SIGN UP

PANGEANET

INTERNATIONAL NETWORK OF INDEPENDANT LAW FIRMS

VISIT OUR WEBSITE

NEWSLETTER 5

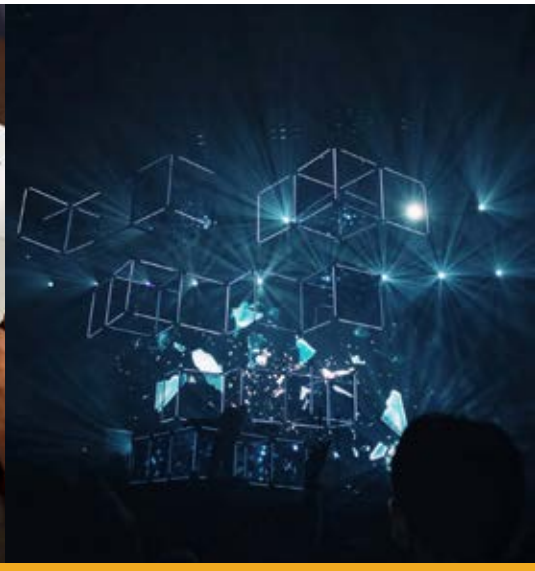
May 2023

DATA, INFORMATION & CYBER LAW

PangeaNet is an association of independent law firms from over 23 countries forming an international law firm network. The Pangea Practice Group for Data, Information and Cyber Law (DICL) consists of experts in IT, data protection law, privacy, cybersecurity and open data issues. We support your digital transformation and guide you in the protection, use and defence of your immaterial assets from a legal perspective.

A multi-jurisdictional experts approach

A group of specialists familiar with their respective local laws and customs



A real curiosity and appetite for the latest technological developments & phenomena

EDITORIAL

IT WOULD BE IMPOSSIBLE TO IGNORE THE RISE OF AI OVER THE PAST FEW MONTHS

With Chat GPT taking most of the headlines but facing competition from Google's Bard and from Amazon and Facebook's own AI offers.

With AI taking the headlines of the day it's easy to forget about some of the other news stories that were (and may yet be) the next big thing, whether that be the continued evolution of the GDPR, the rise of the Metaverse or the implementation of new laws around digital services.

It's a challenging time to be a data lawyer – with lots of potential distractions. In this issue, we've picked up various of these ongoing themes, taking the perspective of different jurisdictions.

They include:

- **The Metaverse** – after all, it takes something significant for a company like Facebook to change its name – Laurent Badiane and Matthieu Bourgeois pick up what's going on in the Metaverse
- "**Erasure**" is not only a 1980s British pop group famous for "A little respect" - but also a fundamental right under GDPR. The right of an individual to have their personal data deleted was tested in the courts of Belgium – as Michiel Beutels of Litiguard law firm explains in his article.
- **AI Art** – don't tell me you've not asked AI software Mid Journey for pictures of Mickey Mouse in the style of Salvador Dali? The thing is, you'll likely get what you ask for, despite the obvious copyright issues involved. Julia Mascini of Valegis looks at the issues of copyright and AI art.
- **Pre-Ticked boxes** – how dare you take my consent for granted?! Julia Bhend of Probst Partner AG looks at the issues of Privacy by design and its application to Swiss law.
- **The Digital Services Act** - this puts specific obligations on large online platforms and the reporting of recipients – Jeanne Kelly and Raymond Sherry of Browne Jacobson (Ireland) look at this.
- **Automated Face Recognition Technology** – the UK is estimated to have around 6 Million CCTV cameras spying on its data subjects (only China, the USA and Germany have more). Now the UK regulator has approved in principle the use of live "face recognition" technology – how close are we to George Orwell's dystopian "1984"? I've picked up that theme in our final article.

Richard Nicholas
Browne Jacobson LLP, United Kingdom

Index

• FRANCE

Metaverse - time for reflection!

The Metaverse seems to be the latest buzzword in the tech era. Similarly to other emerging technologies, Metaverse technologies raise new legal issues and risks. What exactly is the Metaverse? In the article, we explore the Metaverse history and the legal issues that it may give rise to.

A hot topic.

