Lov & Data

Nr. 157
Mars 2024

Nr. 1/2024

Innhold











Lov&Data er et skandinavisk tidsskrift for rettsinformatikk og utgis av

Lovdata
Postboks 6688 St. Olavs plass
NO-0129 Oslo, Norge
Tlf.: +47 23 11 83 00
E-post: lovogdata@lovdata.no
Nettside: www.lod.lovdata.no

Elektronisk: ISSN 1503-8289
Utkommer med 4 nummer pr. år.

Lov&Data er medlemsblad for foreningene Norsk forening for jus og edb, Svenska föreningen för IT och Juridik (ADBJ), Dansk forening for Persondataret og Danske IT-advokater.

Fra 2024 vil Lov&Data kun være tilgjengelig på nett, lod.lovdata.no.

Trykk og layout: Aksell AS

Leder

Det nordiske i teknologiretten

Professor, dr.jur. Henrik Udsen, Det Juridiske Fakultet, Københavns Universitet

Efter mere end 15 år som medredaktør af Lov&Data har jeg valgt at give stafetten videre, og dette bliver derfor min sidste leder. Den vil jeg bruge på nogle reflektioner over Lov&Datas udvikling og ikke mindst rolle som nordisk tidsskrift på et retsområde som i meget høj grad er funderet på EU-lovgivning.

Starter vi med Lov&Datas egen teknologiske udvikling er tidsskriftet gået fra at være rent papirbaseret til at være rent digitalt. Dette har gjort det muligt at gøre tidsskriftet og dets mange artikler gratis og nemt tilgængeligt for alle nordiske teknologijurister. Hvis man orienterer sig i Lov&Datas indhold gennem årene, kan man imidlertid konstatere at også indholdet har undergået ganske store forandringer. Den ene side af dette er selvsagt, at artiklerne fokuserer på de teknologiretlige spørgsmål, der er oppe i tiden, hvilket afspejler den løbende teknologiske udvikling. Den anden side af det er, at indholdet er gået fra at være overvejende nationalt orienteret til i meget høj grad at være orienteret mod EU-regulering. Dette er en naturlig konsekvens af den meget intense teknologiregulering, EU har gennemført i de senere år, oftest ved forordninger, der ikke skal implementeres nationalt.

Den omfattende EU-regulering fører dog ikke til en total harmonisering af teknologiretten, og det nationale og det nordiske spiller derfor stadig en vigtig rolle på mange områder. It-kontraktretten (regulering af teknologianskaffelser), der hviler på den almindelige obligationsret, er et markant eksempel herpå. Også it-sikkerhedsretten vil delvist være nationalt baseret med NIS2-direktivet, der skal implementeres i medlemsstaterne. Selv på forordningsområder vil der ofte være et nationalt råderum som illustreret bl.a. i GDPR.

Det nationale og dermed også det nordiske har derfor fortsat en plads i teknologiretten. Det historiske og kulturelle fællesskab mellem de nordiske lande har altid bevirket et tæt nordisk retssamarbejde og også på det teknologiretlige område, vil afgørelser mv. fra de andre nordiske lande have en særlig interesse og værdi. Og lige præcis her spiller Lov&Data en særlig rolle. Som det eneste nordiske teknologiretlige tidsskrift udgør

Lov&Data en platform for formidling af viden mellem nordiske teknologiretsjurister. Det er derfor mit håb og min opfordring, at bidragsyderne til Lov&Data også fremover vil have blik for dette og formidle viden om nationale afgørelser, vejledninger, standardkontrakter mv. til teknologijurister fra de andre nordiske lande.

Med disse ord takker jeg af som medredaktør men vil med fornøjelse fortsætte som læser og (national) bidragsyder.

Henrik Udsen

Introduction and Analysis from legal perspective of Japan's Latest Draft of AI Guideline[1]

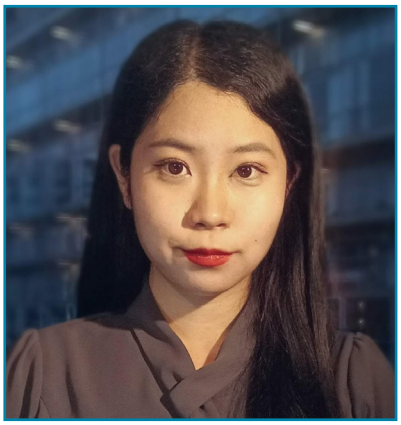
Av Sato Naito

1. Introduction

In the EU, the Council and the European Parliament reached a provisional agreement on the AI ACT 2021/0106(COD) in December 2023. While the approaches may differ, many nations share the desire to ensure the safety of AI use, and efforts to establish AI governance policies, such as the AI ACT, are not limited to the EU alone.

Japan influences both the establishment of rules and technological aspects, impacting the EU and the world. Firstly, concerning international guidelines, Japan has led discussions as the chair country during the establishment of the Hiroshima Principles[2] by the G7. Secondly, in terms of technology, Japanese companies are among those providing AI technology in Europe. For instance, NEC›s subsidiary in Denmark exemplifies its provision of services in the region.

There is limited information regarding Japan's AI regulations and situation. However, Japan has closely observed regulations and discussions in other countries, such as the EU's AI ACT. Analyzing and building upon the systems and laws of other countries has been a key factor in Japan's success in modernization over the past 150 years. Taking a somewhat different approach while considering EU rules and discussions. Japan has adopted a different approach while considering the EU's regulations and discussions. Japan has its unique background. However, while sharing the same goals, Japan's policy of taking a different approach may provide valuable insights into certain EU points of contention, such as "regulations like the AI ACT can hinder innovation" and "The AI ACT may have loopholes and may not be effective[3]".



Sato Naito

Therefore, Japan's draft might serve as a reference point for future EU discussions and elsewhere discussions. Thus, this paper aims to introduce the developments and events in Japan's AI regulation since the beginning of this year, 2024, including a new guideline draft and interpretation of the Copyright Act, while also highlighting the points that Japan should consider in reference to EU law.

> However, while sharing the same goals, Japan's policy of taking a different approach may provide valuable insights into certain EU points of contention, such as "regulations like the AI ACT can hinder innovation" and "The AI ACT may have loopholes and may not be effective".

2. AI regulation in Japan

In Japan, there is no comprehensive AI regulation through hard law, and there are currently no plans to enact hard law regulations. Unlike the EU, rules in Japan have been established through soft law guidelines on a sector-by-sector basis. Currently, Japan aims to consolidate the three guidelines, and as of 2024, the draft AI Guidelines for Business has been released, which will be discussed further in Next Section 2.1.

1 *This work was supported by JST, ACT-X Grant Number JPMJAX22AA, Japan.*

2 The Government of Japan, *The Hiroshima AI Process: Leading the Global Challenge to Shape Inclusive Governance for Generative AI,* KIZUNA *https://www.japan.go.jp/kizuna/2024/02/hiroshima_ai_process.html* , last visited Feb 29th 2024.

3 Veale, Michael and Zuiderveen Borgesius, Frederik, Demystifying the Draft EU Artificial Intelligence Act (July 31, 2021). Computer Law Review International (2021) 22(4) 97-112, Available at SSRN: *https://ssrn.com/abstract=3896852*

2.1 AI Guidelines for Business[4]

On January 19, 2024, the draft of the AI Guidelines for Business was published. This guideline aims to promote innovation and reduce risks in the use of AI. This section will explain the background of the new guideline, why Japan has guidelines for businesses, adopt a soft law approach, and provide an overview of the new guideline.

2.1.1 The background of the new guideline

There have been three guidelines in Japan regarding AI, "Draft AI R&D GUIDELINES for International Discussions[5]", "AI Utilization Guidelines Practical Reference for AI utilization[6]", and "Governance Guidelines for Implementation of AI Principles Ver. 1.1[7]". Japanese Government has decided to integrate and review these three guidelines. Taking into account the characteristics of AI technology that have further developed in recent years and discussions on the social implementation of AI both domestically and internationally[8], the new guideline is formulated for businesses, including the central and local Government, to practice the social implementation and governance of AI[9].

2.1.2 Why does Japan choose to have guidelines for businesses and adopt a soft law approach?

Compared to the AI Act, the distinguishing features of this new draft guideline are that it applies only to businesses[10] and adopts a soft law approach. The approaches of soft law and having guidelines for businesses have not emerged suddenly. Even in domestic regulations, the approaches have been consistently followed since the guidelines of 2019, and this approach continues to be adhered to. Therefore, drawing upon previous documents from the Japanese Government and other sources, this section discusses why Japan adopts these approaches.

According to official documents from the Japanese Government, the adoption of a soft law approach is necessary not only because some businesses desire it but also because there is a desire to establish effective rules. This section explains the rationale behind issuing guidelines targeted at businesses first. Explaining from this perspective elucidates why the adoption of a soft law approach is necessary in Japan.

The reason for targeting businesses is that they are primarily responsible for AI governance. Business activities have become increasingly sophisticated, complex, digitalized, and globalized, making it more challenging for governments to comprehensively understand and monitor them from external perspectives[11].

Ensure incentives for establishing and operating governance systems and compliance programs within organizations function effectively; it is essential for companies to have a clear understanding of what mechanisms should be put in place. On the other hand, due to the high level of variability in circumstances depending on the size and nature of business activities, it is difficult and not advisable to prescribe a one-size-fits-all governance system for all companies. Particularly under agile governance, where there is an expectation of flexible governance that swiftly cycles through the operation and review of goals, relevant rules, and procedures, there is an anticipated challenge in employing traditional approaches such as hard law or

4 The provisional English translation can be referenced from the following. Ministry of Internal Affairs and Communications & Ministry of Economy, Trade and Industry, *(Draft) AI Guidelines for Business,* Jan 2024, *https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240119_4.pdf*, last visited Feb 29th 2024.

5 The Conference toward AI Network Society, *Draft AI R&D GUIDELINES for International Discussions,* Jul 2017, *https://www.soumu.go.jp/main_content/000507517.pdf*, last visited Feb 29th 2024.

6 The Conference toward AI Network Society, *AI Utilization Guidelines Practical Reference for AI utilization*, Aug 2019, *https://www.soumu.go.jp/main_content/000658284.pdf*, last visited Feb 29th 2024.

7 Expert Group on How AI Principles Should be Implemented AI Governance Guidelines WG, *Governance Guidelines for Implementation of AI Principles Ver. 1.1*, Jan 2022, *https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20220128_2.pdf* , last visited Feb 29th 2024.

8 Ministry of Internal Affairs and Communications & Ministry of Economy, Trade and Industry, *Outline of the draft "AI Guidelines for Business",* page 6, Jan 2024 *https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240119_6.pdf* ,last visited Feb 29th 2024.

9 Ministry of Internal Affairs and Communications & Ministry of Economy, Trade and Industry, *supra* note 3 at page 3.

10 However, it has been suggested during the review meetings of this draft guideline that it would be desirable for non-business entities to also refer to this guideline. Ministry of Economy, Trade and Industry, *Summary of Discussions at the Second Meeting of the Ministry of Economy, Trade and Industry's AI Guidelines for Business*, page 1, *https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/2023_002_gijiyoshi.pdf*, only Japanese version is available, last visited Feb 29th 2024. In addition, the guideline itself states that it can be also useful for non-business, including consumers. Ministry of Internal Affairs and Communications & Ministry of Economy, Trade and Industry, *supra* note 4 at page.

11 The Ministry of Economy, Trade and Industry, *GOVERNANCE INNOVATION Ver. 2: A Guide to Designing and Implementing Agile Governance,* page 67, Jul 2021, *https://www.meti.go.jp/shingikai/mono_info_service/governance_model_kento/pdf/20210730_2.pdf*, last visited Feb 29th 2024.

judicial review, which have been traditionally emphasized. In such circumstances, it is believed that to realize the rule of law principle, supervisory authorities should be more proactive in communicating the policies underlying the "goals" and derived behavioral norms and procedural guidelines, thereby enhancing accountability[12].

2.1.3 The overview of the new guideline

The Japanese Government released the draft of the new guideline and an outline for the draft AI Guidelines for Business[13] in January 2024.

From the publicly available information as of the end of February 2024, explicit reasons for why the risk-based approach has been adopted and what influences it could not be found. However, the guideline itself states, "The concept of this 'risk-based approach' is widely shared among AI advanced countries." [14]Additionally, international rules, such as the EU's AI ACT, that adopt a risk-based approach have been compiled, indicating that the movements of various countries have likely become a significant reason for Japan to partially adopt the risk-based approach.

2.2 Characteristics of the AI Guidelines for Business

In short, the highlights of Japan's new AI guideline are twofold: first, balancing innovation and safety, and second, prioritizing effectiveness.

Firstly, the guideline features an abstract definition of AI, which addresses the criticism that the initial AI ACT proposal was too narrow in defining AI, thus potentially inadequately regulating its scope. This abstract definition enables flexibility in adapting to the rapidly evolving field of AI.

Secondly, by not targeting specific technologies, the guideline prevents companies involved in AI development or provision from exploiting loopholes. This approach eliminates the need for a perpetual cycle of updating guidelines to regulate emerging technologies and then revising them again to circumvent such regulations.

Furthermore, merely stating abstract rules may leave businesses uncertain about how to proceed. However, the accompanying documentation of Japan's guidelines provides specific examples of actions taken by companies and failure cases, offering practical guidance for implementation.

> Additionally, international rules, such as the EU's AI ACT, that adopt a risk-based approach have been compiled, indicating that the movements of various countries have likely become a significant reason for Japan to partially adopt the risk-based approach.

2.3 Concerns with the draft of the AI Guidelines for Business

In the draft guideline, issues such as gender discrimination are primarily focused on. Still, it seems there should be more reflection on concerns regarding minorities and an increase in case studies. Furthermore, especially in Japan, it has been pointed out that there is a lack of awareness of rights, as evidenced by the relatively low number of lawsuits per capita[15][16]. Therefore, it is essential to provide robust support, including non-legal means, for safeguarding and preventing rights violations, not only for the government and private sector but also for ensuring that rights infringements do not occur in the first place.

> This approach eliminates the need for a perpetual cycle of updating guidelines to regulate emerging technologies and then revising them again to circumvent such regulations.

2.3.1 Consideration of the Nature Unique to the Public Sector

Citizens practically cannot refuse the utilization of AI by the public sector; it tends to become obligatory in a sense. The competitive principle of citizens choosing the more reliable institution also likely does not work at all. Additionally, since AI usage methods targeting almost all citizens of a nation are possible, the number of people affected could be significant. Therefore, there is a higher possibility of widespread rights infringements than private companies. Especially in Japan, there is a lack of awareness regarding legal rights, as seen in the relatively low number of lawsuits per capita compared to other East Asian countries. It is advisable to provide thorough measures, in-

12 The Ministry of Economy, Trade and Industry, *supra* note 10, at page 75-76.

13 The Ministry of Economy, Trade and Industry, *supra* note 7.

14 Ministry of Internal Affairs and Communications & Ministry of Economy, Trade and Industry, *supra* note 3 at page 3.

15 Courts in Japan, *Court Data Book 2023,* only Japanese version is available, *https://www.courts.go.jp/vc-files/courts/2023/databook2023/db2023_212.pdf*, last visited Feb 29th 2024.

16 Courts in Japan, STATISTICAL TABLES, *https://www.courts.go.jp/english/vc-files/courts-en/file/2022_STATISTICAL_TABLES.pdf*, last visited Feb 29th 2024.

cluding methods other than litigation, to safeguard and prevent rights violations, regardless of whether they occur in the public or private sector. Therefore, it is necessary to reconsider the relationship between the rights of citizens and public sectors, such as administration, and legislative amendments, such as safeguards, which are required.

In particular, there are issues unrelated to AI concerning biases and profiling in Japan's public sector. Even the US embassy, where profiling by AI is a global concern in some states, has called attention to profiling by the Japanese police.

This is not a problem of profiling using AI systems but rather a problem of profiling done by humans. However, the issue of bias in AI usage arises not from discrimination within AI systems but from amplifying societal discrimination. While the Japanese Government denies racial profiling, there are already instances of profiling against foreigners pointed out by foreign embassies, implying the need for deeper consideration, even in the context of crime investigation and categories like race or foreigners, to address concerns regarding transparency and fairness. Japan is a signatory to the Convention on the Elimination of All Forms of Racial Discrimination and prohibits racial discrimination in Article 14 of its Constitution. Furthermore, among the rights of citizens stipulated in the Japanese Constitution, one-third pertains to criminal procedures. In the historical context and provisions of criminal procedures, there are repeated mentions of "any person" rather than specifically "Japanese citizens." From these occurrences, it seems that profiling in investigations and trials should be specifically considered, and it would be desirable to specify such aspects in existing hard law such as the Code of Criminal Procedure. Ironically, the example of COMPAS in the United States demonstrates the realistic dangers of racial profiling in this field and should be heeded by Japan.

2.3.2 Matters to be Further Addressed in Each Item

In the guideline, there are references to human rights, as mentioned above, and discrimination against women is repeatedly addressed.

From the perspective of legal scholars, apart from the issues explicitly stated in the appendix of the guideline, there are specific matters regarding discrimination and bias that need to be addressed. The guideline mentions several times considering the attributes enumerated in Article 14(1) of the Constitution and the rules concerning international human rights[17].
Regarding the Constitution and international human rights rules, there are two points of concern.

Firstly, the current Constitution of Japan, enacted in 1947, remains unamended, making it one of the oldest constitutions in the world. One reason for its lack of amendment is that the Japanese Constitution contains concise and abstract provisions[18], allowing for flexible interpretation, which has been carried out by laws enacted by the Japanese parliament and Government. Article 14, paragraph 1 of the Constitution referred to in the guideline states, "All of the people are equal under the law, and there shall be no discrimination in political, economic or social relations because of race, creed, sex, social status or family origin." However, it is difficult to interpret what exactly is encompassed by "social status." Moreover, some cases concerning discrimination against women may not be straightforwardly identifiable.

2.3.2.1 Regarding Children

During the process of creating the guideline, it was pointed out that there was no mention of minors. Currently, in the proposed version, children have been included as stakeholders. In Japan, there is a tendency to focus on children›s education, which has led to the increasing use of Edtech provided by private companies. Furthermore, in some administrative processes, AI has already been used for risk assessment in child abuse cases[19], sparking discussions.

Children have limited means to collect accurate information, express their opinions, and have them reflected compared to adults. Therefore, more should be done beyond just including them as stakeholders. Consider the nature of children's rights and the dissemination of information regarding AI, drawing lessons from discussions within GDPR and AIA of the EU and its member states. For example, there have been references to providing information in a way that is understandable to children in Finland [20], and such approaches could serve as references for Japan.

---

17 See for example, Ministry of Internal Affairs and Communications & Ministry of Economy, Trade and Industry, *(Draft) AI Guidelines for Business Appendix*, page 78, *https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240119_5.pdf*, last visited Feb 29th 2024.

18 Yokodaido, S. (2019) 'Constitutional stability in Japan not due to popular approval', German Law Journal, 20(2), pp. 263–283

19 In Tsu City, Mie Prefecture, there was a case where child abuse was overlooked, resulting in the death of a child. Some media outlets raised concerns about the use of AI in this case. However, it cannot be solely attributed to AI, considering that there were previous cases of death before AI was introduced in the municipality, and the fact that the responsible personnel had not confirmed the child's situation for about a year in this particular case.

20 Eduskunta, *Regeringens proposition RP 145/2022 rd.* Senast publicerat 20-09-2022, *https://www.eduskunta.fi/SV/vaski/HallituksenEsitys/Sidor/RP_145+2022.aspx*,

2.3.2.2 Regarding people with disabilities

Japan has ratified the Convention on the Rights of Persons with Disabilities. However, within the scope of my search, it seems that neither the main body of these guidelines nor any attached documents explicitly mention people with disabilities. In EU member states, for example, considerations have been made regarding individuals with disabilities in the context of legislative amendments concerning automated decision-making by the administration[21], and amendments related to automation have been considered with this in mind. To prevent unjust discrimination and bias, it is necessary to provide concrete examples of individuals with disabilities or to understand and evaluate the situations surrounding minorities, such as individuals with disabilities.

> One of the reasons Japan leaned heavily towards AI development, compared to the EU, was because Japan lagged behind the United States and China in AI development and adopted "progressive" policies as desired.

3. Latest events in the Interpretation Change of Copyright Law Regarding AI in Japan

As supplementary information, I would like to introduce the latest discussion in Japan regarding copyright law, particularly the interpretation proposal of the new copyright law presented by the Government at the end of February[22]. In essence, the scope of using copyrighted materials for AI learning without the copyright holder's consent has been narrowed compared to previous interpretations.

Under the Copyright Act, copyrighted materials could be used for AI learning and development without the copyright holder's consent as long as they do not unfairly harm the copyright holder's rights. Therefore, Japan has been considered a "machine learning paradise" [23] at least since the 2010s. However, the new interpretation now considers, for example, generating works from a small amount of copyrighted materials from specific creators as copyright infringement[24].

One of the reasons Japan leaned heavily towards AI development, compared to the EU, was because Japan lagged behind the United States and China in AI development and adopted "progressive" policies as desired. For example, Japan allowed the free downloading of data for AI systems, earning it the nickname "heaven." Naturally, there have been movements opposing such policies from creators recently. A group called the "Group of volunteers who concern the future of creators and AI" was formed and made proposals in public[25] in 2023.

It is meaningless to regulate downloads in other countries if one country allows downloads and all AI development without the consent of copyright holders. Considering that provisions related to copyright are ineffective if they do not align transnationally, Japan's policy revision in this regard seems to be welcome.

> [...] Japan's approach may address concerns such as loopholes in laws mentioned in the EU's AI ACT and the inhibition of innovation by hard law.

4. Conclusion

The guidelines in Japan are still in the draft stage, and it's unclear what their final form will be. Since the primary objective of Japan's guidelines is effectiveness, evaluating whether they truly achieve effectiveness will require time and results. Ultimately, whether Japan's guidelines become significantly meaningful from a global perspective regarding effectiveness remains uncertain. Additionally, it's worth noting that Japan has a culture of adhering to government policies

21 For example, there are references to the environment surrounding individuals with disabilities, such as the existence of dispute resolution committees for individuals with disabilities, in Finland. Eduskunta, Regeringens proposition RP 145/2022 rd. Senast publicerat 20-09-2022. *https://www.eduskunta.fi/SV/vaski/HallituksenEsitys/Sidor/RP_145+2022.aspx*

22 Materials distributed at the subcommittee can be downloaded from the following link. However, as of the end of February 2024, all of the materials are only available in Japanese. Agency for Cultural Affairs, *Subcommittee on Copyright Legislation of the Cultural Affairs Council (7th Session),* Feb 2024, *https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/hoseido/r05_07/* , last visited Mar 2nd 2024.

23 Tatsuhiro UENO, *Copyright Issues on Artificial Intelligence and Machine Learning, https://www.f.waseda.jp/uenot/Copyright-AI-IJCAI2017.pdf*, last visited Mar 2nd 2024.

24 Agency for Cultural Affairs, *Perspectives on AI and Copyright (Draft),* Feb 2024, *https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/hoseido/r05_07/pdf/94011401_03.pdf* , last visited Mar 2nd 2024.

25 Group of volunteers who concerns future of creators and AI, *https://support-creators.com/start_page*, last visited Mar 2nd 2024. While the second edition is available only in Japanese, the first edition can be referenced in English.

even without legal binding, as evidenced by its ability to provide AI technology domestically and its response to COVID-19 with minimal use of hard law. However, it cannot be denied that some aspects unique to Japan contribute to this, as mentioned.

Nevertheless, Japan's approach may address concerns such as loopholes in laws mentioned in the EU's AI ACT and the inhibition of innovation by hard law. Therefore, there is potential for Japan's approach to respond to these issues effectively. On the contrary, there is much that EU law and the laws within EU member states can teach Japan, such as the protection of minority rights. Since they share similar overarching goals, comparing the rules to be implemented in each country will become increasingly crucial for better rule-making.

Sato NAITO, PhD student conducting research on «A» with funding support from ACT-X, a grant program for young researchers provided by the Japan Science and Technology Agency.

Illustrasjon: Colourbox.com

Hvordan skille mellom en protest, en slettebegjæring og en klage etter GDPR?

Av Ingrid Hestnes og Ida Thorsrud

Retten til å protestere er en rettighet som vi opplever mange behandlingsansvarlige synes er vanskelig. Utfordringen ligger blant annet i at en protest kan få veldig mange utfall, og de sammenfaller delvis med klage og slettebegjæring. Det er vår erfaring at de registrerte i liten grad har et bevisst forhold til om de bruker retten til å protestere eller om de spør om sletting. Det stiller krav til at den behandlingsansvarlige må se kunne forskjellen. I denne artikkelen vil vi redegjøre for hvordan en behandlingsansvarlig skal kunne skille en protest fra en slettebegjæring eller en klage.

Problemstilling: Hvordan kan en behandlingsansvarlig skille en henvendelse om en protest fra en slettebegjæring eller en generell klage på GDPR?

Ingrid Hestnes

Ida Thorsrud

Innledning

Retten til å protestere er en personvernforpliktelse som mange behandlingsansvarlige sliter med. Dette kan være fordi den har en annen ordlyd i GDPR enn det som var tilfellet etter personverndirektivet. Men kanskje først og fremst tror vi det er knyttet til at dette er en rettighet som den registrerte kan påberope seg selv om behandlingen er lovlig. Dette betyr at behandlingsansvarlig kan ha å gjøre med en lovlig behandling hvor man etterlever alle krav til personvern i GDPR, og likevel vil behandlingsansvarlig måtte etterkomme en protest.

I det så ligger det at videre behandling av den registrertes personopplysninger faktisk blir ulovlig dersom vilkårene for at protesten skal tas til følge er oppfylt. Behandlingen går med andre ord fra å ha vært lovlig, til å ikke lenger være lovlig overfor den registrerte som faktisk har protestert.

Resultatet av en protest betyr at behandlingsansvarlig kan være forpliktet til å slette personopplysningene til den ene personen som protesterte på behandlingen, mens de kan fortsette å behandle andre registrertes personopplysninger.

> I denne artikkelen vil vi redegjøre for retten til å protestere og vise hvordan den behandlingsansvarlige kan skille en henvendelse om protest etter GDPR artikkel 21(1) fra en slettebegjæring eller en generell klage.

Det er ikke noen formkrav på hvordan en protest skal legges frem. Det å påberope seg retten til å protestere fordrer at den registrerte kjenner til retten. Det er vår erfaring at dette er en av de minst kjente personvernrettighetene, og at det derfor er større sannsynlig-

het for at de registrerte vil be om sletting, generelt klage på en behandling eller stille spørsmål til behandlingen, heller enn at de vil påberope seg retten til å protestere. Dette stiller større krav til den behandlingsansvarlige som må tolke hvorvidt en henvendelse er en protest eller ikke.

I denne artikkelen vil vi redegjøre for retten til å protestere og vise hvordan den behandlingsansvarlige kan skille en henvendelse om protest etter GDPR artikkel 21(1) fra en slettebegjæring eller en generell klage.

Vi avgrenser denne artikkelen mot retten til å protestere etter GDPR artikkel 21(2), det vil si om retten til å protestere på direkte markedsføring.

Utgangspunkter for retten til å protestere

GDPR artikkel 21 inneholder en rett til å protestere som er todelt. Det er både en generell rett til å protestere på enhver behandling i GDPR artikkel 21(1), og en mer absolutt rett til å protestere på direkte markedsføring i GDPR artikkel 21(2). Denne artikkelen tar for seg den generelle retten til å protestere i GDPR artikkel 21(1).

1. Behandlingen må være lovlig

Den registrerte har bare rett til å protestere på generelle behandlinger når behandlingsgrunnlaget er GDPR artikkel 6(1) bokstav e) eller f).[1]

Noe av det som gjør retten til å protestere så vanskelig, er at den gjelder når behandlingen er lovlig. Den behandlingsansvarlige *har* lov til å behandle personopplysningene fordi man har et behandlingsgrunnlag. Likevel har den registrerte rett til å protestere på behandlingen, og få gjennomslag for det på visse vilkår.

> Noe av det som gjør retten til å protestere så vanskelig, er at den gjelder når behandlingen er lovlig.

Det gjør at det første spørsmålet som man kan stille for å vurdere om en henvendelse fra en registrert er en protest, eller ikke, er om den gjelder en behandling som er *lovlig*.

Hvis henvendelsen er en påstand om at behandlingen ikke er lovlig, for eksempel at den behandlingsansvarlige har brutt krav til personvern i GDPR, taler det for at henvendelsen ikke er en protest. Det kan heller være snakk om en klage på behandlingen, en slettebegjæring eller kanskje til og med et varsel om et avvik.

2. En protest gjelder personlige forhold på den registrertes side

Retten til å protestere i GDPR artikkel 21(1) er ikke absolutt. Det er en rettighet som bare gjelder hvis den registrerte kan peke på «grunner knyttet til vedkommendes særlige situasjon». Det må altså foreligge individuelle forhold hos den registrerte som tilsier at behandlingen skal stoppes for den personen som har protestert.

I denne artikkelen går vi ikke inn på hvilke krav som kan settes til en individuell begrunnelse for at den registrerte skal få gjennomslag for protesten. Det vil uansett være vanskelig å gi en generell beskrivelse av hvilke individuelle hensyn som vil være nok for å få gjennomslag. Vi nøyer oss med å påpeke at den registrerte må kunne vise til sin egen særlige situasjon. Om denne særlige situasjonen er nok, vil bero på en konkret helhetsvurdering. I helhetsvurderingen vil det være relevant å se på hvor belastende behandlingen er for den registrerte. Dette gjelder særlig der behandlingsgrunnlaget er GDPR artikkel 6(1) bokstav e) – jo mer belastende behandlingen er for den registrerte, desto mer vil det tale for at protesten vil måtte tas til følge.

En protest vil ikke få gjennomslag hvis den bare inneholder argumenter som generelt taler for at en behandling skal stoppe. Dette betyr at en protest som viser til at digitalisering generelt er uønsket, uten å vise til andre, mer personlige grunner hos den registrerte som gjør at akkurat denne registrertes personopplysninger ikke bør behandles på denne måten, ikke vil være en protest etter GDPR artikkel 21(1). En slik mer generell henvendelse, er mest sannsynlig en klage, og trenger ikke behandles som en protest.

Det andre spørsmålet man kan stille for å svare på om en henvendelse er en protest, er derfor om innsigelsen gjelder personlige forhold hos den registrerte. Den registrerte må kunne vise til sider ved seg selv eller eget liv som gjør at behandlingen av deres personopplysninger bør stanses.

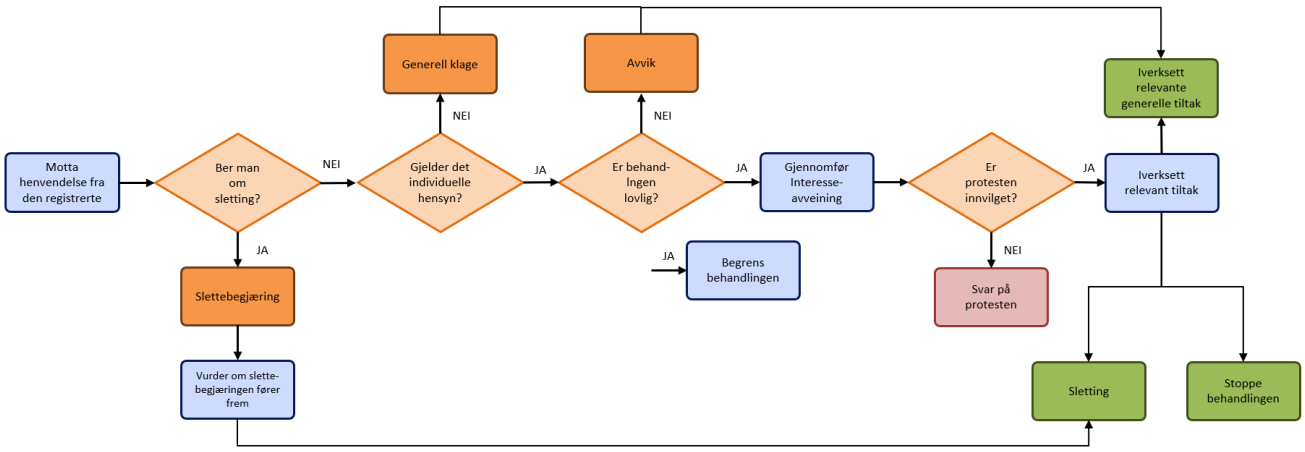
Hvordan kan vi visualisere saksgangen?

Dette er et flytdiagram hvor vi har forsøkt å tydeliggjøre gangen i en protest fra en henvendelse mottas til den er ferdig behandlet. Som figuren viser, kan en protest få flere utfall, også andre utfall enn den en protest isolert vil kunne ha.

Vår tese er at retten til å protestere er vanskelig for den behandlingsansvarlige å forholde seg til nettopp fordi den kan få mange ulike utfall. Imidlertid vil det å svare på følgende spørsmål hjelpe den behandlingsansvarlige til å identifisere om en henvendelse er en protest:

1. Er behandlingen lovlig?
2. Gjelder henvendelsen personlige forhold eller individuelle hensyn på den registrertes side?

1 Dette i motsetning til retten til å protestere på direkte markedsføring, jf. artikkel 21(2), der har man alltid en rett til å protestere, uavhengig av behandlingsgrunnlag.



Hvordan en slettebegjæring skiller seg fra en protest

Retten til sletting er regulert i GDPR artikkel 17. Bestemmelsen fastsetter i punkt 1 at den registrerte skal ha «rett til å få personopplysninger om seg selv slettet av den behandlingsansvarlige uten ugrunnet opphold», og at den behandlingsansvarlige plikter å «slette personopplysninger uten ugrunnet opphold» dersom det foreligger et tilfelle som nevnt i bestemmelsens punkt 1 bokstav (a)–(f).

