IN-DEPTH

Privacy, Data Protection and Cybersecurity

EDITION 10

Contributing editor
Alan Charles Raul
Sidley Austin LLP

LEXOLOGY

Published in the United Kingdom
by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.thelawreviews.co.uk

ISBN 978-1-80449-214-7

Acknowledgements

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

ANDERSON LLOYD

ANJIE BROAD LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS LAW FIRM

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

JACKSON, ETTI & EDU

KALUS KENNY INTELEX

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

Chapter 8

DENMARK

Camilla Sand Fink and Amanda Langeland Knudsen[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] In Denmark, the main legislation concerning processing of personal data is the GDPR and the Danish supplementary act, the Data Protection Act.[3]

In addition to the rules of the GDPR, the Data Protection Act (DPA) and national practice implement 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 21 years old, not much attention was paid to data protection in Denmark until the GDPR was passed in 2016.

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.

II THE YEAR IN REVIEW

Today, most companies are focused on GDPR compliance maintenance, daily compliance work, auditing of data processors' compliance, etc., but some (minor and medium-sized) companies seem to have chosen a more risk-based approach to their compliance work and have not (yet) initiated any structured compliance work, even though more than five years have passed since the GDPR came into full force.

---

1 Camilla Sand Fink is a partner and Amanda Langeland Knudsen is an assistant attorney at CLEMENS Law Firm.

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.

In 2023, the dominant topic in terms of data privacy and data protection continues to be third country transfers. In particular, the focus has been on transfers to the US and the use of subprocessors located in the EU but owned by American mother companies, including Microsoft, Google and Amazon Web Services. Furthermore, there has been an increasing focus on the processing of personal data regarding website visitors and the protection of children's personal data.

Among other developments in the past year, the DPA has issued several new or updated guidelines on data protection in an employment context, TV surveillance for private companies and direct marketing.[4]

Over the past two years, the DPA has been focusing specifically on the use of Chromebooks and Google Workspace (formerly G Suite for Education) in Danish municipalities. In the summer of 2022, the Danish DPA imposed a processing ban on the use of Google Workspace in the municipality of Helsingør, as the Danish Data Protection Agency assessed that the municipality's documentation did not fulfil the requirements of the GDPR. As a result of the ban, Danish elementary school children had to be taught without the use of Chromebooks. The use of Chromebooks in Danish elementary schools is nationwide, resulting in the National Association of Local Authorities in Denmark joining in and trying to legalise the municipalities' use of Chromebooks. The ban was later suspended, but at the time of writing, the case has not yet been settled. The case highlights important issues regarding the use of cloud services, including the obligation to document the data flows, use of data for other purposes, risk and impact assessments and transfers of personal data to third countries.

At the time of writing, the DPA has reported a total of 27 companies and public authorities to the police for infringement of the GDPR with indicated fines between 50,000 kroner and 10 million kroner, since the GDPR came into force.

Eight cases have been settled by the Danish District Court. In three cases, the Danish District Court reduced the indicated fines, one company received a warning and another one was acquitted. In three cases, the Danish District Court agreed with the fines recommended by the DPA. In two of the cases in particular, there has been a significant difference between the fines recommended by the DPA and the size of the fine imposed by the Danish District Court. In the first case (*ID design*), the Danish District Court reduced the indicated fine from 1.5 million kroner to 100,000 kroner, but the ruling was appealed to the Danish High Court. The appeal case should have been resolved in January 2022 but has been postponed indefinitely, as the Danish Ministry of Justice is evaluating whether to go through the preliminary reference procedure for assistance from the CJEU with regard to interpretation of Article 83 of the GDPR and imposing of fines. In the second case (*Taxa 4x35*), the DPA

4 The guidelines from the DPA concerning data protection in an employment context are only available in Danish at https://www.datatilsynet.dk/Media/0/8/Vejledning%20om%20databeskyttelse%20i%20forbindelse%20med%20ansættelsesforhold.pdf. The guidelines from the DPA concerning direct marketing are only available in Danish at https://www.datatilsynet.dk/Media/638237218449834564/Vejledning%20om%20direkte%20markedsføring.pdf. The guidelines from the DPA concerning CCTV surveillance for private companies at https://www.datatilsynet.dk/Media/638234600620556007/Vejledning%20om%20tv-overvågning%20-%20private%20virksomheder.pdf.

recommended a fine of 1.2 million kroner. Almost four years later – on 6 January 2023 – the Danish District Court reduced the indicated fine to 100,000 kroner. The Danish Prosecution Service has appealed the case.