It is the new buzzword in the world of Tech, but also within the large and emblematic companies that have recently announced their positioning in the metaverse:

- Nike: with the launch, in April 2022, of a pair of virtual trainers – associated with a non-fungible token (NFT) – that can be worn by an avatar
- Axa: with the opening in the metaverse of an insurance agency affiliated to the Axa network, in March 2022
- Louis Vuitton: with the launch, in 2021, of a video game retracing the history of the brand and enabling players to buy virtual items to dress their avatar

The digital industry has not been outdone and is also making substantial investments in this area: Microsoft, for example, announced in early 2022 that it is in the process of buying Activision Blizzard (publisher of "Call of Duty" and "Warcraft", immersive video games that are considered as precursors of the metaverse) for nearly $69 billion, and Meta (formerly Facebook) invested $10 billion in 2021 in metaverse technologies.

To understand this craze, we need to look at the estimated revenues that could be generated by the metaverse economy (known as "metanomics" – the combination of the terms "meta" and "economics"): nearly $5 trillion by 2030 (according to a McKinsey study published in June 2022).

The metaverse: a long history.

Originating from science-fiction (the fantasy of a fusion between the real/natural world and virtual/artificial worlds, which would make it possible to improve our capacities by better satisfying our desires), the concept of the metaverse (a term dating back to 1992, when it was used in the novel "Snow Crash" by Neal Stephenson) found its first significant incarnation in "Second Life", a massively multiplayer online game launched in 2003, which was quickly challenged by the then emerging social networks.

A concept that is still nebulous, with uses to be invented.

In this period of fervour, largely maintained by the Tech giants who are attempting to promote their investments in the area, the metaverse is touted as:

(1) being virtual (digital),
(2) being synchronous (events take place in real time, with zero latency),
(3) having no limit (especially in terms of the number of users),
(4) being persistent (it cannot be reset, paused or stopped),
(5) having its own economic system (users can buy digital goods, and often pay for them via a crypto-currency that is sometimes specific to the platform),
(6) being immersive (thanks to the use of connected devices such as headsets or bracelets for example, which enable a digital twin - called an avatar - to follow the movements of the user who controls it and who, in return, will perceive certain sensations resulting from events taking place in this virtual universe), and
(7) plural (there is not only one but several metaverses, which are not natively interoperable).

Among these characteristics, only the last two truly distinguish the metaverse from the Internet (the latter being equally digital, synchronous, having unlimited users, persistent and having its own economy): its immersive nature and its plurality. On this last point, the big challenge for the metaverse(s) will be to be interoperable, in order to maintain the greater logic of openness that presided when the Internet came into being. The main uses of the metaverse imagined to date are still in their infancy: leisure (concerts, games, cultural exhibitions, theme parks, etc.), professional activity (daily remote work, professional training, etc.), new ways of marketing products/services (such as improving the customer experience by testing products or services via virtual visualisation), creation of new sources of revenue (with, for example, digital goods such as NFTs, a kind of "digital twin" of physical goods, provided upon purchase of the latter).

> BEFORE A "METAVERSE ACT", WE SHOULD APPLY THE LAW TO THE METAVERSE, WITHIN WHICH DATA PROTECTION IS KEY.

Before a "Metaverse Act", we should apply the law to the metaverse, within which data protection is key.

Voices are already being raised to question the law that will apply to the metaverse(s), a bit like for the Internet, which - in the early 2000s - raised similar questions. It is as if common law did not a priori have a natural vocation to be applied. These same voices wonder whether the metaverse is subject to criminal law [with its offences of damage to property (theft, fraud) or to people (violence, harassment, etc.)], to civil law (respect for private life, etc.), to contract law and consumer law, or even to civil liability law. On reflection, the challenge for legal professionals will be to show imagination and creativity in the exercise of legal qualification, by mobilising the arsenal of existing texts, before calling too quickly for the adoption of new texts (one or more "Metaverse Acts"). In any event, one thing is clear: data protection will be key in metaverses, where all interactions between avatars (conversations, transactions, etc.) will generate digital data. More than ever, the logic of impact analysis, introduced by the GDPR, is relevant.