Det følger implisitt av bestemmelsen at den behandlingsansvarlige sin plikt til å slette personopplysninger først blir utløst når den registrerte gjør bruk av sin rett til å kreve sletting etter artikkel 17. I denne artikkelen avgrenser vi mot sletting som den behandlingsansvarlige er pliktig å gjennomføre på eget initiativ for å oppfylle prinsippet om lagringsbegrensning i artikkel 5(1) bokstav e). Dette er en forpliktelse som den behandlingsansvarlige har helt uavhengig av om den registrerte har krevd sletting. Vår artikkel tar for seg den behandlingsansvarlige sin plikt til å håndtere en slettebegjæring fra den registrerte.

Det kan være vanskelig for den behandlingsansvarlige å skille en slettebegjæring fra en protest, fordi resultatet av begge henvendelsene kan bli det samme, nemlig at personopplysningene skal slettes. Dette følger av GDPR artikkel 17(1) bokstav c), som sier at den registrerte kan kreve sletting når «den registrerte protesterer mot behandlingen i henhold til artikkel 21(1), og det ikke finnes mer tungtveiende berettigede grunner til behandlingen». Den behandlingsansvarlige må da slette de personopplysningene som den registrerte har protestert mot at blir behandlet, med mindre et av unntakene i artikkel 17(3) gjør seg gjeldende.

> Det kan være vanskelig for den behandlingsansvarlige å skille en slettebegjæring fra en protest, fordi resultatet av begge henvendelsene kan bli det samme, nemlig at personopplysningene skal slettes.

Det er likevel noen forskjeller som kan hjelpe behandlingsansvarlig å skille en protest fra en slettebegjæring. For det første knytter en protest etter artikkel 21(1) seg mot den *behandlingen* som den behandlingsansvarlige gjør med personopplysninger om den registrerte. Den registrerte må altså vise til grunner for at den behandlingsansvarlige skal stoppe en «operasjon eller rekke av operasjoner som gjøres med personopplysninger» om vedkommende, jf. GDPR artikkel 4(2). En slettebegjæring knytter seg derimot til hvilke *personopplysninger* som den behandlingsansvarlige behandler om den registrerte. Med andre ord har det ikke betydning hvordan den behandlingsansvarlige konkret behandler personopplysningene, så lenge sletting av personopplysningene kan begrunnes i et av forholdene som nevnt i artikkel 17(1).

For det andre følger det av artikkel 21(1) at den registrerte «til enhver tid» skal ha rett til å protestere mot behandlingen av personopplysninger om vedkommende. Det betyr at retten til å protestere ikke er begrenset til bestemte forhold som den registrerte må kunne påberope seg som en grunn for å stoppe behandlingen av personopplysninger, så lenge det knytter seg til den registrerte sin «særlige situasjon». Den registrerte sin rett til å kreve sletting av sine personopplysninger gjelder derimot bare dersom «et av de følgende forhold [som nevnt i bokstav (a)–(h)] gjør seg gjeldende». Retten til å protestere kan derfor sies å strekke seg lenger enn retten til å kreve sletting, ettersom den registrerte står fritt i begrunnelsen av sin

«særlige sitasjon».[2] Samtidig har den registrerte rett til å kreve sletting uavhengig av behandlingsgrunnlag, og uavhengig av forhold knyttet til den registrerte sin situasjon.

For det tredje forutsetter retten til å protestere i artikkel 21(1) at den behandlingsansvarlige har et gyldig behandlingsgrunnlag i artikkel 6(1) bokstav e) eller f). En slettebegjæring forutsetter derimot at det ikke er «nødvendig» for den behandlingsansvarlige å behandle personopplysningene, og den behandlingsansvarlige kan dermed heller ikke sies å ha et gyldig behandlingsgrunnlag for den videre behandlingen av personopplysningene, jf. GDPR artikkel 5(1) bokstav c).

I korte trekk kan man altså skille en slettebegjæring fra en protest ved å stille følgende spørsmål:

1. Er den registrerte sin innsigelse knyttet til *hvordan* den behandlingsansvarlige behandler personopplysninger, i motsetning til *hvilke* personopplysninger den behandlingsansvarlige behandler?
2. Gjør den registrerte gjeldende forhold som knytter seg til individuelle forhold som skiller vedkommende fra andre registrerte?
3. Har den behandlingsansvarlige et gyldig behandlingsgrunnlag i artikkel 6(1) bokstav e) eller f) for å behandle personopplysninger om andre registrerte?

Dersom spørsmålene ovenfor kan svares bekreftende tilsier dette at den registrerte har protestert mot behandlingen, jf. artikkel 21(1).

Hvordan en klage på en behandling av personopplysninger skiller seg fra en protest

Reglene om klage er regulert i kapittel VIII i GDPR. Artikkel 77 fastsetter at den registrerte skal ha mulighet til å kunne klage til en tilsynsmyndighet dersom man mener at det foreligger et brudd på reglene om behandling av personopplysninger i GDPR. Det er Datatilsynet som er tilsynsmyndighet for overholdelsen av personvernregelverket i Norge, jf. personopplysningsloven § 20.

> En klage til Datatilsynet skiller seg fra en protest på en behandling ved at det er et påstått brudd på reglene i GDPR.

En klage til Datatilsynet skiller seg fra en protest på en behandling ved at det er et påstått brudd på reglene i GDPR. Som allerede beskrevet, er det en forutsetning at en behandling som en helhet er lovlig for at den behandlingsansvarlige skal vurdere å stoppe behandlingen overfor den registrerte på grunn av vedkommende sin «særlige situasjon». Den behandlingsansvarlige kan altså fortsette behandlingen som den registrerte har protestert mot overfor andre registrerte med behandlingsgrunnlag i artikkel 6(1) bokstav e) eller f).

Dersom den registrerte sin innsigelse mot den behandlingsansvarlige sin behandling avdekker at den behandlingsansvarlige ikke har gyldig behandlingsgrunnlag i bokstav e) eller f), må derimot innsigelsen oppfattes som en klage på behandlingen. Den registrerte kan med andre ord klage direkte til Datatilsynet, mens en protest mot en behandling i første rekke må vurderes av den behandlingsansvarlige selv.

Oppsummert kan man altså si at en protest etter artikkel 21(1) må vurderes ut i fra individuelle forhold, mens en klage skal vurdere den generelle lovligheten av en behandling.

Konklusjon

I denne artikkelen har vi vist at en henvendelse er en protest hvis de to følgende spørsmålene kan svares bekreftende:

1. Er behandlingen lovlig?
2. Gjelder innsigelsen personlige forhold på den registrertes side?

Vi understreker at hvorvidt en registrert skal få gjennomslag for en protest, er en interesseavveining som vi ikke har gått nærmere inn på i denne artikkelen.

Det som skiller en protest fra en generell klage, er det siste spørsmålet. En generell klage på at behandlingsansvarlig ikke overholder krav til personvern i GDPR generelt, vil ikke beskrive den registrertes særlige situasjon. En klage vil i all hovedsak gjelde lovligheten av behandlingen eller andre påstander om brudd på GDPR. En protest er skiller seg fra en klage i den forstand at den *ikke* anfører at behandlingen er ulovlig. Det er den registrertes unike situasjon som gjør at protesten må tas i betraktning.

> I denne artikkelen har vi også vist at retten til å protestere er utfordrende fordi den kan få mange forskjellig utfall.

En slettebegjæring kan både komme sammen med en protest, eller som en egen henvendelse med påstand om sletting fordi behandlingen er ulovlig. Dette for eksempel ved at behandlingsgrunnlaget ikke lenger er gyldig, eller at formålet med behandlinger allerede er oppfylt og at det ikke lenger er nødvendig å behandle personopplysningene (de skal slettes). En slettebegjæring skiller seg først og fremst fra en protest ved at den også forutsetter at behandlingen er ulovlig, eller nærmere bestemt, at man ikke lenger har et behandlingsgrunnlag.

2 Se tilsvarende EDPB, *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR - part 1* (07.07.2020), side 8.

I denne artikkelen har vi også vist at retten til å protestere er utfordrende fordi den kan få mange forskjellig utfall. Det vanligste er at en protest – når den blir tatt til følge – fører til at behandlingen stoppes og at personopplysningene om den registrerte som har protestert blir slettet. Men en protest kan også avsløre personvernrisikoer behandlingsansvarlig ikke opprinnelig hadde tatt stilling til eller svakheter ved behandlingen. Retten til å protestere vil kunne føre til at den behandlingsansvarlige oppdager at det må gjøres generelle endringer i hvordan behandlingsansvarlig behandler personopplysninger, selv om den opprinnelige henvendelsen gjaldt et individuelt forhold.

Det vil kunne gjøre at den behandlingsansvarlige må iverksette generelle tiltak for å redusere personvernrisiko eller endre internkontrollsystemet sitt. Dette er resultater som også en generell klage på behandlingen ville kunne medføre.

Ingrid Hestnes. Jurist, Bergen kommune
Ida Thorsrud. Jurist og prosjektleder for den nasjonale Google-DPIA (KS)

Illustrasjon: Colourbox.com

Tredje gången gillt? – En analys av EU-US Data Privacy Framework

Av Nathalie Bjerselius

1. Inledning och bakgrund

Överföringar av personuppgifter till ett tredjeland är endast tillåtet enligt GDPR under särskilt angivna förutsättningar, bland annat om EU-kommissionen har beslutat att det tredjelandet i fråga säkerställer en adekvat skyddsnivå.[1] EU-kommissionen har tidigare fattat två sådana beslut för USA.[2] Dessa beslut har senare kommit att ogiltigförklaras av EU-domstolen i *Schrems I* och *Schrems II*. Anledningen var i båda fallen att de amerikanska underrättelsemyndigheternas tillgång till och användning av EU-medborgares personuppgifter inte var begränsad till vad som var proportionerligt, och att EU-medborgare vars personuppgifter behandlats inte hade tillgång till ett effektivt rättsmedel för att kunna utmana underrättelsemyndigheternas övervakningsåtgärder.

Den 10 juli 2023 fattade EU-kommissionen, för tredje gången, beslut om adekvat skyddsnivå för USA. Det innebär att personuppgifter nu återigen kan föras över fritt från EU till USA, under förutsättning att det mottagande företaget eller organisationen i USA är certifierat under det nya EU-US Data Privacy Framework (EU-US DPF).[3] Till grund för EU-kommissionens beslut ligger i stora delar Executive Order 14086 (E.O. 14086) som inför nya säkerhetsåtgärder för att åtgärda de problem EU-domstolen tidigare har identifierat.

Nathalie Bjerselius

När EU-kommissionen lät annonsera det nya adekvansbeslutet för USA lät kritiken inte vänta på sig utan röster höjdes snabbt om att många av de brister som EU-domstolen ansåg finnas i Privacy Shield kvarstår i det nya EU-US DPF. Frågan som här ska undersökas är därför om de förändringar som E.O. 14086 har gett upphov till förändrar rättsläget efter *Schrems II* på så vis att USA nu säkerställer en adekvat skyddsnivå eller om EU-US DPF riskerar att gå samma öde som sina föregångare till mötes.

> När EU-kommissionen lät annonsera det nya adekvansbeslutet för USA lät kritiken inte vänta på sig utan röster höjdes snabbt om att många av de brister som EU-domstolen ansåg finnas i Privacy Shield kvarstår i det nya EU-US DPF.

2. Rätten till respekt för privatlivet och skydd av personuppgifter

Rätten till respekt för privatlivet och skydd av personuppgifter är två grundläggande rättigheter som föreskrivs i artiklarna 7 och 8 i EU-stadgan. Ingen av dessa rättigheter är dock absoluta utan får begränsas i enlighet med de krav som ställs upp i artikel 52.1 i EU-stadgan.[4] För att vara tillåten ska en begränsning vara föreskriven i lag, tjäna ett legitimt syfte, vara proportionerlig i förhållande till syftet, samt vara förenlig med bevarandet av den grundläggande rättighetens väsentliga innehåll. Fokus för prövningen i *Schrems I* och *Schrems II* var kravet på proportionalitet. EU-domstolen

1 Artiklarna 44 och 45 i GDPR.

2 Kommissionens beslut 2000/520 av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbour Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (EUT L 215, 25.8.2000, s. 7-47), och Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet och Förenta staterna (EUT L 207, 1.8.2016, s. 1-112).

3 Kommissionens genomförandebeslut (EU) 2023/1795 av den 10 juli 2023 i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 om adekvat skydd av personuppgifter enligt ramen för dataskydd mellan EU och Förenta staterna (EUT L 231/118, 20.9.2023, s. 118-229).

4 Schrems II, p. 172.

framhöll att detta krav innebär att ingrepp i grundläggande rättigheter ska begränsas till vad som är strikt nödvändigt.[5] Det innebär i sin tur att den rättsliga grund som möjliggör ingreppet i rättigheterna i sig måste uppfylla kravet på proportionalitet.[6] För att uppfylla detta krav måste den rättsliga grunden definiera räckvidden av begränsningen i utövandet av den aktuella rättigheten.[7] Den rättsliga grunden måste därför innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden, och som fastställer skyddsåtgärder.[8]

EU-domstolens krav på att den rättsliga grund som möjliggör ingrepp i grundläggande rättigheter ska innehålla *tydliga och precisa bestämmelser* korresponderar med kravet i artikel 52.1 i EU-stadgan på att varje begränsning i utövandet av en rättighet ska vara föreskriven i lag. För att en lag ska uppfylla detta krav måste den ha en rättslig grund i nationell lag men även vara kompatibel med rättsstatsprincipen.[9] Det senare innebär att lagen i fråga måste vara tillgänglig och förutsebar.[10]

Det går att ifrågasätta om EU-US DPF uppfyller kravet på förutsebarhet. Att en lag är förutsebar innebär att den är så tydligt formulerad att det är möjligt för en enskild person att anpassa sitt beteende efter den.[11] Den enskilde måste, med andra ord, kunna förutse de konsekvenser som en viss handling kan medföra.[12] Förutsebarhet när det gäller hemliga övervakningsåtgärder kan dock inte vara densamma som inom många andra områden. I dessa sammanhang kan förutsebarhet inte betyda att en enskild person ska kunna förutse när offentliga myndigheter kan komma att avlyssna dennes kommunikation och anpassa sig därefter,[13] eftersom syftet med övervakningen då skulle gå förlorat. Likväl måste dock den nationella lagen vara tillräckligt tydlig så att enskilda förstår under vilka omständigheter och på vilka villkor offentliga myndigheter har rätt att tillgripa sådana åtgärder.[14]

> Det går att ifrågasätta om EU-US DPF uppfyller kravet på förutsebarhet.

EU-domstolen har i *Schrems II* slagit fast att varken Section 702 FISA eller E.O. 12333 (som är de rättsliga grunder som möjliggör ingrepp i artiklarna 7 och 8 i EU-stadgan) innehåller tillräckligt tydliga och precisa bestämmelser,[15] och dessa har i sig inte förändrats sedan tiden för *Schrems II*. Vad som däremot har förändrats är att PPD-28 har ersatts av E.O. 14086, varigenom nya regler har införts för att stärka skyddsåtgärderna för amerikansk signalspaningsverksamhet. Frågan är därmed om E.O. 14086 kan anses bemöta de brister som tidigare har identifierats av EU-domstolen.

En positiv aspekt är att E.O. 14086 innehåller en förteckning över legitima respektive förbjudna ändamål.[16] Att E.O. 14086 på detta sätt anger för vilka ändamål som insamling av personuppgifter får och inte får ske är positivt eftersom det ökar förutsebarheten för individer. Ett problem är dock att vissa av ändamålen är allmänt hållna och möjliggör en vid tolkning. Till exempel får insamling av personuppgifter ske för att förstå och bedöma transnationella hot som påverkar den globala säkerheten, utan att det närmre specificeras vad som menas med global säkerhet. För bulkinsamling är antalet legitima ändamål färre till antalet än för riktad insamling (det vill säga sex i stället för tolv).[17] EDPB har framhållit att dessa ändamål visserligen är mer detaljerade än de ändamål som angavs i PPD-28, men att omfattningen av den insamling som får göras fortfarande är bred och kan omfatta stora volymer av personuppgifter.[18] Ytterligare ett problem är att USA:s president ges möjlighet att, mot bakgrund av nya tvingande krav avseende den nationella säkerheten, lägga till fler legitima ändamål.[19] Presidenten ges även möjlighet att besluta att dessa nya ändamål inte ska offentliggöras om presidenten anser att ett offentliggörande skulle utgöra en nationell säkerhetsrisk för USA.[20]

> Att E.O. 14086 på detta sätt anger för vilka ändamål som insamling av personuppgifter får och inte får ske är positivt eftersom det ökar förutsebarheten för individer.

Att E.O. 14086 listar ändamål för vilka övervakning får ske och inte innebär förbättringar i förhållande till Privacy Shield, men dessa förbättringar urholkas i samma utsträckning av möjligheten till vida tolkningar av existerande ändamål liksom möjligheterna för USA:s

5 Schrems I, p. 92, och Schrems II, p. 176.
6 Schrems II, p. 175.
7 Schrems II, p. 175.
8 Schrems II, p. 176.
9 Gillion och Quinton mot Förenade kungariket, p. 76.
10 Gillion och Quinton mot Förenade kungariket, p. 76.
11 Gillion och Quinton mot Förenade kungariket, p. 76.
12 Sunday Times mot Förenade kungariket, p. 49, och Silver m.fl. mot Förenade kungariket, p. 88.
13 Sacharov mot Ryssland, p. 229.
14 Sacharov mot Ryssland, p. 229.
15 Schrems II, p. 180 och 183.
16 Section 2(b)(ii)(A) i E.O. 14086.
17 Section 2(c)(ii)(A) i E.O. 14086.
18 EDPB:s yttrande 5/2023, p. 140.
19 Section 2(b)(i)(B) och 2(c)(ii)(A) i E.O. 14086.
20 Section 2(b)(i)(B) och 2(c)(ii)(A) i E.O. 14086.

president att lägga till nya (inte nödvändigtvis offentliga) ändamål. Det skulle tala för att bestämmelserna i E.O. 14086 inte uppfyller kravet på tydlighet och precision. Samtidigt måste detta krav ses mot bakgrund av två domar som meddelades av EU-domstolen år 2022. EU-domstolen vidhåller i dessa domar det krav som den tidigare har ställt upp i *Schrems II*, det vill säga att den rättsliga grund som möjliggör ingrepp i en grundläggande rättighet själv måste definiera räckvidden av begränsningen i utövandet av den aktuella rättigheten.[21] Till skillnad från i *Schrems II* lägger dock EU-domstolen till att detta krav inte hindrar att den lagstiftning genom vilken begränsningen införs har en lydelse som är tillräckligt öppen för att möjliggöra en anpassning till olika situationer och förändrade omständigheter.[22] Det verkar därmed som att EU-domstolen har öppnat upp för en viss flexibilitet som sänker det krav som den tidigare har ställt upp i *Schrems II*. Det är olyckligt eftersom det sänker graden av förutsebarhet och det skydd som rättsstatsprincipen medför.[23] I motsvarande mån ökar dock chanserna för att bestämmelserna i E.O. 14086 ska passera som tydliga och precisa.

3. Rätten till ett effektivt rättsmedel

Där det finns rättigheter måste det finnas rättsmedel eftersom rättigheter annars inte kan upprätthållas och deras skyddande funktion försvinner.[24] Artikel 47 i EU-stadgan föreskriver därför att var och en vars unionsrättsligt garanterade fri- och rättigheter har kränkts har rätt till ett effektivt rättsmedel inför en domstol. EU-domstolen framhöll i *Schrems II* att det följer av artikel 47 i EU-stadgan att enskilda ska ha möjlighet att utöva sin rätt till rättslig prövning inför en oavhängig och opartisk domstol för att erhålla tillgång till, rätta eller radera personuppgifter som rör dem.[25] EU-domstolen ansåg dock inte att Privacy Shields ombudsmannamekanism kunde leva upp till dessa krav, bland annat på grund av dess brist på oavhängighet i förhållande till den verkställande makten.[26]

> Att E.O. 14086 listar ändamål för vilka övervakning får ske och inte innebär förbättringar i förhållande till Privacy Shield, men dessa förbättringar urholkas i samma utsträckning av möjligheten till vida tolkningar av existerande ändamål liksom möjligheterna för USA:s president att lägga till nya (inte nödvändigtvis offentliga) ändamål.

Genom EU-US DPF inrättas en särskild prövningsmekanism bestående i två nivåer för att hantera och lösa klagomål från utländska medborgare i fråga om amerikanska övervakningsåtgärder. På den första nivån kan enskilda lämna in klagomål till ”Civil Liberties Protection Officer” (CLPO). På den andra nivån har enskilda sedan möjlighet att överklaga CLPO:s beslut till den nybildade ”Data Protection Review Court” (DPRC). Nedan undersöks om DPRC kan anses uppfylla de krav på ett effektivt rättsmedel som EU-domstolen ställde upp i *Schrems II*. Att endast DPRC, och inte CLPO, undersöks beror på att Europeiska dataskyddsstyrelsen (EDPB) har slagit fast att CLPO inte är tillräckligt oberoende från den verkställande makten för att kunna anses uppfylla kraven i artikel 47 i EU-stadgan.[27]

EU-domstolens första krav är att enskilda ska ha möjlighet att utöva sin rätt till rättslig prövning inför *en oavhängig och opartisk domstol*. DPRC rapporterar inte till justitieministern och är inte heller föremål för löpande tillsyn från justitieministerns sida.[28] Vidare innehåller EU-US DPF vissa garantier vad gäller domarna i DPRC:s avsättning. Enligt bestämmelserna i E.O. 14086 är det endast möjligt att avsätta en domare innan dennes ämbetsperiod löper ut under snävt definierade omständigheter, som exempelvis vid tjänstefel.[29] Det innebär sammantaget förbättringar jämfört med Privacy Shields ombudsmannamekanism. Trots det finns det omständigheter som gör att det går att ifrågasätta DPRC:s verkliga oberoende i förhållande till den verkställande makten. DPRC inrättas genom ett dekret utfärdat av justitieministern, domarna i DPRC utses av justitieministern (även om det sker i samråd med handelsministern, direktören för den nationella underrättelsetjänsten och ”Privacy and Civil Liberties Oversight Board” (PCLOB)),[30] och även om inte justitieministern kan avsätta domare i DPRC så finns det inget som hindrar USA:s president från att göra det. Enligt Europaparlamentet medför dessa omständigheter att DPRC inte kan anses uppfylla de krav på oavhängighet och opar-

21 Ligue des droits humains, p. 114, och Polen mot parlamentet och rådet, p. 64.
22 Ligue des droits humains, p. 114, och Polen mot parlamentet och rådet, p. 74.
23 Musco Eklund & Brewczyńska (2023).
24 Lebeck (2016), s. 350.
25 Schrems II, p. 194.
26 Schrems II, p. 195 och 197.
27 EDPB:s yttrande 5/2023, p. 216.
28 28 C.F.R §201.7(d).
29 Section (d)(iv) i E.O. 14086, och 28 C.F.R §201.7(d).
30 Section 3(d)(i)(A) i E.O. 14086.

tiskhet som föreskrivs i artikel 47 i EU-stadgan.[31]

EU-domstolens andra krav är att enskilda ska ha möjlighet att använda domstolen i fråga för att erhålla tillgång till, rätta, eller radera personuppgifter som rör dem. EU-domstolen ansåg i *Schrems II* att detta krav inte var uppfyllt eftersom ombudsmannen inte var behörig att fatta bindande beslut i förhållande till underrättelsemyndigheterna.[32] Samma problem finns inte i EU-US DPF eftersom de beslut som fattas av DPRC har bindande verkan.[33] Trots det är det tveksamt om DPRC kan anses uppfylla EU-domstolens krav. I detta fall är det inte domstolens avsaknad av tvingande korrigerande befogenheter som är problemet utan myndigheternas avsaknad av information till den enskilde, vilket många gånger är en förutsättning för att en enskild ska ha möjlighet att tillvarata sina rättigheter.

EU-domstolen har flera gånger betonat vikten av att enskilda informeras. I *Yttrande 1/15* framhöll EU-domstolen att det var *nödvändigt* att flygpassagerare informerades om överföringen av deras uppgifter till Kanada och om användningen av dessa uppgifter för att de i enlighet med artikel 47 i EU-stadgan skulle kunna utnyttja ett effektivt rättsmedel inför domstol.[34] Likaså i *Tele2/Watson* uttryckte EU-domstolen att det var *nödvändigt* att en enskild informerades för att denne skulle kunna utöva sin rätt till rättslig prövning vid kränkning av dennes rättigheter.[35] I såväl *Yttrande 1/15* som *Tele2/Watson* framhöll dock EU-domstolen att information till de enskilda endast behövde lämnas i den omfattning och så snart denna information inte längre äventyrade den verksamhet som myndigheten var ansvarig för.[36] I övervakningssammanhang innebär det rimligen att en myndighet inte behöver informera en enskild om en övervakningsåtgärd förrän denna åtgärd har avslutats.

> I detta fall är det inte domstolens avsaknad av tvingande korrigerande befogenheter som är problemet utan myndigheternas avsaknad av information till den enskilde, vilket många gånger är en förutsättning för att en enskild ska ha möjlighet att tillvarata sina rättigheter.

Justitiedepartementet åläggs ett visst informationskrav ifall departementet avser att använda information inhämtad genom Section 702 FISA mot en svarande i en rättslig eller administrativ process, men det inte är inte fråga om någon generell informationsskyldighet.[37] Vad gäller E.O. 12333 finns det ingen bestämmelse som kräver att en underrättelsemyndighet lämnar information till en person vars personuppgifter har samlats in.[38] Detsamma gäller för E.O. 14086. Att den enskilde i de flesta fall inte informeras gör det svårt för denne att utöva sina rättigheter enligt artikel 47 i EU-stadgan.

Även Europadomstolen är av uppfattningen att det är nödvändigt att en enskild informeras för att denne ska kunna utöva sin rätt till rättslig prövning vid kränkning av dennes rättigheter. Europadomstolen har dock framhållit att denna rättighet kan tillgodoses på ett annat sätt, nämligen genom att göra det möjligt för individer som misstänker att de är föremål för övervakning att vända sig till en domstol vars jurisdiktion *inte* är beroende av att individen i fråga har informerats.[39]

I USA begränsas en enskilds möjligheter att väcka talan mot amerikanska övervakningsåtgärder vid federala domstolar av kravet i artikel III i USA:s konstitution på att den enskilde måste visa att han eller hon har talerätt.[40] Talerätt förutsätter i sin tur att den enskilde kan visa på konkret, specifik och faktisk skada eller överhängande risk för sådan skada.[41] Detta krav är svårt att uppfylla i övervakningsmål eftersom enskilda personer i sådana mål i regel inte informeras om de övervakningsåtgärder som vidtas mot dem ens när dessa åtgärder har avslutats. Inom den nya prövningsmekanismen, däremot, är talerättskravet inte tillämpligt. DPRC:s jurisdiktion är, med andra ord, inte beroende av att en individ har informerats om att han eller hon är eller har varit föremål för övervakning. DPRC skulle därmed kunna vara en sådan domstol som Europadomstolen menar kan utgöra ett alternativ till en domstol vars behörighet är beroende av att en individ har informerats. Problemet är dock att Europadomstolen har framhållit att en sådan domstol måste uppfylla vissa krav, bland annat i fråga om oberoende.[42] Det är ett problem eftersom DPRC:s oberoende i förhållande till den verkställande makten, som redogjorts för ovan, kan ifrågasättas.

4. Rätten till ett rättvist förfarande

Ett rättsmedel kan inte bedömas som effektivt om förfarandet inte är rättvist. Ytterligare en aspekt av artikel 47 (som inte behandlades av

31 Europaparlamentets resolution 2023/2501 (RSP), p. 9.
32 Schrems II, p. 196.
33 Section 3(d)(ii) i E.O. 14086.
34 Yttrande 1/15, p. 220.
35 Tele2/Watson, p. 121.
36 Yttrande 1/15, p. 220, och Tele2/Watson, p. 121.
37 Wen (2016), s. 1211.
38 Wen (2016), s. 1135.
39 Sacharov mot Ryssland, p. 286-288.
40 Förslag till avgörande, Schrems II, p. 67.
41 Förslag till avgörande, Schrems II, p. 67.
42 Kennedy mot Förenade kungariket, p. 167.

EU-domstolen inom ramen för *Schrems I* eller *Schrems II* men som kan vara ett problem under EU-US DPF) är den sekretess som omger domstolsprocessen i DPRC och hur denna påverkar enskildas möjligheter till ett rättvist förfarande, såsom den föreskrivs i artikel 47 i EU-stadgan. Det finns flera grundläggande aspekter av denna rätt, bland annat rätten till ett motiverat beslut som medför en rätt för den enskilde att ta del av skälen för ett beslut.

Under EU-US DPF har klaganden inte möjlighet att få tillgång till de beslut som meddelas av DPRC. När DPRC har avslutat sin granskning av klagandens ansökan ska DPRC inte röja om klaganden har varit föremål för övervakningsåtgärder eller inte. I stället meddelas klaganden endast att några överträdelser som omfattas av regelverket inte har upptäckts eller att DPRC har utfärdat ett beslut med krav på lämpliga korrigerande åtgärder.[43] Det syfte som DPRC:s standardsvar tjänar (det vill säga att skydda känsliga uppgifter om amerikansk underrättelseverksamhet) är generellt sett legitimt, men dess generella tillämpning och avsaknad av undantag kan innebära problem.[44]

> När DPRC har avslutat sin granskning av klagandens ansökan ska DPRC inte röja om klaganden har varit föremål för övervakningsåtgärder eller inte.

Liknande situationer har tidigare varit föremål för EU-domstolens bedömning. I *Kadi II* framhöll EU-domstolen att artikel 47 i EU-stadgan innebär att en person måste ha möjlighet att få kännedom om de skäl som ligger till grund för de beslut som fattas rörande honom eller henne, men att artikel 52.1 i EU-stadgan under vissa förutsättningar tillåter begränsningar i denna rättighet.[45] I fall där tvingande hänsyn rörande den nationella säkerheten utgör hinder för att lämna ut uppgifter eller bevisning till en person ankommer det på en domstol att i varje enskilt fall avgöra om det finns stöd för de skäl som en myndighet anför för att motsätta sig en utlämning av uppgifter.[46] Om det visar sig att dessa skäl utgör hinder för att personen informeras krävs det ändå att domstolen gör en lämplig avvägning mellan rätten till ett effektivt domstolsskydd å ena sidan och den nationella säkerheten å andra sidan.[47] Vid en sådan intresseavvägning kan det vara tillåtet att välja sådana alternativ som att lämna ut en sammanfattning av de uppgifter och den bevisning som är i fråga.[48] Rätten till ett motiverat beslut är med andra ord inte en absolut rättighet men en begränsning av denna måste vara resultatet av en lämplig intresseavvägning som har gjorts av en domstol.

Under EU-US DPF kan det komma att finnas en försenad rätt till ett motiverat beslut. Handelsdepartementet ska nämligen vart femte år kontakta relevanta delar av underrättelsetjänsten för att se om sekretessen har hävts för uppgifter som har att göra med den granskning som domstolen har genomfört.[49] Om så är fallet ska klaganden informeras om detta av lämplig offentlig myndighet.[50] Även om detta skulle anses kunna vara resultatet av en lämplig intresseavvägning så har intresseavvägningen inte gjorts av rätt organ, det vill säga en domstol. I stället är det under EU-US DPF relevanta delar av underrättelsetjänsten som bedömer om sekretessen kan hävas.

> Rätten till ett motiverat beslut är med andra ord inte en absolut rättighet men en begränsning av denna måste vara resultatet av en lämplig intresseavvägning som har gjorts av en domstol.

5. Slutord

En förutsättning för att USA ska anses kunna säkerställa en adekvat skyddsnivå för personuppgifter som överförs från EU till USA är att de brister som EU-domstolen identifierade i Privacy Shield har åtgärdats. Även om EU-US DPF i många delar innebär en förbättring i förhållande till Privacy Shield (som i sin tur innebar en förbättring i förhållande till Safe Harbour) är det tveksamt om så är fallet. I enlighet med vad som har angetts ovan innebär EU-US DPF sannolikt inte att oproportionerliga ingrepp i grundläggande rättigheter förhindras, eller att ett effektivt rättsmedel för att kunna utmana dessa ingrepp tillhandahålls. Två gånger tidigare har EU-domstolen ogiltigförklarat de adekvansbeslut som EU-kommissionen har utfärdat för USA, och sannolikt väntar ett tredje.

> Även om detta skulle anses kunna vara resultatet av en lämplig intresseavvägning så har intresseavvägningen inte gjorts av rätt organ, det vill säga en domstol.

43 Section 3(d)(i)(H) i E.O. 14086.
44 EDPB:s yttrande 5/2023, p. 241.
45 Kadi II, p. 100-101.
46 Kadi II, p. 125-126.
47 Kadi II, p. 128.
48 Kadi II, p. 129.
49 Section 3(d)(v)(B) i E.O. 14086.
50 Section 3(d)(v)(C) i E.O. 14086.