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 legislation shall naturally be interpreted in accordance with the principles of the GDPR.[5]

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 guidelines describing how companies must adhere to the Data Protection legislation.[6] Even though the guidelines are not legally binding, they are generally taken very seriously, given the DPA's role as primary regulator and enforcer of the data protection rules in practice.

ii General obligations for data handlers

Data controllers are not obligated to register with the DPA in relation to their processing of personal data. However, when the nature of the processing of personal data requires a data processing impact assessment (DPIA) according to Article 35 of the GDPR, the data controller is obligated to consult the DPA prior to processing subject to Article 36 of the GDPR.

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.

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

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

To comply with the obligation to notify the data subject in accordance with Articles 13–14 of the GDPR, the data 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 must search for. The data controller may refer to the information on a website or similar with a direct link to the website with the information, but as a rule of thumb the information shall maximum be 'one click away'. The form of notification shall reflect the means of collecting personal data. The data 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.[7]

Prior to transmitting confidential (see Section IV) and special categories of personal data, 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 by the EDPB as standard contractual clauses. The template is available in multiple languages at the DPA's website.[8]

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 and emails.

The controller may request the data subject to clarify or 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. As a clear starting point, most access requests will be considered legitimate, and the data controllers will consequently be obliged to comply, but the DPA has ruled in favour of the data controller in several complaint cases where the data controller refused to comply with an access request. In this regard, the DPA has stated that the data controllers' refusals to comply with the access requests were legitimate because the access requests were excessive, or because the request included a large number of documents that could contain information about the data subject, but where one had to assume that any information about the data subject would only appear 'accessory' in relation to the purpose of the documents (in this context business operations).[9]

According to the Data Protection Act, the controller may derogate from the right of access (and the obligation to notify the data subject of matters concerning Article 13(1)–(3) and 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

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

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

9 DPA Case No. 2021-32-2438 and Case No. 2021-31-5085.

the consideration for the data subject, 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 rectify 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 rectify 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.

The DPA is making special efforts to ensure the data protection of children and making data protection accessible to children, namely by making a page on the website dedicated to children. Furthermore, the DPA clarified in a recent statement that data subject rights are personal and must thus be invoked by the child with the assistance of the parent if necessary.[10]

iv Specific regulatory areas

The DPA distinguishes between 'regular data' and 'confidential data' in respect of personal data under Article 6 of the GDPR. Confidential data 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 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 can generally no longer take place based on consent from the employee in accordance with Article 7 of the GDPR. This has been stated by the DPA in the recent (2023) revised guidance on data protection in employment contexts.[11] Consent in an employment context will rarely fulfil the condition of being freely given due to the unequal relationship that typically exists between employer and employee. Instead, the legal basis for processing personal data in connection with obtaining or disclosing references, obtaining

10 Press release from the DPA regarding parents exercising data subject rights on behalf of their children (only available in Danish): https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/maj/naar-foraeldre-soeger-om-indsigt-i-barnets-oplysninger-.

11 The guidelines from the DPA concerning data protection in an employment context control with data processors are only available in Danish at https://www.datatilsynet.dk/Media/0/8/Vejledning%20om%20databeskyttelse%20i%20forbindelse%20med%20ansættelsesforhold.pdf.

criminal records, publication of recruitment and marketing videos and use of employee photos on the employer's website must typically be found in either Article 6(1)(f) of the GDPR for private employers or Article 6(1)(e) of the GDPR for public employers.

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 autoreply 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.[12]

The 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.

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.[13] Direct marketing means when personal data is used to make direct contact with the data subject, for example, via email, SMS, Messenger or similar.

In particular, a controller cannot 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 prohibited from disclosing 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 declined receiving inquiries for marketing purposes via the CPR register. 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.

Section 99(d) of the Danish Financial Statements Act[14] imposes an obligation on 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.

12 DPA Case No. 2018-31-0977.

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

14 Act No. 1441 of 14 November 2022.

In addition, the Danish Financial Supervisory Authority has added similar requirements in three executive orders on financial reporting.[15] Furthermore, the authority has recently submitted a paper on good practice for data ethics when using AI in the financial sector for public consultation.[16]

v Technological innovation

Cookies

The use of cookies, namely a piece of text stored on the end user's device (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 contains personal data. Regardless of whether the collected data contains 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 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. The DPA has recently clarified the legality of cookie walls in two cases.[19] The DPA stated that an approach where the website visitor can access the content of a website or service in exchange for either giving consent to the processing of his personal data via cookies or payment meets the requirements for a valid consent as long as certain conditions are met in regard to proportionality of the price and similarity in services or content no matter the means of access.

