THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

SEVENTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

© 2020 Law Business Research Ltd

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

SEVENTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

© 2020 Law Business Research Ltd

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Joel Woods

SENIOR ACCOUNT MANAGERS
Pere Aspinall, Jack Bagnall

ACCOUNT MANAGERS
Olivia Budd, Katie Hodgetts, Reece Whelan

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Gavin Jordan

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Claire Ancell

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK
© 2020 Law Business Research Ltd
www.TheLawReviews.co.uk

No photocopying: copyright licences do not apply.
The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at September 2020, be advised that this is a developing area.
Enquiries concerning reproduction should be sent to Law Business Research, at the address above.
Enquiries concerning editorial content should be directed
to the Publisher – tom.barnes@lbresearch.com

ISBN 978-1-83862-485-9

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

© 2020 Law Business Research Ltd

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ADVOKAADIBÜROO NORDX LEGAL

ALLENS

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS&PARTNERS

CLEMENS

CTSU – SOCIEDADE DE ADVOGADOS

GREENBERG TRAURIG LLP

K&K ADVOCATES

nNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VUKINA & PARTNERS LTD

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

© 2020 Law Business Research Ltd

CONTENTS

© 2020 Law Business Research Ltd

© 2020 Law Business Research Ltd

© 2020 Law Business Research Ltd

Chapter 11

DENMARK

Tommy Angermair, Camilla Sand Fink and Søren Bonde[1]

I OVERVIEW

Similar to other countries in Europe, Denmark has passed legislation designed to supplement the requirements of the EU General Data Protection Regulation (GDPR),[2] which came into force on 25 May 2018. In Denmark, the main regulation concerning processing of personal data is the GDPR and the Danish supplementary act, the Data Protection Act,[3] which came into force on 23 May 2018.

In addition to the rules of the GDPR, the Data Protection Act and national practice implements certain derogations concerning the processing of personal data, especially in respect of processing of personal data within the employment sector and the processing of national registration numbers. The Danish Act on Processing Personal Data that implemented Directive 95/46 EC came into force in 2002. But despite the fact that the Danish data protection regulation is more than 15 years old, not much attention was paid to data protection in Denmark until the GDPR was passed in 2016. The term 'data protection' was basically unheard of in the general Danish population and in most companies before 2017–2018. Thus, the GDPR has been the dominant topic in recent years in terms of compliance.

Since the implementation of the GDPR, Danish companies have generally continuously invested substantial resources in data protection compliance, mainly for commercial and legal risk management reasons.

Since 25 May 2018, the Danish and other European supervisory authorities have issued multiple guidelines and decisions concerning the interpretation of the GDPR and the national supplementary legislation, which has allowed Danish companies to conduct substantially more targeted and resource efficient compliance efforts. Denmark has been trailing most other EU Member States, in particular Germany and France, in terms of data protection awareness and compliance. In our opinion, this situation is mostly attributable to the relatively high level of trust in the Danish society. However, Denmark seems to have caught up with most Member States in recent years, mainly because of drastically increased public and corporate awareness of data protection rules as well as massive countrywide corporate resource allocations since 2016.

---

1 Tommy Angermair is a partner, Camilla Sand Fink is a senior associate and Søren Bonde is an associate at Clemens.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3 Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

© 2020 Law Business Research Ltd

II THE YEAR IN REVIEW

Most companies have more or less completed their initial compliance 'projects' and are now more focused on maintenance, daily compliance work, control of data processors compliance, etc., but many (minor and medium sized) companies have not yet started their compliance work, even though more than two years have passed since the GDPR came into full force.

Covid-19 has been the dominant topic since the outbreak in March 2020, also in terms of data privacy and data protection. The covid-19 outbreak resulted in a number of data privacy issues and questions, for example, regarding the registration of employees' health information, performing medical checks, disclosure of employees' health information to colleagues, but also regarding rules and restrictions related to public authorities' collecting and disclosing health information. Both the Danish Data Protection Agency (DPA) and the European Data Protection Board (EDPB) have issued guidelines on processing personal data in the context of the covid-19 outbreak.[4] Among other developments in the past year, the DPA has issued the first standard contractual clauses for the purpose of compliance with Article 28 of the GDPR, which was adopted by the European Commission in December 2019.[5] Furthermore, the DPA has issued a series of podcast guidelines on processing personal data.[6] Furthermore, the DPA has decided to investigate the legal ground and security measures with regard to processing personal data in the worldwide video app TikTok, and at the time of writing the DPA has reported a total of five companies and three public authorities to the police for infringement of the GDPR with indicated fines between 25,000 kroner and 1.5 million kroner, since the GDPR came into force.

Finally, the Court of Justice of the European Union (CJEU) handed down a major ruling on 16 July 2020, invalidating the EU–US Privacy Shield adequacy decision adopted in 2016 by the European Commission, and validating the European Commission's standard contractual clauses allowing the transfer of personal data from the EU to importers established outside the EU.[7]

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The rules governing processing of personal data in Denmark are primarily set forth in the GDPR and the Data Protection Act.

In addition, any rules governing processing of personal data in other legislation (*lex specialis*) shall take precedence over the rules laid down in the Data Protection Act (collectively the Data Protection legislation). National legislations shall naturally be interpreted in accordance with the principles of the GDPR.[8]

4 The DPA's guidelines are only published in Danish and available at https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/hvordan-er-det-med-gdpr-og-coronavirus. The EDPB guidelines are published in English and available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

5 The standard contractual clauses are published in Danish and English and available at https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions.

6 The podcast-guidelines are available in Danish at https://www.datatilsynet.dk/generelt-om-databeskyttelse/podcast.

7 Case C-311/18 *Schrems II*.

8 Section 1(3) of the Data Protection Act.

© 2020 Law Business Research Ltd

In line with the GDPR, the Data Protection legislation applies to the processing of personal data as part of the activities carried out on behalf of a controller or processor established in Denmark, regardless of whether the processing takes place in the EU.