Illustrasjon: Colourbox.com

Källor

Europaparlamentet

Europaparlamentets resolution av den 11 maj 2023 om huruvida ett adekvat skydd säkerställs genom ramen för dataskydd mellan EU och USA (2023/2501(RSP)), Strasbourg, 11 maj 2023

Europeiska dataskyddsstyrelsen (EDPB)

Yttrande 5/2023 om Europeiska kommissionens utkast till genomförandebeslut om ett adekvat skydd för personuppgifter enligt EU:s och USA:s ram för dataskydd (Antaget den 28 februari 2023)

Litteratur

Lebeck, C, *EU-stadgan om grundläggande rättigheter*, 2 uppl, Studentlitteratur 2016

Musco Eklund, A & Brewczyńska, M, "Foreseeability and the Rule of Law in Data Protection after the PNR judgment", *VerfBlog*, 10 maj 2023, *https://verfassungsblog.de/foreseeability-pnr/*, hämtad 24 januari 2024

Wen, C J, *Secrecy, Standing and Executive Order 12333*, Southern California Law Review 2016, s. 1099-1138

Rättsfall

EU-domstolen

Domstolens dom av den 18 juli 2013 i mål C-584/10 P Europeiska kommissionen m.fl. mot Yassin Abdullah Kadi, ECLI:EU:C:2013:518 (cit: Kadi II)

Domstolens dom av den 6 oktober 2015 i mål C-362/12 Maximilian Schrems mot Data Protection Commissioner, ECLI:EU:C:2015:650 (cit: Schrems I)

Domstolens dom av den 21 december 2016 i förenade målen C-2013/15 och C-698/15 Tele2 Sverige AB och Secretary of State for the Home Department mot Post- och telestyrelsen m.fl, ECLI:EU:C:2016:970 (cit: Tele2/Watson)

Domstolens yttrande 1/15 (PNR-avtalet mellan EU och Kanada) den 26 juli 2017, ECLI:EU:C:2017:592 (cit: Yttrande 1/15)

Förslag till avgörande av generaladvokat Henrik Saugmandsgaard Øe föredraget den 19 december 2019 i mål C-311/18 Data Protection Commissioner mot Facebok Ireland Limited och Maximilian Schrems, ECLI:EU:C:2019:1145 (cit: Förslag till avgörande, Schrems II)

Domstolens dom av den 16 juli 2020 i mål C-311/18 Data Protection Commissioner mot Facebok Ireland Limited och Maximilian Schrems, ECLI:EU:C:2020:559 (cit: Schrems II)

Domstolens dom av den 26 april 2022 i mål C-401/19 Polen mot parlamentet och rådet, ECLI:EU:C:2022:297 (cit: Polen mot Parlamentet och rådet)

Domstolens dom av den 21 juni 2022 i mål C-817/19 Ligue des droits humains mot Conseil des ministres, ECLI:EU:C2022:491 (cit: Ligue des droits humains)

Europadomstolen

Sunday Times mot Förenade kungariket, nr 6538/74, dom meddelad den 26 april 1979

Silver m.fl. mot Förenade kungariket, nr 5947/72, 6205/73, 7061/75, 7107/75, 7113/75, 7136/75, dom meddelad den 25 mars 1983

Gillan och Quinton mot Förenade kungariket, nr 4185/0, dom meddelad den 12 januari 2010

Kennedy mot Förenade kungariket, nr 26839/05, dom meddelad den 18 maj 2010

Sacharov mot Ryssland, nr 47143/06, dom meddelad den 4 december 2015

Nathalie Bjerselius arbetar som biträdande jurist på Cirio Advokatbyrå med bland annat frågor om dataskydd och informationssäkerhet. Artikeln är en sammanfattning av författarens examensarbete.

Databasverksamheter med grundlagsskydd vägras allmänna handlingar med hänvisning till GDPR

Av Esa Kymäläinen og Jesper Jakobsson

Esa Kymäläinen

Jesper Jakobsson

Bakgrund – offentlighetsprincipen och dataskyddsreglerna

Umeå tingsrätt och Malmö tingsrätt har i två nyligen meddelade beslut avslagit begäranden om utlämnande av brottmålsdomar respektive förundersökningsprotokoll, såsom allmänna handlingar enligt tryckfrihetsförordningen (”**TF**”). Handlingarna hade begärts ut av två databasföretag med så kallat utgivningsbevis enligt yttrandefrihetsgrundlagen (”**YGL**”) för sina verksamheter. Domstolarna hänvisar till hinder för utlämnande enligt EU:s förordning 2016/679 (”**GDPR**”). Besluten är ett avsteg från tidigare praxis från svenska domstolar.

Huvudregeln i svensk rätt är att allmänna handlingar är offentliga. Denna offentlighetsprincip innebär en rätt för allmänheten – såsom enskilda personer och företag, inräknat massmedier – till insyn i och tillgång till information om det allmännas verksamhet. Rätten att ta del av allmänna handlingar är en grundlagsskyddad rättighet enligt 2 kap. TF.

Rätten att ta del av allmänna handlingar är emellertid inte utan begränsningar. Sekretesslagstiftningen – offentlighets- och sekretesslagen (2009:400) (”**OSL**”) – innefattar en rad begränsningar av offentligheten i olika verksamheter och med avseende på uppgifternas art.

Relativt nyligen har i de svenska mediegrundlagarna, TF och YGL, även införts ett utrymme att under vissa förutsättningar genom lag förbjuda offentliggörande av så kallade känsliga personuppgifter (se exempelvis 1 kap. 20 § YGL). Till denna kategori hör uppgifter om bland annat etniskt ursprung, politiska och religiösa övertygelser samt hälsa. Dessa inskränkningar betyder vidare att det grundlagsskyddade området för offentliggöranden genom massmedier har begränsats i motsvarande utsträckning. Besluten av tingsrätterna i Umeå och Malmö avsåg dock inte i första hand det särskilda undantaget rörande känsliga personuppgifter (jfr dock Kammarrätten i Stockholms dom av den 22 juni 2023 i mål 1128-23, Verifiera AB mot Integritetsskyddsmyndigheten).

I 21 kap. 7 § OSL finns en generell sekretessbestämmelse för personuppgifter som efter utlämnande kan antas komma att behandlas i strid med, såvitt här relevant, GDPR eller lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (”**dataskyddslagen**”).

I syfte att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd för personuppgifter finns föreskrifter i såväl GDPR som dataskyddslagen, vilka ur ett svenskt perspektiv avser att säkerställa att dataskyddslagstiftningen inte ska tillämpas i den utsträckning det skulle strida mot grundlagsbestämmelserna i TF och YGL (se artikel 86 i GDPR; skäl 154 till GDPR; 1 kap. 7 § dataskyddslagen).

> Den vedertagna uppfattningen är att dataskyddslagstiftningen inte ska tillämpas inom området för TF och YGL.

Behandling av personuppgifter som sker i journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande har vidare undantagits, enligt dataskyddslagen, från en stor del av bestämmelserna i GDPR.

Den vedertagna uppfattningen är att dataskyddslagstiftningen inte ska tillämpas inom området för TF och YGL. Av detta skäl har 21 kap. 7

§ OSL inte heller ansetts vara tillämplig när uppgifter ur allmänna handlingar nyttjats i grundlagsskyddade medier (se exempelvis Kammarrätten i Stockholms dom av den 25 september 2020 i mål nr 4825-20; Kammarrätten i Göteborgs dom av den 3 februari 2022 i mål nr 7368-21; SOU 2016: 58 s. 378–390; SOU 2020:45 s. 239).

Närmare om Umeå tingsrätts beslut av den 18 januari 2024, dnr. TUM 2023/675

Under december 2023 kontaktades Umeå tingsrätt av ett företag med en begäran om att få ut samtliga brottmålsdomar från det gångna året. Företaget tillhandahåller en databas med utgivningsbevis som erbjuder tjänster för bakgrundskontroller av enskilda, såsom personer som deltar i rekryteringsförfaranden.

Trots att databasen har ett utgivningsbevis enligt YGL avslogs ansökan med motiveringen att uppgifter om enskildas lagöverträdelse kunde antas komma att behandlas i strid med GDPR och att handlingarna följaktligen omfattades av sekretess enligt 21 kap. 7 § OSL.

Umeå tingsrätt framhöll vidare att ett utgivningsbevis knappast kan innebära ett ”*carte blanche*” för databasägaren ”*att under alla delar av behandlingen bortse från kraven i GDPR*”. I stället konstaterade tingsrätten att GDPR *ska* tillämpas i den utsträckning förordningen inte står i strid med den grundlagsstadgade yttrandefriheten.

I beslutet hänvisar tingsrätten till EU-domstolens dom i mål C-439/19 (Latvijas Republikas Saeima). Målet avsåg en privatperson som ifrågasatte lagenligheten av ett nationellt trafikregister som gav allmänheten tillgång till personuppgifter om ”prickning” vid trafikförseelser. I sitt avgörande uttalar EU-domstolen att de utpekade personernas rätt till privatliv överväger allmänhetens intresse av tillgång till de allmänna handlingarna. Bestämmelserna i GDPR utgör således hinder för den nationella lagstiftningen att tillåta överföring av uppgifter om prickning till ett för allmänheten tillgängligt register.

Umeå tingsrätt konstaterade att det inte finns något EU-rättsligt undantag från kraven i GDPR när det gäller den tänkta behandlingen av personuppgifter om lagöverträdelser. Tingsrätten fann att de syften som uppbär GDPR vägde *väsentligt tyngre* än ett kommersiellt bolags vilja att skapa en databas för allmänhetens egna sökningar avseende personuppgifter om allvarliga brott.

> I stället konstaterade tingsrätten att GDPR ska tillämpas i den utsträckning förordningen inte står i strid med den grundlagsstadgade yttrandefriheten.

Närmare om Malmö tingsrätts beslut av den 23 januari 2024 och den 5 februari 2024, dnr. TMA 2024-56

I januari 2024 kontaktades Malmö tingsrätt av en nyhetsbyrå som begärde att få ta del av samtliga förundersökningsprotokoll inkomna till tingsrätten under de första veckorna på året.

Nyhetsbyråns verksamhet består av att samla in och granska en stor mängd allmänna handlingar i syfte att finna nyhetsmässiga händelser att rapportera om. Nyhetsbyrån antogs, av tingsrätten, att även tillhandahålla en databas med utgivningsbevis i vilken allmänheten kan göra bakgrundskontroller av enskilda.

Tingsrätten konstaterade att vissa delar av nyhetsbyråns verksamhet var av klart journalistisk karaktär. Beträffande databasen för bakgrundskontroller fann domstolen emellertid att denna saknade ett journalistiskt ändamål. Att viss del av verksamheten har journalistiska ändamål medförde enligt tingsrätten inte att verksamheten i sin helhet ska undantas från förekommande krav enligt dataskyddslagstiftningen.

Det skulle strida mot EU-rättens krav på en sammanjämkning mellan yttrandefriheten, handlingsoffentligheten och skyddet för personuppgifter om nyhetsbyrån helt undantogs från dataskyddsreglerna. Tingsrätten fann därför att GDPR skulle tillämpas på nyhetsbyråns verksamhet varför begäran om handlingsutlämnande avslogs med hänvisning till att de omfattades av sekretess enligt 21 kap. 7 § OSL.

Tingsrättens bedömning pekar på att det i varje tillämpningssituation måste göras en avvägning mellan å ena sidan integritetsskyddsintresset såsom det kommer till uttryck i GDPR och EU-domstolens praxis (C-439/19) och å andra sidan de grundlagsfästa rättigheterna enligt svensk rätt. Sådana avvägningar kan, enligt tingsrätten, medföra att svensk rätt behöver sättas åt sidan.

> Att viss del av verksamheten har journalistiska ändamål medförde enligt tingsrätten inte att verksamheten i sin helhet ska undantas från förekommande krav enligt dataskyddslagstiftningen.

En kort tid efter avslaget återkom nyhetsbyrån till Malmö tingsrätt med en ny begäran. I denna begäran lämnade nyhetsbyrån närmare information om sin journalistiska verksamhet och klargjorde att databasen för bakgrundskontroller var under avveckling. Nyhetsbyrån uppgav också att de begärda uppgifterna endast skulle användas inom nyhetsbyråns journalistiska

verksamhet och inte tillgängliggöras för allmänheten på annat sätt.

Mot denna bakgrund ändrade tingsrätten sitt tidigare beslut och fann att nyhetsbyråns begäran inte kunde avslås med tillämpning av 21 kap. 7 § OSL. I stället skulle nyhetsbyrån eventuella tillgång till handlingarna föregås av en sedvanlig sekretessprövning enligt OSL.

> Det får antas att det i det vidare lagstiftningsarbetet också kommer ske ett förnyat ställningstagande till frågan om ramarna för grundlagsskydd bör bestämmas med uteslutande tillämpning av svensk rätt eller om ramarna även bestäms av EU-rätten, det vill säga GDPR.

Det kan tilläggas att nämnda bedömningar av tingsrätterna, såvitt avser hinder mot utlämnande och behandling av uppgifter om lagöverträdelser i grundlagsskyddade databaser, i viss mån föregick det lagstiftningsarbete som initierades av den svenska regeringen i oktober 2023 (se dir. 2023:145, *Ett förstärkt skydd för personuppgifter på tryck- och yttrandefrihetsområdet*).

Utredningen har i uppdrag att bland annat överväga eventuella inskränkningar i det svenska grundlagsskyddet även för söktjänster för offentliggörande av personuppgifter om lagöverträdelser. En sådan inskränkning skulle alltså vara av liknande slag som de begränsningar vilka redan gäller för offentliggörande av vissa känsliga personuppgifter. Det får antas att det i det vidare lagstiftningsarbetet också kommer ske ett förnyat ställningstagande till frågan om ramarna för grundlagsskydd bör bestämmas med uteslutande tillämpning av svensk rätt eller om ramarna även bestäms av EU-rätten, det vill säga GDPR.

> Innan eventuella grundlagsändringar kommer på plats, förefaller en sådan rättstillämplig stå i konflikt med grundlag – samt dataskyddslagen – möjligen även i betydelsen att tillämpningen äventyrar ”principerna för statsskicket”.

Den senare frågan anknyter i sin tur också till föreskriften i den svenska konstitutionen att riksdagen, inom ramen för samarbetet i EU, inte kan överlåta beslutanderätt som *rör principerna för statsskicket*, 10 kap. 6 § regeringsformen. Till principerna för det svenska statsskicket hör exempelvis TF:s offentlighetsprincip, liksom ansvarighetssystemet enligt mediegrundlagarna (se konstitutionsutskottets betänkande 1993/94:KU21, s 27).

Det är måhända något överraskande att svenska domstolar, utan uttryckligt stöd i mediegrundlagarna, ansett att generella hinder kan uppställas mot offentliggöranden i sökbara databaser och andra medier av uppgifter om enskildas lagöverträdelser. Innan eventuella grundlagsändringar kommer på plats, förefaller en sådan rättstillämplig stå i konflikt med grundlag – samt dataskyddslagen – möjligen även i betydelsen att tillämpningen äventyrar ”principerna för statsskicket”.

Esa Kymäläinen är advokat och partner på TIME DANOWSKY Advokatbyrå, specialiserad på media- och IT-rätt, dataskydd, konkurrensrätt och andra regulatoriska frågor.

Jesper Jakobsson är biträdande jurist på TIME DANOWSKY Advokatbyrå. Han är särskilt inriktad på immaterialrätt, medierätt och IT-rätt.

Illustrasjon: Colourbox.com

Ulovlig IPTV-strømming – i hvilken grad kan et forbud håndheves overfor brukeren?

Av Fredrik Wiker og Hans Erik Johnsen

Strømming av lineær-TV over internett uten rettighetshavers samtykke er et fenomen som har økt kraftig de siste årene. Tjenestene har blitt så tilgjengelige og profesjonaliserte at de nesten fremstår som lovlige tilbud i markedet. Hva brukerne risikerer ved å strømme ulovlig, og konsekvensene for kringkastere og distributører er ikke like synlige. I praksis kan det være vanskelig for rettighetshaverne å gjennomføre tiltak uten å involvere politiet. Politiets ressurser er imidlertid begrensede, og gjennomføringsevnen blir da lav.

Fredrik Wiker

Hans Erik Johnsen

Økende bruk av IPTV-strømming

Piratkopiering av musikk, film og TV over internett har foregått i lang tid, både via nedlastning, deling og strømming av innhold. Selv om denne trenden i en periode var nedadgående, kanskje delvis på grunn av lovlige strømmeplattformer slik som Spotify, Netflix og Viaplay, ser man nå at trenden er at piratbruk-/kopiering igjen øker.

Et fenomen som stadig øker i popularitet er strømming av lineær-TV via IPTV-tjenester hvor innholdet er tilgjengeliggjort uten rettighetshavers samtykke. IPTV er en forkortelse av *«Internet Protocol television»*, og betyr rett og slett TV over internett. Før ble det upresist brukt om TV via fiber, men de seneste årene har det blitt brukt som et begrep på strømming av TV over internett uten rettighetshavers samtykke.

> I denne artikkelen skal vi se nærmere på i hvilken grad privatpersoners IPTV-strømming uten rettighetshaveres samtykke er i strid med gjeldende lovgivning, hva konsekvensene av eventuelle lovbrudd er og hvilke muligheter for håndhevelse som finnes for rettighetshavere og politiet.

Slike IPTV-tjenester kan ved første øyekast fremstå som lovlige med profesjonelle nettsider, tilbud om abonnement via betaling og ulike kanalpakker, men skiller seg fra de lovlige TV-distributørenes tilbud ved å tilby tusenvis av kanaler fra alle verdens land til en brøkdel av prisene lovlige aktører kan tilby. Når man ikke betaler for varen man selger, er det selvsagt mulig.

Brukeren kan gjennom disse tjenestene se og strømme nesten hvilken som helst TV-kanal fra både nettleseren, mobilen og TV-en. Disse løsningene kan i det ytre minne om TV-distributørenes egne lovlige TV-tjenester. Tall fra 2023 viser at så mange som 255 000 norske husholdninger bruker ulovlig IPTV, noe som utgjør 11 % av alle husholdninger.[1]

1 Ifølge tall fra Mediavision våren 2023: «Insight Nordic Piracy»

Dette skaper åpenbare utfordringer for norske TV-distributører og rettighetshavere og problemet er langt større i dag enn tidligere tiders piratdekodere og piratkort medførte.

I denne artikkelen skal vi se nærmere på i hvilken grad privatpersoners IPTV-strømming uten rettighetshaveres samtykke er i strid med gjeldende lovgivning, hva konsekvensene av eventuelle lovbrudd er og hvilke muligheter for håndhevelse som finnes for rettighetshavere og politiet.

Forbud mot strømming fra ulovlig kilde ble inntatt i åndsverkloven i 2018

TV-sendinger, og innhold som vises på TV, er som den klare hovedregel beskyttet som åndsverk i henhold til åndsverkloven (åvl.) § 2. Åndsverkloven § 3 oppstiller et forbud mot eksemplarfremstilling (kopiering) og tilgjengeliggjøring (deling) av åndsverk. Det vil si at det er forbudt å laste ned og forbudt å dele innhold fra TV-sendinger med andre, med mindre bruken omfattes av en av de snevre unntaksreglene i åvl. kapittel 3.

I 2018 ble det også lovfestet et forbud mot å konsumere, herunder strømme, innhold i enkelte tilfeller. Bakgrunnen for forbudet var at strømmetjenester for film der rettighetene ikke var klarert hadde blitt stadig mer populært, og lovgiver så et behov for å forby dette. Det tidligere fraværet av forbud hang delvis sammen med at det å beskytte den rene oppfattelsen av åndsverk (altså det å konsumere verket) historisk sett ikke har vært ansett beskyttelsesverdig, og i nyere tid et ønske om å, blant annet, verne om surfing på internett og ytrings- og informasjonsfriheten.

Etter åvl. § 3 tredje ledd er det ikke tillatt *«å strømme eller på annen måte bruke»* åndsverk som *«åpenbart i strid med denne loven er gjort tilgjengelig for allmennheten»* når bruken *«er egnet til å skade opphavers økonomiske interesser i vesentlig grad»*. Ved vurderingen av om privates strømming av IPTV er ulovlige, blir altså det avgjørende om de to siste vilkårene er oppfylt.

Strømming av IPTV er som den klare hovedregel i strid med åndsverkloven

Departementet har i forarbeidene til bestemmelsen uttalt at kravet om at noe «åpenbart» er gjort tilgjengelig i strid med loven er et strengt krav som ikke vil ramme tilfeller der det kan være tvil.[2] Den avgjørende målestokken er likevel ikke brukerens subjektive vurdering, men hvordan den alminnelige internettbruker vurderer det.

Når det gjelder uberettigede IP-TV-tjenester som i sitt umiddelbare ytre kan fremstå profesjonelle med ulike abonnementer og krav om betaling, blir dermed spørsmålet om man generelt kan si at den alminnelige internettbruker måtte forstå at innholdet er ulovlig tilgjengeliggjort. Det er en rekke forhold som tilsier at det er tilfellet.

For det første tilbys ikke tjenestene av de ordinære TV-distributørene som brukerne er vant til å forholde seg til. For det andre har tilbyderne ofte obskure navn og domener, er ikke identifisert med selskapsnavn og tar ofte betalt gjennom kryptovaluta eller andre mindre brukte betalingsmetoder. For det tredje gir IPTV-tilbyderne ofte tilgang til tusenvis av kanaler fra en rekke ulike land. Dette er det i prinsippet ingen lovlige aktører som kan tilby samlet. For det fjerde tilbys tjenestene til en brøkdel av prisene som man betaler hos de lovlige TV-distributørene.

Etter vårt syn er det sannsynlig at det for en alminnelig internettbruker som hovedregel vil være «åpenbart» at slikt innhold er gjort tilgjengelig uten tillatelse fra rettighetshaverne, selv om man ikke kan utelukke at det finnes spesielle unntakstilfeller som kan gjøre den konkrete vurderingen vanskeligere.

Videre må den ulovlige bruken være egnet til å skade rettighetshavernes interesser «i vesentlig grad». Også dette er av departementet i forarbeidene ansett som et strengt vilkår. Samtidig er det presisert at det avgjørende ikke er den enkeltes brukers strømming, men den totale *«virkningene av at det strømmes fra den aktuelle ulovlige kilden»*.[3] Flere rapporter konkluderer med at TV-distributørene taper vesentlige inntekter, og det er anslått at det samlede tapet i Europa var på over 3 milliarder euro i 2021.[4] Flere rapporter viser dessuten at ulovlig IPTV-innhold som utad leveres av ulike aktører ofte stammer fra et fåtall bakenforliggende kilder. For strømming av ulovlig IPTV-innhold fra den type tjenester vi har beskrevet ovenfor er det dermed sannsynlig at dette vilkåret er oppfylt.

Der ulovlig strømming oppdages kan det kreves forbud og vederlag

Virkningen av at strømmingen anses å være i strid med åvl. § 3 tredje ledd er at bruken må opphøre og gjentakelse kan forbys, jf. åvl. § 78.

En rettighetshaver som opplever en krenkelse kan kun kreve vederlag etter åvl. 81 der det foreligger en forsettlig overtredelse av bestemmelsen, jf. åvl. § 3 tredje ledd. Forsett forutsetter subjektiv skyld fra brukeren som har foretatt krenkelsen, noe som i praksis innebærer at brukeren må ha ansett det som *«sikkert eller overveiende sannsynlig»* at IP-TV-innholdet var ulovlig tilgjengeliggjort. I praksis vil forsettsvurderingen bli nokså lik vurderingen av om innholdet «åpenbart» er ulovlig tilgjengeliggjort, men ved forsettsvurderingen må man vurdere hva den konkrete brukeren forstod.

2 Prop.104 L (2016-2017) s. 39 flg.

3 Høringsnotat - forslag til ny lov om opphavsrett til åndsverk mv. 17. mars 2016 s. 42

4 The Audiovisual Anti-Piracy Alliance Illicit IPTV in Europe Economic Report December 2022

Dette underbygger formålet med bestemmelsen, dvs. at det er en høy terskel for å konstatere lovbrudd, og at det kun er det som i forarbeidene omtales som «de klare og bevisste tilfellene» som rammes. Vi tror likevel at det kun vil være svært unntaksvis at domstolene vil frifinne ved konstatert bruk av de organiserte ulovlige strømmetjenestene.

Sivilrettslig håndhevelse kan være utfordrende

Det å håndheve ulovlig strømming av IPTV kan være utfordrende for rettighetshaverne. Til forskjell fra ved mer tradisjonell piratkopiering som skjer med såkalt P2P-teknologi, herunder Bittorrent, hvor IP-adressen til de som piratkopierer er tilgjengelig for andre i piratkopieringsnettverket, blir ikke IP-adressen til de som ser på IPTV eksponert til andre enn IPTV-tilbyderen. Dette innebærer at det kan være vanskelig for rettighetshaverne å gjennomføre effektiv sivil etterforskning og dokumentere krenkelser.

> Vi tror likevel at det kun vil være svært unntaksvis at domstolene vil frifinne ved konstatert bruk av de organiserte ulovlige strømmetjenestene.

Tvisteloven kapittel 28 og 28 A åpner opp for bevissikring utenfor rettssak etter begjæring til retten. Vilkårene for å iverksette dette er noe strenge, og det forutsetter at rettighetshaverne vet hvem som kan sitte på bevis (slik som IPTV-tilbyderen). I de fleste tilfeller er det svært vanskelig å identifisere disse, fordi det skjer gjennom flere ledd av personer og på tvers av landegrenser.

Forutsatt at rettighetshaverne klarer å spore opp IP-adressen til de som strømmer, har åvl. § 87 en særskilt hjemmel for rettighetshavere til å få utlevert abonnementsopplysninger fra internettleverandørene. Dette er nødvendig for å kunne identifisere krenkeren. Slik utlevering forutsetter både samtykke fra NKOM og en kjennelse fra retten, samt at hensynene som taler for utlevering veier tyngre enn hensynet til at abonnementsopplysningene holdes hemmelig (interesseavveining).

I Høyesteretts avgjørelse *HR-2022-328-A*, som gjaldt utlevering av opplysninger ved piratkopiering over BitTorrent, opprettholdt Høyesterett lagmannsrettens nokså strenge terskel for utlevering. Enhver krenkelse vil derfor ikke kunne føre til utlevering, og det ble lagt til grunn av lagmannsretten – i samsvar med forarbeidene – at ren nedlastning av innhold som hovedregel ikke vil kunne føre til utlevering om det bare gjelder noen få verk. Til tross for at IPTV-strømming har en noe annen karakter enn nedlastning av enkeltverk, må det nok likevel legges til grunn at strømmingen må skje med et visst omfang for at abonnementsopplysninger kan utleveres.

Den beskyttelsesmekanismen med størst effekt kan være å hindre tilgang til nettsider hvor IPTV tilbys. Åndsverkloven § 88 har en særregel om at retten kan pålegge bl.a. internettleverandørene å hindre eller vanskeliggjøre tilgang til et nettsted. Også etter denne bestemmelsen må det foretas en interesseavveining hvor hensynet til rettighetshaverne må veie tyngre enn informasjons- og ytringsfriheten. Flere nettsteder som muliggjorde piratkopiering over BitTorrent har gjennom rettens kjennelse blitt sperret i Norge (f.eks. The Pirate Bay). Nettsideblokkering ved hjelp av DNS-blokkering gir imidlertid ingen fullverdig beskyttelse, siden blokkeringen enkelt kan omgås av brukere, og krever dessuten at det aktivt fremsettes nye begjæringer etter hvert som tjenestene gjenoppstår på nye nettsteder.

Strømming av IPTV er straffbart og kan være i strid med straffeloven

Strømming av IPTV i strid med åvl. § 3 tredje ledd er også straffbart. Overtredelse straffes med bot eller fengsel i opptil ett år, jf. åvl. § 79. På tilsvarende måte som for at rettighetshavere skal kunne kreve vederlag for bruken, må det også foreligge forsett fra krenkerens side for at straff kan bli aktuelt.

Strømming av IPTV kan også medføre brudd på straffelovens (strl.) § 203 om uberettiget tilgang til fjernsynssignaler. Dette straffebudet forbyr blant annet den som med forsett *«besitter, installerer, bruker»* en *«dekodingsinnretning»* og ved det skaffer seg *«uberettiget tilgang til en vernet formidlingstjeneste»*, og tilsvarende de som formidler eller distribuerer slik tilgang.

Tradisjonelt har formålet med denne bestemmelsen vært å beskytte TV-signaler som distribueres direkte fra distributøren til brukeren og dermed hindre at brukere omgår sperringene i de fysiske dekoderne som tidligere ble brukt. Bestemmelsen har imidlertid blitt endret en rekke ganger, og et uttalt formål i forarbeidene er at bestemmelsen skal være teknologinøytral. Det at IPTV-strømming ikke innebærer noen bruk av «dekoder» i tradisjonell forstand er dermed ikke nødvendigvis til hinder for at bestemmelsen skal kunne anvendes.

Det følger nemlig direkte av straffebudets ordlyd at «dekodingsinnretning» omfatter både utstyr og programvare som gir tilgang til en vernet formidlingstjeneste. Vernet formidlingstjeneste omfatter «fjernsyns- og radiosignaler». Det kan derfor argumenteres for at en IPTV-tjeneste i seg selv er en «programvare», og den uberettigede bruk av denne for å få tilgang til «fjernsyns- og radiosignaler» vil medføre brudd på straffebudet. Mot dette kan det likevel tenkes enkelte argumenter. For det første at IPTV-tjenesten i seg selv ikke er

programvare i faktisk forstand, men kun inneholder videolenker til TV-strømmen. Samtidig vil lenkene nettopp gjøre at man får uberettiget tilgang, og dekoderinnretningen kan også anses for å være TV-en, datamaskinen eller programvaren som spiller av disse lenkene. For det andre vil TV-signalet som kommer fra IPTV-leverandøren ikke leveres direkte fra TV-distributøren, men være dekodet og re-rutet separat hos IPTV-leverandøren. Bruken av begrepet «signalet» i strl. § 203 kunne tilsi at det må være det samme signalet, og ikke bare det samme innholdet, men forarbeidene viser til at begrepet skal ha tilsvarende betydning som etter kringkastingsloven § 1-1 bokstav a som etter sin ordlyd dekker den audiovisuelle utsendingen i seg selv.

I en dom fra Agder tingrett av 21. desember 2021 la retten tilsynelatende til grunn, uten å vurdere det nærmere, at tilgjengeliggjøring av IPTV-abonnement til andre var i strid med strl. § 203.[5] Etter vårt syn fremstår dette likevel å være riktig. En slik forståelse innebærer også at bestemmelsen vil omfatte private brukeres IPTV-strømming. Selv om legalitetsprinsippet vil sette skranker for bestemmelsens anvendelse, er formålet som kommer til uttrykk gjennom bestemmelsen å hindre uberettiget visning av fjernsynsinnhold som sendes direkte. Hvilken teknisk metode som benyttes burde da i lys av hensynet til teknologinøytralitet være underordnet.

Politiets etterforskning av IPTV-strømming

Overtredelse av strl. § 203 som skjer med forsett om tap for den berettigete, eller vinning for seg selv eller annen, straffes med bot eller fengsel i ett år. I motsetning til brudd på åvl. § 3 tredje ledd straffes de grove overtredelsene med bot eller fengsel i inntil tre år.

Illustrasjon: Colourbox.com

> Man kan jo for eksempel spørre seg hvorfor man ikke har vurdert å innføre lovgivning som vanskeliggjør betaling fra norske brukere, slik man i mange år har hatt på pengespillområdet.

Til forskjell fra ved den sivilrettslige håndhevingen det er redegjort for ovenfor, har politiet flere og mer inngripende virkemidler og metoder som kan tas i bruk ved etterforskning av kriminelle handlinger. Dette kan gjøre det enklere for politiet å etterforske, og avdekke, ulovlig strømming av IPTV gjennom blant annet samarbeid på tvers av landegrenser og ved aksjoner mot konkrete tilbydere. Håndheving, og prioritet, fra politiets side kan også være avskrekkende for brukerne.

Vi har ikke inntrykk av at dette er et område politiet i dag prioriterer, noe som viser seg gjennom de få publiserte dommene som gjelder uberettiget tilgang til fjernsynssignaler. Frem til politiet intensiverer sin etterforskning av IPTV-strømming mot både tilbydere og brukere, er det liten reell oppdagelsesrisiko for de som i dag driver med ulovlig IPTV-strømming. I lys av det store omfanget som er avdekket, og de økonomiske skadevirkningene dette har for TV-distributørene, burde etterforskning prioriteres. Heller ikke lovgiver fremstår som proaktiv for å sikre effektiv håndheving av beskyttelsen lovene gir. Man kan jo for eksempel spørre seg hvorfor man ikke har vurdert å innføre lovgivning som vanskeliggjør betaling fra norske brukere, slik man i mange år har hatt på pengespillområdet.[6]

Fredrik Wiker (Senior Associate, Wiersholm) og Hans Erik Johnsen (Partner, Wiersholm). Begge arbeider i Advokatfirmaet Wiersholms avdeling for teknologi, media, telekom og immaterialrett.

5 Dommen angikk videresalg av *«25 TV-bokser og minst 100 IPTV abonnementer som ga kundene tilgang til diverse vernede betalings-TV kanaler»*. Den siktede tilstod og ble dømt til fengsel i 45 dager og inndragning av utbytte på kr 100 000.

6 Lov om pengespill *(LOV-2022-03-18-12)* § 5.

Arbeidsgivers adgang til å gjøre innsyn i arbeidstakers e-post ved mistanke om pliktbrudd

Av Mahrukh Mahomood og Regine Rolfsen

1. Innledning

Retten til personvern er en grunnleggende menneskerettighet som også gjelder på arbeidsplassen. Det klare utgangspunktet er derfor at arbeidstakere har samme personvern på arbeidsplassen, som ellers i samfunnet. Dette innebærer at arbeidstaker har rett til å holde e-post og andre filer privat. Det kan imidlertid oppstå situasjoner som medfører at arbeidsgiver får et behov for å gjøre innsyn i arbeidstakers e-post, men fordi dette innebærer et inngrep i arbeidstakers personvern og privatliv, kan ikke slike innsyn foretas med mindre nærmere vilkår er oppfylt.

