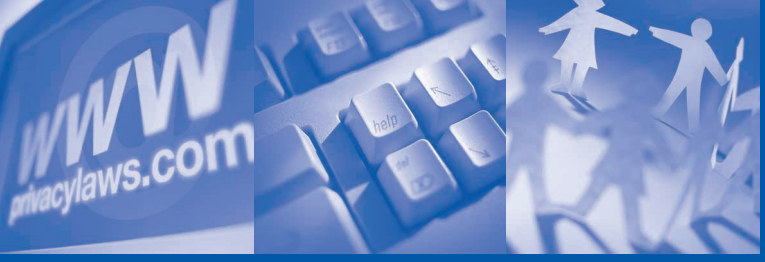


ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Non-material damages for data violations in Germany

Lea Stegemann of Noerr PartGmbB and **Jakob Horn** of Taylor Wessing LLP provide an overview of German case law on non-material damage claims.

The GDPR, with Article 82, explicitly introduced claims for non-material damages ("emotional damages") for data protection violations. In Germany, there are already thousands of court proceedings in which individuals claim non-material damages. Hence, data protection violations are increasingly being pursued not only by public but also by private enforcement, and claims for damages are becoming a

Continued on p.3

France: CNIL sanctions Orange with a hefty fine for ads appearing as emails

Zero-tolerance approach towards Orange's direct marketing practices. By **Nana Botchorichvili** of IDEA Avocats, France.

On 14 November 2024, France's Data Protection Authority (CNIL) issued a fine of €50 million against Orange, France's leading telecommunications operator, for displaying advertising messages in customer email inboxes without their prior consent[1].

Indeed, as part of its Internet, mobile and fixed phone services,

Continued on p.5

Issue 193 **FEBRUARY 2025**

INTERNATIONAL report

ISSUE NO 193 FEBRUARY 2025

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Nana Botchorichvili
IDEA Avocats, France

Jonathan Mendoza Iserte and Jesús Javier Sánchez García
INAI, Mexico

Sergio Maldonado
Privacycloud, US/UK

Lea Stegemann
Noerr PartGmbB, Germany

Jakob Horn
Taylor Wessing LLP, Germany

Roald Chao
International business law graduate, QMUL, UK

Annelies Moens
Privcore, Australia

Xawery Konarski and Mateusz Kupiec
Traple Konarski Podrecki & Partners, Poland

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.
Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Change gathers pace in 2025

The international privacy community has been surprised by news about a new Chinese open source AI large language model Deep Seek. According to the BBC, OpenAI says that Chinese and other companies are "constantly trying to distil the models of leading US AI companies". From the Deep Seek user perspective, the question is about data security.

US President Donald Trump's executive orders affect privacy in the US and elsewhere, for example terminating the membership of the Democratic members of the Privacy and Civil Liberties Oversight Board with immediate effect. At a conference in Brussels on Data Protection Day, 28 January, organised by the European Data Protection Supervisor, the Privacy Salon (CPDP) and the Council of Europe, Marina Kaljurand, 1st Vice-President of the European Parliament's LIBE Committee, declared in the context of the GDPR and the Law Enforcement Directive, this decision is "not what we expect from an ally." Irena Moozová, Deputy Director-General for Justice and Consumers at the European Commission added "the EU won't be shy to use provisions we have available."

The message from politicians and privacy advocates was loud and clear: the EU will retain and defend its privacy principles and values. The main EU-wide task is now to oversee the implementation of the EU Digital Services Package (p.27) of data related legislation and continue work on the GDPR to ensure more consistency in enforcement. Karolina Mojzesowicz of the EU Commission confirmed again that the GDPR will not be reopened – she stressed that "solutions are embedded in the GDPR itself" due to its flexibility. The regulation on procedural rules that is expected soon is an example of this type of adjustment.

While Mexico is abolishing its independent Data Protection Authority (p.8), privacy principles are becoming more firmly established elsewhere. Malaysia's Personal Data Protection Act has been strengthened to significantly increase the powers of the regulator and strengthen individuals' rights (p.20) and South Korea has adopted an AI law (p.14).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura@privacylaws.com.

Germany... from p.1

growing risk for companies. There are already several hundred published judgments on non-material damage claims, forming a solid body of German case law.

To get a clearer picture, we have quantitatively analysed this German case law. Our study shows the extent to which German courts allow or reject claims and the factors on which these decisions depend. It can provide practitioners with an initial impression of the actual financial risk that damage claims may pose for companies following a data protection violation in Germany. Courts in other member states where there is not as much case law available might take guidance from German jurisprudence. At the same time, recent rulings from the European Court of Justice and the German Federal Court of Justice suggest that the case law presented here is likely to evolve further.

Drivers of private enforcement in Germany

Compared to other EU member states, Germany has a particularly high number of lawsuits in which plaintiffs seek non-material damages under Art. 82 GDPR. Normally, people in Germany often have a rational disinterest in pursuing rather small claims in court, as the financial risk is relatively high in these cases. In data protection cases, however, more people decide to take legal action because a number of plaintiff-oriented law firms offer financially attractive enforcement options. These firms specifically seek out claimants with legal expenses insurance, which covers litigation costs for insured claimants, allowing claimants to pursue their claims in court without financial risk. Alternatively, these firms work with litigation funders, who underwrite the risk of legal costs in exchange for a share of any successful claims.

Many of the plaintiff-focused firms were set up to pursue claims in the Volkswagen emissions case. These firms have now expanded into other fields, such as data protection cases. These law firms advertise their services aggressively with big promises and thus reach many people who might not have thought of enforcing their claims themselves.

Since the implementation of the EU Representative Actions Directive, qualified entities can also sue directly for damages on behalf of consumers. In December 2024, the first collective action for compensation in a data protection case was filed against Meta Platforms Ltd.[1]

The examined decisions

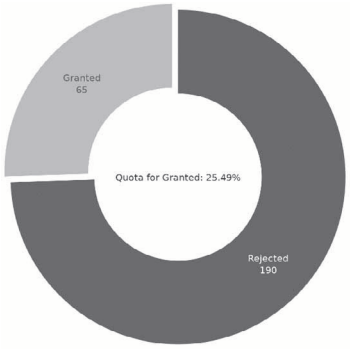
In Germany, there are hundreds of published decisions on non-material damages following data protection violations. At the end of August 2023, we created a dataset with published decisions and analysed them using quantitative analyses. The oldest decision in the dataset dates from 7 November 2018,[2] the most recent from 15 August 2023.[3] The decisions come from courts all over Germany.

The dataset comprises of 255 published[4] decisions, collected on the basis of the Noerr Damages Tracker[5], which is co-managed by author Stegemann. The majority of these cases concern damages claims under Art. 82 GDPR, but some also concern related claims.[6]

Of the 255 decisions, most are judgments and some are orders, such as procedural or legal aid orders. The majority of decisions are first instance decisions of district courts (178 judgments) and appeal decisions of higher regional courts (73 judgments). Some decisions were also handed down by local courts and labour courts. In 34 cases there are several decisions on the same case from different types of court.

The courts have published more judgments every year. While courts only published two judgments in 2018, there were already 86 in 2023.

FIG.1: CLAIMS GRANTED / REJECTED



Any decision in which the awarded amount is greater than zero, regardless of the claim amount, is considered as granted.

It is important to note that only manually researched and published decisions could be included in the dataset. It is therefore possible that not all decisions published by the end of the collection period were found. In addition, the number of unpublished judgments is likely to be high, as in Germany only about 1% of first instance judgments are published.[7]

Therefore, the results presented here cannot claim to be absolute; they must be seen in light of the problem that the authors are unable to resolve: Germany's restricted publication practice limits the accuracy of quantitative analyses.

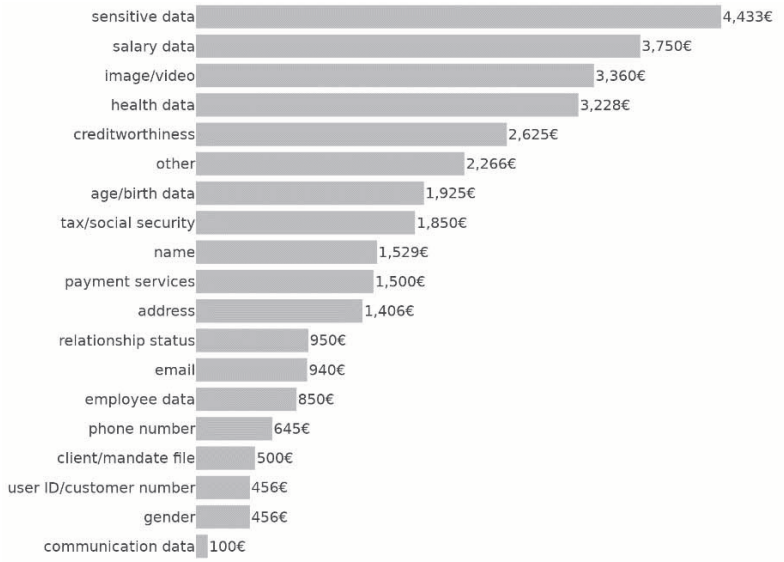
Nevertheless, the analysis is of value to practitioners. It provides an overview of damages awarded, as far as possible within the available data, and offers a broader perspective than the common practical approach of examining isolated decisions found more or less by chance.

Proportion of claims dismissed and claims granted

To help practitioners assess the risk posed by non-material damage claims to a company, it is important to understand how often courts grant such claims at all. In nearly three-quarters of the cases analysed, courts fully dismissed the claim, setting the awarded damages at zero. In other words, a 'high-level' overview of published case law suggests that the likelihood of a defendant actually being liable for damages when a claim is filed is approximately 25%.

A deeper understanding of the high dismissal rate emerges from the reasons given for rejecting claims. Two main observations can be noted here: The vast majority of claims are dismissed because either no damage or no violation of the GDPR could be proven (approximately 95 cases each; in some cases both the lack of a violation of the GDPR and the lack of damage were cited). Other reasons for dismissal, such as the inapplicability of the GDPR or not passing the threshold of seriousness[8] add up to 32 cases. Thus, it appears that it is difficult for the affected individuals to meet the burden of proof for both the violation of the GDPR and the damage. The case law of the CJEU is likely to make this even more challenging, as it explicitly states

FIG.2: MEAN DAMAGES AWARDED BY CATEGORY



Cases can be part of multiple bars if several data categories are affected by a single violation.

that a violation of the GDPR alone is not considered damage; damage must be proven separately.

Amount of damages awarded

For companies wanting to conduct a risk assessment, it is also relevant to consider the average amount of damages that courts award when they rule in favor of the plaintiff. On average (mean[9]), approximately €3,300 was awarded, while the median[10] amount was €1,500. The highest amount awarded was €30,000, the lowest amount €25. It must be noted, though, that the higher amounts were usually not awarded for an ordinary data protection violation, but rather for cases where e.g. pictures of celebrities were published in media outlets or where an employer hired private investigators.

However, when we contrast the amounts awarded to the sums claimed, it becomes clear that plaintiffs are often only partially successful. In particular, plaintiffs often claimed much higher sums than were awarded. In about 60% of cases (38 out of 65 cases where the claim was not fully rejected) the courts awarded 40% or less of the sum original claimed by the plaintiffs. In fewer than 10% of cases (six out of 65 cases, including two cases in which more than claimed was granted) the courts granted the claim almost the full amount or completely, namely between 80% and more of the sum.