Laurent Badiane & Matthieu Bourgeois
Partners, klein • wenner
In charge of the Intellectual Property and Digital Law Team

The Belgian Data Protection Authority acts swiftly regarding complaints relating to requests for data erasure

On 9 February 2023, the Belgian Data Protection Authority issued a decision (09/2023) against a data controller for failing to comply with a request to erase personal data from a data subject. The case concerned unsolicited advertising emails sent by the data controller to the data subject's email address. The data subject had requested the erasure of his email address on 9 and 14 November 2022, but the data controller did not comply, and the data subject received more unsolicited advertising emails on 16 January 2023.

As early as 31 January 2023, the complaint that was filed on 16 January 2023 is declared admissible by the Front Office and transferred to the Litigation Chamber of the Belgian Data Protection Authority.

> THE DECISION HIGHLIGHTS THE IMPORTANCE OF COMPLYING WITH DATA SUBJECTS' REQUESTS TO EXERCISE THEIR RIGHTS UNDER THE GDPR.

The (Litigation Chamber of the) Belgian DPA concluded in its decision that the data controller had violated Articles 12(3) and (4) and 17(1) of the GDPR by not complying with the data subject's request to erase his personal data.

Under Article 12(3) of the GDPR, data controllers must respond to data subjects' requests for access, rectification, erasure, or restriction of processing within one month of receiving the request, while article 12(4) of the GDPR requires them to inform data subjects without delay if they cannot comply with the request and provide reasons for their decision. Article 17(1) of the GDPR gives data subjects the right to request the erasure of their personal data when the data controller no longer needs the data for the purposes for which it was collected, and there is no other legal ground for processing it.

The Belgian DPA ordered the data controller to erase the data subject's personal data within 30 days of the notification of the decision and warned the data controller that it would face an administrative fine of up to 20 million or 4% of its total worldwide annual turnover if it failed to comply. The data controller must also inform the data subject of the erasure and take steps to prevent further processing of his personal data.

The decision highlights the importance of complying with data subjects' requests to exercise their rights under the GDPR. Failure to comply with data subject rights can result in significant administrative fines and reputational damage to the data controller. Data controllers should have clear procedures in place to respond to data subject requests promptly and should train their staff on how to handle such requests.

The present decision is a prima facie decision rendered by the Litigation Chamber on the basis of the complaint filed by the complainant, under the "procedure prior to the decision on the merits". That procedure allows the Belgian DPA to act quickly if a complaint is made. Given the importance of transparency regarding the decision, the decision was published on the website of the Belgian DPA.

Michiel Beutels
Litiguard

THE NETHERLANDS •

AI art: creative invention or infringement?

In America, a group of visual artists has gone to court seeking an end to the use of their art by AI art generators Stability AI, DeviantArt and Midjourney. They are also demanding damages: as much as $5 billion, equivalent to $1 per inferred AI work. The visual artists' legal representation states that the generators use "21st century collage tools remixing copyrighted work by millions of artists"[1].

American artists are not alone in their criticism against this form of artificially generated art, which is offered online (and in many cases: for free) by many parties worldwide. Legal case law is hardly there yet. How would a Dutch judge handle a situation like this?

Is the artwork copyrighted?

The first question that will have to be answered is whether the original work of art used in the creation of the AI art is protected by copyright. According to established case-law of the Court of Justice of the

[1] *L. Verhagen, "Kunstenaars starten rechtszaak: kunstmatige intelligentie maakt inbreuk op ons auteursrecht", deVolkskrant, 16 January 2023.*

European Union, this is the case when that work
(i) is an "intellectual creation of the artist" (read: not derived from another work) that
(ii) reflects the "personality of the artist and is expressed through the free creative choices of that artist in its creation".

The workability of this rule of law and legal certainty for users also require that the work of art can be identified with sufficient accuracy and objectivity. Technically necessary or function-driven decisions do not qualify for protection, as they must remain available to all.

> WHO IS RESPONSIBLE FOR THE WORK ARBITRARILY CREATED BY AN AI ART GENERATOR?

The author's exclusive right to reproduce and disclose a work

If the work of art is protected by copyright, its creator may (subject to legal exceptions) prohibit others from reproducing and/or publishing reproductions of this work without his or her permission.

We speak of a "reproduction" of an original work if the overall impressions of that work, prompted by the copyrighted traits, are so similar to those of the derivative work that the derivative work cannot be considered original. In other words: imitation.