Denne artikkelen tar for seg spørsmålet om når arbeidsgiver lovlig kan gjøre innsyn i arbeidstakers e-post ved mistanke om grovt pliktbrudd, med særlig vekt på typiske situasjoner hvor slikt innsyn kan være aktuelt.

Mahrukh Mahomood

Regine Rolfsen

2. Rettslig utgangspunkt

2.1 Innledning

Rettsreglene som danner utgangspunktet for arbeidsgivers adgang til å gjennomføre innsyn i ansattes e-post finnes dels i GDPR og dels i forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale (e-postforskriften).

For at det skal foreligge rettslig grunnlag for å gjennomføre innsyn i ansattes e-post må flere vilkår være oppfylt i begge regelverkene. I tillegg må det foretas en interesseavveining mellom arbeidsgivers interesse i å gjennomføre innsyn på den ene siden og arbeidstakers rett til personvern og privatliv på den andre siden.

> Denne artikkelen tar for seg spørsmålet om når arbeidsgiver lovlig kan gjøre innsyn i arbeidstakers e-post ved mistanke om grovt pliktbrudd, med særlig vekt på typiske situasjoner hvor slikt innsyn kan være aktuelt.

2.2 Sammenhengen mellom regelverkene

GDPR krever at enhver behandling av personopplysninger har et behandlingsgrunnlag. For å foreta innsyn i arbeidstakers e-postkasse, er en såkalt interesseavveining etter GDPR art. 6 nr. 1 bokstav f det mest aktuelle behandlingsgrunnlaget. E-postforskriften inneholder i denne sammenheng særreguleringer, som innebærer at innsyn bare er lovlig for interessene oppgitt i forskriftens § 2 bokstav a eller b. I denne artikkelen vil vi konsentrere oss om bestemmelsen i bokstav b.

GDPR og e-postforskriften er noe overlappende når det gjelder adgangen til å gjøre innsyn i arbeidstakers e-post. Dette innebærer at selv om behandlingsgrunnlaget finnes i e-postforskriften, må arbeidsgiver også kunne vise til at innsynet følger et nødvendig formål og det må foretas en interesseavveining.

2.3 Når kan arbeidsgiver lovlig foreta innsyn?

2.3.1 Berettiget interesse

Det første vilkåret er at arbeidsgiver må ha en *«berettiget interesse»* i å gjennomføre innsyn.

Det følger av e-postforskriften § 2 første ledd bokstav b at arbeidsgiver har rett til innsyn i arbeidstakers e-post *«ved begrunnet mistanke om at arbeidstakers bruk av e-postkasse eller annet elektronisk utstyr medfører grovt*

brudd på de plikter som følger av arbeidsforholdet eller kan gi grunnlag for oppsigelse eller avskjed».

Bestemmelsen krever for det første at arbeidsgiver har en *«begrunnet mistanke»*. Dette innebærer at arbeidsgivers mistanke ikke kan bygge på løse antakelser, men at arbeidsgiver må kunne vise til konkrete omstendigheter eller bevis som begrunner mistanken. Innsyn er et inngripende virkemiddel, noe som taler for at det bør stilles krav om konkrete omstendigheter som underbygger arbeidsgivers mistanke.

> Innsyn er et inngripende virkemiddel, noe som taler for at det bør stilles krav om konkrete omstendigheter som underbygger arbeidsgivers mistanke.

Videre er det et vilkår at mistanken må knytte seg til forhold som medfører *«grovt brudd»* på arbeidsrettslige plikter. Dette innebærer at mistanke om brudd på alminnelige arbeidsrettslige plikter ikke er tilstrekkelig. Hva som utgjør et grovt brudd, må tolkes konkret i det enkelte tilfellet. Vilkåret kan være oppfylt dersom arbeidsgiver mistenker forhold som kan gi grunnlag for oppsigelse eller avskjed, men også dette vil bero på en konkret vurdering. En nærmere gjennomgang av hvilke konkrete omstendigheter som kan utgjøre grovt pliktbrudd foretas lenger ned i artikkelen.

2.3.2 Nødvendig formål

Selv om arbeidsgiver kan vise til at vilkårene for å gjøre innsyn i arbeidstakers e-post etter e-postforskriften § 2 første ledd bokstav b er oppfylt, må innsynet følge et lovlig og nødvendig formål. Dersom det finnes mindre inngripende måter å oppnå formålet på, kan ikke arbeidsgiver gjennomføre innsyn.

Innsyn kan anses nødvendig av mange ulike grunner, blant annet for å bekrefte eller avkrefte mistanker om straffbare handlinger eller andre alvorlige forhold. Det vil da ofte være nødvendig med innsyn for å fremskaffe tilstrekkelig bevis. Vilkåret vil på denne bakgrunn sjeldent by på problemer ved spørsmål om innsyn knyttet til mistanke om grovt pliktbrudd etter forskriftens § 2 bokstav b.

2.3.3 Interesseavveining

Arbeidsgiver kan bare behandle personopplysninger om ansatte, dersom arbeidsgivers interesse i å gjennomføre innsynet veier tyngre enn hensynet til arbeidstakers personvern. Arbeidsgiver må foreta en avveining som vil bero på en konkret skjønnsmessig vurdering hvor flere forhold vil spille inn.

Som utgangspunkt må et innsyn i e-post anses som et stort inngrep i arbeidstakers personvern, men graden av alvorlighet kan variere. Dersom arbeidsgiver på sin side kan vise til et tungtveiende behov for innsyn, kan innsyn være lovlig. Avveiningen vil med andre ord kunne variere fra situasjon til situasjon.

Sentrale momenter i interesseavveiningen er blant annet graden av grovheten av det antatte pliktbruddet, hvor klare indisier arbeidsgiver har på at det faktisk foreligger pliktbrudd og om det finnes mindre inngripende måter å avdekke pliktbruddet på. Jo grovere pliktbruddet mistanken knytter seg til er, dess mindre skal til for at arbeidsgiver har en berettiget interesse i å foreta innsyn. Det samme gjelder dersom arbeidsgiver har en godt begrunnet mistanke om at det foreligger pliktbrudd. Dersom arbeidsgiver kan avdekke pliktbruddet ved hjelp av mindre inngripende metoder, vil innsyn som hovedregel ikke være forholdsmessig.

3. Den konkrete vurderingen

3.1 Innledning

E-postforskriften § 2 bokstav b oppstiller en høy terskel for innsyn i arbeidstakers e-post, ved at mistanken må gjelde forhold som medfører *«grovt brudd»* på de plikter som følger av arbeidsforholdet. Mistanke om helt bagatellmessige forhold vil aldri kunne gi grunnlag for innsyn etter denne bestemmelsen. Det må foreligge mistanke om et vesentlig mislighold fra arbeidstakers side. I denne vurderingen vil både lov- og avtaleregulering av arbeidstakerens plikter være av betydning.

Forhold som utgjør grove pliktbrudd, vil ofte være forhold som kan begrunne oppsigelse eller avskjed. På bakgrunn av at dette er angitt som et eget alternativ i bestemmelsen, kan det imidlertid legges til grunn at det ikke er *nødvendig* at forholdet vil begrunne oppsigelse eller avskjed. I praksis tillegges ikke dette skillet nevneverdig betydning

3.2 Når foreligger «grovt» pliktbrudd som gir adgang til å gjøre innsyn?

Hva som utgjør et grovt pliktbrudd, vil bero på en konkret vurdering i det enkelte tilfellet. Enkelte typetilfeller kan imidlertid utledes fra rettspraksis og teori.

For det første vil deling av straffbart materiale eller utøvelse av straffbar virksomhet ved hjelp av arbeidsgivers datasystem klart kunne begrunne et innsyn. Som eksempel kan nevnes arbeidstakers deling av seksualisert innhold eller bruk av systemene til omsetning av ulovlige stoffer/ulovlig ervervede varer. Det må selvsagt foretas en konkret vurdering også her, men slike forhold vil nok ofte anses som grove pliktbrudd fra arbeidstakers side. Videre er det her snakk om mistanke som vanskelig kan bekreftes eller avkreftes på andre måter enn ved innsyn i e-post.

Også mistanke om annen utilbørlig adferd, som ikke nødvendigvis er

Illustrasjon: Colourbox.com

straffbar, vil kunne begrunne innsyn. Som eksempel kan nevnes at en arbeidstaker har brukt arbeidsgivers datasystem for utsendelse av e-poster med trakasserende eller sjikanerende innhold. Dette er nok særlig aktuelt ved trakassering av kolleger eller andre med et forhold til virksomheten (for eksempel kunder eller samarbeidspartnere), men også uttalelser til utenforstående kan etter en konkret vurdering omfattes.

Videre vil mistanke om økonomisk utroskap eller annen illojalitet overfor arbeidsgiver kunne gi adgang til å gjøre innsyn. Det samme gjelder mistanke om brudd på taushetsplikt, særlig i relasjon til bedriftshemmeligheter. Som eksempel kan vises til *LB-2021-164489*, hvor lagmannsretten la til grunn at mistanke om økonomisk underslag og spredning av taushetsbelagt informasjon, klart tilfredsstilte vilkåret for innsyn i e-postforskriften § 2 bokstav b. Et annet eksempel er *LA-2021-137694*. I denne saken la lagmannsretten til grunn at mistanke om forfalskning av en bestilling i bedriftens datasystem, for å skjule en tidligere feil, var tilstrekkelig for å oppfylle forskriftens vilkår.

> Gjennomgangen over viser at arbeidsgiver har flere muligheter til å gjøre innsyn i arbeidstakers e-post, men at det også er mange fallgruver.

At forhold av denne karakter ofte anses omfattet av bestemmelsen, er etter vårt syn naturlig. Tillit mellom partene er helt sentralt i et arbeidsforhold, og forhold av denne karakter vil derfor raskt utgjøre vesentlige mislighold fra arbeidstakers side. Felles for de typene brudd som er nevnt over, er også at de i stor grad er egnet til å skade virksomheten, både innad og utad.

4. Avsluttende bemerkninger

Gjennomgangen over viser at arbeidsgiver har flere muligheter til å gjøre innsyn i arbeidstakers e-post, men at det også er mange fallgruver. Arbeidsgiver må derfor sørge for å gjennomføre grundige vurderinger før innsyn foretas, for å forsikre seg om at personvernregelverket er overholdt. I motsatt fall risikerer arbeidsgiver både erstatningskrav fra arbeidstaker og bøter fra tilsynsmyndigheten.

Mahrukh Mahmood er advokatfullmektig ved CMS Kluge advokatfirma. Her arbeider hun blant annet med arbeidsrett og personvern, og i grensesnittet mellom de to rettsområdene.

Regine Rolfsen, advokat i CMS Kluge Advokatfirma. Hun er tilknyttet firmaets arbeidsrettsteam og bistår med et bredt spekter av tjenester innen både arbeidsrett og personvern.

Halvor Manshaus

Halvor Manshaus er leder IP/Media-gruppen i Advokatfirmaet Schjødt AS, Oslo og fast spaltist i Lov&Data.

Handel med kryptoeiendeler – en kort status

Innledning – digital eiendeler i blokkjeden

Det er i skrivende stund over 15 år siden lanseringen av Bitcoin i januar 2009. I de første årene etter lansering var det svært få som i det hele tatt hadde lagt merke til at Bitcoin var blitt lansert. Ved utgangen av 2010, to år etter lanseringen, var en Bitcoin fortsatt ikke verdt mer enn USD 0.30. Som kjent har verdien av Bitcoin steget vesentlig etter dette, en utvikling som har gått i rykk og napp. Interessen for Bitcoin og andre digitale eiendeler basert på blokkjeder har i stor grad vært koblet opp mot den enorme verdistigningen, som også har gitt mye oppmerksomhet i media og ulike internett-fora.

De store fluktuasjonene i verdi har gitt grunnlag for sterkt spekulative handler, der både risiko og potensiell avkastning har vært enorm. Gjennom årene har det dukket opp en rekke ulike alternative digitale valutaer basert på blokkjedeteknologi. Kun et fåtall av disse har klart å oppnå kritisk masse med tanke på interesse hos publikum og faktisk omsetning. De som har klart seg har samtidig gradvis etablert seg og funnet en slags plass i den globale finansverden.

Ulike børser og handelssystemer for kryptoeiendeler har vokst frem til tross for en rekke uavklarte rettslige spørsmål og et mangelfullt regelverk. Dette har medført en stor underliggende eksponering for kunder som handler gjennom slike børser. Et eksempel på dette er kryptobørsen Mt Gox som i 2014 håndterte over 70 % av den globale Bitcoin-omsetningen. Denne børsen ble opprinnelig opprettet i 2007 for å bytte spillekort, og navnet er et akronym for «**M**agic: **T**he **G**athering **O**nline E**x**change». I februar 2014 ble Mt Gox hacket og tapte om lag 850 000 Bitcoin. I ettertid ble en del av disse vunnet tilbake, men Mt Gox gikk konkurs kort tid etter hackingen. Slike tilfeller understreker behovet for rettslig regulering av handelsplasser av denne typen. Likevel har dette latt vente på seg, og i mellomtiden har den ene skandalen avløst den andre. Nedenfor skal vi se nærmere på ett tilfelle som ligger nærmere i tid, den såkalte FTX-skandalen.

Case study: FTX-skandalen

Sam Bankman-Fried og Gary Wang startet i 2019 kryptobørsen FTX (forkortelse for Futures Exchange). Allerede i 2021 hadde FTX med over en million registrerte kunder etablert seg som den tredje største globale børsen for kryptoeiendeler. Alameda Research som handlet i digital valuta var i perioder kunden med størst handelsvolum hos FTX. Dette vekket etter hvert bekymring fra flere eksterne aktører, ettersom Alameda Research var opprettet av den samme Bankman-Fried i 2019 nettopp for å handle med kryptovaluta. Det skulle vise seg at FTX og Alameda inflaterte tall og volumer hos hverandre blant annet ved å kjøpe opp og belåne digitale sertifikater (tokens) utstedt av FTX.

FTX og søsterselskapet Alameda Research viste seg altså i ettertid å være gjensidig avhengige av hverandre gjennom flere skjulte transaksjoner og avtaler. FTX utstedte blant annet en egen FTT token som ga innehaveren rabatt på avgifter ved handler på FTX-børsen, en egen verveprovisjon samt et eget regime for bonuspoeng. I følge FTX selv skulle verdien av slike FTT opprettholdes ved at FTX hadde et program for å kjøpe tilbake FTT som deretter ble destruert.

I en artikkel 2. november 2022 viste nettavisen Coindesk til en gjennomgang av regnskapene til Alameda. Coindesk pekte på flere koblinger mellom søsterselskapene som var uvanlig nære med tanke på de enorme underliggende verdiene det var snakk om. Coindesk viste til at Alameda totalt satt på 14,6 milliarder dollar i verdier, hvorav 3,66 mil-

liarder besto av «unlocked FTT» og en ytterligere post tilsvarende 2,16 milliarder omtalt som «FTT collateral», altså sikkerhet i FTT'er fra FTX. På gjeldssiden sto det oppført over 8 milliarder i lån, hvorav 292 millioner knyttet seg til «Locked FTT». Etter hvert som man la sammen tallene fremsto det som klart at betydelige beløp var knyttet opp mot FTT der den reelle verdien var vanskelig å slå fast. Det var ikke bare snakk om manglende diversifisering i porteføljen til de to virksomhetene, den gjensidige avhengigheten hvilte tilsynelatende på fiktive verdier og et gapende hull på over 8 milliarder dollar i balansen til Alameda. FTX på sin side var et privat selskap som ikke var underlagt de strenge kravene til regnskap og rapportering som andre finansforetak. Det var med andre ord ingen reell kontroll over tallene og den underliggende eksponeringen hos FTX.

Konkurrenten Binance, en annen stor plattform for handel av digitale valutaer hadde meldt interesse for å overta FTX umiddelbart etter artikkelen, man trakk seg raskt. Changpeng Zhao som var leder for Binance viste til pågående undersøkelser fra regulatoriske myndigheter i USA samt tallmateriale som viste at det var gjort omfattende underslag av kundemidler hos FTX. En rekke kunder forsøkte i denne perioden å ta ut sine midler fra FTX samtidig som verdien av FTT stupte. Det skulle ikke ta mer enn en uke etter artikkelen fra Coindesk før FTX var nødt til å slå seg selv konkurs.

Advokaten John J. Ray III ble raskt plassert som bostyrer og ny leder for FTX. Ray hadde allerede sett mye rart i sin karriere der han har spesialisert seg på «fund recovery» fra havarerte selskaper. Han hadde blant annet sjefsrollen i Enron Creditors Recovery Corporation som jobbet å spore opp og gjenvinne midler fra konkursboet til Enron. En uttalelse i hans redegjørelse til konkursretten i Delaware oppsummerer Rays syn på forretningsmodellen til FTX: *«Never in my career have I seen such a complete failure of corporate controls and such a complete absence of trustworthy financial information as occurred here.»*

Problemene med FTX skyldtes ikke bare mangel på kontrollmekanismer, men at det bevisst ble spilt på sammenblandingen mellom FTX og Alameda for å øke handelsvolumer og generere inntekter. Samtidig ble midler beveget frem og tilbake uten at dette ble innrapportert på riktig måte. En bekymret Twitter-bruker påpekte allerede i 2019 at det kunne være grunn til bekymring hvis det ikke var armlengdes avstand mellom de to virksomhetene. Bank-Friedman svarte med en Twitter-melding senere samme dag 31. juli 2019:

«Alameda is a liquidity provider on FTX but their account is just like everyone else's. Alameda's incentive is just for FTX to do as well as possible; by far the dominant factor is helping to make the trading experience as good as possible.»

I den etterfølgende straffesaken mot Bank-Friedman forklarte hans tidligere partner Gary Wang at FTX samme dag sommeren 2019 la inn nye kodeinstrukser i sine systemer. Den tilsynelatende enkle setningen «allow_negative» hadde store konsekvenser for forholdet mellom FTX og Alameda. Kodelinjen i FTX-databasen åpnet for at Alameda kunne ha en negativ handelsbalanse hos FTX uten at dette fikk noen konsekvenser. I praksis åpnet dette for en ubegrenset kredittlinje, altså at Alameda kunne handle på FTX-børsen uten å betale for transaksjonene. Wang forklarte senere at Alameda i praksis hadde en kreditt på 65 milliarder dollar uten at dette ble innrapportert eller fremgikk av regnskapene.

FTX-skandalen skjedde i en periode der det var stor uro knyttet også til andre handelsplasser for digital valuta. Selv store og etablerte valutaer som Bitcoin og Ether hadde rast i verdi gjennom 2022, og mistillit og uro knyttet til flere av handelsplattformene var et viktig moment i denne utviklingen. Det er beregnet at det samlede markedet falt fra et verdinivå på ca. 3 trillioner dollar i 2021 til et estimert nivå på 796 milliarder i perioden like etter FTX-skandalen.[1]

Regulering av handelen – status

Per i dag har flere av disse valutaene klatret oppover og hentet igjen mye av verdien, men som eksempelet

1 https://www.reuters.com/technology/crypto-market-still-bears-scars-ftxs-collapse-2023-10-03/

med FTX ovenfor viser er det åpenbart et behov å stramme inn og regulere handelsplattformene. Det er kanskje paradoksalt at Satoshi Nakamoto, et psevdonym benyttet av skaperen av Bitcoin, kort tid etter lanseringen i 2009 forklarte følgende om fordelene ved å bruke en desentralisert valuta (11. februar 2009):

> *«The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve.»*

Satoshi siktet ikke mot etableringen av sentraliserte banker eller handelsplasser som FTX, i stedet skulle all aktivitet gå direkte gjennom blokkjeden. Han var selv klar på at bruken av mellommenn som sentraliserte handelen i seg selv innebar en risiko: *«It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third-party middleman, money can be secure and transactions effortless.».*

Historien har imidlertid vist at penetrasjonen til Bitcoin som alminnelig gangbar valuta hittil har vært lav. Systemet forutsetter bruk av blokkjeden, som igjen krever en del spesialkunnskap på begge sider av handelen. Denne terskelen har vært en viktig brems for gjennomslagskraften til Bitcoin og tilsvarende valutaer. I tillegg har den store interessen knyttet til digital valuta som investeringsobjekt økt behovet for handelsplasser der transaksjoner kan gjennomføres på tvers av valutaer og med sikkerhet for at det er dekning for overføringene begge veier. Dette er også grunnen til at mellommenn som FTX har vokst frem for å håndtere handelsmarkedet. I dette ligger det en stor utfordring, ved at slike børser raskt blir benyttet av forbrukere som ikke nødvendigvis kan så mye mer om digitale valutaer enn at de rent historisk og over tid har steget noe voldsomt i verdi. I tillegg påvirkes større profesjonelle investorer ved at selve handelsplassen ikke er transparent med den tilhørende risiko dette medfører.

I mange land har såkalte «kryptobørser» vært underlagt alminnelige lokale lover om hvitvasking og terrorfinansiering, men uten den strenge reguleringen som kjennetegner tradisjonelle finansforetak. Dette er nå i ferd med å endre seg, i takt med at det globale finansmarkedet har modnet og i stor grad startet prosessen med å absorbere blokkjeden som konsept. I januar 2024 åpnet U.S. Securities and Exchange Commission (SEC) for at Grayscale Bitcoin Trust kan konverteres til en ETF. Dette fondet sitter på om lag 29 milliarder dollar i Bitcoin og åpnet døren for lignende tillatelser for andre aktører i markedet. ETF står for Exchange Traded Fund og innebærer at et fond kan kjøpes og selges til kjent kurs på en børs akkurat som en aksje. En slik ETF vil i det alt vesentligste falle inn under et eksisterende og kjent regelverk som kan antas å være gunstig for å gi en tryggere ramme rundt handelen av denne type verdipapirer. Det er også en måte å «temme» Bitcoin og andre tilsvarende valutaer på, ved at handelen føres over fra blokkjeden og lirkes inn konvensjonelle handelssystemer. På denne måten fjerner man seg også fra det sentrale konseptet med blokkjeden: Direkte handel mellom kjøper og selger uten mellommann.

Avgjørelsen fra SEC kommer etter et tap i retten mot Grayscale høsten 2023 der SEC fikk kritikk for ulik håndtering av finansielle instrumenter knyttet til Bitcoin. Det var lenge uvisst hvordan SEC ville gå frem, ikke minst fordi formannen Gary Gensler har vært sterkt kritisk til denne typen digitale valutaer. En uttalelse fra Gensler samme dag som SEC til slutt godkjente søknaden fra Grayscale understreker at SEC ønsker å trå varsomt frem:[2]

> *«Importantly, today's Commission action is cabined to ETPs holding one non-security commodity, bitcoin. It should in no way signal the Commission's willingness to approve listing standards for crypto asset securities. Nor does the approval signal anything about the Commission's views as to the status of other crypto assets under the federal securities laws or about the current state of non-compliance of certain crypto asset market participants with the federal securities laws. As I've said in the past, and without prejudging any one crypto asset, the vast majority of crypto assets are investment contracts and thus subject to the federal securities laws.»*

I EU trådte Markets in Crypto Assets Regulation (MiCA/Kryptoeiendelsforordningen) i kraft juni 2023 med anvendelse fra 30. desember 2024. Forordningen vil ved innlemmelse etter EØS-avtalens artikkel 7 «gjøres til del av avtalepartenes interne rettsorden», som i praksis vil si ved lov eller forskrift. Et viktig formål med forordningen er å skape finansiell stabilitet og tillit i markedene for såkalte kryptoaktiva, samtidig som både profesjonelle aktører og forbrukere beskyttes mot risiko. Det legges opp til at nasjonale myndigheter skal kunne regulere, kontrollere og behandle produkter og tjenester i markedet, samt leverandører av relaterte tjenester.

2 https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023

MiCA må sees i sammenheng med blant annet DORA-forordningen (Digital Operational Resilience Act), som stiller krav til aktører i finanssektoren om tiltak mot cyberangrep og andre risikofaktorer, samt regulering av enkelte kryptotransaksjoner i antihvitvaskingsregelverk og andre regelverkskrav som har vokst frem de siste årene.

I forordningen benyttes begrepet «kryptoeiendel», definert som en digital representasjon av en rettighet eller verdi som kan overføres og oppbevares elektronisk ved bruk av distribuert registerteknologi eller tilsvarende løsninger. Tre hovedkategorier kryptoeiendeler er regulert i forordningen:

1. E-Money Tokens (EMT / E-pengetoken): Kryptoeiendeler som utgjør en form for e-penger ved at det anføres en stabil verdi relatert til én offisiell valuta
2. Asset Reference Tokens (ART / Eiendelsbaserte token): Eiendelsbaserte kryptoeiendeler med anført stabil verdi knyttet til andre rettigheter eller verdier, eventuelt kombinasjoner av for eksempel offisielle valutaer og ulike typer investeringsobjekter
3. Utility Tokens: Andre kryptoeiendeler med bruksverdi, eksempelvis Ether, Bitcoin og lignende.

For kryptoeiendeler som faller utenfor de to første kategoriene stilles det krav til tilbyderen, den som søker om at kryptoeiendelen tilbys på en handelsplattform, samt handelsplattformer som på eget initiativ tar opp kryptoeiendelene til handel. Det skal i alle disse tilfellene utarbeides et eget skriv som skal gi potensielle investorer informasjon om egenskaper, funksjoner og risikoer ved de aktuelle kryptoeiendelene.

Regelverket gjelder ikke bare for utstedere og tilbydere av tokens, men også for crypto asset service providers (CASP). Denne gruppen omfatter både fysiske og juridiske personer som tilbyr ulike tjenester knyttet opp mot kryptoaktiva, herunder

- drift av handelsplattform
- kjøp, oppbevaring eller veksling
- rådgivning eller porteføljeforvaltning

For å redusere risikoen for nye FTX-lignende tilfeller innføres krav drift til og «governance», samt at kundemidler må være adskilt fra øvrige selskapsmidler, slik at midlene er sikret også ved konkurs.

Hva med NFT?

Forordningen er ikke ment å avløse eller tre i stedet for dagens regelverk for finansielle instrumenter. I stedet er MiCA å betrakte som et supplement som utfyller dagens finansregulatoriske regelverk. Ordinære digitale valutaer som faller utenfor begrepet kryptoeiendel vil således falle utenfor MiCA. Det samme gjelder andre typer digitale eiendeler som allerede er klassifisert som finansielt instrument under dagens regelverk. Her vil det kunne oppstå utfordringer når man i praksis skal avgjøre om for eksempel en NFT (Non Fungible Token) faller innenfor MiCA. Informasjon om eierskap til en NFT vil lagres i kryptert format på blokkjeden samtidig som den kobles opp mot en konkret og spesifisert angitt eiendel. Denne eiendelen kan være digital eller fysisk. Slike NFT har flere funksjoner, og kan blant annet benyttes som digitale sertifikater for å kunne dokumentere autentisitet og notoritet for digitale kunstverk og annet digitalt gods. I MiCA heter det i fortalens punkt 10 at aktiva med verdi ut ifra distinkte og særegne egenskaper og lav grad av «fungibilitet faller utenfor forordningen.:

> *«This Regulation should not apply to crypto-assets that are unique and not fungible with other crypto-assets, including digital art and collectibles. The value of such unique and non-fungible crypto-assets is attributable to each crypto-asset's unique characteristics and the utility it gives to the holder of the token.»*

I punkt 11 heter det imidlertid at inndeling av et slikt aktiva i flere enkeltelementer eller en større samling med aktiva kan være en indikasjon på fungibilitet, med den konsekvens at MiCA får anvendelse likevel:

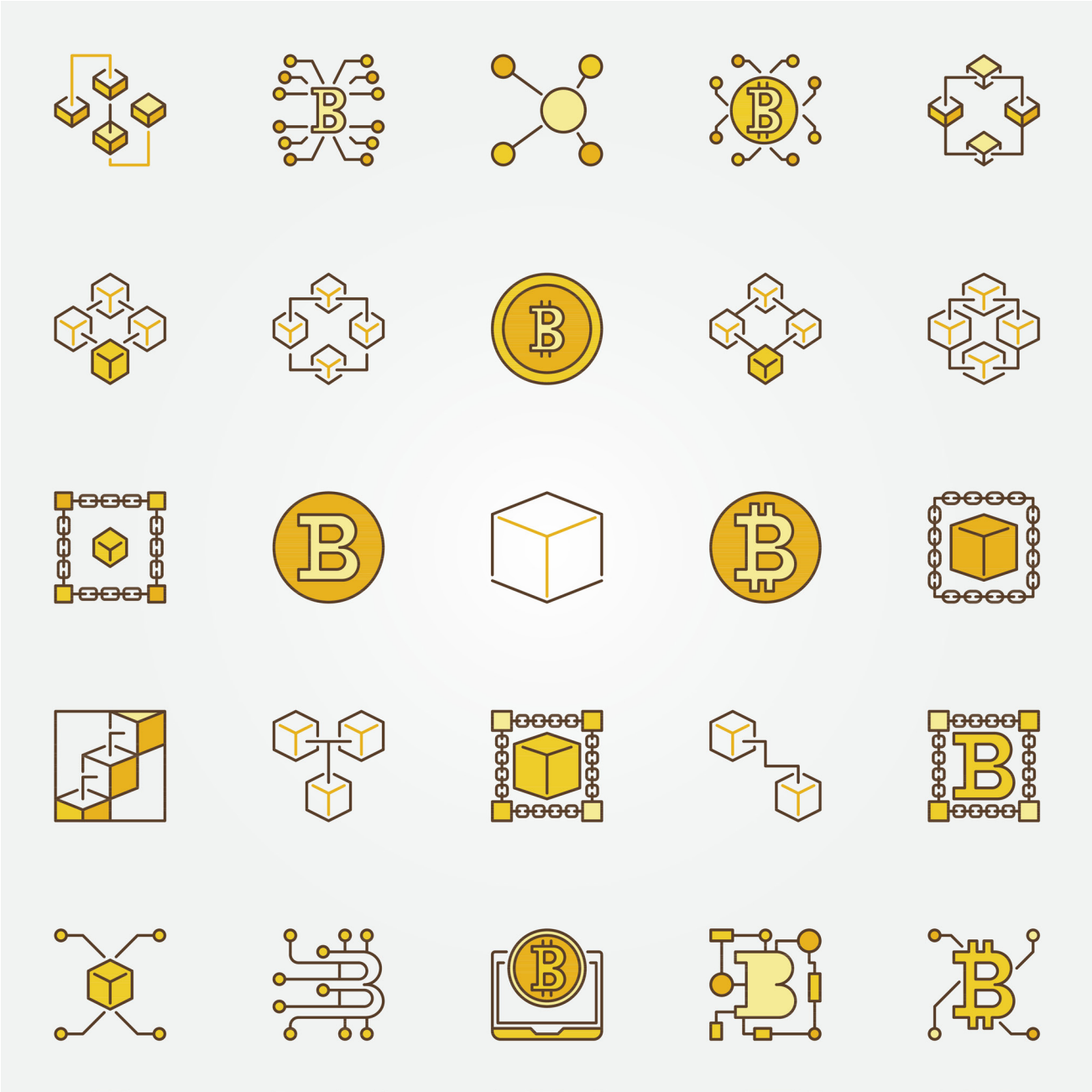
> *«This Regulation should also apply to crypto-assets that appear to be unique and non-fungible, but whose de facto features or whose features that are linked to their de facto uses, would make them either fungible or not unique. In that regard, when assessing and classifying crypto-assets, competent authorities should adopt a substance over form approach whereby the features of the crypto-asset in question determine the classification and not its designation by the issuer.»*

Oppsummeringsvis kan det slås fast NFT i praksis ikke er fullstendig unntatt fra MiCA og at det må gjøres en konkret vurdering i det enkelte tilfelle. Det sier seg selv at den vurderingen ikke alltid vil være like enkel.

> Oppsummeringsvis kan det slås fast NFT i praksis ikke er fullstendig unntatt fra MiCA og at det må gjøres en konkret vurdering i det enkelte tilfelle.

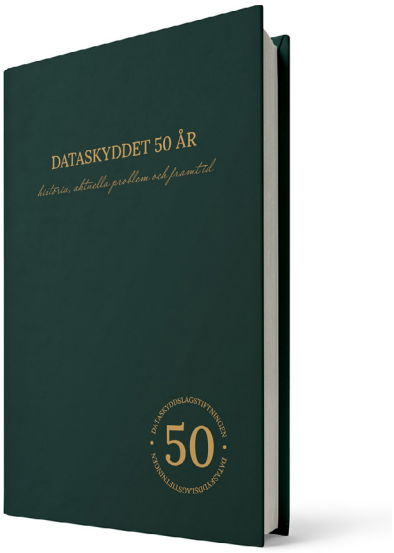
Kunstneren Damien Hirst laget i 2021 10 000 NFT-eksemplarer av verket «The Currency». Hvert enkelt verk var igjen koblet til et underliggende fysisk verk på papir

som Hirst laget tilbake i 2016. Disse papirbildene ble skapt gjennom maskinlæring basert på en database som inneholdt teksten til enkelte av Hirsts favorittlåter, for eksempel: «Totally *Gonna Sell You*», «*Wet Moving Mirror*» og «*Grandfathered to the Gang*». Hvert verk inneholder en tittel generert fra tekstene, samt tilfeldige unike fargeklatter. Samtlige verk er signert og nummerert. I tillegg er det plassert en mikrodott på hvert papirark som inneholder et hologram med portrettbilde av Hirst. Samtlige 10 000 verk ble plassert i et hvelv et ukjent sted i England. Hirst tilbød verkene for salg, men slik at kjøperen mottok verket som en NFT. Innen 27. juli 2022 kl. 15:00 (BST) måtte den stolte eier bestemme seg for å beholde verket som NFT eller veksle dette inn mot det underliggende fysiske verket. Etter dette ville alle de gjenværende fysiske verkene bli brent. Leseren kan selv ta stilling til om Hirsts omsetning av NFT ville ha falt innenfor eller utenfor MiCA.