A possible explanation for unrealistic claims may be that plaintiff's law firms' fees depend on the amount in dispute and that many times these fees are either covered by the defendant (if plaintiff is successful) or by the plaintiff's legal expense insurance. Therefore, law firms have an incentive to claim high amounts.

Damages for various types of personal data

The risk of a company being held liable for damages may, among other factors, depend on the sensitivity of the affected personal data.

To illustrate this, Figure 2 shows the respective awarded damages in relation to the affected data categories.

The trend shows that less sensitive, commonly shared data, which are frequently the subject of data protection violations, tend to correlate with judgments where lower amounts of damages are awarded. In contrast, when more sensitive data is affected, the damages awarded increase to the median, €1,500.

The outlook

The current case law in Germany is expected to continue evolving. In addition to ten judgments from the European Court of Justice, the German Federal Court of Justice (BGH) has recently provided German courts with a new standard for evaluating claims. As described above, many courts have previously dismissed claims on the grounds that plaintiffs did not demonstrate damage which should be compensated. The BGH has now ruled that the mere loss of control over data can itself constitute damage. This concept was previously debated and often rejected by lower courts.

Loss of control as a form of damage provides a relatively straightforward basis for affected individuals to claim compensation for data protection violations, so an increase in successful claims is likely. However, the BGH also determined that a compensation amount of €100 is

REFERENCES

1 www.vzbv.de/pressemitteilungen/nach-bgh-urteil-zu-facebook-datenleck-vzbv-reicht-sammelklage-ein (in German)
2 Labour Court Diez, judgment of 7 November 2018 – 8 C 130/18.
3 Higher Regional Court Hamm, judgment of 15 August 2023 – 7 U 19/23.
4 Sources primarily include openjur.de/ as well as the databases of Beck-Online and Juris. Occasionally, other databases are also used, especially the public judicial databases of the German federal states.
5 /www.noerr.com/de/themen/gdpr-damages-tracker
6 In particular claims for violations of personal rights in the context of suspicion-based reporting under Sec. 823 German Civil Code in conjunction with Art. 1(1) and (2) of the German Constitution.
7 *Hamann*, JZ 2021, 656 (658).
8 Please note that this is not a valid argument anymore as the ECJ has ruled that there is no threshold of seriousness for claims under Art. 82 GDPR.
9 For the mean, the sum of all data points is divided by the number of data points. The mean is sensitive to individual outliers, as these can disproportionately affect the result.
10 The median represents the exact middle value of all data points, meaning that exactly half of the values lie below it and half above it. The median is somewhat more robust against outliers than the mean, as individual extremely high or low values only slightly impact the median.

appropriate for the loss of control in this specific case. This may establish a low benchmark, which could lead German courts to increasingly approve claims in this area but with lower average compensation amounts. Accordingly, the average sums of money awarded may decrease in the future.

AUTHORS

Dr Lea Stegemann is a Senior Associate at Noerr PartGmbB and Dr Jakob Horn is an Associate at Taylor Wessing PartGmbB.
Emails: Lea.Stegemann@noerr.com, j.horn@taylorwessing.com

INFORMATION

The authors will give a presentation on this subject at *PL&B's* 38th International Conference, 7-9 July at St. John's College, Cambridge (p.25).
www.privacylaws.com/PLB2024

Orange... from p.1

Orange offers its customers an email messaging service (the *Mail Orange* service). Following investigations carried out in relation to this service in 2023, the CNIL found that Orange was displaying ads in customer's email inboxes that were in the format of emails among the list of actual emails. More specifically, such messages were inserted between the actual emails, and although they were labelled as "advertisement", without showing a date of sending, the name of the sender and the subject appeared in the same form as for actual emails. When clicking on the ad, the customer was redirected to the advertiser's webpage. The CNIL considered that such advertising messages constitute direct marketing subject to the French anti-spam rules (article L34-V of the French Postal and Electronic Communications Code), which transpose the relevant provisions in this regard of the E-Privacy Directive (article 13). As such, their display required prior consent which Orange had failed to obtain from its customers.

It is the first time a sanction has been issued on this subject in France. This article examines the main takeaways from the CNIL's position and its enforcement approach towards Orange. Although we will only focus on the issue of ads in customer email inboxes, it is to be noted that the fine was also imposed because of Orange's non-compliance with cookie rules in accordance with French data protection law and CNIL guidance. Indeed, Orange was continuing its practice of placing and reading cookies even when a customer had withdrawn consent to their use, an aspect the CNIL had sanctioned several times in the past.

Extensive application of anti-spam rules in line with CJEU position

The CNIL's reasoning and arguments to consider that ads displayed in the form of emails among other messages of an email inbox qualify as direct marketing messages subject to French anti-spam rules largely rely on the position held by the Court of Justice of the European Union (CJEU) in the ruling *StWL Städtische Werke Lauf a.d. Pegnitz GmbH*[2]. In this decision, the CJEU came to this same conclusion as part of a request for a preliminary ruling with respect to very similar ad messages inserted between emails in an inbox. As a result, the CNIL's findings with respect to Orange's practice of displaying ads among emails are not surprising; the CNIL applied the CJEU's ruling which held that the display of such messages must follow the rules on direct marketing as provided by the E-Privacy Directive in particular by obtaining a user's prior consent, extending the scope of application of these rules.

In its defence, Orange had argued that the CJEU's ruling which the CNIL relied on was not applicable to its case. Orange emphasised a difference in drafting between the E-Privacy Directive and the provisions in France's anti-spam law provisions transposing them. In a nutshell, these provisions in the French law which refers to the "use" of an individual's email address with its prior consent for direct marketing shall, according to Orange, be read as requiring a "processing" of this email address to take place. Yet, Orange explained that the ads appearing in the email inbox of customers did not involve an actual "processing" of a customer's email address as the ads were not "sent" to the customer – involving an operation performed with the email address – but merely displayed in his/her inbox.

The CNIL rejected these arguments by holding that:

- The "use" of the email address of a customer shall be understood as the means to reach him/her, i.e., through his/her email inbox. As such, the mere usage of an email inbox, as the medium for displaying an ad is sufficient to consider that the email address is used and hence for the operation to fall under French anti-spam rules which do not require the existence of any operation of processing of the email address.
- The fact that these messages appear together and in a similar manner as actual emails triggers the interest and trust of users/customers of the email messaging service as part of their experience. Therefore, such messages should be treated under the same regime as unsolicited emails, as they hinder access by the customer to the actual emails in a similar way as spam messages. The same does not apply to ads displayed through banners and contextual windows which appear in the margin of the email inbox as they are shown in a distinctively different manner from emails.
- Since the messages displayed by Orange aim at promoting products and services offered by third party advertisers and are directed to individual customers through their email inboxes which they access by individually authenticating themselves (using a login and password), these messages meet the criteria of direct marketing communications.

Responsibility of Orange vs. advertisers

Another reason why Orange was objecting to the application by the

CNIL of the CJEU's *StWL Städtische Werke Lauf a.d. Pegnitz GmbH* ruling to its case was because it deemed that the CJEU had only considered the responsibility of advertisers displaying ad messages in email inboxes without the required consent, but not of the providers of the email messaging service allowing the display of these messages. It is true that the case examined by the CJEU in this request for a preliminary ruling had been triggered by a complaint against an advertiser for which an ad message was shown in email inboxes. The conclusions drawn by the CJEU thus refer to what the advertiser had failed to do to ensure compliance with direct marketing requirements using the email inbox. In this context, it could be asked whether it was indeed for Orange or for advertisers for which the ads were shown to comply with the prior consent requirement to allow the display of ads among emails in the customer inboxes.

According to the CNIL, this CJEU ruling has general application and is not specific to a type of actor that may be involved in the display of ad messages through email inboxes. Most importantly, the CNIL considers that Orange is to be held responsible for compliance with the prior consent requirement of the French anti-spam rules because:

- Orange's role was not limited to technically displaying the ad messages in customer email inboxes;
- On the contrary, it consisted of offering to advertisers within these inboxes dedicated ad spaces that it determines and controls at its own discretion;
- In addition, Orange, in its role of provider of the email messaging service is the only one to be in contact with customers. It is therefore the relevant entity in a position to collect their consent to the display of ad messages within their email inboxes.

CNIL holds Orange as responsible because of its active role in contributing to the targeting of customers with ads through their email inboxes, and hence acting as a controller. The CNIL also adds that Orange's responsibility applies regardless of the possible responsibility of advertisers. The CNIL's approach on this point is very close to the one adopted in the context of use of cookies with respect to website publishers allowing the placing and use of third-party cookies (even when they may not control their functioning). It considers them responsible for compliance with cookie requirements, in particular in obtaining an Internet user's prior consent[3].

Nevertheless, it appears to us that the CNIL's conclusions about Orange's responsibility are to some extent debatable or at least leave certain questions unanswered. First, it is unclear why the CNIL presumes that Orange is the only actor to be in direct contact with customers, and thus best placed to obtain their consent. Depending on the advertisers involved for the display of the ad messages, they may also be customers of such advertisers and interacting with them. Second, the CNIL leaves open the issue of Orange's possible shared responsibility with advertisers for compliance with the anti-spam rules, and the consequences that should be drawn from this for each type of actor both on a legal and practical level.

CNIL'S ZERO TOLERANCE POLICY

To justify the imposition of the fine of €50 million, in particular for the display of ads in customer email inboxes without consent, the CNIL identified the following factors:

- The severity of the breach characterised by the intrusive nature of the practice;
- The number of customers concerned (almost 8 million);
- The fact that Orange should have been aware – because of the above-mentioned CJEU ruling – of its compliance obligations on this topic, and particularly vigilant given its substantial material/human resources;
- The financial benefit gained from the practice;
- Its leading market position in the telecommunications sector.

Despite these findings, the sanction illustrates, in our view, the CNIL's tough enforcement approach considering certain elements in this matter. It is interesting that Orange argued that the CNIL did not specifically highlight the CJEU ruling through its publications, nor did it provide any guidance as part of its referential relating to the processing of personal data of clients and prospects[4]. This referential, which was adopted in January 2022, i.e. after the CJEU issued its ruling in November 2021, contains developments on how to conduct direct marketing operations in line with the GDPR and France's data protection law. It does not, however, refer to this ruling or its consequences in extending the scope of application of the French anti-spam rules to the practice of ads displayed in email inboxes.

It appears that the CNIL chose to directly and specifically sanction Orange for this practice[5], without regarding it necessary to clarify beforehand to organisations how the CJEU ruling was to be interpreted in light of applicable French law. As mentioned above, some of Orange's arguments could legitimately raise questions about the interpretation of these provisions.

This decision contrasts with how the CNIL has proceeded on other topics that trigger new compliance questions. For example, it has paid attention in particular to cookies, and more recently with respect to mobile applications[6]. It has followed a step-by-step approach: first issuing guidance, then granting organisations a transitional period, and only after inspecting and where relevant, imposing sanctions.