The DPA has published several hands-on guidelines describing how companies must adhere to the Data Protection legislation.[9] Despite the guidelines are not legally binding they are generally taken very seriously in the public and private sector given the DPA's role as primary regulator and enforcer of the data protection rules in practice.

ii General obligations for data handlers

Controllers are not obligated to register with the DPA in relation to their processing of personal data.

The Data Protection legislation sets forth the fundamental requirements applicable to all processing of personal data. In particular, the Data Protection Act requires that personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a manner incompatible with those purposes.

According to the DPA, controllers who process special categories of personal data must be able to identify an exception to the general prohibition in either Article 9(1) of the GDPR or national provisions implementing Article 9 and identify an additional legal basis for processing in accordance with Article 6 of the GDPR. However, this requirement for a 'double legal basis' applies only for processing of special categories of personal data and not for the processing of information on criminal offences, national registration numbers and ordinary personal data in accordance with Article 6 of the GDPR.

To comply with the obligation to notify the data subject in accordance with Articles 13–14 of the GDPR, the controller must take active steps to provide the information. Consequently, it is not sufficient that the relevant information is available on a website or similar, which the data subject is required to find by himself. The form of notification shall reflect the means of collecting personal data. The controller must notify the data subject in writing, unless otherwise accepted by the data subject. Furthermore, the notification shall be provided electronically, if appropriate, for example if the personal data is collected via an electronic form.

If a controller receives unsolicited personal data from a data subject, the controller must notify the data subject in accordance with Article 13 of the GDPR as soon as possible, but, no later than 10 days after receipt.[10]

Prior to transmitting confidential (see Section IV) and special categories of personal data by email or SMS, data controllers shall implement appropriate technical and organisational measures to address the identified risks regarding the transfer, such as – but not limited to – encryption or pseudonymisation of personal data. Furthermore, the DPA has issued a template for a data processing agreement that has been adopted be the EDPB as standard contractual clauses. The template is available in multiple languages at the DPA's website.[11]

9 The guidelines are only published in Danish and available at https://www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger-og-skabeloner/.

10 Guideline from the DPA concerning the rights of the data subject, p. 14.

11 https://edpb.europa.eu/our-work-tools/our-documents/decision-sa/dk-sa-standard-contractual-clauses-purposes-compliance-art_da.

© 2020 Law Business Research Ltd

iii Data subject rights

The right of access in relation to Article 15 of the GDPR implies that the data subject has the right to receive information concerning the processing of personal data by a controller. The right of access is not limited and includes all personal data, including personal data processed in IT systems, TV surveillance images, logs, notes, HR files, emails, etc.

The controller may request the data subject to clarify, specify or both the access request. However, the controller may not refuse to comply with the access request if the data subject refuses to clarify or specify the request.

The controller may derogate from the right of access (and the obligation to notify the data subject of matters concerning Article 13(1)–(3), Article 14(1)–(4) of the GDPR, if the data subject's interest in this information is found to be superseded by essential considerations of public or private interests, including the consideration for the data subject himself, for example, if a data controller is processing personal data in a whistle-blower inquiry and keeping confidential such personal data is necessary for investigation purposes.

The general assumption is, however, that exception from the right to access processed personal data has a relatively narrow scope.

In accordance with Article 16 of the GDPR, a controller must correct any inaccurate personal data upon request from a data subject.

However, the situation may arise where a controller does not agree with the data subject that the personal data is inaccurate, for example in a dispute concerning the accuracy of note taking from an HR and employee meeting. The controller is not obliged to correct personal data if the factual belief of the controller is that the personal data processed is accurate.

In such cases, the controller must ensure that a note is made on the disputed information indicating that the data subject does not agree with the accuracy of the personal data, and what the data subject considers to be accurate.

A new legal requirement in Section 99(d) of the Danish Financial Statements Act[12] entails an obligation for large companies to supplement the management's report with an account of the company's policy for data ethics. If the company has no such policy, the management report must include an explanation for the absent policy.

The obligation currently only applies to listed companies. It is, however, expected that similar requirements on data ethics will be introduced for credit institutions, insurance companies, etc., including companies' holding companies (financial entities), which are not covered by the Danish Financial Statements Act.

iv Specific regulatory areas

The DPA distinguishes between 'regular data' and 'confidential data' in respect of personal data under Article 6 of the GDPR, despite this not being explicitly mentioned in the GDPR. Confidential information is considered personal data that, owing to its nature and the context, requires 'special protection' because the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to such personal data may cause greater physical, material or non-material damage for the data subject than regular personal data. Depending on the circumstances, personal data concerning income and wealth, conditions of employment or internal family relationships may be deemed confidential personal data. Furthermore, Danish civil registration numbers (CPR number) and personal data related to

12 Act No. 838 of 8 August 2019.

© 2020 Law Business Research Ltd

criminal convictions is also deemed confidential personal data. Consequently, a controller or processor must distinguish between the different categories of 'regular personal data' in its risk assessment and take any precautions needed to safeguard confidential data in accordance with Article 32 of the GDPR.

Processing of personal data covered by Article 6(1) and Article 9(1) of the GDPR in an employment context may take place on the basis of consent from the data subject in accordance with Article 7 of the GDPR.[13] However, an employer is – as a general rule – allowed to process an employee's personal data to a usual and reasonable extent in connection with the employer's HR administration without obtaining employee consent or DPA authorisation. Such processing will often be justified for operational reasons and may not be offensive to the employee.

When an employee has resigned, his or her email account may be kept active for a short period after the end of employment. This period is determined by the position and function of the resigned employee and cannot exceed 12 months. After the end of employment, an auto-reply must be sent from the email account with notice of the employee's resignation and any other relevant information. The active email account may only be used for receiving emails and forwarding relevant emails internally within the controller's organisation.