Illustrasjon: Colourbox.com

Dataskyddet 50 år – historia, aktuella problem och framtid

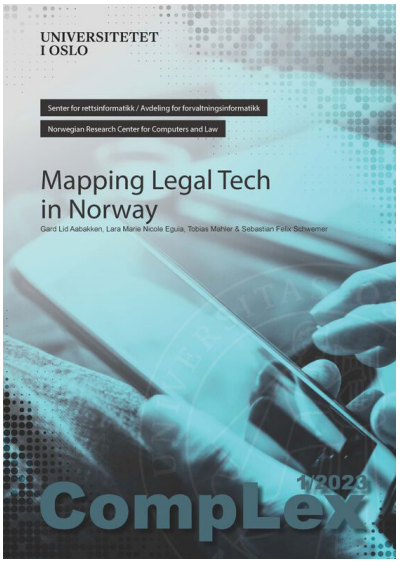


Martin Brinnen (red.), Cecilia Magnusson Sjöberg (red.), David Törngren (red.), Daniel Westman (red.), Sören Öman (red.). Dataskyddet 50 år – Historia, aktuella problem och framtid. Sverige: eddy.se ab, 2023. Isbn 9789189840027

Under 2023 fyller dataskyddslagstiftningen 50 år. Datalagen (1973:289) var världens första nationella lagstiftning som reglerade datoriserad behandling av personuppgifter på ett heltäckande sätt. Lagen ersattes 1998 av personuppgiftslagen (1998:204) som i sin tur upphävdes 2018 när EU:s dataskyddsförordning (2016/679) (GDPR) började tillämpas.

Omtalen er hentet fra Dataskyddslagstiftningen 50: https://dataskyddet.se/

Mapping Legal Technology in Norway



Gard Lid Aabakken, Lara Marie Nicole Eguia, Tobias Mahler & Sebastian Felix Schwemer. Mapping Legal Technology in Norway. Oslo: Universitetet i Oslo, Juridisk fakulte, Senter for rettsinformatikk/Avdeling for forvaltningsinformatikk 2023, 1/2023. ISSN 2703-8777 Complex (online)

«Mapping Legal Technology in Norway». Rapporten kartlegger bruken av «legal tech» i Norge. Rettsteknologi kan brukes til ulike juridiske formål. Blant disse er automatisering av juridiske arbeidsprosesser, beslutningsstøtte i juridiske tjenester, eller juridiske råd og informasjon direkte til sluttbrukere. Rapporten ble til som del av et forskningsprosjekt finansiert av Lovdata i perioden 2022–2023.

Les hele utgivelsen i CompLex 01/23.

Dataskyddsförordningen (GDPR) m.m.

En kommentar

Sören Öman. Dataskyddsförordningen (GDPR) m.m. En kommentar. Sverige: Norstedts Juridik, 2021. ISBN: 9789139023814

Detta är en omfattande kommentar till EU:s dataskyddsförordning (2016/679) – GDPR. Förordningen kommenteras artikel för artikel på traditionellt sätt. Även den kompletterande svenska s.k. dataskyddslagen (2018:218) kommenteras paragraf för paragraf. I verket finns också en utförlig kommentar till bestämmelsen om s.k. dataskyddssekretess i 21 kap. 7 § offentlighets- och sekretesslagen (2009:400).

Första upplagan av kommentaren utsågs 2020 till årets verk av Norstedts Juridik. I denna andra upplaga har bl.a. ny praxis och nya riktlinjer beaktats.

Omtalen er hentet fra Norstedts Juridik. Karnov Group: https://shop.nj.se/products/dataskyddsforordningen-gdpr-m-m-1

EU-Ret. Fri Bevægelighed

Få en grundlæggende viden om gældende EU-ret om fri bevægelighed

Ulla Nergaard og Ruth Nielsen. EU-Ret. Fri Bevægelighed. Danmark: Karnov Group Danmark, 2021. ISBN: 9788761943019

Denne bog giver en fremstilling af principperne om, dynamikken i og hovedstrukturen af gældende EU-ret om fri bevægelighed. Den kan lidt forenklet siges at handle om EU's økonomisk-juridiske forfatning.

Bogen er i princippet en opdatering og udvidelse af 2. udgaven af Ulla Neergaard og Ruth Nielsens »EU RET – fri bevægelighed«, Karnov Group, 2016. Bogen benyttes især på bachelor-faget »EU-ret« på jura-uddannelsen på Københavns Universitet.

Bogen omhandler:

- EU-Domstolen og dens fortolkningsstil
- Fri bevægelighed i det indre marked - generelt
- Varernes fri bevægelighed
- Fri udveksling af tjenesteydelser
- Etableringsfrihed
- Arbejdskraftens fri bevægelighed
- Unionsborgerskab
- Tredjelandsstatsborgere
- Bogen medtager gengivelser af centrale bestemmelser, domspræmisser og væsentlig litteratur.

Omtalen er hentet fra Karnov Group Danmark: https://www.karnovgroup.no/fagboeker/eu-ret-fri-bev%C3%A6gelighed

Rebecka Undén

Sanktionsavgift vid utkontraktering av vårdtjänst

Den svenska Integritetsskyddsmyndigheten (”IMY”) meddelade den 7 juni 2021 beslut i ett tillsynsärende mot Medhelp Sjukvårdsrådgivning AB (”Medhelp”) efter en granskning av hur Medhelp hanterar personuppgifter. Granskningen resulterade i en sanktionsavgift. Beslutet överklagades, men kammarrätten har nu slagit fast en sanktionsavgift om 11,3 miljoner kronor.

Bakgrunden till granskningen är att den svenska webbtidningen Computer Sweden år 2019 avslöjade att man hittat 2,7 miljoner inspelade samtal till rådgivningsnumret 1177. Inspelningarna låg exponerade på en öppen webbplats utan lösenordsskydd eller andra säkerhetsåtgärder. Personuppgiftsansvarig för uppgifterna var Medhelp som bedrivit sjukvårdsrådgivning på uppdrag av ett antal regioner.

Enligt IMY:s granskning har Medhelp dessutom underlåtit att informera de registrerade om behandlingen av deras personuppgifter vid telefonsamtal. Därtill har Medhelp anlitat det thailändska företaget Medicall som underleverantör för att hantera sjukvårdsrådgivningen på nätter och helger. Enligt IMY innebär detta att Medhelp mellan maj 2018 och augusti 2019 olagligt lämnat ut personuppgifter.

Beslutet överklagades till förvaltningsrätten och så småningom till kammarrätten. En av frågorna i målet var om Medicall kunde vara att anse som personuppgiftsansvarig vårdgivare enligt 6 kap patientsäkerhetslagen (PSL) och om Medhelp därför haft rätt att överföra uppgifter till Medicall. Kammarrätten anförde att hälso- och sjukvård är en nationell angelägenhet inom Sveriges gränser. Enligt 2 kap 3 § hälso- och sjukvårdslagen (HSL) kan en eller flera rådgivare bedriva verksamhet inom en huvudmans geografiska område. Medicall hade bedrivit sjukvårdsrådgivning på svenska gentemot patienter i Sverige, men det bedömdes inte vara tillräckligt för att ett bolag i tredje land ska omfattas av den svenska hälso- och sjukvårdslagstiftningen. Kammarrätten slog därmed fast att Medicall inte är att anse som en vårdgivare enligt 2 kap 3 § HSL.

Behandlingen att genom vidarekoppling av samtal och tillhandahållande på annat sätt ge Medicall åtkomst till personuppgifter som till stor del var av känslig karaktär bedömdes sakna rättsligt stöd. Att låta en tredje part i ett tredje land som inte omfattades av en lagreglerad tystnadsplikt enligt kraven i artikel 9.3 GDPR ta del av personuppgifterna bedömdes vara en så allvarlig överträdelse av GDPR att även den grundläggande principen om laglighet, korrekthet och öppenhet i artikel 5.1.a) GDPR ansågs överträdd.

Mot bakgrund av att de inspelade samtalen till rådgivningsnumret 1177 var exponerade på en öppen webbplats utan säkerhetsåtgärder ansågs Medhelp även ha brustit i sina skyldigheter att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig skyddsnivå för uppgifterna. Medhelp ansågs inte heller ha fullgjort sin skyldighet att informera de registrerade.

Enligt kammarrätten har Medhelp brustit i sitt personuppgiftsansvar och ska därför tilldelas en sanktionsavgift om 11,3 miljoner kronor. Detta innebär en ökning jämfört med den sanktionsavgift om 8,8 miljoner kronor som dömdes ut av förvaltningsrätten 2022.

Fallet visar på vikten av att iaktta försiktighet vid utkontraktering av tjänster där behandling av känsliga personuppgifter förekommer och underleverantören befinner sig utanför Sverige. Genom att konstatera att Medicall inte omfattades av lagreglerad tystnadsplikt, har Kammarrätten också givit sin syn på hur artikel 9.3 GDPR bör tolkas.

Rebecka Undén, associate Advokatfirman Delphi.

Gorrissen Federspiel

Tue Goldschmieding

Nyt om persondataret i Danmark og EU

Domstolen i sag om behandling af helbredsoplysninger

Domstolen traf den 21. december 2023 afgørelse i sag C-667/21. Sagen var en præjudiciel forelæggelse indgivet af den tyske forbundsdomstol i arbejdsretlige sager, Bundesarbeitsgericht.

Den tyske forbundsdomstol i arbejdsretlige sager skulle træffe afgørelse i en national sag mellem to parter angående et erstatningsspørgsmål hvor en arbejdsgiver angiveligt havde behandlet oplysninger vedrørende en arbejdstagers helbred ulovligt. I forbindelse med behandlingen af sagen opstod tvivl om fortolkningen af de EU-retlige databeskyttelsesregler.

Tvisten drejede sig om, hvorvidt Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 9, stk. 2, litra h) om undtagelsen til behandling af helbredsoplysninger fandt anvendelse i sagen. I bekræftende fald ønskede den tyske forbundsdomstol at vide, hvilke regler om beskyttelse af helbredsoplysninger der skal overholdes i denne forbindelse, samt i tilfælde der er sket en overtrædelse af GDPR og hvilken erstatning der eventuelt skal betales i henhold til GDPR artikel 82.

Domstolen kom frem til, at GDPR artikel 9, stk. 2, litra h) ikke udelukker, at undtagelsen finder anvendelse på situationer, hvor et medicinsk kontrolorgan behandler helbredsoplysninger om en af sine ansatte i egenskab af medicinsk tjeneste med henblik på at vurdere denne ansattes erhvervsevne. Desuden kom Domstolesen frem til, at pligten til at sikre, at ingen kollega til den registrerede kan få adgang til oplysninger om dennes helbredstilstand ikke følger af GDPR artikel 9, stk. 3, men kan følge af en lovgivning vedtaget af en medlemsstat samt i henhold til princippet om integritet og princippet om fortrolighed som fastsat i forordningens artikel 5, stk. 1, litra f).

Domstolen bemærkede herefter, at en behandling af helbredsoplysninger på grundlag af GDPR artikel 9, stk. 2, litra h) for at være lovlig skal overholde mindst én af de betingelser for lovlig behandling, der er fastsat i GDPR artikel 6, stk. 1. Det er endvidere en betingelse for at den dataansvarlige kan ifalde ansvar i henhold til GDPR artikel 82, at denne har pådraget sig skyld, og at der er en formodning for dette, medmindre den dataansvarlige beviser andet, og at bestemmelse ikke kræver, at der tages hensyn til graden af skylden ved fastsættelsen af størrelsen af erstatningen.

Læs hele dommen her: https://curia.europa.eu/juris/document/document.jsf?text=&docid=280768&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=802131

Domstolen om GDPR's principper om »lovlighed«, behandlingens nødvendighed, ret til sletning

Domstolen traf den 7. december 2023 afgørelse i sag C-26/22 og C-64/22. Sagen var en præjudiciel forelæggelse indgivet af den tyske forvaltningsdomstol, Verwaltungsgericht.

Den tyske forvaltningsdomstol skulle træffe afgørelse i en national sag mellem to parter angående sletning af opbevarede oplysninger om gældssaneringer. I forbindelse med behandlingen af sagen opstod tvivl om fortolkningen af de EU-retlige databeskyttelsesregler.

Tvisten drejede sig om, hvorvidt GDPR artikel 77, stk. 1 om ret til at indgive klage til en tilsynsmyndighed sammenholdt med artikel 78, stk. 1 om adgang til effektive retsmidler over for en tilsynsmyndighed har karakter af en afgørelse af et andragende eller en realitetsafgørelse truffet af en myndighed. Tvisten omhandlede desuden hvorvidt en opbevaring af oplysninger fra et offentligt register hos et privat kreditoplysningsbureau er foreneligt med charterets artikel 7 og 8 samt om adfærdskodekser der indeholder frister for kontrol og sletning, som går ud over opbevaringsfristerne for offentlige registre, som er godkendt af tilsynsmyndighederne i henhold til GDPR artikel 40 suspendere den afvejning, der skal finde sted i hen-

hold til GDPR artikel 6, stk. 1, første afsnit, litra f).

EU-domstolen kom frem til, at GDPR artikel 78, stk. 1, skal fortolkes således, at en klageafgørelse, der er vedtaget af en tilsynsmyndighed, er underlagt en fuldstændig domstolsprøvelse. Herudover udtalte EU-domstolen, at GDPR artikel 5, stk. 1, litra a) sammenholdt med GDPR artikel 6, stk. 1, første afsnit, litra f) er til hinder for en praksis i private kreditoplysningsbureauer, der består i, at de i deres egne databaser opbevarer oplysninger fra et offentligt register om gældssanering om oplysninger vedrørende fysiske personers kreditværdighed i en periode, der er længere end den periode, hvori oplysningerne opbevares i det offentlige register.

Læs hele dommen her: https://curia.europa.eu/juris/document/document.jsf?text=&docid=280428&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=795883

Domstolen har udtalt sig om begreberne »behandling« og »dataansvarlig« i forbindelse med udvikling af en IT-mobilapplikation

Domstolen afsagde den 5. december 2023 dom i C-863/21. Sagen angik en præjudiciel anmodning indgivet af den regionale forvaltningsdomstol i Litauen under en sag mellem det nationale folkesundhedscenter i Litauen (»CNSP«) over for den nationale tilsynsmyndighed for behandling af personoplysninger (»tilsynsmyndigheden«).

Tvisten udsprang af en bøde, som tilsynsmyndigheden havde pålagt CNSP som følge af en overtrædelse af flere bestemmelser i GDPR i tilknytning til anvendelsen af en mobilapplikation. CNSP fik i sin tid udviklet mobilapplikationen af en ekstern IT-virksomhed (»ITSS«) men der blev aldrig indgået en formel kontrakt mellem parterne og erhvervelsesprocessen blev efterfølgende afsluttet uden aftale.

Spørgsmålene for Domstolen angik herefter fortolkning af begreberne »dataansvarlig«, »fælles dataansvarlige« og »behandling« samt muligheden for planlæggelse af administrative bøder.

Domstolen udtalte for det første, at en enhed der har givet en virksomhed til opgave at udvikle en applikation og deltaget ved fastlæggelsen af formålene den heriomfattede behandling af personoplysninger, skal anses for dataansvarlig. Dette gælder uanset, at enheden ikke selv har foretaget behandling eller erhvervet applikationen.

For det andet udtalte domstolen, at to enheder kan anses for fælles dataansvarlige, uanset om der foreligger en ordning mellem dem om fastlæggelsen af formålene eller hjælpemidlerne til databehandling eller vilkår om det fælles dataansvar. Kvalificering som fælles dataansvarlig følger alene af, at flere enheder har deltaget i fastsættelsen af formålene og hjælpemidlerne til databehandling.

Domstolen udtalte for det tredje, at brug af personoplysninger til IT-testning af en applikation udgør »behandling« efter GDPR artikel 4, stk. 1, nr. 2, medmindre der er tale om anonymiserede oplysninger.

Vedrørende spørgsmålet om muligheden for pålæg af administrative bøder, udtalte Domstolen, at det kræver forsæt eller uagtsomhed for at bringe GDPR's administrative sanktioner i anvendelse. Der gælder ingen regel om objektivt ansvar, og der er ikke ved EU-retten overladt de enkelte medlemsstater en skønsmargin i forhold til de materielle betingelser, der kræves for at bringe en bestemmelse om administrativ bøde i anvendelse.

Læs Domstolens afgørelse her: https://curia.europa.eu/juris/document/document.jsf?text=&docid=280324&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=782382

Domstolen træffer afgørelse om registreredes ret til indsigt i patientjournaler

Domstolen afsagde den 26. oktober 2023 afgørelse i sag C-307/22. Sagen vedrørte en tvist mellem FT, der var tandlæge, og DW, der var patient, idet FT havde givet afslag til DW på at give en første kopi af dennes patientjournal gratis. Det gav under behandling af sagen ved Forbundsdomstolen i Tyskland udslag i fortolkningstvivl af GDPR.

Forbundsdomstolen i Tyskland forelagde tre præjudicielle spørgsmål for Domstolen, der vedrørte fortolkningen af artikel 12, stk. 5, artikel 15, stk. 1 og 3, henholdsvis artikel 23, stk. 1, litra i) i GDPR.

Domstolen konkluderede, at artikel 12, stk. 5, om anmodninger fra registrerede og artikel 15, stk. 1 og 3, om retten til indsigt i GDPR skulle fortolkes således, at forpligtelsen for den dataansvarlige til vederlagsfrit at give den registrerede en første kopi af de behandlede personoplysninger om vedkommende gælder, selvom anmodningen ikke er begrundet i et af de i præambelbetragtning nr. 63 nævnte formål.

Derudover fandt Domstolen, at artikel 23, stk. 1, litra i), om begrænsninger i GDPR skulle fortolkes således, at en national lov, der af hensyn til at beskytte den dataansvarliges økonomiske interesser, ikke må pålægge den registrerede at betale udgifterne til en første kopi af de personoplysninger om vedkommende, der er genstand for behandling.

Slutteligt konkluderede Domstolen, at artikel 15, stk. 3, om retten til indsigt i GDPR skal fortolkes således, at det i et læge/patient-forhold gælder, at retten til at modtage en kopi af personoplysninger indebærer, at den registrerede skal have udleveret en nøjagtig og forståelig gengivelse af alle disse oplysninger, og at dette indebærer retten til at få udleveret en komplet kopi.

Læs hele dommen her: https://curia.europa.eu/juris/document/document.

jsf?text=&docid=279125&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=782382

Ny EU-dom om fortolkning af begrebet »behandling« af personoplysninger

Den 5. oktober 2023 afsagde Domstolen afgørelse i sag C-659/22 angående en anmodning om præjudiciel afgørelse indgivet af Tjekkiets øverste forvaltningsretlige domstol.

Anmodningen angik fortolkningen af begrebet »behandling« af personoplysninger, som omhandlet i GDPR artikel 4, nr. 2. Sagen blev indgivet i forbindelse med et nationalt søgsmål mellem RK på den ene side og det tjekkiske Sundhedsministerie på den anden side.

I det nationale søgsmål havde RK anlagt sag mod sundhedsministeriet på baggrund af en foranstaltning, som ministeriet havde opstillet i forbindelse covid-19-pandemien. Foranstaltningen krævede validering af gyldigheden af covid-19-vaccinations-, test- og restitutionscertifikater for adgang til specifikke indendørs- og udendørsområder samt deltagelse i massebegivenheder eller andre aktiviteter. Dette pålagde kunderne (tilskuerne, deltagerne) at fremlægge dokumentation for, at de opfyldte disse betingelser, og pålagde operatørerne (arrangørerne) at kontrollere betingelserne ved hjælp af ministeriets mobilapplikation.

Det præjudicielle spørgsmål vedrørte, hvorvidt kontrollen af disse oplysninger gennem den nationale mobilapplikation udgjorde en »behandling« af personoplysninger som omhandlet i GDPR artikel 4, nr. 2.

Domstolen konkluderede, at begrebet »behandling« skal fortolkes bredt, og at kontrollen af de pågældende betingelser ved hjælp af mobilapplikationen udgjorde en »behandling« i henhold til GDPR artikel 4, nr. 2. Dette blev begrundet ud fra en ordlydsfortolkning, hvor domstolen særligt lagde vægt på udtrykket »enhver aktivitet«, idet EU-lovgiver ved denne formulering har haft til hensigt at give begrebet en vid rækkevidde. Denne fortolkning er i øvrigt i overensstemmelse med GDPR's formål om at sikre effektivitet af den grundlæggende ret til beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

Læs hele dommen her: https://curia.europa.eu/juris/document/document.jsf?text=&docid=278248&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=782382

Cookie-løfte-initiativ skal hjælpe med at beskytte brugernes grundlæggende rettigheder og friheder

Det Europæiske Databeskyttelsesråd (»EDPB«) vedtog på sit seneste plenarmøde den 13. december 2023 et brev som svar til Europa-Kommissionen (»Kommissionen«) vedrørende det frivillige cookie-løfte-initiativ.

Cookie-initiativet havde til formål at beskytte brugernes grundlæggende rettigheder og friheder samt give dem mulighed for at træffe effektive valg og øge gennemsigtighed. Initiativet blev udviklet af Kommissionen og bestod af et frivilligt virksomhedsløfte om at forenkle håndteringen af cookies og brugernes valg af personaliserede reklamer. Kommissionen havde den 10. oktober 2023 bedt EDPB om at overveje, om nogle af principperne i udkastet ville være i konflikt med GDPR samt Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 (»ePrivacy«).

EDPB gjorde i sit svar opmærksom på, at organisationers overholdelse af principperne i cookie-løftet ikke ville være ensbetydende med overholdelse af GDPR eller ePrivacy. Udkastet ville sikre, at brugerne havde større kontrol over behandling af deres data, herunder at der ikke spørges om samtykke igen i et år efter, at dette har været nægtet fra brugerens side. Databeskyttelsesmyndighederne vil fortsat være kompetente til at udøve deres beføjelser, når dette vil være nødvendigt.

Læs pressemeddelelsen her: https://edpb.europa.eu/news/news/2023/edpb-cookie-pledge-initiative-should-help-protect-fundamental-rights-and-freedoms_en

Læs vedtagelsen her: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-reply-commissions-initiative-voluntary-business-pledge_en

EDPB tager stilling til Metas brug af personoplysninger til adfærdsbaseret markedsføring

Det Europæiske Databeskyttelsesråd (»EDPB«) vedtog den 27. oktober 2023 en såkaldt »hurtig bindende afgørelse« vedrørende Meta Ireland Limiteds (»Meta«) brug af brugeres personoplysninger til adfærdsbaseret markedsføring. Det skete efter anmodning fra det norske Datatilsyn.

Det norske Datatilsyn udstedte den 14. juli 2023 i medfør af artikel 66, stk. 1, i GDPR om hasteprocedure et forbud mod Meta og Facebook Norway AS mod behandling af personoplysninger om norske datasubjekter med henblik på adfærdsbaseret annoncering med hjemmel i kontrakter eller legitime interesser. Eftersom forbuddet var tidsmæssigt og geografisk begrænset, anmodede det norske Datatilsyn EDPB om en »hurtig bindende afgørelse« med henblik på en vedtagelse af endelige foranstaltninger med virkning i alle EØS-lande.

EDPB fandt, at Meta løbende overtrådte artikel 6, stk. 1, i GDPR om behandling af personoplysninger. Eftersom det irske Datatilsyn efter anmodning fra det norske Datatilsyn ikke efterkom de almindelige samarbejds- og sammenhængsmekanismer i GDPR, pålagde EDPB derfor det irske Datatilsyn at indføre et forbud mod at anvende kontrakter og legitime interesser

som retsgrundlag for behandling af personoplysninger til brug for adfærdsbaseret markedsføring.

Det irske Datatilsyn traf den 10. november 2023 endelig afgørelse vedrørende Metas brug af brugeres personoplysninger til adfærdsbaseret markedsføring.

Det Europæiske Databeskyttelsesråd vedtager retningslinjer, der skal skabe klarhed over sporingsteknikker omfattet af ePrivacy-direktivet

Det Europæiske Databeskyttelsesråd (»EDPB«) vedtog den 15. november 2023 retningslinjer for det tekniske anvendelsesområde for direktiv 2009/136/EC af 25. november 2009 (»ePrivacy-direktivet«) artikel 5, stk. 3. Retningslinjerne har til formål at præcisere, hvilke tekniske indgreb, navnlig nye sporingsteknikker, der er omfattet af direktivet, og at skabe større retssikkerhed for registeransvarlige og enkeltpersoner.

For at præcisere artiklens anvendelsesområde, analyseres der i retningslinjerne centrale begreber, som fremgår af direktivets artikel 5, stk. 3, såsom »information«, »abonnents eller brugers terminaludstyr«, »elektronisk kommunikationsnet«, »adgang« og »lagret information/lagring«. Retningslinjerne omfatter også praktiske eksempler på fælles sporingsteknikker.

Retningslinjerne vedrører kun anvendelsesområdet for ePrivacy-direktivets artikel 5, stk. 3. De omhandler ikke, hvordan samtykke skal indsamles, eller de undtagelser, der er fastsat i artiklen.

Retningslinjerne vil blive sendt i offentlig høring frem til den 18. januar 2024.

Læs pressemeddelelsen her: https://edpb.europa.eu/news/news/2023/edpb-provides-clarity-tracking-techniques-covered-eprivacy-directive_en

Læs vejledningen her: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en

EDPB vælger emne for sit årlige koordinerede fokuspunkt for 2024

Det Europæiske Databeskyttelsesråd (»EDPB«) offentliggjorde den 17. oktober 2023 en pressemeddelelse om valget af emne for dets tredje koordinerede fokuspunkt-. Fokuspunktet omhandlede implementeringen af dataansvarliges ret til adgang til data og vil endeligt blive lanceret i løbet af 2024.

Ved at vælge et koordineret fokuspunkt, kan EDPB prioritere et særligt emne, som de enkelte medlemslandes databeskyttelsesmyndigheder skal behandle på nationalt niveau. Hensigten er, at de enkelte resultater fra hvert medlemsland kan samles og analyseres således, at der opnås en større indsigt omkring emnet.

Valget af koordineret fokuspunkt for 2024 skal ses i sammenhæng med EDPB's oprettelse af en koordineret håndhævelsesramme (»CEF«) og oprettelse af en støttepulje af eksperter (»SPE«). Ovenstående har samlet til formål at strømline håndhævelse og samarbejde mellem de enkelte medlemslandes databeskyttelsesmyndigheder.

Læs pressemeddelelsen her: https://edpb.europa.eu/news/news/2023/edpb-picks-topic-2024-coordinated-action_en

Den Europæiske Tilsynsførende for Databeskyttelse offentliggør anbefalinger for ny retsakt om kunstig intelligens

Den Europæiske Tilsynsførende for Databeskyttelse (»EDPS«) offentliggjorde den 23. oktober 2023 sin holdning til AI-forordningen. Forordningen sigter mod at regulere udviklingen og brugen af kunstig intelligens (AI) i EU, herunder i EU-institutioner og -organer. EDPS fokuserede på deres fremtidige opgaver som tilsynsmyndighed for AI-systemer i EU›s institutioner.

EDPS understregede vigtigheden af tydeligt definerede opgaver og pligter for EDPS som den kommende AI-tilsynsførende for EU's institutioner. EDPS krævede forbud mod AI-systemer, der udgør uacceptable risici for enkeltpersoner. Desuden støttede EDPS behovet for passende ressourcer og finansiering til at udføre deres rolle som AI-tilsynsførende. Derudover insisterede EDPS på retten til at modtage klager over overtrædelser af forordningen.

EDPS fastslog, at berørte personer bør have ret til at indgive klage over overtrædelser af AI-forordningen. De anbefalede, at databeskyttelsesmyndigheder udpeges som nationale tilsynsmyndigheder under forordningen for at sikre pålidelighed. EDPS bifaldt etableringen af det Europæiske Kunstige Intelligenskontor og ønskede at deltage aktivt i dets arbejde, og appellerer til medlovgiverne om at give EDPS stemmeret som fuldgyldigt medlem af kontorets bestyrelse.

Læs pressemeddelelsen her: https://edps.europa.eu/data-protection/our-work/publications/papers/2023-11-08-study-essence-fundamental-rights-privacy-and-protection-personal-data_en

Læs anbefalingerne her: Title (europa.eu)

Den Europæiske Tilsynsførende for Databeskyttelse offentliggør udtalelse vedrørende erstatningsansvar for AI-systemer

Den Europæiske Tilsynsførende for Databeskyttelse (»EDPS«) offentliggjorde den 11. oktober 2023 på eget initiativ en udtalelse vedrørende EU-Kommissionens (»Kommissionen«) to forslag til direktiver om erstatningsansvar for kunstig intelligens, som blev fremsat af Kommissionen den 28. september 2022.

Det ene forslag til direktiv, COM/2022/495, vedrører produktansvar for defekte produkter (»direktivet om produktansvar«). Det andet forslag til direktiv, COM/2022/496, vedrører civilretligt ansvar uden for kontrakt for kunstig intelligens (»direktivet om

AI-ansvar«). Formålet med forslagene til den nye regulering var at sikre erstatningsansvarsreglers anvendelighed på skade, som er forårsaget af brugen af et AI-system.

EDPS anbefalede i udtalelsen at sikre, at beskyttelsen mod AI-systemer, kommer til at omfatte både skade forvoldt af AI-systemer, som er produceret eller anvendt af EU-organer, såvel som private- og national organer.

EDPB anbefalede yderligere, at direktivet om AI-ansvars artikel 3, som omhandler sikring af fremlæggelse af beviser og afkræftelig formodning om manglende overholdelse, og artikel 4, som omhandler en afkræftelig formodning om årsagsforbindelse i tilfælde af fejl, sikres anvendt på alle AI-systemer. EDPB præciserede, at dette bør gøre sig gældende, uanset risiko-klassificeringen af AI-systemet.

EDPB anbefalede desuden, at det for både udbydere og brugere udtrykkeligt præciseres, at disse vil være forpligtede til at videregive oplysninger til sikring af beviser efter artikel 3. I forlængelse heraf opfordrede EDPS Kommissionen til at overveje, om der kunne indføres yderligere foranstaltninger, som letter bevisbyrden og derved tilsikrer et ansvar for AI-systemer.

EDPB anbefalede endeligt, at det ligeledes udtrykkeligt præciseres i direktiverne, af hensyn til sikring af klagemuligheder, at reguleringen ikke vil have betydning for databeskyttelseslovgivningen.

Læs hele pressemeddelelsen her: https://edps.europa.eu/data-protection/our-work/publications/opinions/2023-10-11-edps-opinion-422023-two-directives-ai-liability-rules_en

*Læs hele udtalelsen her: https://edps.europa.eu/system/files/*2023-10/23-10-11_opi*nion_ai_liability_rules.pdf*

Global Privacy Assembly har vedtaget nye resolutioner vedrørende brug af kunstig intelligens

Global Privacy Assembly (»GPA«) vedtog på deres årlige møde i oktober 2023 en række resolutioner om databeskyttelsesemner.

GPA's formål er at fremme samarbejdet mellem nationale databeskyttelsesmyndigheder gennem vedtagelse af rapporter og resolutioner om databeskyttelsesemner. Disse rapporter og resolutioner forberedes i arbejdsgrupper bestående af repræsentanter fra nationale databeskyttelsesmyndigheder.

GPA vedtog resolutioner om AI i forbindelse med ansættelse, sundhedsdata og forskning, opnåelse af globale databeskyttelsesstandarder, oprettelse af et bibliotek med vejledning og fortolkning af databeskyttelsesprincipper, generiske systemer for kunstig intelligens, nedssættelse af en arbejdsgruppe om intersektionel kønsperspektiv inden for databeskyttelse og en GPA-pris for privatliv og menneskerettigheder.

Der blev ligeledes vedtaget en resolution om GPA's strategiske plan for 2023-2025.

Læs de enkelte resolutioner her: https://globalprivacyassembly.org/document-archive/adopted-resolutions/

Læs Datatilsynets pressemeddelelse om resolutionerne her: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2023/nov/nye-resolutioner-fra-global-privacy-assembly

Det Kongelige Teater indstilles til bøde for manglende procedure for sletning af kundeoplysninger

Det danske Datatilsyn (»Datatilsynet«) har politianmeldt Det Kongelige Teater og Kapel for ikke at have fastsat frister eller procedurer for sletning af kundeoplysninger til brug for markedsføring. Dette oplyser Datatilsynet i en pressemeddelelse den 9. januar 2024. Det Kongelige Teater havde opbevaret oplysninger på ca. 520.000 kunder og modtagere af nyhedsbreve.

Forud for politianmeldelsen havde Datatilsynet foretaget en undersøgelse af Det Kongelige Teater af egen drift, og dermed gjort Det Kongelige Teater opmærksom på, at der ikke var etableret sådanne regler for sletning og opbevaring af personoplysninger.

Datatilsynet indstiller til en bøde på 250.000 kr., henset til at der er tale om en overtrædelse af grundlæggende principper for behandling af personoplysninger, og henset til at overtrædelsen angår et meget stort antal registrerede personer, hvis oplysninger er blevet anvendt aktivt i markedsføringsøjemed.

Læs Datatilsynets pressemeddelelse her
Det Kongelige Teater indstilles til bøde (datatilsynet.dk)

Datatilsynet behandler 10 typiske brud på persondatasikkerheden

Det danske Datatilsyn (»Datatilsynet«) udtalte sig i en pressemeddelelse den 8. januar 2024 om 10 typisk forekommende brud på persondatasikkerheden i virksomheder.