Another point which is striking is that Orange stopped displaying ads among other emails in its customers' inboxes as early as November 2023, following the CNIL's inspections the same year. However, this did not stop the CNIL from opening a sanction procedure in April 2024.

The CNIL, while explaining that it sanctioned Orange for past actions, acknowledges in its decision the compliance actions undertaken by the company and that it has taken this factor into account when making its decision. It is not being transparent, however, on how much weight this consideration carries in determining the size of the fine.

In light of all these elements, the proportionality and fairness of the CNIL's enforcement approach in this matter can be questioned. We wonder whether other alternative corrective measures than a fine could have been used. In any event, the case sends a warning to other organisations, especially those in a leading position,

not to expect any leniency from the CNIL, including on novel issues. Orange has announced that it intends to appeal the decision but no information was available at the time of writing on whether it has done so or not.

AUTHOR

Nana Botchorichvili is Counsel at IDEA Avocats, France.
Email:
nana.botchorichvili@idea-avocats.com

REFERENCES

1 CNIL, Sanction Committee Decision n°SAN-2024-019 of 14 November 2024 (available in French at www.legifrance.gouv.fr/cnil/id/CNILTEXT000050760620).
2 CJEU, Case C-102/20, StWL Städtische Werke Lauf a.d. Pegnitz GmbH, 25 November 2021.
3 See notably, CNIL Sanction Committee Decision n° SAN-2021-013 of 27 July 2021 against the newspaper Le Figaro (available in French at www.legifrance.gouv.fr/cnil/id/CNILTEXT000043867129). This position in the context of cookies had been confirmed by the French higher administrative Court (Conseil d'Etat), Decision n°412589 of 6 June 2018
4 CNIL, Referential on the processing of personal data for the purpose of management of commercial activities (available in French at www.cnil.fr/sites/cnil/files/atoms/files/referentiel_traitements-donnees-caractere-personnel_gestion-activites-commerciales.pdf)
5 To note that the CNIL's investigation was performed on its own initiative and was not triggered by a complaint. It is unclear why the CNIL specifically chose to target Orange while according to Orange other e-mail messaging service may be having the same practice
6 CNIL, Mobile applications, CNIL publishes its recommendations for better privacy protection, 24 September 2024. www.cnil.fr/en/mobile-applications-cnil-publishes-its-recommendations-better-privacy-protection

Meta Platforms Ireland Limited fined €251 million

Ireland's Data Protection Commission (DPC) said, announcing the decision on 17 December 2024: "This data breach impacted approximately 29 million Facebook accounts globally, of which approximately 3 million were based in the EU/EEA. The categories of personal data affected included: user's full name; email address; phone number; location; place of work; date of birth; religion; gender; posts on timelines; groups of which a user was a member; and children's personal data. The breach arose from the exploitation by unauthorised third parties of user tokens on the Facebook platform. The breach was remedied by MPIL [Meta Platforms Ireland Limited] and its US parent company shortly after its discovery."

The decision, which was made by the Commissioners for Data Protection, Dr. Des Hogan and Dale Sunderland, included a number of reprimands in addition to the fine.

The DPC said that it had submitted a draft decision to the GDPR cooperation mechanism in September 2024, as required under Article 60 of the GDPR. No objections to the DPC's draft decision were raised.

• *See www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-meta-eu251-million*

IAB submits views on consent or pay to the EDPB

IAB Europe, the European-level association for the digital marketing and advertising ecosystem, has submitted to the European Data Protection Board (EDPB) a feedback paper outlining key remarks and concerns after the EDPB's stakeholder event in November 2024 on the forthcoming draft Guidelines concerning "Consent or Pay" (CorP) models.

"A major concern is the assessment of 'freely given consent' in the context of CorP. CorP models inherently provide users with autonomy by offering clear options for accessing an online service involving paying a fee or accepting the processing of personal data for personalised advertising purposes to have free access. Users also retain full freedom to choose neither option and seek alternative services instead," IAB Europe says.

"Additionally, there is no obligation for businesses to provide their services for free, nor is there any obligation for businesses to provide their services at a loss which would inevitably be the case should a third, free alternative without personalised advertising be required where CorP models are used. Personalised advertising is a significant revenue driver for many online services, with contextual advertising falling short as a viable alternative. Studies indicate that contextual ads generate significantly less revenue and are less effective in filling available ad slots. It will therefore no longer be feasible for many businesses to maintain a free (or lower-priced) access option funded by advertising due to much lower revenues should such an alternative be required - which would ultimately be to the detriment of users."

The EDPB issued in April 2024 its Opinion on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms.

• *See iabeurope.eu/iab-europe-sends-feedback-paper-to-the-edpb-after-the-stakeholder-event-regarding-the-consent-or-pay-models/*

Mexico risks losing its independent Data Protection Authority

The dissolution of Mexico's Data Protection Authority, the INAI, now looks inevitable. By **Jonathan Mendoza Iserte** and **Jesús Javier Sánchez García** of the INAI.

On 20 November 2024, Mexico's Chamber of Deputies presented, voted on, and approved the administrative simplification reform that includes the dissolution of the INAI, Mexico's Data Protection Authority. The constitutional reform, that would also abolish six other agencies, progressed in December as the Senate also gave its approval. This marked a period of up to 90 days for the drafting, approval, and publication of the new legislation that will regulate the rights to access information and personal data protection in Mexico.

The publication of the reform in the Official Gazette of the Federation could now happen at any time, depending solely on the administrative processes involved. While the votes have already been cast, and we can consider this a definitive decision, the lack of secondary legislation leaves us in a state of uncertainty until those laws are published.

Why this is important

In an era defined by the digital revolution, where artificial intelligence, quantum computing and other disruptive technologies are reshaping our interactions and decisions, control over our personal data has become a cornerstone of the free development of our personality. More than a technical or legal issue, personal data protection is, and must be recognized as, a human right that ensures our ability to decide who can access our information and how it is treated. However, in Mexico, this right is at a critical juncture that could sever our ties with international standards and leave us vulnerable in a digital world, where privacy is the foundation for safeguarding not only our dignity but also our essential freedoms in an increasingly interconnected environment.

The recent government initiative to simplify administration dissolves the National Institute for Transparency, Access to Information, and Personal Data Protection (INAI) and will leave Mexico without a specialized authority in this field. This decision, which has sparked significant debate, not only created an institutional vacuum but also jeopardized the country's ability to meet international data protection standards. Mexico, recognized as a regional leader known for its innovative legislation and best practices implemented in both the public and private sectors, now finds itself on uncertain ground, with its citizens left less protected.

The consequences of this decision extend beyond the realm of human rights. They also have profound economic implications. In a world where the digital economy is an ever-growing reality, safeguarding personal data is essential to maintain competitiveness and market trust.

Moreover, Mexico is one of the nine non-member countries that has signed and ratified Convention 108 of the Council of Europe[1], the only binding international instrument on this matter. This Convention offers economic and diplomatic benefits by enabling the secure flow of data among member countries, facilitating trade, investment, and international cooperation. Without an independent oversight authority, Mexico's adherence to Convention 108 is at risk, along with the advantages it brings: from attracting technology companies to consolidating Mexico's position as a reliable partner in the global digital ecosystem. At a time when e-commerce is no longer optional but is the future of economic transactions, we cannot afford to overlook the importance of this right.

Mexico may fall behind

In the words of Alessandro Mantelero, an independent expert on artificial intelligence and human rights, "The reassignment of INAI's functions, as proposed in the constitutional reform, could significantly reduce the level of personal data protection due to excessive fragmentation of control authority responsibilities, the lack of full independence, and the absence of specific expertise within these control authorities. Furthermore, international collaboration and its central role in the cross-border flow of data would be so significantly affected that it could hinder the data free flow at the transnational level under Convention 108 between Mexico and other countries that are Parties to the Convention."

While other countries in the region, such as Brazil, Peru, Chile, and El Salvador, are moving forward with modern legislation and strong control authorities, Mexico risks falling behind. Brazil, for instance, has not only strengthened its National Data Protection Authority (ANPD) by incorporating more than 200 new staff positions into its structure, but has also positioned itself as a regional leader, attracting investments and consolidating its digital economy. In Peru, a new law aligned with the principles enshrined within the European Union's General Data Protection Regulation (GDPR) was approved, and both Chile and El Salvador have taken significant steps by enacting laws that not only protect personal data but also foster trust and economic growth through legal certainty.

The contrast with these international advancements is alarming. Mexico risks lagging behind not only in regulatory terms but also in international cooperation. Without a supervisory authority, it will be difficult to actively participate in global forums or exchange information securely with other countries, which will impact sectors as diverse as trade, technology, and security. Even more concerning is the impact on individuals, as the lack of oversight opens the door to abuse ranging from the misuse of personal information to an increase in fraud and privacy breaches.

What can be done now?

The outlook may seem bleak, but it is not irreversible. This moment of crisis must be transformed into an opportunity to reflect on what is at stake and take action from our respective roles to ensure that data protection remains a priority in Mexico. Even without a specialized supervisory authority, companies, civil society organizations, universities, and citizens can and must uphold their commitment to this right. The private sector must continue to implement internal policies to safeguard user data, while civil society and academia must demand that this issue returns to the public agenda.

Likewise, the future of personal data protection does not depend solely on institutions but also on the individuals driving its development. In Mexico and across Latin America, there is a significant shortage of professionals specialized in this field, and this issue is not exclusive to our region: globally, the demand for experts in data protection, cybersecurity, digital ethics, and disruptive technologies far exceeds the available supply. To ensure this human right remains alive and relevant in our country, investing in professionalization is essential.

Mexico needs more experts who combine technical, legal, and ethical knowledge to tackle current and future challenges. Investing in the training of professionals is an urgent necessity, as they are the ones who will ensure that, no matter what happens, personal data protection does not become a forgotten concept but rather a strengthened right, adapted to today's challenges.

Unresolved questions

The future raises many questions that remain unanswered, so to those who consider the dissolution of INAI to be justified, we invite you to reflect on the following unresolved issues:

- In whose hands will the oversight of principles, rights, and obligations in the private sector rest?
- How will fines be imposed?
- What will the channels of communication with the new authority be like?
- And finally, how will certainty and legal security be guaranteed to clients?

In this scenario, professionalization becomes more important than ever. Initiatives such as certifications in personal data protection are essential to train specialists capable of confronting these challenges and ensuring that, beyond institutional changes, personal data protection remains an effective right.

For this reason, personal data protection is neither a luxury nor a secondary issue; it is a pillar of our democracy and an essential requirement for our digital sovereignty. Globally, the trends are clear: countries that fail to protect their citizens' privacy are not only exposed to internal risks but also lose credibility and competitiveness in a world where the economy and society increasingly rely on digital trust.

The challenge for Mexico is enormous, but we cannot allow this setback to become a definitive defeat. Looking ahead, it is our responsibility as a society to ensure that human rights are not subject to political or economic decisions. Despite the uncertainty, we must continue to move forward and maintain hope so that Mexico may one day reclaim its position as a Latin American leader in personal data protection.