If a controller wants to record customer calls, for example for quality assurance or for educational purposes, the controller shall obtain consent from the individual involved before the conversation is recorded. In a specific case concerning the use of telephone recordings for training purposes, the DPA issued a temporary order to ban the processing of personal data for internal use, as such processing activities are not within the legitimate interest of the controller.[14] In one case (pre-GDPR), the DPA has specifically stated that storing of telephone recordings from securities trading could take place without consent for documentation reasons. Due to the recent cases from the DPA, the assumption is that the exception has a relatively narrow scope

Processing of a child's personal data based on consent in connection with the offering of information society services is lawful provided that the child is no younger than 13.

Television surveillance is governed by rules laid down in the Danish TV Surveillance Act.[15] The term 'television surveillance' means continuous or regularly repeated monitoring of persons by means of a remote or automatic camera. It is irrelevant whether image capture occurs or whether the images are simply displayed on a TV screen or the like.

The rules of the Data Protection legislation apply to the processing of personal data in surveillance videos, etc., in addition to the TV Surveillance Act.

In addition to the rules on notifying the data subject in accordance with Articles 13–14 of the GDPR, the controller conducting television surveillance must clearly indicate that surveillance activities take place by signage or similar.

Recordings containing personal data originating from television surveillance for crime prevention purposes must generally be deleted 30 days after recording.

13 Section 12(1) of the Data Protection Act.

14 DPA Case No. 2018-31-0977.

15 Act No. 1190 of 11/10/2007.

© 2020 Law Business Research Ltd

In addition to the Data Protection legislation, the rules of the Danish Marketing Act limit the processing of personal data in connection with direct marketing.[16] Direct marketing means when personal data is used to make direct contact with the data subject, for example via email, SMS or a letter.

In particular, a controller may not contact the data subject by use of electronic means for direct marketing purposes unless such processing is based on the consent of the data subject.

A data subject has the right to withdraw the consent to the processing of personal data for direct marketing purposes. If the data subject withdraws his or her consent, the personal data may no longer be used for marketing purposes.

Furthermore, a controller is not entitled to disclose personal data collected for marketing purposes without explicit consent from the data subject.

This prohibition does not apply in the case of 'general customer information', which is the basis of categorisation into customer categories, and the interest of the data subject does not exceed the interest of the trader. In this case, the controller must make sure that the consumer has not made inquiries for marketing purposes via the CPR. General customer information does not include detailed information on the data subject's consumption habits, such as information on the data subject's purchase of a car on credit or what goods the data subject has purchased.

v Technological innovation

Cookies

The use of cookies, namely, a piece of text stored on the end user's medium (e.g., tablet or computer, which may collect and transmit data), is subject to the rules of the Personal Data Legislation if the data stored or collected by the cookie includes personal data. Regardless of whether the collected data includes personal data, the placement and functionality of cookies are governed by the Cookie Act.[17]

In accordance with the CJEU's ruling in the *Planet49* case,[18] data controllers are – apart from strictly necessary cookies – prohibited from using pre-checked checkboxes on consent banners to collect and process personal data. Furthermore, scrolling and continued browsing or cookie walls (forced consent) does not constitute a valid consent. Thus, the only valid form of consent for processing personal data is an explicit, specific and actively given consent in accordance with the rules in the GDPR.

Social media

Social media is increasingly becoming an important part of business worldwide, especially in terms of marketing and collection and disclosure of personal data. With multiple international providers and billions of data subjects using different services worldwide, data breaches such as the 'Cambridge Analytica scandal' persistently emphasise the importance of data protection in terms of social media. Thus, there is an increasing number of cases

16 The Danish Marketing Act No. 426 of 03/05/2017.

17 Act No. 1148 of 09/12/2011.

18 C-673/17.

© 2020 Law Business Research Ltd

regarding the processing of personal data related to social media. According to the CJEU, data controllers collecting personal data via social platforms may be considered as a joint controller with the social media provider.[19]

Furthermore, the DPA has recently announced an *ex officio* investigation regarding the legal grounds and security measures with regard to processing personal data in the TikTok app.

Surveillance

With effect from 1 July 2020, the Video Surveillance Act[20] has been amended. According to the Video Surveillance Act, private surveillance of publicly accessible areas is prohibited. However, a number of companies, including banks, petrol stations, shopping malls, wholesalers and restaurants are exempt from this ban, as they have the right to monitor their own entrances and facades. In addition, these companies have access to monitor areas that are directly adjacent to the company's entrances and facades at a distance of up to 30 metres. In this context, however, surveillance must be 'clearly necessary' and have the purpose of preventing and combating crime.

Companies monitoring publicly accessible areas must be registered in the Danish Police Camera Register (POLCAM). The registration must be made within 'reasonable time', and any subsequent significant changes must be registered in POLCAM.

In addition to the rules on notifying the data subject in accordance with Articles 13–14 of the GDPR, the controller conducting television surveillance must clearly communicate that surveillance activities take place by signage or similar. Recordings containing personal data originating from surveillance for crime prevention purposes must generally be deleted no more than 30 days after the recording.

Furthermore, data handlers using video surveillance must be able to redact other individuals and personal data from the surveillance material while adhering to the right of access by the data subject in Article 15 of the GDPR.

Monitoring of employees is not prohibited; however, such processing of personal data is subject to the data protection legislation and the employer must comply with the GDPR, including the rules on notification in Article 13 of the GDPR.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

International data transfer is subject to the provisions in the GDPR.

There are no other restrictions related to international transfer of personal data in the European Economic Area (EEA)[21] other than the restrictions related to national transfers of personal data in the GDPR or special national legislation. According to the GDPR, any transfer of personal data to a third country or international organisations may only take place under specific circumstances and if the conditions in the GDPR, Chapter V, are complied with by the involved controllers and data processors. The basic circumstances and conditions are outlined in the following.