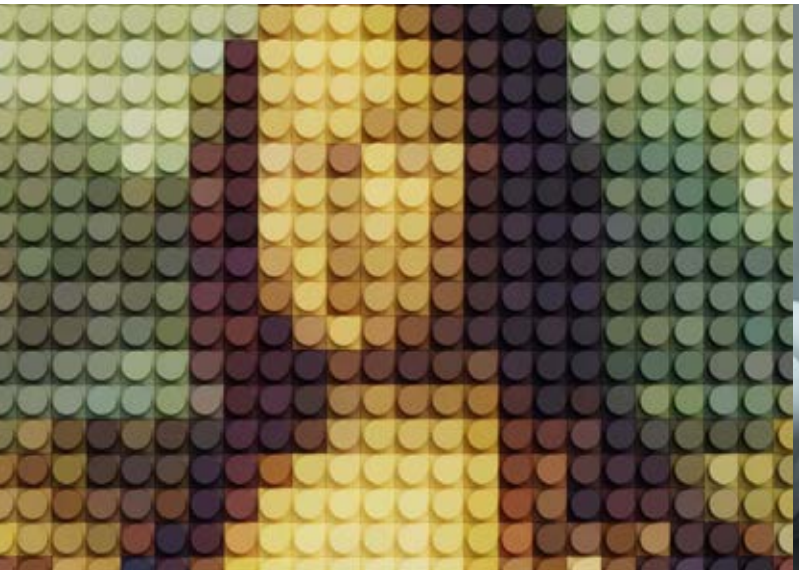
What can you do against an AI art generator?

Looking at the final product, AI art, where the derivative work is usually the result of a combination of a large number of works, the burden of proof could still present quite a challenge. After all, abstract styles, trends and ideas as such cannot be monopolised through copyright. So the artist will really have to compare his concrete individual works with the AI work. And then there is the question: who is responsible for the work arbitrarily created by an AI art generator?

It would be faster and simpler if the operator of the AI art generator - as I deduce from the above-mentioned statement of the authors' lawyers - uses a database of (protected) works of art by third parties to operate this software. After all, it is easy to imagine that the operator, when creating that database (which is nothing but a collection of 1-to-1 copies), is already performing acts that can be regarded as "reproduction" of original works within the meaning of the Copyright Act, against which the creators of the latter works (or their later assignees) can exercise a right of prohibition.

We await developments in this area with interest!

Julia Mascini
Valegis Advocaten



Pre-ticked boxes and opting-out under the new Swiss Data Protection Act

Under the current protection law in Switzerland, it is permitted that control settings on a website or app for personalization or analytics functions that the provider performs based on the users' personal data are defaulted on, if the principle of transparency is adhered to. For example, obtaining and analysing data on consumer habits based on purchases made in a webshop is lawful as long as the processing of the user's data for the proposed purposes (e.g. personalization and analytics) has been made transparent for the user before the data is obtained.

On 1 September 2023, the fully revised Swiss Federal Data Protection Act of 25 September 2020 ("nDPA") and the new Data Protection Ordinance of 31 August 2022 ("nDPO") will enter into force. While the basic concept and principles of Swiss data protection law remain unchanged, the new law introduces new obligations and concepts following the standards of the EU-GDPR. One of these new concepts is the concept of "privacy by default": The controller is bound to ensure through appropriate pre-defined settings that the processing of the personal data is limited to the minimum required for the purpose, unless the data subject directs otherwise.

> "THE QUESTION ARISES WHETHER PRE-TICKED BOXES, OPTING-OUT CHOICES AND SIMILAR SETTINGS WILL STILL BE LAWFUL UNDER THE NEW CONCEPT OF "PRIVACY BY DEFAULT".
>
> Julia Bhend
> *Probst Partner AG*

The question arises whether pre-ticked boxes, opting-out choices and similar settings will still be lawful under the new concept of "privacy by default".

As this principle is not yet applicable in Switzerland, there is no guidance or case law available yet, and it is not clear how this principle will be interpreted in practice. What seems to be clear is that the principle of "privacy by default" does not require that a system or tool can be used without any personal data being processed or with only those required for the main functionality (e.g. only for purchases in a webshop). Neither is the provider of a service or tool required to offer users choices. If he does not offer the user any (technical) options for self-controlling data processing, it cannot make any default settings and the privacy by default obligation does not apply.