AUTHORS

Jonathan Mendoza is Secretary for Personal Data Protection and
Jesús Sánchez is Deputy Director, Officer for Data Protection at INAI, Mexico.
Emails: jonathan.mendoza@inai.org.mx
jesus.sanchez@inai.org.mx

REFERENCE

1 www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108

EDPB expects more detail in EU adequacy assessments

A letter from the European Data Protection Board (EDPB) to the new EU Commissioner of Justice, Michael McGrath in December 2024, draws attention to the EU Commission's renewed adequacy decisions.

The group says: "As no adequacy decision was repealed, amended or suspended by the Commission, the EDPB did not provide an opinion as per Article 70(1)(s) of the GDPR, neither for the part related to the data protection framework nor for the part related to access to personal data by public authorities, which was assessed for the first time."

The EDPB points out, however, that as some of the old decisions were from a long time ago, there could have been more extensive explanations on how the current (positive) assessments were conducted, and their methodology.

"EDPB would have found it useful if this report contained a more comprehensive description of the elements of the adequacy assessment for each country and territory. The EDPB would also suggest, for future reports on the re-evaluation of the data protection frameworks related to these eleven adequate third countries and territories, that they contain a detailed description of the elements of the adequacy assessment for each country and territory or at least include references to previous reports or adequacy decisions where those elements are referred to."

• *See www.edpb.europa.eu/system/files/2024-12/edpb_letter_20241205_european-commission-review-of-11-existing-adequacy-decisions_en.pdf*

Avoiding the scope of the ePrivacy Directive in advertising

Sergio Maldonado of Privacycloud discusses AI-driven anonymisation, server-side solutions, and the recently adopted EDPB ePrivacy Directive Guidelines in the context of tracking.

The European Data Protection Board's (EDPB) October 2024 Guidelines on the Technical Scope of Art. 5(3) address the emergence of new tracking methods to replace cookies. In light of the Guidelines, a blanket consent requirement will now be triggered by any act of temporary storage or access on a data subject's device. This goes well beyond the use of cookies, encompassing multiple practices that many considered either privacy-preserving or mostly innocuous and inherent to the inner workings of the Internet (including pixels, local processing, URL parameters, or browser-based APIs).

A good illustration of the former is Protected Audiences, an API (or Application Programming Interface) developed over the past few years under the umbrella of Chrome's Privacy Sandbox. A recent Boston University study has concluded that such protocol, which does not track devices individually, can be just as effective as a means of retargeting as third-party cookies, provided that a significant number of publishers adopt it. It is however unlikely that such adoption will materialise in the short term, or that there is any benefit in making the effort, given that consent will still be required.

As interpreted, Article 5.3 of the ePrivacy Directive is not only resulting in a further departure from the principle of data minimisation, but also running counter to Network Centricity, an essential quality attribute of common privacy engineering and Privacy by Design frameworks. Whereas a decentralisation of data processing activities results in a lower risk of data leakage and enhanced user controls, it is precisely the proximity to a device that will result in greater scrutiny under the ePrivacy Directive.

Should the severe impact of the new guidelines not appear sufficient, supervisory authorities are simultaneously stepping up the enforcement of valid consent standards in the context of digital marketing and online tracking activities. For the leading Data Protection Authorities these actions have become increasingly easier to handle and automate. As an additional incentive, fines based on the ePrivacy Directive can circumvent the One-Stop-Shop otherwise applicable in the context of the GDPR.

Beyond cookies, unique identifiers… and consent

A considerable drop in consent rates for cookies or their ID-based substitutes (browser-based technologies that can replace third-party cookies) has followed the wider adoption of "reject all" options on consent banners, rendering the effort futile for smaller stakeholders who lack large enough data volumes to give significance to the resulting sample. This has led to a loss of reliable grounds for campaign planning, targeting, or measurement. Things are likely to get even worse when Chrome's announced introduction of a single cross-site consent prompt for third-party cookies takes effect in the coming months.

> Circumventing the DP framework altogether can be done by working with fully anonymous data.

With all of this in mind, two areas of focus have taken prominence among privacy engineers and legal advisors in the marketing technology space: server-side processing and data anonymisation. In other words, avoiding the scope of the ePrivacy Directive and escaping the data protection regime altogether, respectively.

Revisiting server-side solutions

A circumvention of the data subject's terminal equipment allows data controllers to potentially avail themselves of other legal bases provided by the GDPR, namely legitimate interest and contractual necessity. Both are surely a tall order, but they appear preferable to a direct violation of the core elements of valid consent through the use of dark patterns. We are also putting aside the use of "Consent or Pay" prompts - highly controversial and only available to online publishers in certain countries.

Both Conversion APIs (server-side APIs that allow servers to contact directly third-party advertising platforms) and Data Clean Rooms (secure digital spaces where organisations can share and analyse data from multiple sources while protecting user privacy) rely on a combination of server-side processing techniques and a data controller's ability to collect relevant signals about their own actual or potential customers.

Conversion APIs

When so-called "walled gardens" (large online platforms such as Meta, TikTok, Amazon or Google) are involved, advertisers are being encouraged to regularly upload a batch of online or offline signals associated with a given campaign ("conversion data") that can then feed the optimization loop. This does not always require a parallel effort to broadcast successful events in real time through tracking pixels, but most platforms will encourage a combination of both practices. In the latter case, the *lex specialis* will apply.

Although the EDPB has made it

clear that social media platforms (in the specific context of Meta) would not be able to rely on either legitimate interest or contractual necessity for the purposes of behavioural advertising, there may be room for a less restrictive approach whenever it is an advertiser, with limited access to user data, that act as the sole data controller, as appears to be the case when Conversion APIs are in use.

That said, the ePrivacy Directive will once again show its teeth whenever the signals being uploaded have been collected through client-side technologies.

Data Clean Rooms

Data Clean Rooms (DCRs) have been evolving for quite some time now, in parallel to the explosive growth of alternative digital advertising networks and platforms. In particular, retail media networks have given these data collaboration environments increased prominence.

Various DCR offerings (and in-house initiatives) are built on well-known Privacy Enhancing Technologies like "trusted execution environments" in order to isolate an advertiser's first-party data in a securely locked repository, ensuring that all operations performed on such data remain within the control and supervision of a data controller. In other cases, "multiparty computation" will allow different business partners to perform joint operations on separate, previously encrypted datasets.

Given that first-party data has been collected in the context of direct relationships between advertisers, retailers or publishers and their own customers, no need arises for additional consent requests if it can be understood that data collaboration efforts do not fall out of the scope of the originally stated purpose.

However, the generation of look-alike audiences that can be targeted on either the open market or walled gardens, will require matching encrypted identifiers, and the associated data processing could still require consent if it is understood that personal data will be shared with new recipients or categories of recipients. Additionally, both parties to the audience deduplication effort are likely to be deemed joint controllers.

Contextual ads and AI-generated synthetic data

A more drastic measure, beyond avoiding the ePrivacy Directive, would be circumventing the data protection framework altogether. This can be done by working with fully anonymous data. How far can such an approach be taken?

There is little use for fully anonymous data beyond a basic statistical analysis of aggregated data for audience planning purposes. Recent progress in "differential privacy" (or the programmatic addition of noise) allows for more sophisticated queries on combined datasets, but these efforts tend to cross the very thin line that would render such data pseudonymised, and thus subject to the GDPR.

As a matter of fact, even contextual advertising, considered by many the holy grail of privacy-preserving advertising, relies on IP addresses and requires basic fraud-detection signals to function, contrary to the recently expanded interpretation of the ePrivacy Directive. In other words, albeit it may technically avoid personal data per se, consent is still required regardless of the level of intrusiveness of the chosen formula, be it purely contextual ads or cross-site, interest-based ads.

As a recent addition to the range of options at hand, generative AI-powered synthetic data does however allow companies to work with truly anonymized data that is both granular and impossible to re-identify. This enables more advanced solutions for cohort definition or targeting criteria, either in isolation or in combination with a common taxonomy of interests. Although previously-trained large language models (LLM) will underpin the generation of such data, the very intentional process of generating a synthetic audience facilitates the introduction of the necessary safeguards, compensating for bias or introducing additional levels of noise.

Exceptions and opportunities

Needless to say, all of the above would change considerably if competent authorities (not necessarily the EDPB) were to subject article 5.3 exceptions to a similar update to the one that the notions of storage and access have now been subjected to. In particular, the concept of "technical necessity" was originally conceived to give cover to technical solutions addressing the so-called "statelessness" of HTTP environments, in a way that shopping carts, language preferences, or account details would be remembered throughout a session. More than 20 years have gone by, and it would make sense to extend these exceptions to the inner workings of privacy-preserving advertising that is inherent to a news publisher, retailer, or otherwise content-based offering.

In the absence of an ePrivacy Regulation that brings device-level protections in line with a risk-based approach, such exceptions would open up the door to a legitimate interest test or data minimisation efforts along the lines of those expressly accepted, under certain conditions, by the French or Spanish data protection agencies with regards to certain cookies previously deemed non exempt: those required for analytics purposes.

AUTHOR

Sergio Maldonado is CEO of Privacycloud.
Email: smaldonado@privacycloud.com

INFORMATION

The EDPB guidelines are at www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf

Appointment of the next EDPS is delayed

The frontrunners are Bruno Gencarelli of the EU Commission and the current postholder Wojciech Wiewiórowski. **Laura Linkomies** reports.

There is a further delay to an already late-running appointment process of the next European Data Protection Supervisor (EDPS) for 2025-2030. The hearings did not take place until 16 January at the European Parliament due to the European Commission failing to produce a shortlist of four in a timely manner. While the MEPs' preferred candidate is Bruno Gencarelli, Head of International Data Flows Unit at the European Commission, the Council favoured Wiewiórowski, who has held the role since December 2019, and was the assistant Commissioner before that. At the time of writing, 29 January, the Parliament and the Council were due to meet to negotiate over the appointment, but it was uncertain how quickly a decision could be reached.

The other two short-listed candidates were François Pellegrini, Professor of Informatics at the University of Bordeaux, and Anna Pouliou, Chair of the Data Protection Commission at CERN. All four presented their case and answered questions by the European Parliament's LIBE Committee, culminating in a vote where MEPs could vote for more than one candidate.

The voting was not without a glitch as there were technical issues with some of the MEPs' electronic voting buttons. While they were told to move to another seat where the system worked, at least two persons were heard on the Parliament TV broadcast to complain that they did not manage to get their vote in. Considering the importance of the occasion, it makes one wonder why the vote was not delayed to ensure that the technology worked impeccably.

The result of the vote was Gencarelli 32 votes, Pellegrini 30, Wiewiórowski 26 and Pouliou 11.

The top candidates

At the European Parliament hearing, all four candidates were presented largely with the same questions. They all had the opportunity to submit written answers to certain questions beforehand.

Gencarelli highlighted cooperation between Data Protection Authorities in the EU and globally, as well as between the EU institutions. He said that he would, in the first weeks of his mandate, reach out to the Parliament, as well as to the Council and the Commission, to explore ways to make advisory support most effective in terms of timing, approach, or focus. Similarly, he would cooperate proactively with other DPAs and digital regulators with a view to sharing information at an early stage to avoid, as much as possible, conflicting outcomes.

Were he to be appointed, Gencarelli would leave one top EU data privacy job for another. At the European Commission, Gencarelli has been developing and overseeing the implementation of the GDPR and the Law Enforcement Directive, and has been in the driving seat in negotiations for international agreements and arrangements for data flows, including hearings/meetings at the European Parliament and national legislative bodies.

