such as data protection impact assessments or accountability. Finally, the book devotes considerable attention to the notion of risk. It explains key terms such as risk assessment and management. It discusses in-depth the role of harms in data protection, the meaning of a data protection risk, and the difference between risks and harms. It also critically analyses prevalent data protection risk management methodologies and explains the most important caveats for managing data protection risks.

This book discusses the necessity and perhaps urgency for the regulation of algorithms on which new technologies rely; technologies that have the potential to re-shape human societies. From commerce and farming to medical care and education, it is difficult to find any aspect of our lives that will not be affected by these emerging technologies. At the same time, artificial intelligence, deep learning, machine learning, cognitive computing, blockchain, virtual reality and augmented reality, belong to the fields most likely to affect law and, in particular, administrative law. The book examines universally applicable patterns in administrative decisions and judicial rulings. First, similarities and divergence in behavior among the different cases are identified by analyzing parameters ranging from geographical location and administrative decisions to judicial reasoning and legal basis. As it turns out, in several of the cases presented, sources of general law, such as competition or labor law, are invoked as a legal basis, due to the lack of current specialized legislation. This book also investigates the role and significance of national and indeed supranational regulatory bodies for advanced algorithms and considers ENISA, an EU agency that focuses on network and information security, as an interesting candidate for a European regulator of advanced algorithms. Lastly, it discusses the involvement of representative institutions in algorithmic regulation.

Hallinan argues that the substantive framework presented by the GDPR offers an admirable base-line level of protection for the range of genetic privacy rights engaged by biobanking.

An essential, in-depth analysis of the key legal issues that governments face when adopting cloud computing services.

This volume constitutes the proceedings of the 12th IFIP WG 8.1 Conference on the Practice of Enterprise Modeling held in November 2019 in Luxembourg, Luxembourg. The conference was created by the International Federation for Information Processing (IFIP) Working Group 8.1 to offer a forum for knowledge transfer and experience sharing between the academic and practitioner communities. The 15 full papers accepted were carefully reviewed and selected from 35 submissions. They are grouped by the following topics: modeling and ontologies; reference architectures and patterns; methods for

architectures and models; and enterprise architecture for security, privacy and compliance.

Countries are increasingly introducing data localization laws, threatening digital globalization and inhibiting cloud computing adoption despite its acknowledged benefits. This multi-disciplinary book analyzes the EU restriction (including the Privacy Shield and General Data Protection Regulation) through a cloud computing lens, covering historical objectives and practical problems, showing why the focus should move from physical data location to effective jurisdiction over those controlling access to intelligible data, and control of access to data through security.

This handbook provides practical guidance for the (junior, medior and senior) Data Protection Officer (DPO) to assemble a work plan as per applicable EU GDPR guidelines. At present EU's GDPR is largely recognized as a gold standard all over the world, also for the ever-growing community of DPOs as per national legislations. This publication is part of official mandatory training materials for Certified Data Protection Officer from the European Association of Data Protection Professionals (EADPP) as per the EADPP CDPO Certification Scheme and applicable CDPO Body of Knowledge (Part D) as provided by Privacad. The practical approach followed in this richly illustrated handbook is of relevance for any (future) Data Protection Officer active in any part of the World performing tasks as per local, regional or international norms and regulations. This books explicitly explains the roles and responsibilities of the DPO as envisaged in the GDPR. As stated by the European Data Protection Board (EDPB) it is best practice for the DPO to have a work plan. What does such a work plan look like? Providing an answer to that question lies at the core of this publication. Two key pillars are followed to assemble a professional and practical DPO work plan. First, the text as enshrined in the General Data Protection Regulation (GDPR) itself codifies an important line of orientation in the embodiment of Articles 37 to 39 of the GDPR in which the designation, positions and tasks of the DPO are discussed. Second, the typical role the DPO is playing in the "daily data protection practice" which can be inferred from, among others, an action plan (or work plan) from an enterprise (institution or organisation). In pursuit of compliance with the obligations pursuant to the GDPR, at least the following steps usually be distinguished. Establish GDPR (privacy and data protection) policies. Make an inventory of personal data. Perform a GDPR (privacy and data protection) baseline. Perform a GDPR (privacy and data protection) gap-analysis. Perform a GDPR (privacy and data protection) implementation. Perform GDPR (privacy and data protection) review and update. Perform GDPR (privacy and data protection) assurance and audit. Compose and communicate the GDPR accountability and reports. According to the European Data Protection Board (formerly operating as WP29), the DPO (or the organisation) should avail of a work plan which the organisation will use as a basis for providing, among others, 'necessary resources' for the DPO. With the entry into force of the GDPR as of 25 May 2018, the need to work on professional maturity of the Data Protection Officer (DPO) became more and more urgent. This handbook is part of the 'Privacy and Data Protection' series offered under auspices of Honorary Visiting Professor Romeo Kadir, acting Editor-in-Chief and author of the first publications in this series. At present professor Romeo Kadir (with over 25 years of experience as privacy and data protection professional) is Constituent President of the GDPR Certification Committee Academic Board of the European Association of Data Protection Professionals (EADPP) and President of the European Institute for Privacy, Audit, Compliance and Certification (EIPACC) and lecturer with the International Privacy Academy (Privacad). He holds several positions as Board Member, Corporate Consultant and Government Advisor related to privacy and data protection affairs.

The book presents timely and needed contributions on privacy and data protection seals as seen from general, legal, policy, economic, technological, and societal perspectives. It covers data protection certification in the EU (i.e., the possibilities, actors and building blocks); the Schleswig-Holstein Data Protection Seal; the French Privacy Seal Scheme; privacy seals in the USA, Europe, Japan, Canada, India and Australia; controversies, challenges and lessons for privacy seals; the potential for privacy seals in emerging technologies; and an economic analysis. This book is particularly relevant in the EU context, given the General Data Protection Regulation (GDPR) impetus to data protection certification mechanisms and the dedication of specific provisions to certification. Its coverage of practices in jurisdictions outside the EU also makes it relevant globally. This book will appeal to European legislators and policy-makers, privacy and data protection practitioners, certification bodies, international organisations, and academics. Rowena Rodrigues is a Senior Research Analyst with Trilateral Research Ltd. in London and Vagelis Papakonstantinou is a Senior Researcher at the Vrije Universiteit Brussel in Brussels.