Where the provider does offer options, there is a controversial discussion as to whether implicit consent, pre-ticked boxes, opt-out options or similar settings are still possible at all or whether the concept of privacy by default requires opt-in whenever a choice is possible.

The Federal Data Protection and Information Commissioner ("FDPIC") stated that "privacy by default protects users of private online services who have not considered the terms of use or the rights to objection that these terms contain, by ensuring that only the data that is absolutely necessary for the intended purpose is processed, as long as users do not actively authorise further processing."

This statement is not really clear. It can be argued that it is still lawful to have defaulted settings (such as pre-ticked boxes) that are not the least intrusive settings as long as the user is provided with a choice of settings when registering for an online service, because in this case the objection right is actually granted and the user has made an active choice if he/she does not change the settings. If, on the other hand, the user can skip the settings without having made a choice (by confirming or changing it), the default setting must correspond to the minimum.

Julia Bhend
Probst Partner AG

Update on the Digital Services Act – Important Dates and Deadlines Looming

How is the definition of "online platforms" likely to be interpreted?

The DSA is structured to have special obligations for very large platforms which have a greater impact on society, and lesser obligations on smaller platforms. The obligations on "online platforms" in the middle of this sliding scale of small to large platforms will form the new bedrock of what is expected in the general sense of most platforms under the DSA. The definition of "online platform" is therefore quite broad, and the EU Commission is likely to encourage a broad interpretation of the Regulation given the narrative surrounding the DSA. The recitals to the DSA also make clear that the EU Commission is trying to standardise and harmonise regulation on online platforms across the internal market.

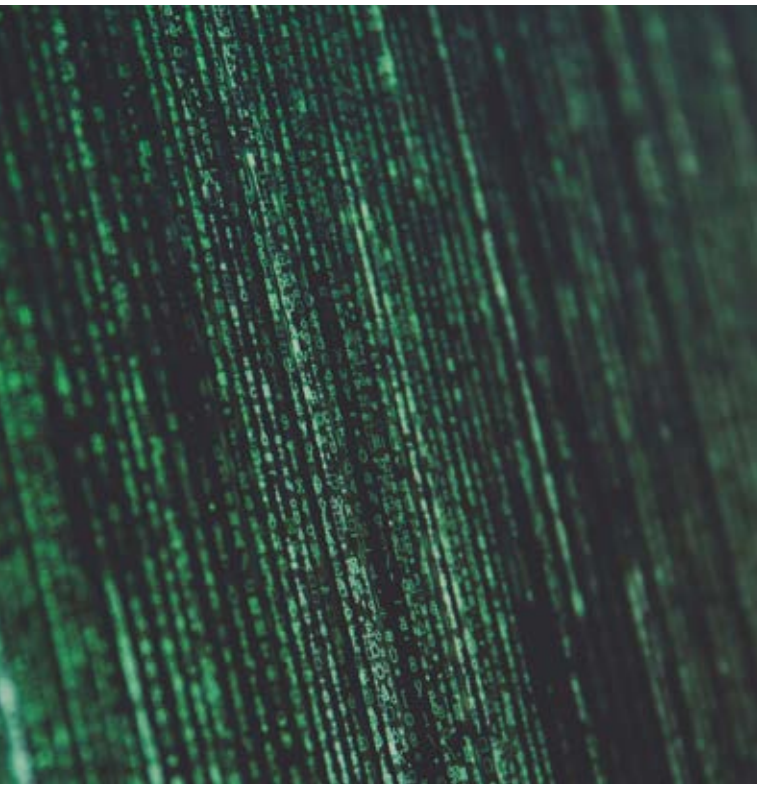
Exceptions

There is an exception to the definition of "online platforms" applying and this should be carefully explored before committing on a particular compliance path with the DSA.

A platform will not be an "online platform" within the meaning of the DSA where it meets the following cumulative criteria:

1. where an activity is a minor and purely ancillary feature of another service and
2. for objective and technical reasons, the ancillary feature cannot be used without that main service; and,
3. the integration of the feature into the main service is not a means to circumvent the applicability of this Regulation.