While he has invaluable insights into EU institutions, international privacy governance and cooperation, some commentators have wondered whether his approach would be too favourable to the European Commission which has been investigated by the EDPS regarding its use of Microsoft 365. The EDPS decision of 8 March 2024 found that the European Commission infringed several provisions of the EU's data protection law for EU institutions, bodies, offices and agencies (EUIs), including those on transfers of personal data outside the EU/European Economic Area (EEA). Essentially the question is about the possibility of access to EU citizens' data by US law enforcement or intelligence agencies.

The European Commission responded with a compliance report in December 2024. At the time, EDPS Wojciech Wiewiórowski said: "The EDPS is currently reviewing the information provided to assess whether the European Commission has complied with the decision of March 2024. Given the extensive scope of the information and the complexity of the processing operations involved, this analysis will require careful consideration and will be conducted thoroughly within an appropriate timeframe."

If Wiewiórowski were to continue in the role, he said he would be well positioned to face the challenges of the coming years – development and deployment of AI, quantum computing, blockchain, neurodata etc – due to his 30 years in academia, 15 in the data protection field and 10 in business. He said that "none of these challenges is generally incompatible with the principles of the GDPR and that for all of them, data protection rules can and should provide important guidance". He said that going forward he would put emphasis on creating better data protection awareness for people who work in EU institutions - in the past the EDPS has been more focused on enforcement.

Statements prior to Hearings

In his written answers to the LIBE Committee, Wiewiórowski said his vision for the future of the EDPS is for it to be an agile and proactive authority.

"I do not foresee the establishment of a 'single European digital authority' any time soon. Different expectations towards competent authorities resulted in the European lawmakers creating a number of regulations with their own governance models and a complex matrix of interactions. That is indeed one of the challenges that the EDPS anticipated in its legislative opinions being in the avant-garde of promoting and calling for coherence."

"My experience with the COVID-19 crisis and with the Russian invasion

of Ukraine shows that data protection can work, help and enable us to react to crisis in an effective way. I strongly believe we can build on positive examples of privacy-friendly solutions we achieved. I will advocate that the EDPS has played a tremendous role in shaping such developments, like interoperable COVID passports and apps. I am also proud of the EDPS' role in [the] establishment of Eurojust's war crimes databases."

He said that while the EDPS has multiple roles – supervisor, advisor to legislator, EDBP secretariat and the market surveillance authority according to the AI Act - the EDPS is uniquely positioned to be a hub for ideas and for their implementation across the regulatory framework.

"That is how I see the role of the EDPS, combining its core activities with participation in the European Data Protection Board, the European Data Innovation Board, the Artificial Intelligence Board, the Interinstitutional Cybersecurity Board and the High Level Group on Digital Markets Act. I am ready to supplement the EDPS' role with the recently announced digital clearinghouse 2.0, bringing regulators together at one table. This is an integral part of my proactive vision for the authority, because I understand the need to be united in a moment where Europe is under scrutiny and attack for its alleged lack of innovation. I simply but firmly believe that innovation and fundamental rights can go hand in hand."

In his written answers to the LIBE committee, Gencarelli stated that his main motivation to apply for the role was that "the European Data Protection Supervisor can significantly and concretely contribute to safeguarding this human-centric approach to the digital transformation." He said that as EDPS he would not hesitate to use enforcement powers when needed. He stated that a supervisory authority must, "not only be independent but be seen to be independent".

"When it comes to the EDPS supervisory functions, I believe that asking the right questions facilitates a better understanding of the EU Institutions compliance needs but also helps to prevent or address possible violations of privacy rules, including through enforcement actions. I also consider that regular exchanges with the scientific community, academia, civil society and businesses on emerging technological and commercial trends would be essential to keep the EDPS abreast of relevant developments, as regard both their potential impact on privacy and solutions to limit possible risks. Similarly, I would promote discussion and exchange between colleagues across the authority. Last but not least, I would ensure that engagement with citizens is always an area of focus for the EDPS – whether it is through providing accessible information, organising thematic citizens' dialogues or ensuring quick resolution of complaints – and that it informs the performance of its different tasks."

Gencarelli believes that the EDPS can contribute concrete suggestions and examples of good practice, promote compliance mechanisms and tools such as model clauses, codes of conduct, certification schemes, regulatory sandboxes, etc. "I am convinced that helping entities processing data 'to get it right' in complying with privacy rules is ultimately one of the most effective ways to serve the interests of individuals," he said.

Views on AI

Gencarelli stated in his written answers to LIBE the "need for effective cross-regulatory cooperation. By being placed at the juncture, on the one hand, of the EU and national privacy governance systems (as a member of the EDPB) and, on the other hand, of the privacy and broader digital governance systems (through its participation in the DMA High Level Group, the AI Board, the European Data Innovation Board, etc.), the EDPS is uniquely positioned to foster a coherent approach … "taking on of additional responsibilities that go beyond its 'traditional' role. Artificial Intelligence provides a good illustration of this evolution, as the EDPS will combine new tasks assigned under the AI Act (for example as market surveillance authority of the EU Institutions (EUIs) for high-risk AI systems) – that should be carried out under the specific conditions and objectives of that legislation – alongside its role as a DPA supervising EUIs' compliance with privacy requirements, including when using AI."

Wiewiórowski wrote: "I will prioritise … discussion on … Artificial Intelligence. I am sure that EU institutions need in the nearest future guidelines on how Europe can play a leading role in ensuring the safe deployment of AI across a variety of sectors. That is what the EDPS does for subjects it has chosen for its 'TechSonar' forecast for 2025, such as retrieval-augmented generation, on-device AI, a machine unlearning, multimodal AI, scalable oversight and neuro-symbolic AI."

The importance of the EDPS

The previous European Data Protection Supervisors, including Wiewiórowski have developed the EDPS role and influence way beyond what could have been envisaged when the office was first set up. It is a major player in the international field despite its regulatory powers being limited to EU institutions. The EDPS says on its website that its remit includes "developing and communicating an overall vision, thinking in global terms and proposing concrete recommendations and practical solutions". It also provides policy guidance to meet new and unforeseen challenges.

INFORMATION

The candidates' written submissions are at www.europarl.europa.eu/committees/en/appointment-of-the-european-data-protect/product-details/20250113CHE12861

CJEU awards an individual compensation in a data transfer case

The Court of Justice of The European Union (CJEU) has awarded a German citizen €400 to compensate for the loss of control of his personal data that was transferred to the United States.

The transfer in question relates to Mr Bindl registering via Facebook for a conference listed on the European Commission's website in March 2022. The EU Commission's Directorate-General for Communication was the data controller for the purposes of the website of the conference.

In his complaint, Mr Bindl asked the Commission to annul the transfers of his personal data to third countries that do not have an adequate level of protection (in this case the US).

The court says that "by means of the 'Sign in with Facebook' hyperlink displayed on the EU Login webpage, the Commission created the conditions for the applicant's IP address to be transmitted to Facebook. That IP address constitutes the applicant's personal data, which, by means of that hyperlink, was transmitted to Meta Platforms, an undertaking established in the United States. That transmission amounts, therefore, to a transfer of personal data to a third country, within the meaning of Article 46 of Regulation 2018/1725 [on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data]."

The CJEU ordered the EU Commission to pay the damages sought by the applicant in compensation for the non-material damage which he sustained as a result of the disputed transfer on signing in to EU Login on 30 March 2022.

The case's importance lies in the fact that it sets a precedent for future privacy litigation. If such cases were in a class-action in their thousands and millions, the ramifications for organisations would be enormous.

• *See the decision of 8 January 2025 at curia.europa.eu/juris/document/document.jsf?text=&docid=294090&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2243662*

South Korea passes AI law

South Korea's National Assembly passed the *Basic Law on the Development of Artificial Intelligence* on 26 December 2024, following in the footsteps of the EU AI Act.

The tiered approach is reminiscent of the EU AI Act. The AI Basic Act is set to take effect in January 2026, giving businesses one year to prepare, law firm Linklaters reports.

"The AI Basic Act follows the suite of core principles that regional observers will have seen crop up in numerous APAC regulatory playbooks and frameworks for AI: ethical AI development, human oversight, responsible use, fundamental rights protection, etc."

Linklaters lawyers say that AI systems are divided in this law into:

- High-impact AI systems which impact "life, bodily safety, and fundamental rights" in activities relating to prescribed sectors (e.g. energy supply, healthcare, medical devices, public services). This parallels with the EU AI Act's labelling of "high-risk AI systems" and deemed classification within the specified Annex III categories; and
- Generative AI systems that mimic input data to generate outputs such as text, sound, images, and other creative content.

• *See likms.assembly.go.kr/bill/billDetail.do?billId=PRC_R2V4H1W1T2K5M1O6E4Q9T0V7Q9S0U0 and techinsights.linklaters.com/post/102js56/koreas-wonsouth-koreas-ai-basic-act-asias-first-comprehensive-ai-legislatio*

Italy's *Garante* fines OpenAI €15m over ChatGPT data protection mistakes

Italy's Data Protection Authority (The *Garante*) has fined OpenAI €15m for its data protection failures related to the ChatGPT chatbot. The company must also educate the Italian public on the use of ChatGPT by means of a six-month public awareness campaign across Italian media and the Internet.

The *Garante* says that the company did not notify the Authority of the data breach that took place in March 2023, has processed users' personal data to train ChatGPT without first identifying an appropriate legal basis and has violated the principle of transparency and the related information obligations toward users. "Furthermore, OpenAI has not provided for mechanisms for age verification, which could lead to the risk of exposing children under 13 to inappropriate responses with respect to their degree of development and self-awareness."

The European Data Protection Board has also been involved, prompted by the issues identified in Italy. Its Opinion identifying a common approach to some of the most important issues related to the processing of personal data in the context of the design, development and deployment of AI-based services was issued in December 2024 (Opinion 28/2024).

• *See garanteprivacy.it/home/docweb/-/docweb-display/docweb/10085432#english*

Cambodia's draft data privacy law: Too much is left to delegated *prakas*

The draft law is limited only to the private sector and does not have extra-territorial scope.

By **Graham Greenleaf**, Honorary Professor at Macquarie University, Australia.

Cambodia is one of the last four of the 11 ASEAN countries that has not enacted a data privacy law.[1] Cambodia's Ministry of Posts and Telecommunications (MPTC) released for consultation a draft *Law on Personal Data Protection* (LPDP) on 25 July 2023, but the draft Law is not known to have progressed any further toward enactment.

The key limitation on the draft Law is that its scope is limited to the private sector, plus a few aspects of what could be regarded as the public sector. It does not apply to the "collection, use, and disclosure of personal data by Public Authorities", which the Law says "are governed by other legal instruments" (art. 2). "Public authorities" are defined as "not including public establishment of administrative character and public enterprises" (Appendix to the Law). Limitation to the private sector is also found in the data privacy laws of Malaysia and Singapore, although expressed differently, but not in the more recent laws of Thailand and Indonesia. It is therefore essential to consider the extent to which Cambodian authorities can obtain access to personal data held by the private sector, and the limitations placed on their use of this data.