The Ministry of Industry, Business and Financial Affairs, which is the supervisory authority of the Cookie Act, has announced that it will not prioritise auditing the use of simple statistical cookies used solely for traffic measurement and optimising the website in line with the approach of several other EU Member States. When (statistical) cookies collect personal data, the GDPR will nonetheless continue to apply and thus such use will still be audited by the DPA.

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 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.[20] In a recent case, the DPA ordered a Danish company to bring the

15 Executive Order no. 1593 of 9 November 2020, No. 771 of 31/05/22, and No. 460 of 2 May 2023.

16 Only available in Danish: https://www.finanstilsynet.dk/Nyheder-og-Presse/Sektornyt/2023/Hoering_dataetik_ai_170523.

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

18 C-673/17.

19 DPA Case No. 2021-31-4871 and Case No. 2021-31-5553.

20 C-210/16.

use of Facebook Business Tools into compliance with the GDPR. Specifically, the joint data controller terms provided by Meta referred to by the company were deemed insufficient in determining their respective responsibilities for compliance with the obligations under the GDPR.[21]

Surveillance

According to the Video Surveillance Act,[22] private surveillance of publicly accessible areas is prohibited. However, numerous 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 TV Surveillance Act, the rules of the Data Protection legislation apply to the processing of personal data in surveillance footage, including the rules on notifying the data subject in accordance with Articles 13–14 of the GDPR. The controller conducting TV 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.

Artificial intelligence (AI) and facial recognition

The DPA has established a task force for the use of AI and the data protection challenges arising from such technologies with the ambition to publish guidelines on the use of AI in compliance with the GDPR as well as a subsequent inspection hereof.

Just as with artificial intelligence, the interest for using facial recognition is increasing. In a ruling from the DPA, a data controller's use of facial recognition as access control based on consent was deemed in compliance with the GDPR. However, the ruling included a clear statement from the DPA, emphasising that use of facial recognition for statistical and business optimising purposes is likely to be prohibited.[23] Additionally, the EDPB has adopted guidelines on the use of facial recognition technology regarding law enforcement.[24]

21 DPA Case No. 2021-7329-0052.

22 Act No. 1190 of 10 November 2007.

23 DPA Case No. 2021-431-0145.

24 https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en.

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)[25] 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 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.

At 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, the Isle of Man, Israel, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom, the United States (commercial organisations participating in the EU–US Data Privacy Framework (DPF)) and Uruguay.

Until the *Schrems II* ruling, the United States was limited to the EU–US Privacy Shield adequacy decision recognised by the European Union for providing adequate protection, but the adequacy decision was invalidated by the CJEU on 16 July 2020.[26] On 10 July 2023, the European Commission adopted an adequacy decision for the DPF. This means that personal data can be transferred from the EU to US organisations certified under the framework without the need for additional data protection and security measures.[27] The framework introduces new binding safeguards to address concerns raised by the European Court of Justice in relation to the *Schrems II* case (C-311/18), including limiting access to EU data by US intelligence services to what is necessary and proportionate, and establishing a Data Protection Review Court (DPRC), to which EU individuals will have access. The adequacy decision can only be used as a legal basis for a transfer when transferring personal data to US organisations certified under the DPF with the US Department of Commerce. Companies such as Google, Amazon and Microsoft have already been certified, opening the door for companies and governments within the EU to transfer personal data by use of programs such as Google Analytics and clouds with a parent company in the US once again. However, several challenges remain with the use of these tools, which the DPA has also emphasised in the wake of the adequacy decision.[28] Furthermore, NOYB has already declared that it is going to challenge the DPF; therefore many organisations are tensely awaiting the fate of the DPF and whether enough has changed compared to the EU–US Privacy Shield Framework.

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 to enforce data subject rights and effective remedies are available.

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

26 Case C 311/18 *Schrems II*.

27 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

28 Press release from the Danish DPA (only available in Danish): https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/jul/brug-af-google-analytics-kraever-ikke-kun-lovlige-overfoersler-til-usa.