According to the GDPR, international transfer of personal data to a third country or international organisation may take place without any specific authorisation, where the

19 C-210/16.

20 Act No. 1190 of 10 November 2007.

21 The European Economic Area includes all EU countries, Iceland, Liechtenstein and Norway.

© 2020 Law Business Research Ltd

European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.

In the time of writing, the European Commission has recognised the following countries as providing adequate protection: Andorra, Argentina, Canada (commercial organisations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay. Furthermore, adequacy talks are ongoing with South Korea.[22]

The United States was, until recently, limited to the EU–US Privacy Shield adequacy decision recognised by the European Union for providing adequate protection, but the adequacy decision was invalided by the CJEU on 16 July 2020.

In the absence of an adequacy decision, a controller or processor may transfer personal data to a third country or international organisation, if the controller or processor has provided appropriate safeguards that enforceable data subject rights and effective remedies are available.

In relation to international data transfers between private companies or organisations it is common that appropriate safeguards are provided by standard contractual clauses or binding corporate rules. Binding corporate rules only include international data transfers between group companies, and application of the rules requires that the competent supervisory authority (DPA) approves the rules. Furthermore, the work related to adopting binding corporate rules is extensive and hence exclusively recommended for large international groups. As opposed to binding corporate rules, standard contractual clauses require no approval from the DPA and may be used to transfer personal data between group companies as well as between external companies. The CJEU has recently validated the European Commission's standard contractual clauses allowing the transfer of personal data from the EU to importers established outside the EU.[23]

Furthermore, the standard contractual clauses may be included in other contractual material, such as data-processing agreements or trade agreements provided that no changes are made to the clauses. There are three types of standard contractual clauses, all of which are available on the European Commission's website.[24]

Appropriate safeguards may also be provided between private parties by an approved code of conduct or an approved certification mechanism, both together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards. Such certifications and codes of conducts will probably be important contributions to more transparent access to conduct international data transfers. However, at the time of writing neither codes of conduct nor certifications have been approved in Denmark.

Finally, appropriate safeguards may be provided between private parties by ad hoc contractual clauses between the controller or processor in Denmark and the controller or processor in the third country, subject to DPA approval.

22 The European Commission's list of approved countries at any given time is available on the European Commission's website: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

23 Case C-311/18 *Schrems II*.

24 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

© 2020 Law Business Research Ltd

In the absence of an adequacy decision or appropriate safeguards, international transfers of personal data to third countries are restricted to very limited circumstances, including:

a if the data subject has explicitly consented to the proposed transfer after having been informed of the possible risks (except if the activities are carried out by public authorities in the exercise of their public powers);

b if the transfer is necessary for the performance of a contract between the controller and the data subject or the implementation of pre-contractual measures taken at the data subjects requests (except if the activities are carried out by public authorities in the exercise of their public powers);

c if the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person (except if the activities are carried out by public authorities in the exercise of their public powers);

d if the transfer is necessary for important reasons of public interests; or

e if the transfer is necessary for the establishment, exercise or defence of legal claims.

Furthermore, international transfer of personal data in the absence of an adequacy decision or appropriate safeguards may only take place under the following circumstances:

a if the transfer is not repetitive;

b if the transfer only concerns a limited number of data subjects;

c if the transfer is necessary for the purpose of compelling legitimate interests pursued by the controller that are not overridden by the interests or rights of the data subject;

d if the controller has assessed all the circumstances surrounding the transfer;

e if the controller – prior to the transfer – has informed the DPA hereof;

f if the controller has informed the data subject of the transfer and on the compelling legitimate interests pursued (in addition to providing the information referred to in the GDPR, Articles 13 and 14); and

g if the controller or processor reliable for the data transfer has documented the above assessments in the records referred to in GDPR Article 30.

V COMPANY POLICIES AND PRACTICES

To be compliant with the Data Protection legislation, it is essential to know (1) which personal data your company is processing; (2) for how long; (3) why; (4) where the personal data is processed as well as (5) recipients of personal data provided by your company.

The most common measures to obtain essential knowledge of the company's processing activities and to document the company's compliance level are performing a dataflow analysis on a regular basis (e.g., once a year) to keep track of any changing processing activities and preparing a gap analysis indicating any compliance gaps.

It is important to note that GDPR compliance is predominantly based on a basic principle of accountability and the company's individual risk assessments, which means that several measures necessary for GDPR compliance in practice do not follow directly from the GDPR, for example dataflow mapping or ensuring that employees processing personal data have sufficient knowledge of applicable rules and restrictions for processing personal data.

The range of policies and practices required to comply with the GDPR will therefore vary depending on the company's processing activities. The following represents the

© 2020 Law Business Research Ltd

minimum statutory and non-statutory procedures and documentation regarding private companies' most common general processing activities relating to employee and private customer personal data.

The minimal recommended documentation and procedures regarding all processing activities are as follows:

a documented overview of personal data processed, such as dataflow mapping and gap analysis;

b statutory records of processing activities (Article 30 of the GDPR);

c general privacy policy on websites including statutory information according to Articles 13–14 of the GDPR;

d education of employees, including for example internal guidelines outlining the rules and restrictions of processing personal data in general and regarding the company's specific processing activities (e.g., the use of emails and access rights in IT systems), the company's security measures, how and when to respond to data subject rights requests, and how to identify data breaches etc.; e-learning or other relevant education regarding the processing of personal data; and internal GDPR awareness campaigns etc.;

e cookie policy regarding all websites and technical measures to ensure end user consent to placement of cookies on end user terminal equipment;[25]

f documented assessment of whether or not the company is obliged to designate a data protection officer, if it is questionable whether or not the company is obliged to according to Article 37 of the GDPR;

g statutory private impact assessments regarding high-risk processing activities (Articles 35–36 of the GDPR);