This article reviews the draft Law, and places it in the context of the Cambodian legal system and government, and criticisms of privacy protections.

Cambodia's government and legal system

Modern Cambodia emerged from the shattered country that resulted from an estimated 500,000 deaths during the Indochina war (1970-75) and one million deaths during the Khmer Rouge regime led by Pol Pot (1975-79).[2] The government that emerged, led by Hun Sen (a former Khmer Rouge commander), was initially a client of Vietnam until it withdrew its troops in 1989. Hun Sen's Cambodian People's Party (CPP) won elections (often of dubious fairness) every four years from 1993, culminating in winning all seats in the 2018 election. In 2021 Hun Sen announced he would hand over the role of Prime Minister to his son, Hun Manet, which he did after the CPP won the 2023 election convincingly. Cambodia is an authoritarian state which has now been led by one family and its party for over 30 years.

Cambodia's legal system, based largely on French civil law, and all institutions supporting it, were destroyed during the Khmer Rouge period (1975-79), with most legal officials and lawyers killed. Reconstruction from scratch has continued since the 1980s but is incomplete.

The 1993 Constitution provides for a government headed by the King (Norodom Sihamoni, son of Norodom Sihanouk) and the Prime Minister (Hun Manet), and a bicameral legislature. The Constitution provides that pre-Khmer Rouge laws, if consistent with the Constitution, remain in force until new laws replace or modify them.

Most new laws are based on civil law principles, although the penal law was based on the principles of the common law and required modification by customary law. Judges apply the texts of legislation and do not adopt the common law approach of following judicially-developed precedents. Civil law approaches, consistent with Cambodian custom and other Asian countries, place a heavy reliance on conciliation, with judges attempting mediation between the parties and trials only taking place if conciliation fails. This is reflected in how the data privacy draft Law deals with complaints of breaches. Customary law is also often used to supplement incomplete legislation.

Cambodian criminal law is based on the inquisitorial system, with local tribunals at first instance, a court of cassation and a supreme court. Judicial police act on the request of the prosecutor, and a judge carries out the investigation, consistent with civil law approaches. This approach is reflected in the draft data privacy Law.

> A data controller must conduct an assessment of whether a data breach is a notifiable data breach.

Existing data privacy protections

Although Cambodia does not yet have any specific law dealing with data privacy, various aspects of privacy protection are included in the Civil Code (2007) as "personal rights", the Penal Code (various types of interception of data and communications), the Law on Electronic Commerce (2019) (requirement of security measures), and a wide variety of industry-specific legislation (including credit reporting, money laundering, and medical information).[3]

Structure of the draft data privacy Law

The scope of the draft Law (subject to it

only applying to the private sector) is that it applies to the "collection, use, and disclosure of personal data by data controllers and data processors located in" Cambodia, regardless of whether it takes place outside Cambodia. If the controller is located outside Cambodia, the Law only applies to collection etc taking place within Cambodia (art. 2). The extra-territorial scope of the GDPR is not included. There is the usual exception for "personal or household activities".

The MPTC is the authority responsible for data protection "supported by a unit in charge of personal data protection as the secretariat", with the details to be provided in a Sub-Decree proposed by MPTC (art. 4). The "data protection authority" is this data protection unit of the MPTC and is obviously not independent of government. However, nor does its scope cover government actions.

Definitions of key terms are in the Appendix to the draft Law, including "personal data" (based on identifiability), "processing", "data controller" and data breach. They are all conventional definitions found in other data privacy laws.

Conditions for collection, use and disclosure

Any collection, use or disclosure of personal data must come under one of two categories (art. 6):

(i) Collection etc *with consent* of the data subject, for a defined purpose; or

(ii) Collection etc *without consent*, in accordance with art. 15, or some other law.

In both cases, collection etc must be "for a purpose that is reasonable in the circumstances" (art. 6). What is "reasonable in the circumstances" will involve considerable and difficult interpretation, by either judicial police or in some cases, a court. This could place difficulties on a system which emphasises applying legislation, not interpreting it, and does not have any system of applying judicial precedents.

Where collection etc is *with consent*, it will only be valid if the data controller has provided notice under Article 10, and the data subject gives consent to the purpose (art. 8). Notice, in writing or orally, must include (a) a clear and appropriate statement of purpose, (b) activities of the business relevant to the collection etc, and (c) contact information of a representative able to answer questions (art. 10). If the collection etc with consent "poses a high risk" to the rights of the data subject, the data controller must conduct a "personal data impact assessment", the "conditions, formalities and procedures" for which will be determined by *prakas*[4] issued by the Minister responsible for MPTC. Use or disclosure of personal data for other purposes is only allowed if the data subject is notified and provides consent (art. 10).

Consent is not defined, and is not valid if the data subject's intent is expressed as a result of an error, the data controller's fraud, duress or misrepresentation, or the data controller's "exploitation of the situation to obtain excessive gains" (art. 11). Consent may be withdrawn, but not where collection etc does not require consent (art. 13).

The second category under Article 6 is where collection etc is allowed without consent, which can occur in two situations: (i) where Article 15 provides no consent is required (statutory consent); and (ii) where there is deemed consent under art. 12.

There are nine situations where no consent is required for collection etc (statutory consent), which can be paraphrased as follows (art. 15):

a) life-threatening emergencies;
b) contacting a relative or friend of a person injured, ill, or deceased;
c) where in the national interest, or necessary for exercise of the data controller's official authority;
d) personal data that is publicly available and has become so in a lawful manner;
e) where necessary for the performance of a contract to which the data subject is a party, or pre-contractual steps;
f) where necessary to conduct public or peer-reviewed scientific, historical, or statistical research in the public interest, which research is not possible using anonymised data;
g) where necessary for the legitimate interests of the data controller or another person, and they override the *prakas*;
h) where necessary for the data controller to comply with a law or regulation; and
i) other cases determined by *prakas*.

There are dangers of abuse by data controllers in some of these provisions, particularly "national interest" (c), "legitimate interests" as determined by *prakas* (g), and the open-ended ability to create more exceptions through *prakas* (i).

The data subject is deemed to consent to collection etc for a specific purpose if they voluntarily provide their personal data to the data controller for that specific purpose, and this provision is a reasonable act in the circumstances (art. 12). Once again, officials will have to exercise wide powers of interpretation to decide whether voluntary provision of data to data controllers is a "reasonable act".

"Special categories" of personal data include "but is not limited to biometric data, genetic data, health data, and data related to ethnicity and religion", a list which can be expanded by *prakas*. The "special protections" for such data are also to be determined by *prakas* (art. 16). Many of the usual "special categories" (see GDPR art. 9(1)) are as yet missing, as are the resulting protections (see GDPR art. 9(2)-(4)).

It is an unlawful practice to impose extra fees or otherwise discriminate against a data subject because they "exercise any right under this law" (art. 17).

Obligations to protect personal data

The obligations of data controllers are in Chapter 5 "Care of Personal Data" (arts. 19-24) and Chapter 6 "Notification of Data Breach" (arts. 25-28).

Data controllers must ensure the following protections are provided:

- Any personal data it collects must be accurate and complete for these purposes (art. 19): to make a decision affecting the data subject; or for disclosure to another person.
- A security system to prevent: (a) "unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks"; (b) "the loss of any storage medium or device on which personal data is stored" (art. 20).
- It must cease to retain personal data (or the means to make it identifiable) "as soon as it is reasonable to assume that the retention of the personal

data no longer serves the purpose for which that personal data was collected or is no longer necessary for legal or business purposes" (art. 21).
- A record of collection etc of personal data with details of all significant uses of the data (art. 23).

Prakas will ensure the conditions and procedures for the above obligations in arts. 19-24.

A **notifiable data breach** is a data breach (as defined in the appendix) if it: (a) "results in, or is likely to result in, significant harm to a data subject"; or (b) "is, or is likely to be, of a significant scale" (art. 25). A data controller must conduct an assessment of whether a data breach is a notifiable data breach. Data processors must notify the data controller of any data breach (art. 26). A data controller must notify MPTC if its assessment finds that there is a notifiable data breach, within three working days of that assessment (art. 27). The data controller must also notify the affected data subject(s), if the breach is likely to result in significant harm (art. 27), but no time limit is specified). *Prakas* will determine the details. A data processor who processes personal data on behalf of a public authority must immediately notify the public authority and MPTC of a data breach (art. 28), without need for any assessment that it is a notifiable data breach.

Data controllers must store collected personal data in Cambodia, either in its own personal data storage system or a data center or a secure cloud system.

Data controllers and data processors must appoint a **data protection officer** (art. 40) if their core activities: (a) "require regular and systematic monitoring of data subjects on a large scale"; or (b) "consist of collecting, using, or disclosing special categories of personal data on a large scale". This does not cover all large-scale processing, only that involving special categories of data. The role, responsibilities, and duties of such an officer will be determined by *prakas*.

Rights of data subjects

Data subjects have seven specified rights in Chapter 5:

- Right to notification (art. 31) – The data subject has the right to be notified, by the data controller, of the "purpose and means for collection" etc.
- Right to access (art. 32) – The data subject has the right to access and to obtain a copy of his/her personal data, and also to "other information related to" that personal data. The copy must be provided free of charge, and only reasonable administrative costs charged for additional copies.
- Right to rectification (art. 33) – The right to request rectification (correcting errors, completing insufficient data, updating data), based on the purpose of collection etc.
- Right to object (art. 34) – Data subject may object to collection etc, subject to the national interest, exercise of official authority, or legitimate interests of others (as per art. 15(1) (c) and (g)), unless the data controller demonstrates compelling legitimate grounds, or the collection etc is necessary "for the establishment, exercise, or defence of legal claims"
- Right to restriction (art. 35) – In some cases the data subject does not want the personal data deleted, but only to have its use restricted.
- Right to erasure, destruction or anonymisation (art. 36) – Data subjects can require these actions for five specified reasons: personal data no longer important for purpose; consent withdrawn; art. 34 objections; use contrary to law; use contrary to other laws. This does not apply if other laws require retention of the data.
- Right to data portability (art. 37) – Applies to data collected used or disclosed by automated means (only); data subject has right to receive data in a structured machine-readable format, and to specify such transmission to other parties.

Breaches of any of these rights by a data controller or processor gives rise to "the right to fair judicial or extrajudicial redress" (art. 38), discussed below. In addition, breaches of these data subject rights can result in transactional fines of varying amounts (arts. 64-69). "Conditions, formalities, and procedures for implementing the rights provided for under [Chapter 5] shall be determined by *prakas*" (art. 39).

Many of the obligations on data controllers and processors discussed in the previous section create de facto rights in data subjects, such as the right to be notified of a data breach likely to result in significant harm.

Enforcement by Data Protection Inspectors

The Minister of MPTC is to appoint Data Protection Inspectors to administer the Law. Inspectors are accredited as judicial police in relation to offences under the Law, in accordance with the Code of Criminal Procedure. Procedure for appointment etc is to be determined by inter-ministerial *prakas* of the Ministers of MPTC and Justice (art. 41). Inspectors must wear a uniform and have a mission order during law enforcement operations (art. 42). Inspectors have duties to investigate and suppress offences under the Law (art. 43), and to call for support from other authorities in doing so (art. 44), but they do not have any role in relation to resolving complaints of breaches of the Law and disputes in relation to it.