Care is needed in navigating this exception. One example given of an appropriate exception falling within the three parts above is the comments section in a newspaper. This would, in principle, fall within this exclusion on the basis that the newspaper website is hosting the content, and the comments section is merely providing the ancillary service of commenting on the news content provided.
If you are unclear as to whether your platform may come within the DSA or the exception above, our team is on hand to assist.



Key Requirements for "online platforms".

Online platforms had until 17 February this year to report their average number of active recipients (AMARs). This will facilitate the designation of "very large online platforms" (platforms exceeding 45 million reach). This figure is to be calculated as a six-month average. There is also an obligation to update this information at least once every six months, or more frequently for rapidly scaling platforms.

The DSA provides that the number of average monthly active recipients of an online platform should reflect all the recipients which are:

- engaging with the service at least once in a given period of time;
- exposed to the information disseminated on the online interface of the online platform; or
- providing information, such as traders on an online platform allowing consumers to conclude distance contracts with traders.

Calculating the total number of AMARs will no doubt present practical difficulties, particularly in regard to what constitutes exposure to and use of a platform. Online platforms will have to be careful in order to avoid unintentionally over or under reporting AMARs.

> "THE OBLIGATIONS ON "ONLINE PLATFORMS" IN THE MIDDLE OF THIS SLIDING SCALE OF SMALL TO LARGE PLATFORMS WILL FORM THE NEW BEDROCK OF WHAT IS EXPECTED IN THE GENERAL SENSE OF MOST PLATFORMS UNDER THE DSA.

Commission Guidance on AMARs

The DSA states that the Commission can adopt delegated acts to supplement the DSA, this includes a methodology for calculating the number of average monthly active recipients of the service in the EU. Apparent headway is being made on that guidance, and on 24 January 2023, the Commission delivered a webinar to national authorities on the designation of very large online platforms. Commission guidance is still not published however, and until concrete guidance is provided, online platforms will have to create and adopt their own methodology to determine their AMAR reporting.

In selecting a methodology to calculate AMARs, it is important that online platforms keep a detailed record of the data utilised and should be able to justify the methodology adopted. It may be advisable for online platforms to seek external legal advice in determining the methodology behind and the limits of this calculation, given that it will be the basis of much of a platform's approach to compliance with the new DSA regime.

Jeanne Kelly & Raymond Sherry
Browne Jacobson

Face Recognition and CCTV

"Springwatch" – is a BBC documentary series in which cameras are left filming in the wild waiting for something interesting to happen.

In urban settings in the UK you'll also find (CCTV) cameras left recording to see what shows up, but those cameras are trained specifically on humans and where they congregate (e.g. shopping centres, supermarkets) and going about their daily business, foraging for food in supermarkets, forming orderly queues, getting into fights...

What's different about more recent CCTV technology however is that, when linked to the right database of human faces, they can identify individuals in real time (i.e. the CCTV will identify and verify faces in crowds against a database - rather than simply passively recording footage that could be interrogated later).

Specifically these cameras are looking out for "Subjects of Interest" (humans pre-identified as potential criminals) to show up and be instantly identified and tracked as they appear using state of the art facial recognition cameras. By relying on a network of such cameras an operator could potentially find an individual anywhere in the UK the moment that they show up on camera and track their movements from place to place.

What does the Information Commissioner's Office say about this apparently intrusive invasion of privacy?

Actually it's relatively relaxed. Last week it dropped its investigation into Facewatch Limited, a company behind this technology (indeed if you look on Facewatch's website now you'll see its boast of being found "Fully compliant" by the ICO), comfortable that the "Legitimate Interest" could potentially be relied upon to justify the use of technology.

> "SPECIFICALLY THESE CAMERAS ARE LOOKING OUT FOR "SUBJECTS OF INTEREST" (HUMANS PRE-IDENTIFIED AS POTENTIAL CRIMINALS) TO SHOW UP AND BE INSTANTLY IDENTIFIED AND TRACKED AS THEY APPEAR USING STATE OF THE ART FACIAL RECOGNITION CAMERAS

So what does that mean for face recognition cameras in the UK?