h internal IT and security policy outlining the rules and restrictions of the company's security measures, for example, regarding the use of mobile devices, computers, physical access to buildings or offices, electronic access to IT systems, back-ups, firewalls etc.;

i internal procedures to assess, document and report data breaches. The controller is obligated to register all data breaches internally notwithstanding the company's potential obligation to notify the supervisory authority competent in accordance with Article 33 of the GDPR or communicate the data breach to the data subject in accordance with Article 34 of the GDPR;

j procedures for the erasure of personal data and retention schedules outlining the retention periods for all personal data processed by the controller or processor. There are few rules and guidelines on specific retention periods in Denmark, and most retention periods are set out by the controller's or processor's legitimate purposes to retain the data based on the Danish Limitation Act; Danish legislation on bookkeeping, accounting and tax as well as on DPA case law. Furthermore, the period of limitation for infringement of the GDPR and the Data Protection Act or rules issued in pursuance hereof is five years according to Article 41(7) of the Data Protection Act. The recommended retention periods regarding the most typical processing activities regarding employee and private costumer personal data are set out below; and

k control procedures to ensure the ongoing compliance level, including for example sampling in relation to internal policy compliance and erasure of personal data

25 Bek nr. 1148 af 09-12-2010 om krav til information og samtykke ved lagring af eller adgang til oplysninger i slutbrugerens terminaludstyr (The Cookie Order) implementing Directive 2002/58/EC (the ePrivacy Directive).

© 2020 Law Business Research Ltd

in accordance with the outlined retention periods, supervision of data processors, controlling and updating the statutory records of processing activities, performing a dataflow analysis on a regular basis, etc.

In addition to the minimum documentation and procedures listed above, the below documentation and procedures are recommended regarding the processing of personal data relating to applicants, present and former employees:

a privacy policy regarding the processing of personal data in the recruitment process including statutory information according to Articles 13–14 of the GDPR;

b procedures for collecting applicant consent for retaining application material for a specific period after the end of recruitment for future relevant vacancies. Retention of the application post-recruitment requires consent from the applicant, except if the purpose for further processing is the defence of a legal claim;

c procedures for erasure of application material after the end of the outlined retention period, which is most commonly a period of six to 12 months from the end of recruitment or time of receipt of unsolicited applications;

d internal privacy policy regarding the processing of HR-related personal information including statutory information pursuant to Articles 13–14 of the GDPR;

e internal guidelines and procedures regarding surveillance, for example, GPS tracking, video monitoring, website logging, mobile device tracking etc.;

f employee consent to process photographs or videos of employees at the company website, social media relating to employees' contact information at the company website and to marketing material, posts, brochures etc.;

g procedures for closing (and erasing) employee email accounts as soon as possible after the end of employment as discussed in Section III.iv; and

h procedures for erasure of the employee's personal file after expiry of the outlined retention period, typically five years after the end of employment based on DPA case law and the limitation period of five years as set out in the Danish Limitation Act regarding claims arising from an employment relationship.

In addition to the minimum documentation and procedures listed above, the following documentation and procedures are recommended regarding the processing of personal data relating to private costumers:

a procedures for collecting consent to approach anyone by means of electronic mail, an automated calling system or fax for the purpose of direct marketing[26] and consent to approach consumers by telephone for the purpose of direct marketing;[27]

b internal guidelines and procedures for collecting and processing personal data in CRM systems;

c procedures and company rules on processing personal data in relation to digital marketing tools, the use of social media etc. (e.g., in relation to Google Analytics,

26 According to the Danish Marketing Act, Article 10, a trader may not approach anyone by means of electronic mail, an automated calling system or fax for the purpose of direct marketing unless the party concerned has given his or her prior consent.

27 According to the Danish Consumer Act, a trader may not approach consumers by means of telephone for the purpose of direct marketing unless the consumer has given his or her prior consent.

© 2020 Law Business Research Ltd

Facebook competitions or inquiries via LinkedIn), especially outlining the rules of international transfer of personal data, the rules for collection consent to publish personal data and the rules in the Danish Marketing Act; and

d procedures on how to give customers the statutory information according to Articles 13–14 of the GDPR if customer calls are recorded (including recording for educational purposes) as discussed in Section III.iv.

VI DISCOVERY AND DISCLOSURE

Denmark has no general discovery or disclosure scheme in relation to civil litigation corresponding to the rules in countries such as the US and the UK and it is generally left to each party to decide which information they are willing to provide/introduce into evidence. By operation of the GDPR data subjects now have wider access to their personal data than ever before.

Under the jurisdiction of the GDPR, disclosure of personal data is basically a processing activity equal to all other processing activities. Disclosure of personal data therefore requires a legitimate purpose according to Article 5 the GDPR, and legal grounds according to Article 6 of the GDPR (ordinary personal data), Article 9 of the GDPR (special categories of personal data), the Article 8 of Data Protection Act (personal data about criminal offences) or Article 11 of the Data Protection Act (national identification numbers). The Data Protection legislation equally applies to private companies and public authorities; however, in practice, public authorities' legal basis for processing personal data has a wider scope in special legislation than that of private companies.

If the Danish government or the Danish civil courts request disclosure of personal data in relation to a specific investigation or case, the controller will in practice in most cases have legal grounds for disclosing the data to the government or the civil court if special legislation authorises the government or the civil court to require the disclosure of the personal data in question (e.g., Sections 298(1) and 299(1) of the Danish Administration of Justice Act[28] according to which the court may order disclosure of documents relating to the matters in question). If the Danish government or the Danish civil courts do not have legal grounds to request disclosure of the personal data, the controller must have other legal grounds for disclosing the personal data in the Data Protection legislation. The controller may, for example, disclose information regarding national identification numbers 'if the disclosure is a natural element of the ordinary operation of enterprises etc. of the type in question and the disclosure is of decisive importance for unique identification of the data subject or the disclosure is demanded by a public authority' according to the Data Protection Act, Article 11(3). This legal basis may for example be used by real estate agents and lawyers in relation to their disclosure of the parties' national identification numbers to the Danish registry when applying for registration of documents regarding property transactions.