There is an appeals procedure. "Any person aggrieved by any measure of a Personal Data Inspector may submit a written complaint to the Minister of MPTC within 30 days from the date of receipt of the notice of the measure" (art. 46). The Minister must issue a decision within 30 days, and if a person does not agree with the decision, they can file a complaint with a competent court (art. 46).

Personal Data Inspectors are responsible for imposing transactional fines (art. 49), which are the most common form of enforcement under the draft Law. They are one form of criminal penalty, with penal fines being more serious. Payment of transactional fines shall extinguish prosecution, but if they are not paid, the Inspector may prepare a case file and forward it to a

competent court (art. 49).

Arts. 51-69 (Chapter 12) set out, for 19 different breaches of the draft Law, the range of transactional fines or penal fines that are applicable. The highest fine specified is 600 million riels (approximately USD $150,000) for failure to carry out a data breach assessment, with the fine able to be doubled if the offence is committed again within a year (art. 51), as is commonly provided in Cambodian law. The most common range of transactional fines is 20-40 million riels (i.e. a maximum of USD $10,000). A minority of these offences also carry a potential sentence of imprisonment of from six months to one year.

Other potential penalties that can be imposed by line ministries responsible for each sector, or by MPTC, are licence restrictions, suspension or revocation, where applicable (art. 49).

Complaints and dispute resolution

Disputes between data subjects and data controllers or processors go through a number of steps (art. 47):

(i) "All disputes related to personal data shall be conciliated by MPTC prior to lodging a complaint to a competent court". (The data protection unit within MPTC is presumably involved).
(ii) MPTC must conduct the conciliation within 30 days from receiving the complaint.
(iii) The extent of conciliation must be minuted by MPTC and implemented within 30 days.
(iv) If a party fails to comply (or no settlement is reached), the party (any party?) "may continue to arbitration procedures or lodge a complaint to a competent court".

The data subject then has a "right to remedy": "A data subject has the right to fair judicial or extrajudicial redress when his or her rights have been violated by a data controller or data processor" (art. 38). There is no mention of payment of compensation, but this is probably implied.

Access by public authorities to personal data

European data privacy authorities and courts have made it clear that any assessment of the strength of data protection in a country must include as one of its key indicators the conditions under which public authorities in the country can obtain access to personal data held by the private sector.

In its 2024 review of "adequacy" determinations made under the previous data privacy Directive in order to consider whether their protections were still "adequate" under the GDPR,[5] the European Commission said: "… in its *Schrems II* ruling … the Court of Justice … elaborated on the standard of "essential equivalence", in particular with respect to the rules on access to personal data by public authorities for law enforcement and national security purposes…" and must ensure "that such authorities cannot access data beyond what is necessary and proportionate to pursue legitimate objectives, and data subjects enjoy effective and enforceable rights against such authorities.[6]"

In its 2024 report on Cambodia, the NGO Freedom House ranked Cambodia as 43/100 ("partly free"),[7] and was particularly critical of government surveillance of the private sector: "Art. 97 of the 2015 Law on Telecommunications criminalises eavesdropping by private individuals but permits secret surveillance with approval from an undefined 'legitimate authority.' The law includes no legal or procedural safeguards and appears to authorise undeclared monitoring of 'any private speech via telecommunications.'[8] The passing of the NIG sub-decree,[9] it said, allows for the government's unfettered surveillance of individuals' online activity, but the extent to which this law will be implemented is not yet known ...".

Freedom House says "Service providers are required to provide communication information to the government, though this process lacks judicial oversight. art. 6 of the 2015 Law on Telecommunications mandates that all telecommunications operators provide ICT service data to the MPTC.[10] There is no requirement for a judicial warrant or other safeguards, and the law places no limits on how long data can be stored.[11]"

"Under this clause, bulk data must be collected and maintained with no clear purpose.[12] One source reported that ISPs are struggling to identify affordable options for storing the bulk data required by the sub-decree.[13]"

Although some aspects of these Cambodian surveillance proposals have not yet been implemented, it is clear enough that controls on public sector access to private sector personal data is a very weak aspect of data privacy in Cambodia and would not at present meet international standards.

Criticisms of the draft Law

Criticisms of the draft Law, from both civil liberties NGOs and business groups, have concentrated on two controversial provisions, on data exports (art. 22) and data localisation (art. 24).

- **Data exports** – "A data controller may not transfer personal data to any country or territory outside the Kingdom of Cambodia unless authorised under this law and relevant legal instruments". Conditions, formalities, and procedures for doing so will be set by *prakas* (art. 22). Until such *prakas* are issued businesses will not know whether data exports are subject to prohibitive or reasonable export conditions, and in any event, they will be changeable by further *prakas*.
- **Data localisation** – Data controllers must store collected personal data in Cambodia, either in its own personal data storage system or a data center or a secure cloud system of a third party licensed by MPTC (art. 24). "Technical specifications, conditions, and rules" for these means of storage shall be determined by MPTC *prakas*. There is no prohibition on the data also being stored overseas, but the data export rules will need to deal with that.

The Asia Internet Coalition, an industry lobby comprised of US and Asian platforms[14] made a submission to the Cambodian government in October 2024[15] which simply claims that both the data export and data localisation provisions would be economically harmful to Cambodia and should be scrapped in their entirety. This is an extreme point of view which does not suggest any more moderate provisions on data export limitations, such as in the EU's GDPR, or on data localisation such as variations of what is in article 24, to allow data exports while requiring

local storage of a copy, and with no requirement of local processing.

Another business group, the Global Data Alliance,[16] in its submission,[17] is far more flexible in supporting a wide range of data export conditions that would be acceptable in place of an outright prohibition, and also in allowing MPTC to authorise some storage of personal data outside Cambodia.

NGOs such as Access Now and the International Center for Not-for-Profit Law warn of the dangers of mandatory local storage where government access does not require a warrant or other judicial oversight.[18]

Conclusions: A profusion of *prakas*

Far too much is left by the draft Law to be determined by *prakas*, with even a short article like this mentioning over 20 occasions when they can be issued. Until many such *prakas* are issued, businesses will not have a clear enough idea of their obligations, nor citizens of their rights. The draft Law has the superficial appearance of a reasonably modern and international quality data privacy law, at least to the standard of other ASEAN countries, but in the absence of the *prakas* necessary to "fill in the gaps" it is impossible to know whether this is reality or illusion.

AUTHOR

Graham Greenleaf is the *PL&B* Asia-Pacific Editor and Honorary Professor, Macquarie University, Australia.
Professor Greenleaf will give a presentation on *New data laws in major Asian countries: India, Thailand and Indonesia* at *PL&B's* 38th International Conference, 7-9 July at St. John's College, Cambridge (p.25)
www.privacylaws.com/plb2025

INFORMATION

Fiona Kelliher, freelance journalist, has provided information for this article, but the author is responsible for all content.

REFERENCES

1 The other ASEAN countries lacking such laws are Brunei, Laos and Myanmar. A Lao law provides partial coverage.
2 For a brief history of Cambodia to 2014 see G. Greenleaf *Asian Data Privacy Laws* (OUP 2014) pgs. 392-95.
3 Jay Cohen and Chandavya Ing 'Cambodia' in *Regional Guide to Cybersecurity and Data Protection in Mainland Southeast Asia*, Tilleke and Gibbins 2024 www.tilleke.com/wp-content/uploads/2024/07/Tilleke-Cybersecurity-and-Data-Protection-in-Mainland-Southeast-Asia-2024.pdf
4 '*Prakas*' are official proclamations, issued by Ministers or Inter-Ministerial bodies. They have a similar function to delegated legislation in other systems. All references to prakas in this article are to those issued by the Minister of the MPTC, unless noted otherwise.
5 European Commission 'Report From The Commission To The European Parliament And The Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC' {SWD(2024) 3 final} 15 January 2024 COM(2024) 7 final
6 *Schrems II*, points 180-182.
7 Freedom House *Cambodia: Freedom on the Net 2024 Country Report* freedomhouse.org/country/cambodia/freedom-net/2024
8 LICADHO, "Cambodia's Law on Telecommunications: A Legal Analysis," March 2016, www.licadho-cambodia.org/reports.php?perm=214
9 'In February 2021, the government adopted the highly controversial sub-decree on the Establishment of the National Internet Gateway (NIG sub-decree). The NIG sub-decree seeks to centralise the government's control over all incoming and outgoing domestic and international web traffic through a single Internet gateway.' The operation of NIG has been suspended.
10 "Law on Telecommunications", Telecommunications Regulator of Cambodia, 2015 trc.gov.kh/en/laws/
11 Licadho *op cit*
12 "Joint Statement: Discard the Sub-Decree on the Establishment of the National Internet Gateway, set to detrimentally impact human rights online in Cambodia," PEN International, February 18, 2021, www.pen-international.org/news/discard-sub-decree-establishment-national-internet-gateway-detrimentally-impact-human-rights-online-cambodia
13 Fiona Kelliher, "Cambodia's internet gateway debut leaves analysts in the dark," *Southeast Asia Globe*, February 15, 2022, southeastasiaglobe.com/cambodias-internet-gateway-leaves-analysts-in-dark-technology-and-rights/
14 Asia Internet Coalition aicasia.org
15 See 'Asia Internet Coalition (AIC) Industry Submission on Cambodia's Draft Law on Personal Data Protection' at aicasia.org/policy-advocacy/?_sf_s=data%20protection
16 Global Data Alliance globaldataalliance.org
17 Global Data Alliance 'Comments on Draft Law on Personal Data Protection of the Kingdom of Cambodia' 5 October 2023 globaldataalliance.org/wp-content/uploads/2023/10/10052023gdacambodiadatapro.pdf
18 Fiona Kelliher 'Cambodia's draft data protection law fans fears of government abuse' *Nikkei Asia* 8 December 2023 asia.nikkei.com/Politics/Cambodia-s-draft-data-protection-law-fans-fears-of-government-abuse

Customer's gender identity is not necessary data for the purchase of a transport ticket

The Court of Justice of the European Union (CJEU) has ruled that the collection of data regarding customers' titles is not objectively indispensable, in particular where its purpose is to personalise commercial communication.

The case originated in France where a railway company asked people to fill in their title (Monsieur or Madame) (Mr or Ms) when purchasing transport tickets online. In 2021, the CNIL said in response to a complaint that the practice did not constitute an infringement of the GDPR. However, the CJEU's decision states that the railway company could choose to communicate based on generic, inclusive expressions when addressing a customer, which have no correlation with the presumed gender identity of those customers. That would be a workable and less intrusive solution, the court says.

• *See curia.europa.eu/jcms/upload/docs/application/pdf/2025-01/cp250002en.pdf*

Asia's revised data laws shape the region's business environment

Roald Chao compares recent updates in Malaysian and Singaporean data protection regulations, and analyses their impact for business.