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. On 4 June 2021, the EU Commission adopted a new set of modernised standard contractual clauses expanding the safeguards to include transfers between exporting and importing data processors and exporting data processors and importing data controllers, hence the standard clauses now include four modules for transferring personal data to third countries (module one: data controller to data controller, module two: data controller to data processor, module three: data processor to data processor and module four: data processor to data controller).[29]

Furthermore, the standard clauses (modules two and three) also include a data processing agreement in accordance with Article 28 of the GDPR. From 27 December 2022, all existing and future transfers based on the standard contractual clauses shall be concluded on the new standard clauses.

The standard contractual clauses may be included in other contractual material, such as trade agreements provided that no changes are made to the clauses.

Finally, following the *Schrems II* ruling, the exporting party is obligated to assess whether the data protection level in the third country is essentially equivalent to the level of protection in the EU and identify and implement appropriate supplementary measures to ensure an equivalent level of security if deemed necessary. On 21 June 2021, the EDPB issued guidelines on such supplementary measures.[30]

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. Nonetheless, in 2022 the EDPB published guidelines on both codes of conduct and certifications as transfer tools, which will hopefully contribute to and accelerate the future work with developing and adopting such codes of conducts or certifications.[31]

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.

29 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

30 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

31 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_en and https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-072022-certification-tool-transfers_en.

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 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 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 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 the transfer is necessary for important reasons of public interests; and

e 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 and appropriate safeguards may only take place under the following derogating circumstances listed in Article 49(1) of the GDPR:

a the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject as a result of the absence of an adequacy decision and appropriate safeguards;

b the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

c 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;

d the transfer is necessary for important reasons of public interest;

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

f the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; and

g the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where also none of the above derogations apply, transfer may lastly take place in accordance with the second subparagraph of Article 49(1) of the GDPR. In 2022, the DPA issued new guidelines regarding the use of cloud service providers, which to some extent establishes the scope of legal transfers to third countries. First of all, the DPA advises data exporters to apply the assumption that all third countries have 'problematic' legislation or practice, or both. Furthermore, specifically regarding 'problematic' legislation in the US, which in practice is the most important third country when it comes to cloud service providers, the DPA further stated that it will be difficult in practice for the exporter to document that the specific types of personal data being transferred to cloud service providers in the US will not be subject to

the surveillance programmes authorised under, inter alia, FISA 702. However, the safeguards that have been put in place by the US government in connection with the adequacy decision for the DPF in the area of national security (including the redress mechanism) apply to all data transferred to the US, regardless of the transfer tool used. Therefore, when assessing the effectiveness of the chosen transfer tool, data exporters should take into account the assessment conducted by the Commission in the adequacy decision.

Furthermore, if a cloud service provider is based in the EU or EEA and solely processes the personal data geographically within the EU or EEA, Chapter V of the GDPR does not apply. Following an inquiry regarding the guidelines on the use of cloud service providers, the DPA has stated that a transfer of personal data to a cloud service provider in the EU or EEA that is ultimately owned by a mother company in a third country will be classified as a third country transfer subject to Chapter V of the GDPR, if the data processing agreement between the data controller and the cloud services provider includes a provision giving the cloud service provider the right to disclose the personal data on the basis of a request from a public authority in a third country where the mother company is located.[32] In such circumstances, Chapter V of the GDPR will apply. However, if the cloud service provider is part of a group and ultimately owned by a mother company located in a third country, and the cloud service provider due to the group structure is forced to comply with a request from law enforcement authorities in the third country where the parent company is established and the disclosure will be in violation of the data processing agreement between the data controller and the cloud service provider, the transfer is to be considered as an 'unintentional' transfer by the cloud service provider and consequently classified as a data breach rather than a transfer regulated by Chapter V of the GDPR.

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

32 DPA Case No. 2022-212-3529.

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, how to identify data breaches, e-learning or other relevant education regarding the processing of personal data and internal GDPR awareness campaigns;

e cookie policy regarding all websites and technical measures to ensure end user consent to placement of cookies on end user terminal equipment;[33]

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 do so 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;

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, legislation on bookkeeping, accounting and tax and DPA case law. The retention period must, however, always be determined in the context of the specific processing activity, including, for example, a storage purpose in order to defend a legal claim. Consequently, the controller must determine how long after the end of the processing activity a dispute is likely to arise based on the data controller's experience. It will not be lawful to store information if there is only a hypothetical interest in storing personal data for the identified purposes. General statutes of limitation therefore cannot solely justify a certain retention period;[34]

33 Proclamation 1148 of 9 September 2010 on requirements for information and consent when storing or accessing information in the end-user's terminal equipment (The Cookie Order) implementing Directive 2002/58/EC (the ePrivacy Directive).