The processor may also disclose personal data about criminal offences 'if the disclosure takes place to safeguard private or public interests which clearly override the interests of secrecy, including the interests of the person to whom the data relates' according to Article 8(2) of the Data Protection Act. This legal basis may, for example, be used by an employer in relation to its disclosure of personal data about an employee's criminal offence to the police as part of an investigation regarding the employee.

28 Lov 2018-11-14, nr. 1284 Retsplejeloven (the Danish Administration of Justice Act).

© 2020 Law Business Research Ltd

In relation to disclosure of requests or demands from foreign prosecutors, courts or governments, the above-mentioned GDPR rules on international transfer of personal data also apply if a foreign government requests the disclosure of personal data stored under the jurisdiction of the GDPR.

Especially with regards to the US government disclosure requests to US-based organisations storing personal data under the jurisdiction of the GDPR or the former Directive on the protection of personal data,[29] the legal situation may cause major conflicts for US-based organisations obligated to disclose the data in question under US law and prohibited from disclosing the data in question under European law. After the enforcement of the US CLOUD Act,[30] which essentially provides that the obligation for organisations under the US jurisdiction to comply with US law enforcement agencies' search warrant to gain access to data regardless of whether data in question is located within or outside the United States, the legal state regarding transfer of personal data from EU to the United States is still uncertain although the US CLOUD Act to some extent tries to deal with the above mentioned conflicts, for example, by stating that any disclosure of data must adhere to local law.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Based on the Data Protection legislation, the DPA is essentially the only enforcement agency with regards to data protection and privacy in Denmark with one minor exception (according to the Danish Act on Data Protection regarding supply of public electronic communications services,[31] the Danish Business Authority is the primary enforcement agency when it comes to security issues and security breaches in the telecommunications and internet sector).

According to the Data Protection Act, the DPA has several investigatory powers. The DPA may, for example, request access to any information relevant for its activities, including for the decision of whether a particular matter falls within the provisions of the Data Protection legislation. Furthermore, DPA staff must at any time – against satisfactory proof of identity but without a court order – be given access to all premises from where a processing activity is carried out, including any data processing equipment. If required, the police will help to secure access. The DPA therefore has the authority to audit private companies and public authorities – announced as well as unannounced – and conduct investigations of the controller's or processor's adherence to the Data Protection legislation.

Before the GDPR came into force, the DPA also had investigatory powers, including audits, but these powers was utilised to a much lesser extent than today. In 2017 the DPA held 73 audits; in 2018, when the GDPR came into force, the DPA held 329 audits;[32] and in 2019 the DPA held 256 audits.[33] The numbers include planned written and physical audits and raids. After the GDPR came into force, the DPA's audits have increased substantially,

29 The European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

30 The Clarifying Lawful Overseas Use Of Data Act, 23 March 2018 (The US CLOUD Act).

31 Bek. nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.

32 Datatilsynets årsrapport 2018, p. 10.

33 Datatilsynets årsrapport 2019, p. 11.

© 2020 Law Business Research Ltd

and the DPA has now announced a number of planned written and physical audits regarding different business areas and different data protection subjects twice a year. For example, the DPA plans to audit data processors' security measures and use of sub-processors and employers' surveillance of employees.[34] Furthermore, the DPA also perform a number of audits based on the DPA's own initiative, complaints etc., but it seems that such audits also are notified to the controller or processor being audited prior to the audit. The DPA has not published the number of actual raids or unannounced audits after the GDPR came into force, but it seems to be quite few if any at all.

According to Article 58 of the GDPR, the DPA also has a number of corrective and sanctioning powers, including the power to issue warnings about intended processing operations likely to infringe the Data Protection legislation; to issue reprimands where processing activities have infringed the Data Protection legislation; to order processing operations brought into compliance with the GDPR and to impose temporary or definitive limitations including bans on processing activities.

The Danish legal system does not provide for administrative fines, which means that the processing activity infringing the Data Protection legislation is reported to the police by the DPA with an indicated fine, after which the prosecution will build a case against the defendant. The procedure is subject to the general rules of criminal procedure set out in the Danish Administration of Justice Act, which governs all aspects of civil and criminal proceedings. In Denmark, any fine for infringement of the Data Protection legislation is therefore imposed by the courts of Denmark.

Private companies and persons infringement of the GDPR (and the Data Protection Act) is subject to fines up to €10 million or in the case of an undertaking, up to 2 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, regarding among other things infringement of the provisions regarding children's consent in relation to information society services (GDPR, Article 8), Data protection by design and by default (GDPR Article 25) and codes of conduct and certification (GDPR, Articles 41–43).

Private companies and persons infringement of the GDPR (and the Data Protection Act) is subject to fines up to €20 million or in the case of an undertaking, up to 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, regarding among others infringement of the provisions regarding the basic principles and legal grounds (GDPR Articles 5–7 and 9), data subject rights (GDPR, Articles 12–22), international transfer of personal data (GDPR, Articles 44–49) and the Data Protection Agency's corrective orders (GDPR, Article 58).

Any infringement of the Data Protection legislation by Danish public authorities and institutions is subject to a fine of up to 4 per cent of the annual operating grant up to a maximum of 16 million kroner.

The DPA registered 15,681 cases in 2019, including hearings regarding the drafting of laws and executive orders of importance for the protection of privacy, investigations, audits, security breaches and international cases, as opposed to 5,024 registrations in 2017 and 12,205 in 2018.[35]

Data protection and privacy did not have great importance in Denmark before 25 May 2018, and the most obvious reason for this is without a doubt that infringement of

34 The DPA's published audit plans for the first half of 2019: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/jan/planlagte-tilsyn-i-foerste-halvaar-af-2019/.