Datatilsynet supplerede pressemeddelelsen med en informationsside, der beskrev de 10 brud og præsenterede en række gode råd, der kan bruges til at hjælpe med at undgå bruddene.

Informationen er hovedsageligt målrettet medarbejdere, der har mulighed for at udfærdige og/eller ændre på organisationens regler, procedurer mv., for derved at beskytte organisationen mod brud. Datatilsynet understregede dog også, at enhver der arbejder digitalt med personoplysninger, kan have gavn af en indføring i de forskellige scenarier, da de udgør en »*meget betragtelig andel af de brud*«, som jævnligt anmeldes til Datatilsynet.

De 10 typiske brud omfatter: Data til forkerte modtagere i udgående post, fejlagtig eksponering af beskyttet adresse, fejludlevering af

data ved sagsbehandling, manglende sletning af data i forbindelse med brug af digitale værktøjer, auto-complete i e-mail fører til forkerte modtagere, tab/tyveri af transportable enheder med ukrypteret data, for bred adgang til data på netværksdrev mv., uautoriseret adgang til data grundet dårligt design mv., videregivelse af data i skabelon- og blanketløsninger, tab og misbrug af data som følge af ondsindet software.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jan/de-10-brud

Læs Datatilsynets informationsside om de 10 brud her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed/de-10-brud

Nye vejledninger præciserer regler om tv-overvågning foretaget af myndigheder og boligorganisationer

Den 13. december 2023 offentliggjorde Det danske Datatilsyn (»Datatilsynet«) to nye vejledninger om tv-overvågning. Vejledningerne er rettet mod boligorganisationer og offentlige myndigheder, der ønsker at anvende eller allerede anvender tv-overvågning til bekæmpelse og forebyggelse af kriminalitet.

Formålet med vejledningerne er at præcisere de mest relevante regler, som offentlige myndigheder og boligorganisationer skal være opmærksomme på i forbindelse med tv-overvågning. Dette omfatter reglerne i lovbekendtgørelse nr. 182 af 24. februar 2023 (»den danske tv-overvågningslov«), Lov nr. 502 af 23. maj 2018 (»den danske databeskyttelseslov«) samt GDPR.

For så vidt angår boligorganisationer, bliver organisationer dataansvarlig for den behandling af personoplysninger, som finder sted i forbindelse med tv-overvågningen. Boligorganisationerne skal derfor sikre sig, at der er hjemmel til at iværksætte tv-overvågning, at den iværksatte tv-overvågning er indrettet lovligt, og at optagelser fra tv-overvågningen behandles lovligt.

For så vidt angår offentlige myndigheder, skal myndighederne sikre sig, at der er hjemmel til at iværksatte tv-overvågningen, at den iværksatte tv-overvågning er indrettet lovligt, og at optagelser hidrørende fra tv-overvågningen behandles lovligt. I visse tilfælde vil offentlige myndigheders beføjelse til at iværksætte tv-overvågning følge direkte af lovgivningen. I visse andre tilfælde kan en offentlig myndighed iværksætte tv-overvågning, selvom dette ikke specifikt fremgår af lovgivningen, navnlig hvis tv-overvågningen må anses for at være naturligt som led i myndighedens øvrige opgavevaretagelse.

Begge vejledninger er udarbejdet med bidrag fra det danske Justitsministerium.

Læs Datatilsynets pressemeddelelse om vejledningerne her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/dec/nye-vejledninger-om-tv-overvaagning

Læs vejledningen om TV-overvågning for offentlige myndigheder her: https://www.datatilsynet.dk/Media/638380803567559289/Vejledning om tv-overv%C3%A5gning til offentlige myndigheder.pdf

Læs vejledning om TV-overvågning for boligorganisationer her: https://www.datatilsynet.dk/Media/638380803505815050/Vejledning om TV-overv%C3%A5gning til boligorganisationer.pdf

Datatilsynet offentliggør ny vejledning om adgangsrettigheder

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 7. december 2023 en ny vejledning om adgangsrettigheder. Vejledningen giver organisationer vejledning i, hvordan de kan sikre deres rettighedsstyring i forbindelse med adgang til organisationernes it-systemer og således styrke deres informations- og behandlingssikkerhed.

Vejledningen belyser indledende, hvordan organisationerne med fordel kan skabe overblik over deres it-miljø, som skaber grundlag for håndtering af de problemstillinger, som er knyttet til rettigheds- og adgangsstyring.

Vejledningen fremhæver herefter, hvornår en utilstrækkelig eller manglende rettighedsstyring kan føre til risikofyldte situationer. Datatilsynet giver en oversigt over, hvilke konkrete foranstaltninger, som organisationerne med fordel kan tage i konkrete situationer, som udføres i organisationen, for eksempel ved personalemæssige ændringer.

Læs hele vejledningen her: https://www.datatilsynet.dk/Media/638374509275042076/Styr%20p%C3%A5%20rettighedsstyring.pdf

Læs kataloget med relevante foranstaltninger her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed/katalog-over-foranstaltninger/

Læs hele pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/dec/ny-vejledning-om-rettighedsstyring

Datatilsynet udtaler sig om anvendelse af undtagelse til oplysningspligten

Det danske Datatilsyn (»Datatilsynet«) udstedte den 4. december 2023 efter anmodning fra den danske Uddannelses- og Forskningsstyrelsen (»UFS«) en pressemeddelelse vedrørende anvendelsen af artikel 14, stk. 5, litra c, i GDPR om oplysningspligt.

Spørgsmålet omhandlende, hvorvidt UFS med henvisning til GDPR artikel 14, stk. 5, litra c, kunne undlade at oplyse forældre om, at oplysninger om deres indkomst var genstand for behandling med henblik på udregning af uddannelsesstøtte efter lov nr. 395 af 13. april 2023 om statens uddannelsesstøtte (»SU-loven«).

Datatilsynet fandt, at SU-lovens § 25, stk. 5 og 6, om forældreindkomst og § 39, stk. 1, om indhent-

ning af oplysninger »ikke i fornødent omfang kan anses for udtrykkeligt at fastsætte indsamling/videregivelse i overensstemmelse med databeskyttelsesforordningens artikel 14, stk. 5, litra c.« Ifølge Datatilsynet var det ikke tilstrækkeligt, at loven hjemler mulighed for at indsamle eller videregive oplysninger, da dette ikke for den registrerede giver klarhed om, at den pågældende er genstand for indsamling af oplysninger.

Bestemmelserne i SU-loven giver således ikke ifølge Datatilsynet en tilstrækkelig klarhed for den registrerede om, at der sker indsamling af oplysninger om den pågældende, og hvilke oplysninger, der er tale om.

Læs afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/dec/udtalelse-om-anvendelse-af-undtagelse-til-oplysningspligten

Nyt katalog fra Datatilsynet med vejledende sikkerhedsforanstaltninger til virksomheder og myndigheder

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 28. november 2023 et nyt katalog over sikkerhedsforanstaltninger, som virksomheder og myndigheder kan bruge i deres håndtering af GDPR-lovgivningen.

Kataloget indeholder en lang række tekniske og organisatoriske foranstaltninger, som skal bidrage til, at virksomheder og myndigheder lettere kan identificere og håndtere risici forbundet med behandlingen af personoplysninger. Til hver foranstaltning følger en præcisering af, hvilke risici der kan nødvendiggøre implementeringen af foranstaltningen, samt en vejledning om den praktiske gennemførelse.

Det er hensigten, at kataloget skal fungere som et værktøj for virksomheder og myndigheder, der skal sikre sig, at de har passende sikkerhedsniveau. Målet er, at kataloget gradvist vil blive udvidet til at omfatte en bredere række af foranstaltninger, og at og fremtidige vejledninger kan henvise til forskellige tiltag i kataloget.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/nov/nyt-katalog-over-sikkerhedsforanstaltninger

Det danske Datatilsyns afgørelse om Aarhus Universitetshospitals sletning af patientoplysninger fra Instagram

Det danske Datatilsyn (»Datatilsynet«) traf den 27. november 2023 afgørelse i en sag med journalnummer 2023-432-0016, vedrørende Aarhus Universitetshospitals (»AUH«) offentliggørelse af patientoplysninger på Instagram. I sagen havde AUH offentliggjort billeder af patienter på deres Instagram.

Datatilsynet vurderede, at AUH behandler personoplysninger om patienter på Instagram uden overholdelse af GDPR artikel 9, stk. 2, og artikel 6, stk. 1, litra a. Det skyldtes manglende opfyldelse af samtykkebetingelserne, da patienterne i en sårbar situation ikke kunne anses for at have et reelt frit valg.

Datatilsynet påpegede, at AUH måtte påvise, at samtykke var givet og at det skulle opfylde alle relevante kriterier. Kravet om frivillighed var særligt afgørende, da patienter i en sårbar situation ikke nødvendigvis kunne give frivilligt samtykke.

Datatilsynet fastslog, at behandling af personoplysninger skulle ske på en lovlig, rimelig og gennemsigtig måde, hvilket offentliggørelsen af helbredsoplysninger om patienter på Instagram ikke gjorde.

Datatilsynet rettede alvorlig kritik mod Region Midtjylland og pålagde dem at slette alle opslag indeholdende helbredsoplysninger om patienter fra Instagramkontoen »auhdk«. Fristen for efterlevelse af påbuddet var 4 uger fra udstedelsen.

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/nov/hospital-kan-ikke-bruge-samtykke-til-at-offentliggoere-billeder-af-patienter-paa-instagram

Det danske Datatilsyns udtalelse om behandlingsgrundlag til udvikling og drift af AI-løsning inden for sundheds- og omsorgsområdet

Det danske Datatilsyn (»Datatilsynet«) har, efter anmodning fra Københavns Kommune, den 17. november 2023, udtalt, hvorvidt kommunen har hjemmel til udvikling, drift og gentræning af en AI-løsning, der kan identificere borgere med behov for vedligeholdende træning og rehabiliterende indsats.

Datatilsynet udtalte, at hjemlen findes i GDPR artikel 6, stk. 1, litra e, samt artikel 9, stk. 2, litra g. Datatilsynet fandt dog også, at et supplerende nationalt retsgrundlag der forpligter eller berettiger myndigheden til at udføre bestemte myndighedsopgaver, også var nødvendigt.

Ved behandling af personoplysninger til udvikling og gentræning, fastslog Datatilsynet, at der kan henvises til de allerede eksisterende bestemmelser i lovbekendtgørelse nr. 1089 af 16. august 2023 (»den danske servicelov«) der forpligter kommunen til at træffe afgørelse om og levere vedligeholdende træning og rehabiliterende indsats. Datatilsynet lagde i sin vurdering vægt på, at AI-løsningen, ikke indebærer, direkte konsekvenser for borgeren.

I forhold til behandling af personoplysninger ved driften af AI-løsningen, udtalte Datatilsynet, at bestemmelserne i den danske servicelovs § 86 og § 112 var relevante. Datatilsynet udtalte dog, at bestemmelserne ikke udgjorde et tilstrækkeligt supplerende nationalt retsgrundlag, i lyset af hvor indgribende en behandlingsaktivitet, der var tale om.

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/nov/udtalelse-om-behandlingsgrundlag-til-udvikling-og-drift-af-ai-loesning-inden-for-sundheds-og-omsorgsomraadet

Rigsrevisionen tilvejebringer personoplysninger inden for rammerne af databeskyttelsesreglerne

Det danske Datatilsyn (»Datatilsynet«) traf den 14. november 2023 afgørelse i en sag med journalnummer 2023-432-0022, der angik Rigsrevisionens behandling af personoplysninger i forbindelse med Rigsrevisionens revisionsvirksomhed.

Datatilsynet indledte den 19. august 2023 en sag om Rigsrevisionens behandlingsgrundlag til at indhente personoplysninger, når Rigsrevisionen udførte revisionsvirksomhed. Det skete som led i Datatilsynets målrettede tilsynsaktiviteter i 2023, som inkluderede Folketinget og Folketingets institutioner.

Efter anmodning fra Datatilsynet oplyste Rigsrevisionen, hvordan Rigsrevisionen i forbindelse med sin revisionsvirksomhed tilvejebragte materiale der indeholdt personoplysninger, samt hvilken hjemmel Rigsrevisionen havde hertil, og tilsendte en liste over gennemførte revisioner i 2022. Endvidere oplyste Rigsrevisionen, at personhenførbare oplysninger blev indhentet, når det af rigsrevisorerne skønnedes relevant og nødvendigt.

På baggrund heraf fandt Datatilsynet, at Rigsrevisionen havde hjemmel til at indhente personoplysninger, når Rigsrevisionen udførte sin revisionsvirksomhed, jf. artikel 6, stk. 1, litra e, i GDPR om behandling af personoplysninger suppleret af § 12, stk. 1, i lov nr. 321 af 26. juni 1975 (»Rigsrevisorloven«) om Rigsrevisionens tilvejebringelse af oplysninger. Datatilsynet fandt desuden, at Rigsrevisionen sikrede overholdelsen af princippet om dataminimering i artikel 5, stk. 1, litra c, i GDPR.

Datatilsynet fandt således, at Rigsrevisionens tilvejebringelse af personoplysninger, når Rigsrevisionen udførte revisionsvirksomhed, skete inden for rammerne af databeskyttelsesreglerne.

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/nov/rigsrevisionens-tilvejebringelse-af-oplysninger-sker-inden-for-rammerne-af-databeskyttelsesreglerne

Datatilsynets kritik af Digitaliseringsstyrelsen behandling af personoplysninger og risikovurdering

Det danske Datatilsyn (»Datatilsynet«) traf den 9. november 2023 afgørelse i en sag med journalnummer 2023-432-0025. Sagen omhandlede den danske Digitaliseringsstyrelses (»Digitaliseringsstyrelsen«) behandling af personoplysninger i forbindelse med MitID-login, hvor JavaScript blev anvendt.

En borger havde henvendt sig med bekymringer om sikkerheden ved JavaScript. Datatilsynet kritiserede, at Digitaliseringsstyrelsen ikke havde vurderet risikoen for borgernes rettigheder ved brug af JavaScript og ikke havde påvist passende tekniske sikkerhedsforanstaltninger. Datatilsyn udtalte på den baggrund kritik af Digitaliseringsstyrelsen for manglende overholdelse af GDPR's bestemmelser.

Datatilsynet konkluderede, at Digitaliseringsstyrelsen ikke havde overholdt reglerne i GDPR og forventede, at Digitaliseringsstyrelsen fremover foretager en specifik vurdering af risici ved JavaScript og implementerede passende sikkerhedsforanstaltninger.

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/nov/digitaliseringsstyrelsen-faar-kritik-for-utilstraekkelig-risikovurdering

Nyt tiltag fra Datatilsynet skal effektivisere tilsynets vejledning ved sikkerhedsbrud

Siden oktober 2023 effektiviserede Det danske Datatilsyn (»Datatilsynet«) sin vejledning ved brud på persondatasikkerheden ved at sende emnespecifik vejledning ud umiddelbart efter modtagelse af underretninger om sikkerhedsbrud. Formålet bag tiltaget var at give hurtig og praktisk bistand til organisationer, der står over for sådanne brud.

Hvert år modtager Datatilsynet tusindvis af underretninger om sikkerhedsbrud fra organisationer. For at styrke vejledningen i konkrete sager sendte Datatilsynet nu specifik vejledning til organisationerne kort efter modtagelsen af underretningerne, så organisationerne ikke selv skulle opsøge vejledningen. Der forelå blandt andet konkret vejledning ved brud, der vedrører ransomware, passwordsikkerhed, logning og phishing. Derudover dækkede vejledningen emner som fremsendelse af oplysninger til forkerte modtagere, ofte forårsaget af uhensigtsmæssig opsætning af funktionen auto-complete i e-mails.

Datatilsynet evaluerede løbende tiltaget og havde planlagt at udvide antallet af emner, der kunne vejledes om, for at give konkret vejledning i alle relevante sager på længere sigt. Organisationer, der havde spørgsmål om sikkerhedsbrud, blev også opfordret til at kontakte Datatilsynet telefonisk for yderligere vejledning.

Læs hele nyheden her:
Nyt tiltag skal give hurtigere vejledning ved brud (datatilsynet.dk)

Ny vejledning om offentlige myndigheders brug af AI

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 5. oktober 2023 en ny vejledning om offentlige myndigheders brug af AI. Vejledningen fokuserer på de overvejelser, offentlige myndigheder skal gøre sig, forud for udviklingen af AI-løsninger. Overvejelserne, Datatilsynet henviser til i vejledningen, angår oplysningspligt, behandlingsgrundlag og konsekvensanalyse mm.

Datatilsynet udgav samtidig en kortlægning over omfanget af offentlige myndigheders brug af AI. Kortlægningen giver et indblik i offentlige myndigheders brug af kunstigintelligensløsninger og deres da-

tabeskyttelsesretlige overvejelser i den forbindelse. Konklusionerne fra kortlægningen er blandt andet, at AI-løsningerne i den offentlige sektor typisk materialiserer sig i standardiserede løsninger, at de offentlige myndigheder i overvejende grad lever op til at sikre sig et relevant behandlings-grundlag i forbindelse med brugen af kunstig intelligens, men at det halter efter med at foretage konsekvensanalyser rettidigt.

Læs Datatilsynets pressemeddelelse her Ny vejledning om offentlige myndigheders brug af AI og kortlægning af AI på tværs af den offentlige sektor (datatilsynet.dk)

Læs vejledningen om offentlige myndigheders brug af AI her https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/okt/ny-vejledning-om-offentlige-myndigheders-brug-af-ai-og-kortlaegning-af-ai-paa-tvaers-af-den-offentlige-sektor

Læs kortlægningen over brugen af AI i den offentlige sektor her Brug af kunstig intelligens i den offentlige sektor: Kortlægning (datatilsynet.dk)

Finanstilsynet: Personovervågning bør være forsikringsselskabers sidste redskab

Det danske Finanstilsyn (»Finanstilsynet«) oplyste i en pressemeddelelse den 28. november 2023, at det havde gennemført en undersøgelse af forsikringsselskabers praksis og procedurer for personovervågning af skadelidte kunder.

Finanstilsynet konkluderede på baggrund af undersøgelsen, at forsikringsselskaberne generelt overholdte reglerne i bekendtgørelse nr. 1779 af 6. september 2021 (»den danske bekendtgørelse om god skik for forsikringsvirksomheder«) og bekendtgørelse nr. 1377 af 22. juni 2021 (»den danske bekendtgørelse om undersøgelser foretaget af forsikringsselskaber«). Finanstilsynet konkluderede dog også, at der stadig var plads til forbedring på visse punkter i forsikringsselskabernes procedurer.

Finanstilsynet indskærpede som følge heraf, at forsikringsselskaberne skal sikre, at personovervågning kun bliver anvendt, når det er absolut nødvendigt, og kun hvis der i øvrigt foreligger en velbegrundet og dokumenteret mistanke. Det følger af princippet om, at selskaberne altid skal vælge den mindst indgribende undersøgelsesmetode.

Selskaberne skal herudover sikre ordentlig kommunikation med kunden, hvilket medfører, at de skal underrette kunden om grundlaget for en eventuel personovervågning samt i øvrigt sikre saglig, ordentlig og transparent kommunikation i selskabets kontakt med kunden.

Læs Finanstilsynets pressemeddelelse her: Personovervågning bør være forsikringsselskabers sidste redskab (finanstilsynet.dk)

Danske lovændringer udvider børns beskyttelse på internettet

Det danske Folketing vedtog den 14. december 2023 lov nr. 1783 af 28. december 2023 om ændring af lov 2018-05-23 nr. 502 (»den danske databeskyttelseslov«) og lov nr. 1784 af 28. december 2023 om ændring af den danske databeskyttelseslov og lovbekendtgørelse 2023-06-23 nr. 1010 (»den danske lov om Det Centrale Personregister«)

Lov nr. 1783 medfører, at aldersgrænsen for, hvornår et barn kan give samtykke til behandling af personoplysninger i forbindelse med udbud af informationssamfundstjenester, hæves fra 13 år til 15 år. Loven har afsæt i en anbefaling fra en ekspertgruppe om tech-giganter og har til formål at beskytte børn og unge på internettet.

Lov nr. 1784 ophæver § 13, stk. 1-3 og 5-9 i den danske databeskyttelseslov, om behandling af personoplysninger i forbindelse med markedsføring. Lovændringen indebærer også, at det danske Procesbevillingsnævn undtages fra oplysningspligten og indsigtsretten efter GDPR ved nævnets behandling af personoplysninger i sager vedrørende appeltilladelse. Endelig tilpasses adgangen til indsigt hos den danske Folketingets Ombudsmand i sagsakter fra myndigheder, der er sendt til ombudsmanden som led i behandlingen af en sag hos ombudsmanden.

Lovene trådte i kraft den 1. januar 2024.

Læs det danske Justitsministeriets pressemeddelelse her: https://www.justitsministeriet.dk/nyhedsbrev/nyhedsbrev-af-5-januar-2024/

Læs lov om ændring af den danske databeskyttelseslov her: https://www.retsinformation.dk/eli/ft/A20230178330

Læs lov om ændring af den danske databeskyttelseslov og den danske lov om Det Centrale Personregister her: https://www.retsinformation.dk/eli/ft/A20230178430

Tue Goldschmieding er partner i Gorrissen Federspiel og en av de danske redaktørene for Lov&Data.


simonsen vogtwiig

Henning Wahlberg og Rune Ljostad

Endringer i åndsverkloven på høring

22. november 2023 sendte Kultur- og likestillingsdepartementet forslag til endringer i åndsverkloven mv. på høring. Endringene er foreslått som ledd i gjennomføringen av direktiv (EU) 2019/790 (digitalmarkedsdirektivet) og direktiv (EU) 2019/789 (nett- og videresendingsdirektivet). Høringsfristen er 15. mars 2024.

Dette er noen av endringene som er foreslått:

Plattformansvar

Digitalmarkedsdirektivet artikkel 17 innfører regler om opphavsrettslig ansvar for tilbydere av nettbaserte innholdsdelingstjenester (slik som YouTube, Instagram mv.). Et av formålene er å redusere det såkalte «verdigapet», som sikter til tapet rettighetshavere påføres når innhold deles på plattformer uten at rettighetene klareres. Ifølge de foreslåtte reglene vil tilbydere på visse vilkår være ansvarlig for sine brukeres opplasting av opphavsrettslig beskyttet materiale, med mindre tilbyderne oppfyller visse handleplikter. Et av vilkårene er at tilbyderen må gjøre sitt beste for å innhente tillatelse som hjemler bruken. Dette vil kunne innebære at tilbydere må henvende seg til rettighetshavere og kollektive forvaltningsorganisasjoner for å søke inngå avtale om verkstyper som deles av brukerne på tjenesten. Videre kreves det at tilbyderen gjør sitt beste for å fjerne beskyttet der rettighetshaver gir melding om dette, samt forhindre fremtidig opplastning av innholdet.

Tekst- og datautvinning

I høringsnotatet er det lagt frem forslag til regler om tekst- og datautvinning ('text and data mining'). Dette er foreslått definert som «enhver automatisert metode som brukes for å analysere tekst og data i digital form for å fremskaffe informasjon». Høringsnotatet fremhever utvikling av kunstig intelligens som et eksempel der det benyttes slik tekst- og datautvinning for å utvikle nye tjenester og ny teknologi.

Det er foreslått en regel om tekst- og datautvinning som skal gjelde generelt, og en som skal gjelde spesifikt for vitenskapelig forskning. Den store forskjellen mellom disse to reglene er adgangen for rettighetshavere til å reservere seg mot slik bruk. Den generelle adgangen oppstiller som hovedregel at enhver med lovlig tilgang til et verk, skal kunne fremstille eksemplar av verket for tekst- og datautvinningsformål, *med mindre* rettighetshaver har forbeholdt seg retten til slik bruk av verket. Der dette skjer med henblikk på vitenskapelig forskning, kan imidlertid ikke rettighetshaver motsette seg dette.

Kontraktsregler

Digitalmarkedsdirektivet inneholder regler om rimelig vederlag ved avtale om utnyttelse av verker. Artikkel 18 inneholder en regel om *rimelig vederlag* ved overdragelse av opphaverens eksklusive rettigheter. Åndsverkloven har allerede en slik regel i § 69. Artikkel 19 inneholder en bestemmelse om opplysningsplikt, som skal gi opphaveren krav på informasjon om hvordan verket utnyttes. Formålet bak regelen er bl.a. å sette opphaveren i stand til å vurdere om det avtalte vederlaget er rimelig. Artikkel 20 inneholder en bestemmelse om avtalejusteringsordning, som kan gi krav på revisjon av kontrakten dersom vederlaget viser seg å være urimelig lavt. Artikkel 22 innebærer at opphaveren skal kunne heve avtaler dersom verket ikke utnyttes innen rimelig tid. Artikkel 21 pålegger medlemsstaten å sikre alternative tvisteløsningsmetoder på opphavsrettens område. Departementet foreslår her at Vederlagsnemnda omdøpes til Opphavsrettsnemnda og får utvidet kompetanse til å behandle tvister knyttet til de nye kontraktsreglene.

Dom fra Høyesterett om «produsent»-begrepet i åndsverkloven § 20

5. desember 2023 avsa Høyesterett dom i sak mellom Mutual Intentions AS (med FONO og IFPI Norge som partshjelpere) og Noam Ofir. Dommen har saksnummer *HR-2023-2282-A* (sak nr. 23-033460SIV-HRET).

Åndsverkloven § 20 sier at en produsent av lydopptak har enerett til å råde over opptaket ved å fremstille varig eller midlertidig eksemplar av det og å gjøre opptaket tilgjengelig for allmennheten. Uenigheten for Høyesterett var om Noam Ofir hadde produsentrettigheter med krav på royalty for dette.

Bakgrunnen for saken var at Ofir hadde gjort opptak av egenkomponerte enkeltspor med eget utstyr. Disse enkeltsporene ble deretter inkorporert i tre sanger som ble utgitt av Mutual Intentions, med Ofirs samtykke. Det var ubestridt at Mutual Intentions hadde produsentrettighetene til de endelige sangene. Det konkrete spørsmålet for Høyesterett var om det var Ofir eller Mutual Intentions som måtte anses som «produsent» til enkeltsporene som Ofir tok opp, og som inngikk i de endelige sangene.

Høyesterett vurderte at ordlyden kan forstås både slik at en «produsent» er den som rent fysisk forestår opptakene, og den som mer overordnet sørger for at opptakene blir foretatt. Høyesterett finner flere momenter som taler for at begrepet må forstås på sistnevnte måte, og viser til at «produsent» i dagligtale normalt brukes om foretak som produserer noe, og ikke om enkeltpersoner som utfører konkrete produksjonsoppgaver. Høyesterett viser også til formålene bak bestemmelsen, herunder å gi insentiv til kulturell produksjon til de som skaper, fremfører eller investerer i åndsverk eller nærstående prestasjoner og arbeider.

På bakgrunn av dette finner Høyesterett at «produsent» må forstås som «den som forestår, i betydningen tilrettelegger og bærer omkostningene med, produksjonen av opptakene. Det er ikke fabrikanten eller fremstilleren av fysiske eksemplarer, uten at det er noe til hinder for at de ulike rollene kan være samlet på en hånd» (avsnitt 64).

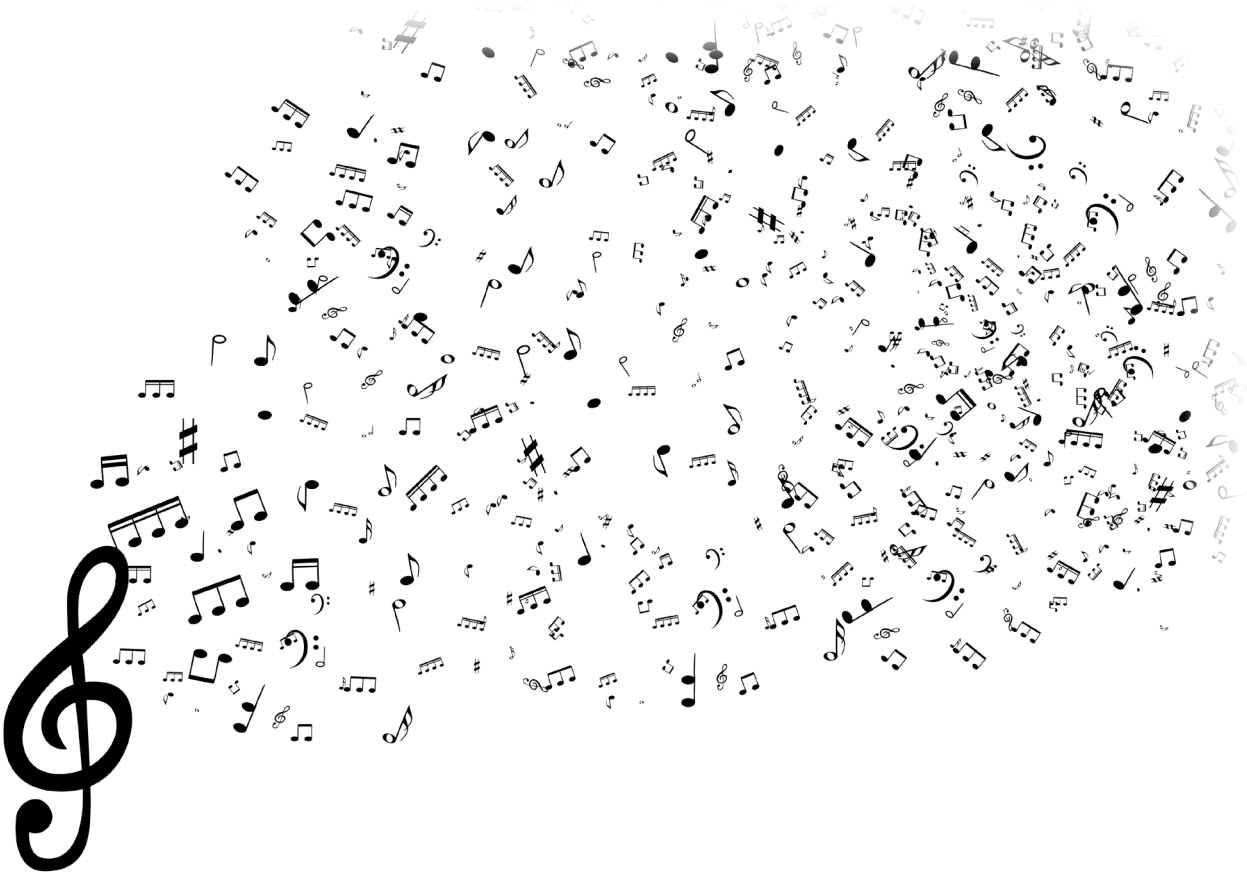
Ofir hadde anført at det var han selv som foretok lydopptakene, uten å være underlagt instrukser fra Mutual Intentions, eller noen avtale dem imellom. Han stod derfor fritt til å gjøre som han ville med lydopptakene.

Høyesterett viser imidlertid til at initiativet til prosjektet kom fra Mutual Intentions, og at lydskissen som dannet utgangspunktet og rammene for prosjektet kom fra noen tilknyttet Mutual Intentions. Høyesterett fant at også etterfølgende omstendigheter underbygger dette, herunder at Mutual Intentions har organisert samarbeid med andre artister på sangene, mikset sangene, utformet cover, produsert plater og sørget for markedsføring. Dermed mente retten at Mutual Intentions har stått for de oppgaver og investeringer som er typiske for en produsent, mens Ofirs bidrag i det vesentlige var av kreativ art.

På denne bakgrunn kom Høyesterett til at det var Mutual Intentions som måtte anses som «produsent» for lydsporene, og frifant derfor Mutual Intentions for kravet på produsentroyalty fra Ofir.

Henning Wahlberg er advokatfullmektig i Advokatfirmaet Simonsen Vogt Wiig AS.

Rune Ljostad er advokat (H) og assosiert partner i Advokatfirmaet Simonsen Vogt Wiig AS og leder firmaets faggruppe for IP. Han har prosedert flere prinsipielle saker innen IP og personvern



Illustrasjon: Colourbox.com

Bird & Bird

Gunnar Hjalt

Omedelbart vitesförbud om 10 MSEK mot att använda beteckningen TRAV & GALOPP i Sverige, PMT 8100-22

Patent- och marknadsöverdomstolen (PMÖD) meddelade den 25 januari 2024 en dom som innebär ett förbud för Svenska Spel Sport & Casino AB (Svenska Spel), vid vite om 10 000 000 kronor, att vid marknadsföring eller försäljning av spel på hästar använda kännetecknen TRAV & GALOPP eller TRAV OCH GALOPP på visst sätt. Dessutom upphävdes Svenska Spels Svenska varumärkesregistrering nr 605536 TRAV & GALOPP (fig).

Den rättsliga grunden för förbudet att använda kännetecken som innehåller TRAV & GALOPP, liksom för hävningen av den svenska varumärkesregistreringen, var risken för förväxling med kärandens Aktiebolaget Trav & Galopp företagsnamn som använts i stor utsträckning i Sverige i samband med spel på hästar.

PMÖDs dom motsvarar i stora delar domen från underinstansen PMD där domstolen kom fram till att genomsnittskonsumenten ”*får anses uppfatta trav och galopp (i gemener) som beskrivande termer som associerar till hästsport, och i vissa fall till spel på hästar*”. Däremot ansåg PMD att det sammansatta uttrycket Trav och Galopp inte var generiskt begrepp för vadhållning på hästar. Beteckningen TRAV & GALOPP ansågs ha svag inneboende särskiljningsförmåga men genom långvarig och omfattande användning hade den uppnått en normal grad av särskiljningsförmåga. Här menade PMÖD, till skillnad mot PMD, att företagsnamnet ”*i någon mån måste ha fått draghjälp av den kännedom som finns om bolagets förkortning och varumärke ATG*”. Det var emellertid inte visat att beteckningen TRAV & GALOPP skulle ha uppnått något anseendeskydd.