34 The Danish Data Protection authority's guidelines regarding retention of documentation and data minimisation (only available in Danish): https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/samtykke/paavisningskrav-og-dataminimering.

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 in accordance with the outlined retention periods, auditing 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;

f internal guidelines and procedures to ensure employees are informed in accordance with Articles 13–14 of the GDPR when employers 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. If the processing of employee photos is based on their consent exceptionally, there must be procedures and privacy policies ensuring the validity of the consent (underlining the free nature of the consent);

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[35] and consent to approach consumers by telephone for the purpose of direct marketing;[36]

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

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

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), Article 8 of the 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 (according to Sections 298(1) and 299(1) of the Danish Administration of Justice Act,[37] 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

35 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.

36 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.

37 Act 2020-09-29, No. 1445 (the Danish Administration of Justice Act).

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 Article 11(3) of the Data Protection Act. 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.

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.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Based on the Data Protection legislation, the DPA is essentially the only enforcement agency with regard 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,[38] 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 were 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;[39] and in 2022, the DPA held 513 audits.[40] The numbers include planned written and physical audits and raids. After the GDPR came into force, the DPA's audits have increased substantially, and the DPA regularly announce planned written and physical audits regarding different business areas and different data protection subjects. Furthermore, the DPA also performs a number

38 Executive Order No. 462 of 23 May 2016 on personal data security in connection with the provision of public electronic communications and services.

39 The DPA's annual report for 2018, p. 10.

40 The DPA's annual report for 2022, p. 24.

of audits on the DPA's own initiative or based on complaints, etc. 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 in violation of the GDPR (and the Data Protection Act) may be subject to fines of 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 in violation of the GDPR (and the Data Protection Act) may be 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 other things 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 16,896 cases in 2022, 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.[41]

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 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 a result of the DPA's increased activities as discussed above. Between 2018 and 2023, the DPA issued a series of reprimands, bans

41 The DPA's annual report for 2022, p. 18.

and warnings. In 27 cases the DPA reported a private company or public authority to the police for infringement of the GDPR with indicated fines of between 50,000 kroner and 10 million kroner.

ii Recent enforcement cases

The most significant cases are still some of the first data protection enforcement cases in Denmark.

The first case concerns Danske Bank, which had stored customer information in more than 400 IT systems for a longer period than necessary for the purpose for which the personal data had been collected. Furthermore, the bank did not have sufficient retention policies in place or any procedures to ensure deletion of personal data in the 400 IT systems. Consequently, the DPA reported the infringement to the police with an indicated fine of 10 million kroner, which is the highest indicated fine in Denmark to date. At the time of writing, the case has still not been settled.

The second case concerns a publishing company, which had stored personal data regarding 685,000 former book club members for a longer period than necessary for the purpose for which the personal data had been collected. Personal data from 395,000 of the former members had been stored for more than 10 years after the end of their membership. The DPA reported the infringement to the police and indicated a fine of 1 million kroner. At the time of writing, the case has still not been settled.

The third case relates to a cancer charity organisation which failed to implement the safety measures that the organisation had previously deemed necessary in connection with a safety breach in 2018. As a result, health data from 1,448 persons was compromised in several later cyberattacks that could have been prevented had organisation implemented the appropriate safety measures. The DPA reported the infringement to the police and indicated a fine of 800,000 kroner in 2021, but the case has not been settled yet.

Additionally, the DPA has reported several public authorities to the police for infringement of the GDPR with indicated fines of between 50,000 kroner and 500,000 kroner, several regarding infringement of Article 5(1)(f) and Article 32 of the GDPR.

Looking generally at the DPA's post-GDPR practice, it is still very difficult to deduce any guidance as to which which infringements will result in a police report with an indicated fine and a subsequent criminal case; or deduce how the Danish courts will settle the cases and which infringements will entail less severe sanctions, such as a ban or a reprimand. However, hopefully it 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 or loss 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 data protection lawsuits are not common in Denmark, before and 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.

As a result of 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 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 compensation amounts in the range of 5,000–25,000 kroner. Only one civil lawsuit has been settled in Denmark post-GDPR, where the Danish District Court awarded the plaintiffs compensation of between 7,000 kroner and 30,000 kroner; thus the Danish courts have not increased compensation amounts post-GDPR, which is mainly because compensation is regulated by the Danish Liability for Damages Act as opposed to the Data Protection legislation. Furthermore, it is not 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 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

i Cybersecurity

Denmark's latest national strategy for cyber and information security was launched in December 2021. Several ministries were involved in the strategy work, which reflects an ambitious intention to upgrade the overall level by operation of four main efforts, involving 34 new concrete key initiatives and a new total state investment of 270 million kroner. The efforts consist of:

a robust protection of vital social functions;
b increased level of skills and management commitment;
c strengthening of the cooperation between the public and private sector; and
d active participation in the international fight against the cyber threat.