There have been other decisions on live face recognition of course and guidance that those wishing to use it will need to comply with - but the decision by the ICO to drop its investigation would suggest that, like many other technologies that we have become accustomed to (body scanning at airports, Automatic Number Plate Recognition, CCTV cameras everywhere) now it would seem we might need to get used to the idea that those cameras may have built in face recognition technology.

From the perspective of an in house lawyer however (or someone tasked with deciding if the use of face recognition is appropriate) the question is likely to be whether or not the underlying database was collected and used correctly and on what basis the "person of interest" is decided.

Since first writing this article a retailer in the UK has received high profile complaints about its use of live face recognition technology in stores and the way that it was used by staff. Proof that – even if you do get the law right (i.e. you get the correct legal grounds, carry out a DPIA and LIA and follow the regulator's guidance), you still need to bear in mind what the consequences could be for the reputation of the business in the minds of the (privacy-conscious) public.

Richard Nicholas
Browne Jacobson

DATA, INFORMATION & CYBER LAW

Members & Contacts

Laurent Badiane
klein • wenner
19 rue Danielle Casanova, 75001 Paris, France
T: +33 1 44 95 20 00
E: laurent.badiane@kleinwenner.eu

Michiel Beutels
Litiguard Law Firm
Tabakvest 52-54, 2000 Antwerpen
T: +32 (0)3 205 68 40
E: mb@litiguard.eu

Julia Bhend
Probst Partner AG
Bahnhofplatz 18, CH-8401 Winterthur, Switzerland
T: +41 52 269 14 00
E: julia.bhend@probstpartner.ch

Matthieu Bourgeois
klein • wenner
19 rue Danielle Casanova, 75001 Paris, France
T: +33 1 44 95 20 00
E: matthieu.bourgeois@kleinwenner.eu

Theresa Castelan
klein • wenner
19 rue Danielle Casanova, 75001 Paris, France
T: +33 1 44 95 20 00
E: theresa.castelan@kleinwenner.eu

Jeanne Kelly
Browne Jacobson
6-7 Fitzwilliam Square East Dublin 2D02 Y447 Ireland
T: +35315743915
E: jeanne.kelly@brownejacobson.com

Marta Margiocco
Cocuzza & Associati Studio Legale
Via San Giovanni Sul Muro 18, 20121 Milano, Italy
T: +39 02-866096
E: mmargiocco@cocuzzaeassociati.it

Julia Mascini
Valegis Advocaten
Apollolaan 151, 1077 AR Amsterdam, The Netherlands
T: +31 (0)6 82 13 53 62
E: j.mascini@valegis.com

Michał Matuszczak
Babiaczyk, Skrocki i Wspólnicy Sp. K
ul. Wyspianskiego 43, 60 – 751 Poznan, Poland
T: +48 61 8441 733
E: m.matuszczak@bsiw.pl

Sebastian Meyer
BRANDI Rechtsanwälte
Adenauerplatz 1, 33602 Bielefeld, Germany
T: +49 521 96535 812
E: sebastian.meyer(at)brandi.net

Razvan Miutescu
Whiteford
7 St. Paul Street, Baltimore, MD 21202-1636, USA
T: +1 410 347 8744
E: rmiutescu@whitefordlaw.com

S. Keith Moulsdale
Whiteford
7 St. Paul Street, Baltimore, MD 21202-1636, USA
T: +1 410 347 8721
E: skmoulsdale@whitefordlaw.com

Tomáš Mudra
UEPA advokáti s.r.o.
Voctárova 2449/5, 180 00 Prague, Czech Republic
T: +420 234 707 444
E: TMU@uepa.cz

Richard Nicholas
Browne Jacobson
103 Colmore Row, Birmingham B3 3AG, The UK
T: +44 1 21 237 3992
E: richard.nicholas@brownejacobson.com

Natascha Niewold
Valegis Advocaten
Apollolaan 151, 1077 AR Amsterdam, The Netherlands
T: + 31 (Q)6 12 11 61 77
E: n.niewold@Valegis.com

READ OUR ANNUAL REPORT 2021/2022

CONNECT WITH US

PANGEANET
INTERNATIONAL NETWORK OF INDEPENDENT LAW FIRMS

To find our other publications and newsletters

CLICK HERE

Email: info@pangea-net.org
Website: www.pangea-net.org
Linkedin: /company/pangeanet