Svenska Spel lyckades inte få gehör för att beteckningen TRAV & GALOPP skulle ha använts utan uppsåt eller oaktsamhet eftersom PRV godkänt varumärket utan att ha anfört några hinder mot registreringen och ingen invändning gjorts mot registreringen. Vidare försökte Svenska Spel utan framgång få en omställningstid om minst fyra månader för att hinna fasa ut spelprodukter som marknadsförs under beteckningen TRAV & GALOPP.

Avgörandet speglar det starka skydd som även till synes svaga företagsnamn kan ha enligt svensk rätt, i synnerhet om de används konsekvent och under lång tid.

https://www.domstol.se/patent--och-marknadsoverdomstolen/patent--och-marknadsoverdomstolens-avgoranden/2024/139882/

Gunnar Hjalt, Senior Counsel, Bird & Bird Advokat

Illustrasjon: Colourbox.com

Gorrissen Federspiel

Tue Goldschmieding

Retten træffer afgørelse om varemærkeretlig beskyttelse af LEGO-figur

Den Europæiske Unions Ret (»Retten«) afsagde den 6. december 2023 afgørelse i sag T-297/221 mellem tyske BB Services GmbH (»BB«) og Den Europæiske Unions Kontor for Intellektuel Ejendomsret (»EUIPO«) med Lego Juris A/S som intervenient.

Sagen vedrørte et patent registreret i Nichearrangementet klasse 28. BB Services GmbH nedlagde for Retten påstand om annullation og omgørelse af EUIPO's afgørelse i sag R 1355/2021-5. EUIPO havde i denne afgørelse afslået en af BB fremsat ugyldighedserklæring over for Lego Juris A/S' EU-varemærke for et tredimensionelt tegn i form af en legetøjsfigur.

BB gjorde over for Retten gældende, at EUIPO havde tilsidesat forordning (EF) nr. 40/94 af 20. december 1993 (»EF-varemærkeforordningen«), artikel 7, stk. 1, litra e, nr. i), som udelukker registrering af tegn, hvis udformning alene følger af varens egen karakter, samt artikel 7, stk. 1, litra e, nr. ii), som udelukker registrering af tegn, hvis udformning er nødvendigt for at opnå et teknisk resultat. BB gjorde gældende, at registreringen af tegnet dermed var ugyldigt.

Det indledende spørgsmål for Retten var, hvorvidt der alene var tale om en »legetøjsfigur« eller om der ligeledes var tale om en »sammenføjelig byggelegetøjsfigur«. Retten fastlog, at varen havde en dobbeltkarakter ved at have henholdsvis leg og modularitet med intervenientens øvrige produkter, som formål.

Vedrørende EF-varemærkeforordningens artikel 7, stk. 1, litra e, nr. i) vurderede Retten, at både et menneskeligt udseende og de dekorative og fantasifulde elementer samt funktionen med modularitet, kunne anses for væsentlige kendetegn. Retten bemærkede, at det ikke alene var den grafiske gengivelse, som skulle vægtes ved fastlæggelsen af de væsentligste kendetegn, men også den relevante kundekreds' kendskab og opfattelse. Retten fastlog, at disse kendetegn ikke kunne anses for at være knyttet til varens generiske funktion eller egen karakter, hvilket udelukkede anvendelse af artikel 7, stk. 1, litra e, nr. i).

Vedrørende EF-varemærkeforordningens artikel 7, stk. 1, litra e, nr. ii) vurderede Retten i forhold til varens funktionalitet, at varen havde, dels en ikke-teknisk funktionalitet i form af legetøjsfigurens menneskelige træk ved at have hoved, hals, overkrop, arme og ben, som ikke var nødvendige for at opnå et teknisk resultat, og dels en teknisk funktionalitet ved modulariteten. Figuren indeholdt således et kreativt element, hvilket udelukkede anvendelsen af artikel 7, stk. 1, litra e, nr. ii).

Læs hele dommen her: *https://curia.europa.eu/juris/document/document.jsf?text=&docid=280404&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=782382*

EU-Dom om EU-ordmærket »CROSSWOD Equipment« kontra tidligere ordmærker inden for »CROSSFIT« og »CROSS«

Den Europæiske Unions Ret (»Retten«) afsagde den 29. november 2023 dom i sag T-506/22 mellem CrossFit LLC og EUIPO. CrossFit LLC havde indgivet appel mod Pitk Pelotas' registrering af EU-varemærket »CROSSWOD Equipment«, idet førstnævnte mente, at mærket »CROSSWOD« kunne forveksles med deres tidligere »CROSSFIT«-mærker.

Retten fandt, at der ikke forelå forvekslingsrisiko mellem mærkerne. Retten lagde i den sammenhæng vægt på, at de tidligere »CROSSFIT«-mærker havde svagt særpræg. I forlængelse heraf udtalte Retten, at selv hvis det kunne godtgøres, at der forelå øget særpræg, ændrede det ikke ved, at der ikke forelå forvekslingsrisiko, idet der alene forelå lav visuel, fonetisk og begrebsmæssig lighed.

Endvidere fandt Retten, at »CROSSFIT«-mærkets omdømme ikke var tilstrækkeligt velkendt i Den Europæiske Union og følgelig forelå ingen utilbørlig udnyttelse af et velkendt varemærke efter reglerne herom i varemærkeforordningens art. 8, stk. 5.

Læs hele dommen her: *https://curia.europa.eu/juris/document/document.jsf?text=&docid=280228&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=782382*

PayPal ændrer vilkår efter henvendelse fra europæiske forbrugermyndigheder

I en pressemeddelelse af 20. december 2023 udtalte Forbrugerombudsmanden, at betalingstjenesten PayPal havde forpligtet sig til at ændre sine vilkår og betingelser efter de europæiske forbrugermyndigheder, herunder Forbrugerombuds-

manden, havde vurderet, at flere af PayPals formuleringer var urimeligt svære at forstå for forbrugerne.

PayPals vilkår og betingelser levede derfor ikke op til direktivet om urimelige kontraktvilkår, som Danmark har implementeret i lovbekendtgørelse nr. 193 af 2. marts 2016 (»den danske aftalelov«). PayPals nye vilkår og betingelser træder i kraft den 28. maj 2024.

Læs Forbrugerombudsmandens pressemeddelelse her: *https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2023/paypal-aendrer-vilkaar-efter-henvendelse-fra-europaeiske-forbrugermyndigheder/*

Læs EU-Kommissionens pressemeddelelse her: *PayPal commits to amending terms & conditions (europa.eu)*

EUIPO fremlægger opgørelse af regnskab for håndhævelse af IP-rettigheder ved EU's grænser

Den Europæiske Unions Kontor for Intellektuel Ejendomsret (»EUIPO«) fremlagde i den 28. november 2023 en opgørelse af resultater for håndhævelse af IP-rettigheder ved EU's grænser og i EU's indre marked i 2022.

Opgørelsen, der har til formål at støtte analyse af IP-rettighedskrænkelser og udvikling af passende modforanstaltninger, er baseret på indberettet data om tilbageholdelser ved EU's grænser af de 27 EU-medlemslande samt data om tilbageholdelser i det indre marked rapporteret fra alle EU-medlemslande med undtagelse af Østrig, Tyskland og Luxembourg.

Det årlige antal varer tilbageholdt ved *EU's grænser* faldt i 2022 med 15% sammenlignet med det forgangne år. Den anslåede værdi af de tilbageholdte produkter er dog steget med 11 %.

Opgørelsen fastslår endvidere, at mængden af varer, der krænkede IP-rettigheder og blev tilbageholdt i *EU's indre marked*, steg med næsten 26 % i forhold til det foregående år. Til trods for denne stigning i antallet af tilbageholdte genstande, faldt den anslåede værdi af genstandene med ca. 2%, hvilket forklares ved at være et skift mod billigere produkter.

Til trods for en begrænset stigning i antallet af genstande er den anslåede værdi af tilbageholdte forfalskede genstande steget med 3 % til over 2 mia. EUR i 2022. Tilbageholdelsen i det indre marked udgjorde ca. 60%, hvor resten udgjorde tilbageholdelsen ved EU's grænser.

Læs pressemeddelelsen her: *https://www.euipo.europa.eu/en/publications/eu-enforcement-of-iprs-results-at-the-eu-border-and-in-the-eu-internal-market-2022-november-2023*

Forbrugere kan kræve skjulte abonnementsbetalinger refunderet fra netbutikker

Højesteret afsagde den 7. december 2023 afgørelse i sagerne BS-37131/2022-HJR, BS-37142/2022-HJR og BS-37160/2022-HJR mellem den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) og netbutikkerne buuks.dk, pluus.dk og sayve.dk. Sagerne omhandlede, hvorvidt de tre virksomheder havde tegnet skjulte abonnementsaftaler over for forbrugerne og som følge heraf var forpligtet til at tilbagebetale abonnementsbetalingerne.

I overensstemmelse med Forbrugerombudsmanden fandt Højesteret, at netbutikkerne ikke havde overholdt deres forpligtelser til klart og tydeligt at angive, at forbrugeren ved købet af en vare tillige blev pålagt en forpligtelse til at betale for et abonnement. Netbutikkerne havde automatisk trukket mellem 89 og 119 kroner om måneden på forbrugernes konti for et såkaldt »abonnement«, som gav adgang til at handle varer til »medlemspriser« i netbutikkerne. Højesteret fandt, at abonnementsbetalingerne var opnået ved en fremgangsmåde, der ansås for groft vildledende og klart retsstridig efter lov nr. 1457 af 17. december 2013 (»den danske forbrugeraftalelov«) § 8 og § 12.

På baggrund heraf blev netbutikkerne dømt til at tilbagebetale abonnementsbetalingerne med renter fra opkrævningstidspunkterne.

Læs Forbrugerombudsmandens pressemeddelelse her: *https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2023/hoejesteret-abonnementsbetalinger-til-buuks-pluus-og-sayve-skal-tilbage-til-forbrugerne/*

Læs et resumé af dommen her: *https://domstol.fe1.tangora.com/Domsoversigt-(H%C3%B8jesteretten).31478.aspx?recordid31478=2532*

Læs hele dommen her: *https://domstol.dk/media/0mzkln-nx/37131-37142-37160-dom-hjemmesiden.pdf*

Blankmedieordningen var i strid med EU-direktiv, men der var ikke grundlag for erstatning

Højesteret traf afgørelse den 16. november 2023 i sag BS-21863/2022-HJR mellem Copydan KulturPlus (»Copydan«) og det danske Kulturministeri. I tidligere instans var sagen afgjort af Østre Landsret den 19. maj 2022 (BS-25897/2019-OLR).

Dommen omhandlede gyldigheden af Blankmedieordningen der i perioden 2014-2021, kompenserede rettighedshavere for privatkopiering. På baggrund af EU-Domstolens tidligere afgørelser (sag C-467/08 af 21. oktober 2010 og sag C-462/09 af 16. juni 2011) udtalte Højesteret, at den danske ordning var i strid med Europa-Parlamentets og Rådets direktiv 2001/29/EF af 22. maj 2001 (»Infosoc«). Højesteret konkluderede, at de danske myndigheder havde kvalificeret overtrådt EU-retten i den nævnte periode og derfor kunne pådrage sig erstatningsansvar.

Højesteret udtalte derudover, at Copydan kun ville have lidt et erstatningsretligt tab, hvis det kunne påvises, at rettighedshaverne ville have modtaget en højere kompensa-

tion ved korrekt implementering af Infosoc. I sidste ende konkluderede Højesteret, at Copydan ikke havde bevist, at de havde lidt et tab i perioden fra 2014 til 2021. Derfor var der ikke grundlag for erstatning. Dette stod i kontrast til Landsrettens tidligere afgørelse, der var nået frem til en anden konklusion.

Læs et resumé af dommen her: *https://domstol.fe1.tangora.com/page31478.aspx?recordid31478=2525*

Læs hele dommen her: *https://domstol.fe1.tangora.com/media/-300016/files/BS-21863_Dom_til_hjemmesiden.pdf*

Østre Landsret stadfæster midlertidige forbud mod Sony og Huawei

Østre Landsret traf den 20. oktober 2023 afgørelse i sagerne BS-25520/2022-OLR, BS-25521/2022-OLR, BS-26192/2022-OLR og BS-49377/2023-OLR vedrørende beskyttelse af Sonions patentrettigheder til en vibrationssensor, en såkaldt »Voice Pick Up Bone Sensor«, som indgik i høretelefoner markedsført af Sony og Huawei.

Sagen var tidligere behandlet ved Sø- og Handelsretten, som den 21. juni 2022 i sagerne BS-24619/2021-SHR og BS-32103/2021-SHR afsagde midlertidige forbud og påbud mod Sony og Huawei. Kendelserne blev af Sony og Huawei påkæret til Østre Landsret.

Spørgsmålet for Østre Landsret var navnlig, hvorvidt stridsrettighederne var ugyldige som følge af manglende basis. Retten skulle herved tage stilling til: 1) betydningen af, at Opposition Division ved Den Europæiske Patentmyndighed ved en afgørelse af 25. maj 2023 havde antaget, at patentet var ugyldigt i sin oprindelige form grundet manglende basis, men at patentet kunne opretholdes i ændret form, og 2) om Sony og Huaweis produkter krænkede patentet.

Landsretten fandt i henhold til 1) henset til hensynet til effektiv retsbeskyttelse, som forbuds- og påbudsinstituttet i kapitel 40 i lovbekendtgørelse nr. 1655 af 25. december 2022 (»den danske retsplejelov«) har til formål at sikre, at Opposition Divisions afgørelse ikke kunne medføre, at de udstedte midlertidige forbud og påbud ikke kunne opretholdes. Til 2) fandt landsretten, at Sonions patentrettigheder var gyldige, og tiltrådte, at stridsprodukterne måtte anses for teknisk ligeartede med det i patentrettighederne beskrevne.

Landsretten tiltrådte således, at Sonys og Huaweis produkter krænkede Sonions rettigheder efter stridspatentet, og stadfæstede herved de påkærede kendelser om forbud og påbud.

Læs kendelsen her: *https://domstol.dk/media/cvep5ipu/bs-25520-22.pdf*

Udbyder af online platform inden for juridiske discipliner samt tidligere samarbejdspartner frifundet for at have begået kontraktbrud og at have overtrådt danske lovregler

Sø- og Handelsretten afsagde den 9. januar 2024 dom i de kumulerede sager BS-18002/2023-SHR og BS-41784/2023-SHR mellem Forlaget Andersen A/S (sagsøger) og Koan A/S, Colloquium ApS (nu under konkurs), Torben Lund Lindskrog Rasmussen og Peter Korsaa Andersen (sagsøgte). Sagerne handlede om, hvorvidt sagsøgte begik kontraktbrud i forbindelse med en samarbejdsaftale med sagsøger, samt hvorvidt sagsøgte havde overtrådt lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) og lov nr. 309 af 25. april 2018 (»den danske lov om forretningshemmeligheder«).

Sagsøger nedlagde påstand om, at Koan A/S skulle forbydes at markedsføre og sælge videnspakker og kurser inden for erhvervsjura, virksomhedsøkonomi og ledelse på abonnementsbasis, der hviler på samme koncept og indhold som udbudt af sagsøger. Sagsøger nedlagde desuden påstand om, at de sagsøgte skulle forbydes at udnytte de oplysninger om kunder hos sagsøger, som de sagsøgte erhvervede i forbindelse med deres samarbejde og ansættelse hos sagsøger. Sagsøger nedlagde endelig påstand om, at de sagsøgte skulle betale erstatning til sagsøger og, at de sagsøgte skulle idømmes en af retten fastsat straf.

Sø- og Handelsretten fandt indledningsvist, at sagsøgers første påstand om forbud skulle afvises, da påstanden var for uklar og bred til, at den kunne danne grundlag for en dom. Sø- og Handelsretten fandt dernæst, at det ikke var bevist, at de sagsøgte var i besiddelse af oplysninger om kunder hos Forlaget Andersen A/S, som de havde erhvervet i forbindelse med deres samarbejde med forlaget. De sagsøgte blev derfor frifundet for den anden påstand. Af samme grund blev de sagsøgte frifundet for de øvrige påstande.

Læs hele dommen her: *https://domstol.fe1.tangora.com/media/-300011/files/Dom_(sambehandling)_BS-18002-2023-SHR_og_BS-41784-2023-SHR.pdf?rev1*

Et selskabs tidligere direktør og ejer var personlig ansvarlig for at foretage parallelimport i strid med sagsøgernes varemærkerettigheder.

Sø- og Handelsretten afsagde den 3. januar 2024 afgørelse i sag BS-9911/2021-SHR mellem sagsøger Hewlett-Packard Development Company L.P. (»HPE«) og sagsøgte »A«.

Tvisten i sagen angik parallelimport, hvor HPE påstod, at A som eneejer og direktør i Konzept ApS havde medvirket til parallelimport i strid med HPE's varemærkerettigheder. Ifølge HPE's havde Konzept ApS uberettiget solgt varer påført HPE's varemærker inden for det Europæiske Økonomiske Samarbejdsområde »EØS«). HPE havde oprindeligt solgt produkter til distributører uden for EØS, og disse di-

stributører havde kun tilladelse til at sælge produkterne i et nærmere bestemt område uden for EØS.

Sø- og Handelsretten fandt, at A var personligt involveret i og havde en afgørende indflydelse på de omfattede indkøb og salg inden for EØS. Retten lagde til grund, at A efter den 1. marts 2018 vidste, at der skete krænkelser af HPE's varemærker og på trods af dette fortsatte salg i EØS igennem Konzept ApS.

På denne baggrund pålagde Sø- og Handelsretten A at betale skønsmæssigt vederlag og erstatning på 7.500.000 kr. til HPE. A hæftede solidarisk med Konzept ApS.

Læs hele dommen her: *https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-9911-2021-SHR.pdf?rev1*

Sø- og Handelsrettens afgørelse i sagen vedrørende Novartis patentstridssag mod Glenmark

Sø- og Handelsretten afsagde kendelse den 21. december 2023 i sag BS-42600/2023-SHR. Novartis AG, Novartis Pharma AG og Novartis Healthcare A/S (»sagsøgerne«) nedlagde påstand om, at Glenmark Pharmaceuticals Nordic AB (»sagsøgte«) havde krænket deres patentrettigheder ved at udbyde, markedsføre og anvende lægemidlet »Fingolimod« i strid med lovbekendtgørelse nr. 1655 af 25. december 2022 (»den danske retsplejelov«) § 413.

Sagsøgerne havde sandsynliggjort deres ret til beskyttelse i henhold til retsplejelovens § 413, nr. 1. På trods af sagsøgtes påstand om, at der ikke var krænkelse, fastslog retten, at stridspatentet beskyttede mod en daglig dosis på 0,5 mg fingolimod, uanset formuleringen, da lægemidlet »Fingolimod Glenmark« indeholdt 0,56 mg fingolimod hydrochlorid,

Retten konstaterede, at sagsøgerne sandsynliggjorde krænkelse i henhold til den danske retsplejelovs § 413, nr. 2. De udviste ikke passivitet, og havde rimelig grund til at afvente sagsøgernes frivillige tilbagetrækning af produktet jf. den danske retsplejelovs § 413, nr. 3.

Sagsøgerne fik medhold i deres krav, og sagsøgte blev pålagt forbud mod sælge at »Fingolimod Glenmark« i Danmark. Sagsøgte fik desuden påbud om tilbagekaldelse og blev pålagt at betale sagsomkostninger og at stille sikkerhed.

Læs hele kendelsen her: *https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_BS-42600-2023-SHR.pdf*

Sø- og Handelsretten fandt, at Flatpay havde krænket Nets' ordmærke »Dankort«

Sø- og Handelsretten afsagde den 18. december 2023 dom i sagen BS-27718/2023-SHR mellem NETS Denmark A/S (»NETS«) over for FLATPAY ApS (»FLATPAY«)

Sagen omhandlede, hvorvidt FLATPAY's anvendelse af ordmærket »DANKORT« krænkede NETS' varemærkeretlige eneret efter lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) § 4, stk. 1. Ordmærket DANKORT havde været registreret for NETS i 50 år og FLATPAY havde ikke en aftale med NETS om at benytte ordmærket.

FLATPAY påstod, at ordmærket var degenereret som følge af, at det var blevet til en almindelig betegnelse inden for branchen, efter den danske varemærkelov § 26, stk. 1 nr. 1. Sø- og Handelsretten fandt det dog ikke godtgjort, at DANKORT var blevet en almindelig betegnelse i branchen, hvorfor ordmærket ikke var degenereret.

FLATPAY påstod tillige, at NETS havde forholdt sig passivt, hvilket Sø- og Handelsretten afviste, da NETS gentagne gange havde henvendt sig til FLATPAY.

Sø- og Handelsretten lagde herefter til grund, at FLATPAY ved at anvende betegnelserne »Visa/Dankort« og »Dankort« på deres hjemmeside og i Google søgninger, ikke alene havde anvendt betegnelserne deskriptivt, hvorfor FLATPAY havde krænket NETS' varemærkeretlige eneret, efter den danske varemærkelov § 4, stk. 1.

FLATPAY blev pålagt forbud og påbud mod anvendelse af ordmærket »DANKORT, blev yderligere pålagt at betale sagsomkostninger.

Læs hele kendelsen her: *https://domstol.fe1.tangora.com/media/-300011/files/BS-27718-2023-SHR_Kendelse.pdf*

Sø- og Handelsretten fastslår krænkede Coops varemærkerettigheder til Irmapigen

Sø- og Handelsretten afsagde den 5. december 2023 kendelse i sag BS-30388/2023-SHR mellem Coop Danmark A/S (»Coop«) over for kunstgalleriet Artpusher Gallery ApS (»Artpusher«) og Love Party, kunster og direktør af Artpusher. Sagen angik, hvorvidt Artpusher havde krænket Coops rettigheder efter den lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) § 4, stk. 2, nr. 3, ved at anvende både Irmapigen som figurmærke, og ordmærkerne »IRMA« og »COOP« i Love Partys kunstværker samt i reproduktioner solgt af Artpusher som både plakater, krus, tøj, klistermærker m.v., både før og efter, at Irma-butikkerne blev omdannet til Coop.

Coop nedlagde på den baggrund påstand om midlertidigt forbud og påbud over for Artpushers anvendelse af varemærkerne. Artpusher gjorde gældende, at brugen af Irmapigen var inden for rammerne af hans kunstneriske frihed, og at reproduktionen var uden kommercielle formål.

Sø- og Handelsretten fandt det imidlertid ubetænkeligt, at Artpushers motiver på dennes kunstværker, såvel som på merchandise, lignede de beskyttede varemærker. Retten lagde vægt på, at Artpushers reproduktioner alle indeholdt elementer af Irmas beskyttede figur-

og ordmærker, at motiverne på varerne var centrale elementer, og at varerne blev markedsført med en reference til Irma. Sø- og Handelsretten bemærkede hertil, at der var tale om en udnyttelse i så massivt et omfang, at hensynet til ytringsfriheden og den samfundsmæssige relevant, ikke kunne føre til andet resultat.

På den baggrund gav Sø- og Handelsretten Coop medhold i deres påstand om nedlæggelse af midlertidigt forbud og påbud mod anvendelse af varemærkerne i kunstværker såvel som reproduktioner. Sø- og Handelsretten fandt dog, at forbud og påbud ikke kunne opretholdes over for »omtale«, som var indeholdt i Coops påstande. Sø- og Handelsretten frifandt Artpusher for så vidt angik beslaglæggelse af værkerne.

Læs hele kendelsen her: *https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_BS-30388-2023-SHR.pdf?rev1*

Forretningskendetegn var ikke beskyttet som følge af virksomhedsoverdragelse, da kendetegnene ikke var benyttet forud for overdragelsen

Sø- og Handelsretten afsagde den 20. november 2023 kendelse i sag BS-40346/2023-SHR mellem Houkjær Begravelse ApS (»Houkjær«) og Søhøjlandets Begravelser & Blomstergalleri ApS (»Søhøjlandet«). Sagen angik varemærkerettigheder, og hvorvidt der skulle meddeles midlertidigt forbud mod, at Søhøjlandet anvendte kendetegnene »Gitte Pallisby« og »Pallisby« i forbindelse med bedemandsforretning.

Gitte Pallisby ejede en begravelsesforretning, som hun overdrog aktiviteterne og tilhørende immaterielle rettigheder til Houkjær i 2019. Gitte Pallisby tog efterfølgende ansættelse i Søhøjlandet.

Sagens hovedspørgsmål var, hvorvidt den af Gitte Pallisby overdragne virksomhed anvendte kendetegnene »Gitte Pallisby« og »Pallisby« før overdragelsen til Houkjær, således at Houkjær erhvervede retten til brug af kendetegnene ved erhvervelsen.

Sø- og Handelsretten fandt det ikke sandsynliggjort, at de omtalte kendetegn var blevet anvendt forud for overdragelsen af forretningen, hvormed disse kendetegn ikke var beskyttet. Retten fandt endvidere ikke grundlag for at udstede et forbud imod Søhøjlandets anvendelse af kendetegnene. Retten udtalte dog, at Søhøjlandets markedsføring var i strid med god markedsføringsskik, idet udsagn på deres hjemmeside om Gitte Pallisby's ejertid fremstod vildledende.

Læs afgørelsen her *Kendelse_BS-40346-2023-SHR.pdf (tangora.com)*

Sø- og Handelsrettens afsiger dom i sag om immaterialretlig beskyttelse af modetøj

Sø- og Handelsretten traf den 31. oktober 2023 afgørelse i sag BS-49115/2018-SHR, som var anlagt af den tyske streetwearproducent Naketano GmbH (herefter Naketano) mod den danske virksomhed IKS ApS (herefter IKS), der sælger og producerer modetøj. Tvisten omhandlede dels spørgsmålet om, hvorvidt 9 specificerede trøjemodeller fra Naketano nød ophavsretlig, designretlig og/eller markedsføringsretlig beskyttelse, dels om IKS krænkede disse rettigheder.

Retten fandt, at trøjemodellerne ikke udgjorde originale nyskabelser i henhold til § 1 i lovbekendtgørelse nr. 1093 af 20. august 2023 (»den danske ophavsretslov«). Dette gjaldt, selvom trøjemodellerne indeholdt visse designelementer, der adskilte dem fra andre trøjemodeller på markedet.

Yderligere tog retten stilling til, om modellerne nød beskyttelse efter artikel 11 i Rådets forordning (EF) nr. 6/2002 af 12. december 2001 (»designforordningen«) om ikke-registrerede EF-designs. Én af Naketanos modeller blev af retten betragtet som et generisk produkt, der ikke nød beskyttelse efter designforordningen. De øvrige trøjemodeller blev karakteriseret ved forskellige designelementer og disse nød derfor beskyttelse i henhold til § 11 i designforordningen

Retten fandt, at 8 af Naketanos trøjemodeller havde tilstrækkeligt særpræg til at nyde beskyttelse mod meget nærgående efterligninger i henhold til § 3 i lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) om god markedsføringsskik.

Endeligt fandt retten, at 7 trøjemodeller krænkede Naketanos rettigheder efter den danske markedsføringslovs § 3, fordi IKS havde anvendt samme designelementer som Naketano. Samtidig krænkede 2 af IKS' designs Naketanos rettigheder efter designforodrningen, idet disse var blevet markedsført og solgt inden for den periode, hvor Naketano nød beskyttelse efter forordningen. Af den grund skulle IKS betale vederlag og erstatning til Naketano for lidt tab. Vederlaget og erstatningen blev af retten opgjort skønsmæssigt til 2 mio. kr.

Læs Sø- og Handelsrettens afgørelse her: *https://domstol.fe1.tangora.com/media/-300011/files/Dom_-_BS-49115-2018-SHR.pdf*

Sø- og Handelsretten ophæver varemærket »PANSERGLAS«

Sø- og Handelsretten afsagde den 24. oktober 2023 dom i sag BS-17838/2020-SHR mellem PANZERGLASS A/S (»Panzerglass«) mod WePack ApS (»Wepack«). Sagen angik primært, om Wepack havde krænket Panzerglass' varemærkerettigheder samt gyldigheden af Panzerglass' varemærke »PANSERGLAS«.

Vedrørende gyldigheden af varemærket »PANSERGLAS« lagde retten afgørende vægt på et »væsentligt bevis« i form af en udtalelse fra dansk sprognævn om, at »*panser og pansre/pansret* er udbredte i sproget, og at deres brug ikke er begrænset

til mobiltelefoner, laptops, tablets og skærmbeskyttelse. *Panserglas* bruges ofte om skærmbeskyttelse, men anvendes omtrent lige så hyppigt om skudsikkert glas«.

Dertil kom, at den danske Patent- og varemærkestyrelse af 2 omgange havde afvist varemærkeregistrering under henvisning til, at panserglas er beskrivende for skærmbeskyttelsesprodukter. Den beskrivende brug havde været til stede på ansøgningstidspunktet, og retten erklærede derfor varemærket PANSERGlAS ugyldigt grundet manglende oprindeligt særpræg jf. lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) § 28, stk. 1, jf. § 13, stk. 1, nr. 2 og 3.

Ved krænkelsesvurderingen tog retten stilling til, om Wepacks brug af betegnelserne »panserglas« og »panser cover« udgjorde en krænkelse af varemærkerne PANZERGLASS og PANZER. Retten fandt, at brugen af det beskrivende ord panser ikke kunne forbydes, da der ikke er hjemmel for en rettighedshaver til at forbyde brug af angivelser uden særpræg jf. den danske varemærkelov §10, stk. 1, nr. 2

Wepack blev derfor frifundet.

Læs hele afgørelsen her: *https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-17838-2020-SHR.2466.aspx*

Sø- og Handelsretten træffer afgørelse om krænkelse af patent ved udbud af hjerteklapprotese mod en sikkerhedsstillelse på 2.000.000 kr.

Sø- og Handelsretten afsagde den 23. oktober 2023 kendelse i sag BS-48141/2022-SHR mellem Edwards Lifesciences Corporation (»ELC«) og Edwards Lifescience A/S (»EL«) over for Mermaid Medical A/S (»MM«).

Sagen angik, hvorvidt MM krænkede ELC og EL's rettigheder ved at udbyde Mycal Octacor. ELC og EL nedlagde på den baggrund påstand om midlertidigt forbud og påbud uden sikkerhedsstillelse.

Det centrale spørgsmål i sagen var, hvorvidt MM krænkede patentet ved, at visse af patentets beskyttede krav var realiseret i Myval Octacor. Sø- og Handelsretten fastslog, at stridsproduktet krænkede patentet på to elementer. Første element vedrørte det materiale, som stridsproduktets ramme var fremstillet af og andet element vedrørte selve rammestrukturen.

Retten bemærkede til første krænkelse, at ud fra en ordlydsfortolkning af de patenterede træk, så måtte den omstændighed, at kravet indeholdt nogle træk, som indgik i stridsproduktet *sammen med* andre træk, udgøre en krænkelse af patentet, selvom stridsproduktets ramme ikke udelukkende bestod af dette materiale.

Retten anlagde samme vinkel i forhold til den patenterede rammestruktur, som tillige fandtes i stridsproduktet. Her fastlog retten, at på trods af, at der i rammestrukturen af stridsproduktet var et yderligere træk i form af en anderledes celle, sammenlignet med den beskyttede rammestruktur, så besad stridsproduktet uagtet det beskyttede træk. Retten fastlog, at dette førte til, at stridsproduktet krænkede patentet. Retten lagde vægt på, at denne anderledes celle, dels ikke udgjorde en selvstændig celle og, dels ikke havde et selvstændigt teknisk formål.

På den baggrund gav retten ELC og EL medhold i deres påstand om nedlæggelse af midlertidigt påbud og forbud, men med en sikkerhedsstillelse på 2.000.000 kr., jf. lovbekendtgørelse nr. 1655 af 25. december 2022 (»den danske retsplejelov«) § 415.

Kendelsen blev kæret til Østre Landsret den 2. november 2023.

Læs hele kendelsen her: *https://domstol.fe1.tangora.com/media/-300011/files/BS-48141-2022-SHR_Kendelse.pdf*

Zebra design får tildelt ophavsretlig beskyttelse i Sø- og Handelsretten

Sø-og Handelsretten afsagde en 16. oktober 2023 dom i sag BS-540445/2022-SHR mellem ZEBRA A/S (»Zebra«) over for UPSTRÖM ApS (»Upström«). Sagen angik, om Upström havde krænket Zebras rettigheder efter lovbekendtgørelse nr. 1093 af 20. august 2023 (»den danske ophavsretslov«) og lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) ved fremstilling, salg og markedsføring af kabelskjuleren »Cirkulär«.

Sø- og handelsretten slog først og fremmest fast, at Zebras egen kabelskjuler havde originalitet og var en intellektuel frembringelse, som udsprang af designerens personlige, skabende og frie kreative indsats. Den var derfor beskyttet efter den danske ophavsretslov § 1, stk. 1, jf. § 2, stk. 1.

Retten fandt herefter, at Upströms »Cirkulär« var identisk med Zebras kabeskjuler på nær helt underordnede elementer vedrørende logo og indløbsmærker. Der forelå dermed en identitetsfornemmelse og forvekslingsrisiko, som krænkede Zebras ophavsrettigheder.

Zebras kabeskjuler nød ligeledes beskyttelse efter danske markedsføringslovs regler om forbud mod nærgående produktefterligninger. Bortset fra de underordnede elementer, som nævnt ovenfor, var denne en »slavisk efterligning af Zebras kabelskjuler«. Upström havde derfor handlet i strid med den danske markedsføringslov § 3, stk. 1 om god markedsføringsskik.