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

infrastructure and IT systems in Denmark. For example, one of the initiatives in the strategy is the 'data warehouse'. The purpose of this data warehouse is to create a public database with broad and updated data on reported data breaches.

Denmark ranks 17th in the latest update of the international National Cybersecurity Index (NCSI), which is a fall from 11th in 2020.[42] The lower ranking is primarily as a result of the fact that Denmark has not contributed to global cybersecurity or cyber crisis management recently, which aligns with the announced main efforts of the new strategy for cyber and information security; however, the relatively high ranking does show that Denmark is generally regarded as a competent nation in respect of cybersecurity.

ii 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.[43]

The DPA receives between 600 and 1,000 data breach notifications per month from private and public authorities. It is, however, believed that a number of data breaches are still not reported to the DPA. More than 50 per cent of all notifications concern isolated errors, where personal data are sent to a wrong recipient; however, breaches as a result of phishing, malware or hacking are gradually increasing.[44]

X SOFTWARE DEVELOPMENT AND VULNERABILITIES

Software development and vulnerabilities is in part subject to the GDPR and the Network and Information Security Directive (NIS2) that entered into force replacing the NIS Directive 2016/1148.[45] In terms of the GDPR the legal requirements are centred on privacy by design and by default, implementing adequate technical and organizational measures and the obligation to report data breaches to the DPA. Although NIS2 has yet to be implemented in Danish law the NIS Directive has been implemented with an array of Danish sector specific laws that also requires covered operators to put appropriate technical and organisational measures into place as well as incident reporting requirements.[46]

Furthermore, the NIS2 Directive expands the scope of incident reporting as also 'near miss' events defined as events that could have compromised the availability, authenticity,

42 https://ncsi.ega.ee/.

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

44 The DPAs webpage about statistics for reported data breaches: https://www.datatilsynet.dk/sikkerhedsbrud/statistik-over-anmeldte-sikkerhedsbrud.

45 Directive (EU) 2022/2555 (NIS2) replacing Directive (EU) 2016/1148 (NIS).

46 Implemented by the Law on network and information security for domain name systems and certain digital services (Law No. 436 of 8 May 2018), Law on security in network and information systems in the transport sector (Law No. 441 of 8 May 2018), Law on safety requirements for network and information systems in the health sector (Law No. 440 of 8 May 2018), Law on security in network and information systems for operators of major internet exchange points (Law No. 437 of 08 May 2018), Executive Order on disclosure and disclosure obligations regarding network and information security (Executive Order No. 258 of 22 February 2021) and Executive Order on IT Preparedness for Electricity and Natural Gas Sectors (Executive Order No. 2647 of 28 December 2021).

integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise. It will be possible to report these voluntarily. In addition, Denmark's latest national strategy for cyber and information security states an ambition to launch a pilot of a government CVD (coordinated vulnerability disclosure) policy describing the framework for government agencies to allow private individuals (i.e., 'helpful hackers') to identify and report vulnerabilities in ICT systems.[47] However, the policy has yet to be published.

XI DIGITAL GOVERNANCE AND CONVERGENCE WITH COMPETITION POLICY

Technology platforms such as social media, search engines, cloud providers and internet companies are predominantly regulated, governed and restrained by the EU Digital Markets Act, Digital Services Act and Data Governance Act, supplemented by general Danish regulatory frameworks such as the data protection regulation, marketing regulation and competition regulation.

Furthermore, the Nordic Competition authorities in Denmark, Finland, Iceland, Norway and Sweden have collectively published recommendations and policy suggestions for EU competition law framework handling anticompetitive behaviour in the digital economy.[48]

XII 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 five years have now passed since the GDPR came into force. In the years to come, DPA sanctioning and the pending criminal cases in Denmark and 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.

47 https://digst.dk/media/27024/digst_ncis_2022-2024_uk.pdf.

48 https://www.kfst.dk/analyser/kfst/publikationer/dansk/2020/20200928-digital-platforms-and-the-potential-changes-to-competition-law/.

ISBN 978-1-80449-214-7