35 The DPA's annual report for 2019, p. 11.

© 2020 Law Business Research Ltd

the data protection regulation was subject to none or hardly any sanctions pre-GDPR. This is emphasised by the fact that the highest fine issued in Denmark prior to 25 May 2018 was 25,000 kroner.

It is safe to say that post-GDPR, data protection has been taken seriously by Danish companies and public authorities, which is largely as a result of the DPA's increased activities as discussed above. In 2019 and 2020, the DPA has issued a series of reprimands, bans and warnings, and in three cases the DPA has reported a private company to the police for infringement of the GDPR with indicated fines of 1.5 million, 1.2 million kroner and 1.1 million kroner respectively, all three regarding infringement of Article 5(1)(e) of the GDPR, because said companies stored personal data for longer periods than necessary for the purposes for which the data was processed.

ii Recent enforcement cases

The most significant recent cases are the above-mentioned cases, which are the first data protection enforcement cases in Denmark.

The first case relates to a taxi company that had stored approximately 9 million collection and drop-off points linked to customer telephone numbers that could therefore be linked to specific people. The taxi company had attempted to anonymise the information by erasing customer names and argued that a longer retention period regarding the telephone numbers was necessary for business development purposes and that telephone numbers were 'the key to the database'. The DPA stated that the taxi company had no legitimate purpose for the separate retention period regarding telephone numbers, and that a controller or processor cannot base a processing activity's purpose on the fact that a system makes it difficult to comply with the GDPR. The DPA reported the infringement to the police with an indicated fine of 1.2 million kroner.

The second case relates to a retail company that had stored personal data regarding approximately 385,000 private customers in a primarily phased system without setting a retention period for the data in question. In this case, the DPA has reported the infringement to the police with an indicated fine of 1.5 million kroner.

The third case relates to a hotel group that had stored customer profiles regarding approximately 500,000 private customers in a booking system for a longer period than necessary for the purpose for which the personal data was collected and the group's internal established retention periods.

All three cases are based on DPA planned audits, and the indicated fines will – if sanctioned by the court – be the highest fines ever imposed in Denmark regarding a data protection infringement.

Neither case has been settled by the Danish district court, and due to their public importance, it is expected that both cases will be appealed to the Danish High Court and possibly even to the Danish Supreme Court.

Furthermore, the DPA has reported two city governments to the police for infringement of the GDPR with indicated minor fines of 25,000 kroner and 50,000 kroner respectively, both regarding infringement of Article 5(1)(f) and Article 32 of the GDPR, because work computers containing nonencrypted personal data, including social security numbers, regarding the city government employees and city residents was stolen.

In other cases, the DPA has refrained from reporting infringements to the police, even though the infringement appeared to be of the same nature as those mentioned above. The DPA has instead issued reprimands, ordered a processing activity to be brought into

© 2020 Law Business Research Ltd

compliance with the GDPR or imposed temporary or definitive limitations on processing activities. The DPA, for example, imposed a temporary ban on one of Denmark's largest telecommunication companies for recording costumer calls without customer consent, even though the reason that the company did not collect costumer consent was that their system did not support this. The number of customer call recordings without legal grounds has not been published, but it seems that the nature of this infringement is at least as serious as the above-mentioned cases resulting in a police report.

Looking generally at the DPA's post-GDPR practice, it is still very difficult to deduce any guidance revealing which infringements will result in a police report with an indicated fine and a subsequent criminal case, and which infringements will entail less severe sanctions, such as a ban or a reprimand. However, it is hope that this will become clear in the years to come, when more criminal cases have been settled and DPA sanctions have been imposed.

iii Private litigation

According to Article 82 of the GDPR, any person who has suffered material or non-material damage as a result of an infringement of the GDPR (or the Data Protection Act) shall have the right to receive compensation for the damage suffered. In many cases, private persons have insurance that covers legal expenses related to lawsuits, and there are almost no other options for free legal aid in Denmark. Private lawsuits regarding data protection are not common in Denmark, neither before nor after the GDPR came into force. Furthermore, Denmark has no tradition for pursuing claims by class action, which was first legalised in Denmark in 2008.

Due to the significantly increased public awareness regarding data protection post-GDPR, we may see more lawsuits where private individuals seek recovery (e.g., regarding data breaches or infringement of data subject rights). Nonetheless, an important basic principle of Danish law on damages is that a claim for damages can only cover the plaintiff's actual loss. In special cases – primarily criminal offences – the plaintiff may seek a special compensation (tort law) in addition to damages. According to Danish case law and the Danish Liability for Damages Act, a plaintiff may claim such compensation in cases regarding data protection; however, awarded amounts so far have been relatively small. Pre-GDPR, Danish courts awarded amounts of 5,000–25,000 kroner of compensation. No civil lawsuits have been settled in Denmark post-GDPR, but it is not expected that Danish courts will increase compensation amounts in future, mainly because compensation is regulated by the Danish Liability for Damages Act as opposed to the Data Protection legislation. It is thus likely that we will see more class actions in future, because the costs of a civil lawsuit in practice will be significantly higher than the potential compensation.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The principle of accountability in the GDPR entails that data handlers must be able to provide sufficient documentation for complying with the data protection legislation. In addition to the mandatory documentation (e.g., records of data processing activities in accordance with Article 30 of the GDPR or data processing agreements in accordance with Article 28 of the GDPR), data handlers are recommended to maintain clear and transparent documentation of their compliance efforts, and should be ready to hand over the documentation to the

© 2020 Law Business Research Ltd

DPA upon request. The documentation should provide evidence of general compliance, including but not limited to education of employees, policies, retention, risk assessments and the technical and organisational measures

Furthermore, it is recommended that data handlers implement efficient management and control procedures to adhere to the deadlines in the GDPR, for example, responding to personal data breaches within 72 hours or replying to data subject access requests within 30 days.