Sø- og handelsretten tog derfor Zebras påstande om forbud mod fremstilling, markedsføring, salg mv., af »Cirkulär«, tilbagekaldelse af denne samt rimeligt vederlag og erstatning til følge. Det samlede rimelige vederlag og erstatning blev fastsat til 50.000 kr., og Upström blev ligeledes pålagt at offentliggøre domkonklusionen på deres hjem-

meside i en periode på 30 dage fra endelig dom.

Læs Sø- og Handelsrettens dom her: *https://domstol.fe1.tangora.com/media/-300011/files/Dom_-_BS-54045-2022-SHR.pdf*

Markedsføringsloven og varemærkeloven anvendt i sag mellem danske selskaber selvom tvisten navnlig vedrørte leverance til Taiwan

Sø- og Handelsretten afsagde den 10. oktober 2023 dom i sag BS-14139/2022-SHR mellem sagsøger BBI Engineering A/S (»SE«) og sagsøgte Weiss ApS (»SG«).

Tvisten i sagen angik, hvorvidt SG havde krænket SE's rettigheder til brug af navnet, teknologien og varemærket »Envikraft«/»Envicraft«, og i den forbindelse om lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) og lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) fandt anvendelse, uanset at tvisten navnlig vedrørte en erklæring afgivet i forbindelse med en levering til Taiwan.

Sø- og Handelsretten fastslog indledningsvist, at rettighederne til de omtvistede varemærker blev overdraget til SE ved en overdragelsesaftale af 15. februar 2018 mellem SE og SG.

Herefter konkluderede retten, at SG havde overtrådt den danske markedsføringslovs § 3, § 20 og § 22 om god markedsføringsskik, vildledning og uretmæssig benyttelse af forretningskendetegn ved at afgive tilbud og erklæringer vedrørende et produkt i strid med denne overdragelsesaftale. Selvom leverancen af produktet var sket til en virksomhed i Taiwan, fandt retten, at kravene havde en sådan tilknytning til det danske marked, at den danske markedsføringslov fandt anvendelse.

Dernæst konstaterede Sø- og Handelsretten, at SG havde eksporterede produktet til Taiwan under anvendelse af mærket »Envicraft«, hvilket måtte anses at være i strid med SE's varemærkerettigheder i henhold til den danske varemærkelovs § 4, stk. 3, nr. 3, som blandt andet omfatter eksport under en andens varemærke.

På denne baggrund gav Sø- og Handelsretten SE medhold i deres påstande og tilkendte SE 450.000 kr. I erstatning og vederlag for tabt avance og markedsforstyrrelse.

Læs hele dommen her: *https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-14139-2022-SHR.pdf*

Indskærpelse af vildledningsforbuddet for markedsføring af emballage lavet af OWP (plastik indsamlet fra havet)

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) indskærpede den 13. december 2023 vildledningsforbuddet over for en virksomhed, der markedsførte deres emballage som om, at denne var lavet af havplast (OWP - Ocean Waste Plastic).

I januar 2021 blev Forbrugerombudsmanden opmærksom på, at en virksomhed markedsførte deres emballage som lavet af havplast. Dette blev af Forbrugerombudsmanden anset for vildledende og i strid med lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 20, stk. 1, da virksomheden ikke kunne dokumentere, at emballagen faktisk var fremstillet af havplast. Virksomheden ændrede derefter sin markedsføring og fjernede henvisningen til havplast. Hermed indskærpede Forbrugerombudsmanden vildledningsforbuddet i den danske markedsføringslov §§ 20, stk. 1 og 5, stk. 1, sammenlignet med § 8, stk. 1.

I efteråret 2023 genindførte virksomheden imidlertid beskrivelser om, at emballagen var lavet af havplast. Denne gang kunne virksomheden dog dokumentere, at emballagen indeholdt den angivne mængde havplast. Forbrugerombudsmanden gjorde opmærksom på, at sagen kunne blive genoptaget, hvis der fremkom nye oplysninger, der antydede noget andet.

Læs Forbrugerombudsmandens afgørelse her: *https://www.forbrugerombudsmanden.dk/find-sager/sager/markedsfoeringsloven/indskaerpelse-af-vildledningsforbuddet-for-markedsfoering-af-emballage-lavet-af-owp-plastik-indsamlet-fra-havet/*

Løbende aftaler skal kunne opsiges på samme medie eller tekniske platform, som aftalerne er indgået på

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) oplyste i en pressemeddelelse den 5. oktober 2023, at Forbrugerombudsmanden har orienteret en fitnesskæde om § 28 a i lov nr. 1457 af 17. december 2013 (»den danske forbrugeraftalelov«) om opsigelse af aftaler om løbende levering af tjenesteydelser. Det skyldtes, at fitnesskæden ikke sikrede, at forbrugere kunne opsige aftaler om fitnessmedlemskab på samme medie eller tekniske platform, som aftalerne var indgået.

Fitnesskæden skrev i deres vilkår, at tilmelding af et fitnessmedlemskab kunne ske via deres hjemmeside eller ved telefonisk henvendelse. Opsigelse skulle derimod ske ved personligt fremmøde i et af virksomhedens centre eller ved fysisk brev. Efter Forbrugerombudsmandens henvendelse ændrede fitnesskæden deres vilkår, så det var muligt både at indgå og opsige aftaler om et fitnessmedlemsskab via virksomhedens hjemmeside. Forbrugerombudsmanden afsluttede derfor behandling af sagen.

Læs Forbrugerombudsmandens afgørelse her: *Det skal være muligt at opsige en løbende aftale på samme medie eller tekniske platform, som aftalen er indgået på (forbrugerombudsmanden.dk)*

Klagenævnet for Domænenavne træffer afgørelse i sag vedrørende domænenavne mellem ELGIGANTEN A/S og Mikkel Jespersen

Klagenævnet for Domænenavne træf den 15. november 2023 afgørelse i sagerne med journalnumrene 2023-0196 (»elgigannten«) og 2023-0198 (»elgigantén«). Sagerne vedrørte tvister om domænenavne mellem ELGIGANTEN A/S (klager) og Mikkel Jespersen (indklagede).

I elgigannten havde klageren, en del af Elkjøp-koncernen, påstået, at indklagede krænkede deres varemærkerettigheder til ELGIGANTEN ved at registrere og anvende domænenavnet »elgigannten.dk.« Klagenævnet konkluderede den 15. november 2023, efter vurdering af klagerens rettigheder og indklagedes handlinger, at »elgigannten.dk« skulle overføres til klageren.

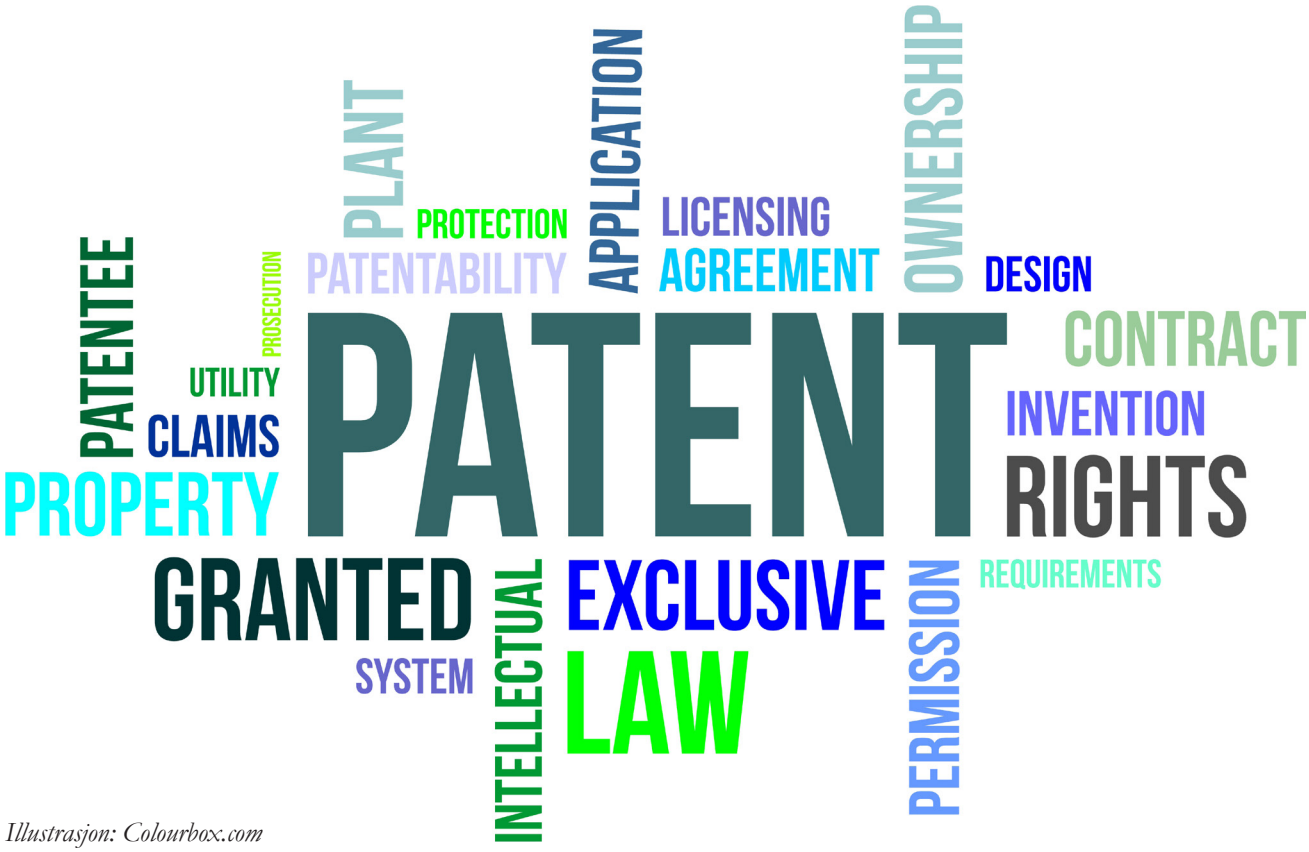
I elgigantén krævede klageren overførsel af domænenavnet »elgigantén.dk« fra indklagede. Indklagede undlod at samarbejde om overførslen, og klagenævnet afgjorde ligeledes, at »elgigantén.dk« skulle overføres til klageren.

I begge sager besluttede Klagenævnet at klagegebyrerne skulle tilbagebetales til klageren.

Læs afgørelserne her: *https://www.domaeneklager.dk/sites/default/files/decision-pdf/2023-0198_elgiganten.dk_.pdf*

Læs afgørelserne her: *https://www.domaeneklager.dk/sites/default/files/decision-pdf/2023-0196_elgigannten.dk_.pdf*

Tue Goldschmieding er partner i Gorrissen Federspiel og en av de danske redaktørene for Lov&Data.



Illustrasjon: Colourbox.com

Selmer

Øystein Kolstad Kvalø

Trussel- og risikovurderinger i 2024: Hvordan påvirkes IT-anskaffelser?

Sammendrag

Artikkelen belyser hvordan oppdaterte trussel- og risikovurderinger fra sikkerhetsmyndighetene påvirker IT-anskaffelser. Sikkerhetsmyndighetene peker på økt risiko fra Kina og Russland, som søker tilgang til kritisk informasjon gjennom leverandørroller. For å håndtere dette, anbefaler NSM grundige risikovurderinger, sikkerhetsklausuler i kontrakter og tettere oppfølging av leverandører.

Samtidig innfører digitalsikkerhetsloven og NIS2-direktivet nye plikter for leverandører av digitale tjenester og samfunnsviktige tjenester. De må gjennomføre risikovurderinger, iverksette sikkerhetstiltak og håndtere leverandørrisiko. Sertifisering av IKT-produkter, -tjenester og -prosesser kan også bli viktig i anbudsprosesser.

1 Hva sier risiko- og trusselvurderingene?

Nasjonal sikkerhetsmyndighet (NSM), Etterretningstjenesten og Politiets sikkerhetstjeneste (PST) kom i midten av februar med sine årlige trussel- og risikovurderinger. Det overordnede bildet viser at trusselsituasjonen er mer alvorlig enn på flere tiår. Sikkerhetstjenestene peker særlig på at Kina og Russland har betydelige interesser i å få tilgang til kritisk informasjon gjennom å være leverandører til norske virksomheter. Kina og Russland har også betydelige interesser i å få tilgang til teknologi utviklet i Norge.

NSMs risikovurderinger peker særlig på at privat næringsliv har fått større betydning for nasjonal sikkerhet som følge av endrede sikkerhetspolitiske og teknologiske utviklingstrekk. Dette skyldes i stor grad utviklingen mot mer komplekse leverandørkjeder, noe det må tas særlig hensyn til. Fremmede trusselaktører går ofte veien om underleverandører for å få tilgang til informasjon fra sitt egentlige mål, ettersom underleverandørene gjerne er mindre aktører og ikke nødvendigvis har det samme sikkerhetsnivået som oppdragsgivere de leverer til.

På denne bakgrunn fremhever NSM at det er viktig at kritisk infrastruktur beskyttes mot innsyn og påvirkning fra fremmede aktører, blant annet ved at anskaffelser ses i sammenheng med nasjonal sikkerhet. NSM erfarer at flere virksomheter ikke gjør gode nok sikkerhetsvurderinger i forbindelse med anskaffelser, og er særlig bekymret for at anskaffelser av teknologi gjør både virksomheter og samfunnet som helhet for avhengig av teknologi fra enkeltland. Dette er en bekymring som har vokst i takt med den økende digitaliseringen av samfunnet.

1.1 Særlig risiko knyttet til Kina og Russland

Etterretningstjenesten mener det er særlig risiko for at kinesiske myndigheter tilegner seg kritisk informasjon fra norske virksomheter, ettersom Kina subsidierer kinesisk næringsliv for å vinne anbudskonkurranser for teknologi i vestlige land. Samtidig pålegger kinesisk lovgivning kinesiske virksomheter å utlevere informasjon til kinesisk etterretning, noe som øker risikoen for at kinesisk etterretning får tilgang til sensitiv eller gradert informasjon som er tiltrodd kinesiske leverandører. Etterretningstjenesten understreker videre at det tar lang tid å bygge opp alternative verdikjeder som er mindre avhengige av enkeltland, og anskaffelser som gjøres i dag kan dermed ha stor betydning i lang tid fremover.

Blant enkeltland er også Russland en aktør med interesser i det vestlige markedet, men Etterretningstjenesten peker på at sanksjonsregimet som følge av krigen i Ukraina har gjort det vanskeligere for Russland å slippe inn i vestlig infrastruktur. Det er likevel risiko for at russiske aktører forsøker å omgå sanksjonsregelverket gjennom innviklede eierskapsstrukturer og

uoversiktlige forsyningskjeder, og at Russlands tilgang på kritisk informasjon i Norge derfor vil være en trussel også fremover.

1.2 NSMs anbefalinger til fremgangsmåte

NSM anbefaler at virksomheter som skal gjennomføre anskaffelser

1) gjør gode risikovurderinger for å ha et grunnlag for hvilke sikkerhetskrav som skal stilles i kontraktene, inkludert å undersøke virksomhetens verdier, sårbarheter og trusler,
2) har personer med kompetanse innenfor anskaffelser, avtaler og helhetlig sikkerhet som deltar i anskaffelsen,
3) tar inn gode sikkerhetsklausuler i kontraktene, og
4) har gode rutiner for oppfølging av leverandørforholdet, blant annet gjennom varsling av endringer i leverandørens eierskapsstruktur og sikkerhetstruende hendelser.

2 Noen utvalgte plikter oppdragsgivere og leverandører er underlagt

2.1 Digitalsikkerhetsloven gir nye plikter til leverandører av samfunnsviktige tjenester og digitale tjenester

Stortinget vedtok før jul i fjor en ny lov om digital sikkerhet (digitalsikkerhetsloven), som gjennomfører NIS-direktivet og cybersikkerhetsforordningen. Leverandører som er underlagt sikkerhetsloven må allerede oppfylle strenge sikkerhetskrav, og må blant annet gjøre risikovurderinger av sine leverandører. Med digitalsikkerhetsloven er flere leverandører forpliktet til å oppfylle lignende sikkerhetskrav. Loven gjelder nemlig for leverandører av samfunnsviktige tjenester innen sektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur, samt for leverandører av digitale tjenester i form av nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester.

Leverandører som er omfattet av loven plikter å gjennomføre risikovurderinger av de nettverks- og informasjonssystemene som benyttes for å levere tjenesten. Videre skal leverandører iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak for å sørge for et sikkerhetsnivå som er tilpasset risikoen ved tjenestene. Digitalsikkerhetsloven gir ikke konkrete plikter rettet mot anskaffelser, men det er grunn til å forvente at både oppdragsgivere og leverandører som er omfattet av loven kommer til å stille krav til leverandører og underleverandører om å ha tilfredsstillende sikkerhetstiltak for å beskytte informasjon i nettverks- og informasjonssystemene. Aktører som er omfattet av loven vil også bli nødt til å gjennomføre strengere risikovurderinger i forbindelse med sine anskaffelser, og dette vil trolig føre til at leverandører blir vurdert mer nøye og grundig enn tidligere.

I lys av sikkerhetstjenestenes risiko- og trusselvurderinger kan oppdragsgivere videre bli nødt til å sørge for at leverandører eller underleverandører fra bestemte land ikke får tilgang til informasjonen i systemene. Oppdragsgivere kan også bli nødt til å hindre at leverandører fra enkeltland dominerer som leverandør i systemene og samlet sitter på en for stor mengde informasjon. I tillegg vil det bli nødvendig for oppdragsgivere å gjøre større anstrengelser for å klare opp i innviklede eierskapsstrukturer og forsyningskjeder. Dette vil være nødvendig for å finne ut hvilke aktører som reelt får tilgang til kritisk informasjon som betros til leverandører.

2.2 Ny felleseuropeisk sikkerhetssertifisering

Digitalsikkerhetsloven gir også forskriftshjemmel for ordninger for sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser, som er en del av gjennomføringen av cybersikkerhetsforordningen.

I forordningen er IKT-prosesser definert som «et sett av aktiviteter som utføres for å utforme, utvikle, levere eller vedlikeholde et IKT-produkt eller en IKT-tjeneste», og IKT-prosesser omfatter altså også aktiviteter i forbindelse med anskaffelse av IKT-tjenester.

Forordningen innfører et felleseuropeisk rammeverk for frivillig sertifisering av IKT-produkter, -tjenester og -prosesser, og i forordningens fortale er det eksplisitt nevnt at den felleseuropeiske sertifiseringen kan gjøre det enklere for selskaper å delta i anbudsprosesser på tvers av landegrenser, fordi selskapene slipper å få produktene sertifisert i flere land. For Norges del innebærer det at sertifiseringsordningen som i dag ligger under SERTIT på sikt vil opphøre. Den felleseuropeiske sertifiseringsordningen kan potensielt få stor betydning for IT-anskaffelser i Norge. På sikt vil trolig flere oppdragsgivere stille krav om sertifisering for å delta i anbudsprosesser, og leverandører som ikke oppfyller kravene kan dermed miste muligheten til å bli vurdert i anskaffelsesprosessen.

2.3 NIS2-direktivet gir plikter til flere leverandører

Digitalsikkerhetsloven har ennå ikke fått sin ikrafttredelsesdato, og det vil allerede være behov for endringer i loven. I november 2022 vedtok nemlig EU NIS2-direktivet, som opphever det forrige NIS-direktivet som digitalsikkerhetsloven gjennomfører. NIS2-direktivet skal være gjennomført i EU innen 17. oktober 2024. I det nye direktivet er virkeområdet utvidet til å inkludere flere sektorer og alle mellomstore og store bedrifter i utvalgte sektorer. Når endringene trer i kraft, vil derfor enda flere leverandører være omfattet av de strenge kravene til risikovurderinger og hensiktsmessige sikkerhetstiltak. Konsekvensene av å bryte regelverket blir også større etter NIS2-direktivet, hvor leverandører kan få bøter opptil EUR 10 000 000 eller 2 % av

global omsetning dersom de ikke overholder pliktene.

Det pågår et løpende lovgivningsarbeid i EU for regulering av sikkerhet i nettverks- og informasjonssystemer, og det er derfor grunn til å tro at både pliktene og gruppen som omfattes av reglene blir ytterligere utvidet i årene som kommer.

3 Hvordan bør oppdragsgivere og leverandører tilpasse seg de oppdaterte trussel- og risikovurderingene og det nye regelverket?

Oppdragsgivere som skal gjennomføre IT-anskaffelser må ta inn over seg sikkerhetsmyndighetenes oppdaterte trussel- og risikovurderinger. Det må vurderes hvilke land de aktuelle leverandørene har forbindelser til, og om anskaffelsene kan bidra til en avhengighet av enkeltland. Et godt utgangspunkt vil være NSMs anbefalte fremgangsmåte for virksomheter som skal foreta anskaffelser, slik disse er beskrevet på NSMs hjemmeside.

Virksomheter som leverer tjenester som faller inn under digitalsikkerhetsloven og NIS2-direktivet bør allerede nå sette seg inn i hvilke plikter de blir underlagt når reglene trer i kraft, og starte arbeidet med å gjøre gode risikovurderinger av sine leverandører og underleverandører. Ettersom det pågår et løpende lovgivningsarbeid i EU, bør også andre virksomheter sette seg inn i regelverket og være forberedt på eventuelle endringer som kan påvirke dem.

Øystein Kolstad Kvalø er advokatfullmektig i Advokatfirmaet Selmer, og bistår klienter med regulatoriske spørsmål innenfor blant annet telekom, teknologi, digitalisering og personvern. Øystein har erfaring fra større regulatoriske prosjekter.

Illustrasjon: Colourbox.com


Wikström & PARTNERS

Christina Wikström og Anton Karlsson

Uppdatering av eSams allmänna villkor för it-tjänster

eSamverkansprogrammet (eSam) har i slutet av november 2023 uppdaterat sina allmänna villkor för it-tjänster. eSam är ett medlemsdrivet samverkansprogram bestående av 38 svenska myndigheter som samarbetar kring digital utveckling, och löpande publicerar it-avtalsvillkor, vägledningar och rättsliga uttalanden. eSam har sedan tidigare publicerat fem allmänna villkor, omfattande it-konsulttjänster, it-drift, it-support, it-projekt och agila it-projekt.

Den nya sekretessbrytande bestämmelsen i 10 kap. 2 a § offentlighets- och sekretesslagen (2009:400) (OSL), som trädde i kraft den 1 juli 2023, innebär att sekretess inte hindrar att en myndighet lämnar ut en uppgift till en enskild eller till en annan myndighet som för den utlämnande myndighetens räkning har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgiften, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut.

Den nya sekretessbrytande bestämmelsen har skapat behov av ett it-avtalsvillkor som reglerar it-tjänster som omfattar ”endast teknisk bearbetning eller teknisk lagring”. eSam har därför valt att anpassa eSams Allmänna villkor för it-drift till begreppet ”endast teknisk bearbetning eller teknisk lagring”, som blir avgörande för om den sekretessbrytande bestämmelsens tillämplighet i samband med utkontraktering av it-tjänster. Utgångspunkten är, efter uppdateringarna, att eSams Allmänna villkor för it-drift är anpassat till it-tjänster som utgör ”endast teknisk bearbetning eller teknisk lagring”, vilket bland annat återspeglas i uppdaterade definitioner, uppdaterad reglering om sekretess och uppdaterad reglering om underleverantörer m.m.

Som en följd av den nya sekretessbrytande bestämmelsen, samt uppdateringar av eSams Allmänna villkor för it-drift, har även behov uppkommit för mindre anpassningar vad gäller eSams övriga allmänna villkor. Dessa it-avtalsvillkor är inte anpassade för it-tjänster som faller inom begreppet ”endast teknisk bearbetning eller teknisk lagring”.

Christina Wikström, advokat och partner, och Anton Karlsson, biträdande jurist, verksamma vid Wikström & Partners Advokatbyrå i Stockholm och specialiserade på IT, IP och dataskydd.

Illustrasjon: Colourbox.com

Gorrissen Federspiel

Tue Goldschmieding

Andet nyt fra Danmark og EU

EU's historiske milepæl: AI Act vedtaget efter langstrakte forhandlinger

Den 8. december 2023 vedtog Europa-Parlamentet og Rådet en politisk aftale om den såkaldte AI Act, fremsat af EU-Kommissionen i april 2021. Forordningen er det første globale regelsæt for regulering af kunstig intelligens på EU-plan og sikrer en ansvarlig udvikling blandt EU-medlemslandene. Forordningen træder i kraft 2 år efter vedtagelsen af EU-rådet og EU-parlamentet, undtagen visse bestemmelser, herunder forbuddene, der træder i kraft efter 6 måneder.

Regelsættet anvender en risikobaseret tilgang, som inddeler AI-systemer i niveauer for henholdsvis lav risiko, høj risiko, uacceptabel risiko samt specifik transparensrisiko. Lavrisikokategorien omfatter flertallet af AI-systemer uden særlige forpligtelser, mens højrisikokategorien pålægger strenge krav som risikominimering, aktivitetslogning, menneskeligt tilsyn, mv. Derudover vil AI-systemer i kategorien uacceptabel risiko omfattes af et totalt forbud, mens kategorien for specifik transparensrisiko bl.a. kræver tydelig mærkning af AI-genereret indhold som ikke-autentisk.

I tilfælde af regelbrud kan virksomheder sanktioneres med bøder, der varierer efter risikoniveau. Forbudte AI-systemer kan sanktioneres med en bøde på 35 millioner euro eller 7% af den årlige globale omsætning afhængigt af, hvilket beløb der er højest. Andre overtrædelser kan medføre bøder på 15 millioner euro eller 3% af den årlige globale omsætning, hvortil levering af ukorrekte oplysninger kan resultere i bøder på 7,5 millioner euro eller 1,5% af den årlige globale omsætning.

Kompetente myndigheder for markedsovervågning vil håndhæve de nye regler på nationalt plan, og vil suppleres på EU-niveau af et nyetableret AI-kontor under Kommissionen.

Læs pressemeddelelsen her: *https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473*

Nye lovforslag til implementering af NIS2, DORA og CER på vej

Den 3. oktober 2023 blev den danske regeringens lovprogram præsenteret. Lovprogrammet indeholdt de lovforslag som den danske regering vil fremsætte i 2024. På det digitale område vil det medføre en række lovforslag, som skal implementere eller gennemføre den fælleskabsretlige regulering på cyberområdet. Hertil hører direktiv (EU) 2022/2555 af 14. december 2022 (»NIS 2-direktivet«) og direktiv (EU) 2022/2557 af 14. december 2022 (»CER-direktivet«) samt forordning (EU) 2022/2554 af 14. december 2022 (»DORA forordningen«), der vil træde i kraft i henholdsvis 2024 og 2025.

I forhold til den danske lov om implementering af NIS 2-direktivet, vil »lovforslaget bl.a. fastsætte krav om gennemførelse af cybersikkerhedsforanstaltninger, hændelsesrapportering samt tilsyns- og håndhævelsesbeføjelser, herunder regler om sanktioner«. Arbejdet med implementeringen af NIS2-direktivet er forsinket, og et lovforslag er planlagt fremsat i oktober 2024.

I forhold til den danske lov der skal implementere CER-direktivet, vil »lovforslaget bl.a. fastsætte krav om gennemførelse af modstandsdygtighedsforanstaltninger, underretning til myndighederne om hændelser samt tilsyns- og håndhævelsesbeføjelser, herunder regler om sanktioner«

Med ændringer i bl.a. lov om finansiel virksomhed »foreslås det bl.a. at fastsætte skærpede krav til risikostyring og rapportering for finansielle datacentraler og it-operatører af detailbetalingssystemer (…)«.

Læs regeringens lovprogram her: *https://www.stm.dk/statsministeriet/publikationer/lovprogram-for-folketingsaaret-2023-2024/*

Læs om lovforslagene og høringslisten her: *https://hoeringsportalen.dk/Hearing/Details/68137*

Regeringen fremlægger et nyt lovforslag, der tildeler Konkurrence- og Forbrugerstyrelsen opgaven med at overvåge onlineplatforme i Danmark

Det danske Folketing vedtog den 14. december 2023 lov nr. 1765 af 28. december 2023 om håndhævelse af

Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester. Loven trådte i kraft den 17. februar 2024. Med loven blev den danske Konkurrence- og Forbrugerstyrelsen (»Konkurrence- og Forbrugerstyrelsen«) udpeget som kompetent myndighed til at føre tilsyn med de online platformes overholdelse af reglerne i Europa-Parlamentets og Rådets forordning (EU) 2022/2065 af 19. oktober 2022 (»Digital Services Act eller DSA«). Konkurrence- og Forbrugerstyrelsen fører således tilsyn med og håndhæver Digital Services Act. Hvis en onlinemarkedsplads ikke overholder reglerne i Digital Services Act, kan klage indgives til Konkurrence- og Forbrugerstyrelsen.

Digital Services Act, der pålagde EU-medlemsstaterne fælles krav, havde til formål at skabe en tryg og sikker færden på internettet, særligt for børn og unge. Kravene omfattede bekæmpelse af ulovligt indhold, beskyttelse af børn online og forhindring af misinformation. Onlineplatforme skulle overholde kravene i Digital Services Act, herunder kravet om begrænsning af spredning af ulovligt indhold. Tilsyn med store platforme som Youtube og Facebook varetages af Europa-Kommissionen i samarbejde med medlemslandene.

Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester supplerede Digital Services Act. Digital Services Act pålagde EU's medlemslande at fastsætte en række nationale regler, der skal supplere bestemmelserne i forordningen og har medført en række krav for onlineplatforme i Danmark, herunder et forbud mod rettet reklame til børn baseret på personoplysninger indsamlet fra børnene. Onlineplatformenes manglende efterlevelse af kravene kan medføre bøder. Desuden indeholdt Digital Services Act regler om udpegning af danske tilsynsmyndigheder, fastsættelse af supplerende regler om tilsyn og regler om håndhævelse og straf. Den nye lov supplerede således reglerne i Digital Services Act om tilsynsbeføjelser og sanktioner. Som DSA-tilsyn er Konkurrence – og Forbrugerstyrelsen blevet tildelt beføjelser, herunder at påbyde udlevering af oplysninger, kontrolundersøgelser, påbudshåndhævelse og udstedelse af bødeforelæg.

Læs hele nyheden her: *Tilsyn skal kunne slå hårdt ned på onlineplatforme | Erhvervsministeriet (em.dk)*

Kampen mod digital svindel styrkes

Det danske Erhvervsministeri meddelte den 13. november 2023, at ministeriet i samarbejde med Finans Danmark, Teleindustrien, Forbrugerrådet Tænk og Ældre Sagen havde søsat en række initiativer, der skal forhindre digital svindel.

Initiativerne består til dels af en sænkelse af bankernes loft over, hvor mange penge, der på egen hånd kan straksoverføres pr. døgn. Beløbsgrænsen sænkes fra et udgangspunkt på 500.000 kr. til et udgangspunkt på 50.000 kr., der kan overføres uden at have kontakt med sin bank pr. døgn.

Teleindustriens bidrag består af et samarbejde mellem teleselskaberne om etablering af mulighed for beskyttelse af afsendernavn i SMS'er, således at det forhindrer svindlere i at kunne udgive sig for at være fra en bank eller en offentlig myndighed.

Læs Erhvervsministeriets meddelelse her *Kampen mod digitale svindlere styrkes | Erhvervsministeriet (em.dk)*

Danmark udnævner Konkurrence- og Forbrugerstyrelsen som koordinator for digitale tjenester

Det danske Folketing vedtog den 14. december 2023 lov nr. 1765 af 28. december 2023, om *håndhævelse af* Europa-Parlamentets og Rådets forordning (EU) 2022/2065 af 19. oktober 2022 (»lov om forordning om digitale tjenester«). Formålet med loven er at styrke og supplere den eksisterende forordning for at sikre effektivt tilsyn og håndhævelse af reglerne i Danmark.

EU's forordning om digitale tjenester sigter mod at skabe et velfungerende indre marked for digitale tjenester, der er sikkert og beskytter fundamentale rettigheder, herunder ytringsfriheden. Den *gælder for diverse digitale tjenester rettet mod EU-brugere, såsom cloudtjenester, onlineplatforme som sociale medier og online markedspladser.* Ifølge forordningen om digitale tjenester, som medlemsstaterne skal implementere senest den 17. februar 2024, skal der udnævnes kompetente myndigheder til at føre tilsyn med overholdelsen af reglerne.

Med loven bliver den danske Konkurrence- og Forbrugerstyrelse udpeget som kompetent myndighed og koordinator for digitale tjenester i Danmark. Dette giver styrelsen mulighed for at håndtere nationale klager og eventuelt føre dem videre til EU-Kommissionen, som kan iværksætte en markedsundersøgelse. Loven indeholder desuden bestemmelser om myndigheders undersøgelses- og håndhævelsesbeføjelser, herunder muligheden for at udstede administrative bødeforelæg for visse overtrædelser. Endeligt bestemmelser om prioriteringsadgang, administrativ rekurs, aktindsigt og undtagelser fra GDPR.

Loven trådte i kraft den 1. februar 2024.

Læs lovforslaget som vedtaget her: *https://www.ft.dk/ripdf/samling/20231/lovforslag/l60/20231_l60_som_vedtaget.pdf*

Læs det danske erhvervsministeriums pressemeddelelse om loven her: *https://em.dk/aktuelt/nyheder/2023/okt/regeringen-udpeger-dansk-vagthund-til-at-toejle-tech-giganter-*

Tue Goldschmieding er partner i Gorrissen Federspiel og en av de danske redaktørene for Lov&Data.

LOVDATA

Produksjon: Aksell AS