IX CYBERSECURITY AND DATA BREACHES

Cybersecurity

Denmark's latest national strategy for cyber and information security was launched in May 2018. Thirteen ministries were involved in the work on the strategy, which reflects an ambitious intention to upgrade the overall level by operation of three main efforts, involving 25 concrete initiatives and a total state investment of 1.5 billion kroner. The efforts consist of:

a technical upgrades of cyber-defence;

b general knowledge and awareness about cyber- and information-security threats among citizens, companies and authorities; and

c coordination and cooperation between the responsible authorities.

The main purpose of the strategy is to ensure that Danish citizens, companies and authorities are able to handle digital risks should they occur.

Denmark ranks 11th in the latest update of the international National Cybersecurity Index (NCSI), which is a fall from seventh in 2019.[36] The lower ranking is primarily due to the fact that Denmark has not contributed to global cybersecurity recently; however, the relatively high ranking does show that Denmark is generally regarded as a competent nation in respect of cybersecurity.

Data breaches

In the case of a personal data breach, the controller shall, without undue delay and where feasible not later than 72 hours after having become aware of it, notify the personal data breach to the DPA, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. All data breach notifications should be handed in electronically via the website virk.dk.[37]

The DPA receives between 600 and 800 data breach notifications per month from private and public authorities. It is, however, believed that a number of data breaches are not reported to the DPA. Seventy per cent of all notifications concern isolated errors, where personal data are sent to a wrong recipient; however, breaches due to phishing, malware or hacking are gradually increasing.[38]

36 https://ncsi.ega.ee/.

37 https://indberet.virk.dk/myndigheder/stat/ERST/Indberetning_af_brud_paa_sikkerhed#tab1.

38 The DPAs quarterly report on personal data breaches: Anmeldelser af brud på persondatasikkerheden, Fjerede kvartal 2019, February 2020.

© 2020 Law Business Research Ltd

X OUTLOOK

The GDPR has probably had more effect on Danish society in general, including the Danish business community and public authorities than any other legislation ever implemented in Denmark. Most companies still have comprehensive compliance work ahead, and many have still not commenced their compliance work even though more than two years have now passed since the GDPR came into force. In the years to come, DPA sanctioning and the pending criminal cases in Denmark as well as in Europe will form applicable case law and guidelines, both regarding the sanctioning level and, for example, specific retention periods; the extent of the legal grounds in the Data Protection legislation and will hopefully answer many of the unanswered key questions arising from the GDPR.

© 2020 Law Business Research Ltd

Appendix 1

ABOUT THE AUTHORS

TOMMY ANGERMAIR

Clemens

Tommy Angermair is a partner in the Danish law firm Clemens and the head of the law firm's employment, data protection and corporate immigration law practice group. Tommy is one of the most experienced Danish experts on data protection law (including GDPR) compliance having provided advice on this topic since 2004. Tommy and the rest of Clemens' very experienced data protection team is currently heavily involved in several GDPR compliance projects for mainly medium-sized and large companies, including several large multinationals. Furthermore, Tommy is specialised in corporate immigration law (WPs, business visas for inbound personnel, advising high net worth individuals etc.), which means that he has a profound understanding of the data protection consideration in relation to running an immigration law practice. Tommy Angermair annually speaks at international legal conferences across the globe. Among other things, he is a frequent speaker at the AILA GMS annual conference in the US and the biennial IBA Global Immigration & Nationality Law conference on topics related to immigration, data protection and mobility. He has contributed to several primarily international publications within his area of expertise, including the chapter on Denmark in the recent editions of the *Global Business Immigration Handbook* and *The Employment Law Review*.

CAMILLA SAND FINK

Clemens

Camilla is a senior associate and head of data privacy team in the Danish law firm Clemens, and part of one of the leading and most experienced data protection law practice groups in Denmark. Camilla has a background as corporate legal counsel and GDPR compliance officer in an international energy group headquartered in Denmark. Camilla provides data protection advice within all areas of data protection law, including compliance assessments and implementation issues, interpretation of the GDPR as well as handling of rights request, data breaches and complaints to the Danish Data Protection Agency. Camilla advises all client types and has been involved in several national and international compliance projects for mainly medium-sized and large companies and multinationals. In addition, Camilla is network leader in a data protection network facilitated by one of the leading legal network and course providers in Denmark, and regularly gives presentations on personal data challenges and issues. Finally, Camilla has extensive litigation experience and is qualified to appear before the Danish high courts.

© 2020 Law Business Research Ltd

SØREN BONDE

Clemens

Søren is third-year associate in the Danish law firm Clemens, and part of one of the leading and most experienced data protection law practice groups in Denmark. Søren has a background as a legal manager in a multinational IT company headquartered in Denmark. With his background as a master of business law (MSc Law) as well as a master of law (LLM), Søren is particularly skilled at the analysis of complex legal issues with a view to obtaining the best possible commercial result. Søren has extensive experience with assisting clients in their purchase and development of IT applications and new technologies in an efficient and pragmatic manner, especially in connection with assessment of legal consequences when developing or utilising new products and technologies in relation to protection of personal and corporate data. Moreover, Søren advises all client types on data protection issues, including in particular compliance assessments and general implementation issues and interpretation of the GDPR, preparation of data processor agreements and privacy policies. In addition, Søren regularly gives presentations on personal data challenges and issues.

CLEMENS

Skt. Clemens Straede 7
8000 Aarhus C
Denmark
Tel: +45 87 32 1250
Fax: +45 87 32 1251
tma@clemenslaw.dk
csf@clemenslaw.dk
sbo@clemenslaw.dk
www.clemenslaw.dk

© 2020 Law Business Research Ltd

an LBR business

ISBN 978-1-83862-485-9

© 2020 Law Business Research Ltd