Historically, Malaysia has had a hand in the technology manufacturing sphere going back as far as 1972 when Intel first opened their semiconductor factory in Penang. Now caught between the US and China chip war, Prime Minister Anwar Ibrahim has approached US technology companies to attract new technology investment. The recent influx of investment commitments from international technology firms (AWS, NVIDIA, Oracle, etc.) to Malaysia creates a new challenge for Malaysia's data protection laws. Collectively, investments pledged by technology firms reached 74.5 billion Malaysian ringgit (£13.58 billion) for building new AI, data and cloud services centres.

Malaysia's Southern neighbour, Singapore, which has strategically placed itself on the global innovation stage, is no stranger to navigating challenges in advanced technology. Recently, shifting its focus to tech startups through $1 billion Singapore dollars (£599 million) investment and partnering with global tech firms on AI, Singapore has been at the forefront of technology with its robust digital infrastructure and advanced data centres.

So how do the two neighbours compare in terms of their data protection laws? This article will assess Malaysia and Singapore's recent amendments to their privacy laws.

Malaysia's Personal Data Protection Act (PDPA) 2010 ACT 709

Malaysia's first Personal Data Protection Act was passed in 2010 and was effective by 2013. This act established the Personal Data Protection Department (PDPD) which operates directly under the Ministry of Communication and Multimedia Commission (MCMC). The Personal Data Protection Commissioner enforces the Act through the Personal Data Protection Appeal Tribunal, and the powers granted to the commissioner are stated in Part IX of the PDPA 2010 from sections 110 to 127.

Registration requirement with Malaysia's PDPA

"Data controllers" are specified by classes. To operate in Malaysia, they will have to be registered with the PDPD to ensure compliance. This criterion is found in the Personal Data Protection (Class of Data Users) Order 2013.

Currently, there are 13 classes of data users that are required to register with the PDPA:

1. Banking/financial institutions
2. Communications
3. Direct selling
4. Education
5. Health
6. Insurance
7. Money lender
8. Pawnbroker
9. Real estate
10. Services: accountancy, architecture, audit, engineering and legal
11. Tourism/hospitality
12. Transportation
13. Utilities

Amendments in 2025

A public inquiry was conducted in 2020 with the Public Consultation Paper No.01/2020 (PC01/2020) on 22 areas that aimed to improve Malaysia's privacy laws.

Based on this paper, the PDPA 2010 was amended to include a number of key changes which will come into effect on 1 April 2025 and 1 June 2025. These key changes significantly increase the powers of the PDPD and strengthen data subject rights.

Effective on 1 April 2025

Compliance with the security principles: Data processors must follow the seven security principles as stated in S.5(1) of the PDPA Act 709, requiring a more focused approach to reasonable steps to ensure better security measures in case of personal data breaches. There are increased penalties for failures to comply. Additionally, these steps require organisations to give guarantees of security measures taken.

Cross border transfer rules: Another area of concern for technology firms is the introduction of cross-border data transfer rules. Transfers of personal data would be permitted outside Malaysia under certain conditions. Firstly, transfers are possible to a country where laws are substantially similar to the PDPA. Secondly, the level of data protection offered must have the equivalent levels of protection in comparison with Malaysia's PDPA. Further measures regarding cross border transfers, especially focusing on Transfer Impact Assessments are yet to be introduced.

Definitions for sensitive personal data: The definition of "sensitive personal data" will now include "biometric data" and the narrowed definition of "personal data" will now exclude personal data of deceased individuals.

Increased penalties: Data controllers and processors are now liable for higher penalties. Infringing any of the seven personal data protection principles will result in criminal penalties which may reachup to three years imprisonment and/or a fine of 1 million ringgit (£183,000).

Effective on 1 June 2025

Appointing Data Protection Officers: At least one DPO must be appointed by the data controller and processor to their organisation who will oversee compliance and can be held accountable under the PDPA. The Commissioner must then be notified of the appointment. However, it should be noted that there are proposals to suggest that future DPOs must have certain qualifications, reporting lines, and expertise. Organisations can expect

further guidelines to be released.

Mandatory breach notifications: Another key change is the introduction of mandatory data breach notifications. Organisations will now need to notify the Commissioner "as soon as practical" and notify data subjects "without unnecessary delay" where the breach would significantly affect the data subjects. While the scope of the language is not clear, not all data breaches may need to be notified.

Data portability rights: Data subjects will have the right to request a transmission of their personal data from one data controller to another. Data controllers will now have the responsibility to adhere to these porting requests.

Case law: In 2022, a landmark case law was decided regarding the constitutional right to privacy. The case of *Genting Malaysia Sdn Bhd v Pesuruhjaya Perlindungan Data Peribadi & Ors* [2022] 4 CLJ 399 clarified that blanket requests would infringe rights of privacy. The two contentious points of the case were whether the data protection principles would apply to the Inland Revenue's authority under Section 81 of the Income Tax Act (ITA) 1967 and whether the disclosure of personal data should be considered a breach of the PDPA principles. It was found that the Inland Revenue had no right to issue blanket disclosures under Section 81 ITA and such requests were considered a breach of the data protection principles. However, under certain strict conditions and legal tests or court orders, specific disclosure requests could still be made.

Singapore's Personal Data Protection Act (PDPA) 2012

Singapore's data protection law came into effect in 2012 and was amended in 2020 with the Personal Data Protection (Amendment Act) 2020. The Act complements sector specific laws such as the Banking Act, Insurance Act and Securities and Futures Act which has established provisions that addressed certain aspects of personal data protection.

An interesting provision of the PDPA is that it establishes the Do Not Call (DNC) registry where individuals could register their phone numbers. The registry prevents telemarketers from contacting these individuals.

Singapore's PDPA has an extraterritorial effect, which means that organisations will have to adhere to the PDPA despite not having a physical presence in Singapore.

Enforcement of the Act is carried out by the Personal Data Protection Commission (PDPC). The PDPC may issue orders and guidelines, and sanction both breaches against the PDPA and the DNC registry. Orders, such as asking an organisation to delete data, or injunctions, can be registered with the Singapore District Courts thus making them enforceable court orders. The PDPC also operates an independent appeals body called the Data Protection Appeal Panel.

Registration requirements under Singapore's PDPA

Currently, there is no registration requirement for organisations under the PDPA, but the Commission does encourage organisations to register their Data Protection Officers with it.

Amendments in 2021/2022

The amendments made in 2020 brought significant changes to the Act; mandatory breach notifications, data portability obligations, changes to consent provisions and increased penalties for breaches.

Mandatory breach notifications: Organisations that suffer a data breach will have to notify the PDPC of any breaches of a significant scale (involving 500 or more individuals). In such cases, the PDPC has to be notified of the breach as soon as practicable within a timeframe of 72 hours. This requirement extends to situations where the breach could result in significant harm to individuals.

Higher penalties: Data breach penalties have been raised so that organisations with an annual turnover exceeding 10 million Singapore dollars (£5.95 million) can be fined up to 10% of their annual turnover in Singapore. Previously, the maximum fine was 1 million Singapore dollars (£595,000).

Data portability obligations: The 2020 update introduced data portability for individuals who want to have greater control and autonomy over their personal data. This enables consumers to switch telecommunication providers more easily by creating data porting requests where the porting organisation must transmit the data to the receiving organisation. This is subject to certain exceptions but is similar to the EU GDPR's Right to Data Portability.

Expanded scope of consent: The scope of consent has been extended to cover two new points. Freely given consent by notification, and consent by contractual necessity. Consent by notification provides that individuals must be notified of the purpose of the data collection, disclosure and use. There must be an option to opt out of the collection. Contractual necessity comes into effect when there is a reasonable necessity for a contract or transaction to conclude, hence its collection of personal data.

In case law

In 2024, the largest fines issued by the PDPC were to Singhealth and IHiS that were fined 250,000 Singapore dollars (£149,000) and 750,000 Singapore dollars (£446,000) respectively for their failure to ensure reasonable security arrangements were in place. Furthermore, in the landmark case regarding Singapore's digital privacy, *Michael Reed v Alex Bellingham & Attorney General, intervener* [2022] SGCA 60, the question was whether a private action may be commenced from the emotional distress suffered by contravention of the PDPA. The Court of Appeal clarified that "loss or damage" is sufficient to trigger s.32 PDPA (amended to s.480) and clarified emotional distress stating "emotional distress is an actionable loss of damage, whereas a simple loss of control is not". This position aligns with England and Wales (*Vidal-Hall v Google Inc* [2015] EWCA Civ 311, *PL&B UK Report* May 2015 p.1).

A wild west for privacy laws?

Firms looking to establish a presence in Malaysia and Singapore will have to consider future privacy law measures that may affect their expansion across South East Asia. The recent 2025 reforms in Malaysia and 2022 reforms in Singapore brought alignments in some areas of privacy law; mandatory breach notifications, data portability and introduction of higher penalties. The amendments to Malaysia's PDPA

have a considerable impact for businesses in terms of compliance. Areas such as the appointment of DPOs and internal compliance protocols should be planned or reviewed to avoid costly compliance risks. Despite the possibility of additional costs for businesses, the changes show a move towards a global privacy law standard such as the GDPR. Thus, businesses could potentially anticipate future amendments to follow a certain trajectory.

Singapore's PDPC has been known to be actively enforcing and issuing fines to organisations found guilty of inadequate security measures.

The reforms in Malaysia indicate that future legal actions may be imminent. Case law for both countries has been sparse. The small number of case law leaves room for legislative interpretation which carries the risk of different outcomes in Malaysia and Singapore resulting in different compliance measures for multinational firms.

AUTHOR

Roald Chao is a paralegal in Cruickshanks Solicitors and an LLM (International Business Law) graduate of Queen Mary, London.
Email: RESCwork@outlook.com

INFORMATION

www.ft.com/content/4e0017e8-fb48-4d48-8410-968e3de687bf

www.pdp.gov.my/ppdpv1/en/principles-of-personal-data-protection/

www.pwc.com/my/en/assets/publications/2024/pwc-my-pdpa-bills-key-consideration.pdf

stb.ft.com/article/inside-singapores-rise-global-hub-artificial-intelligence

www.linklaters.com/en/insights/data-protected/data-protected—-singapore

OECD assesses risks and benefits of AI

The OECD Expert Group on AI Futures (Expert Group), while identifying benefits in AI accelerating scientific progress, advancing economic growth and productivity, also says that AI could change societal norms and expectations regarding institutional transparency. AI's ability to sort, filter, and summarise vast amounts of information could lower barriers to disclosure. On the other hand, AI systems that lack sufficient explainability and interpretability erode accountability.

Privacy related risks include malicious cyber activity, manipulation, disinformation, fraud and harms to democracy. Invasive surveillance could limit individuals' freedom of expression and assembly.

The paper, issued in November 2024 recommends ten priority policy actions:

1. Establish clearer rules, including on liability, for AI harms;
2. Consider approaches to restrict or prevent certain "red line" AI uses;
3. Require or promote the disclosure of key information about some types of AI systems;
4. Ensure risk management procedures are followed throughout the lifecycle of AI systems that may pose a high risk;
5. Mitigate competitive race dynamics in AI development and deployment that could limit fair competition and result in harms;
6. Invest in research on AI safety and trustworthiness approaches, including AI alignment, capability evaluations, interpretability, explainability and transparency;
7. Facilitate educational, retraining and reskilling opportunities to help address labour market disruptions and the growing need for AI skills;
8. Empower stakeholders and society to help build trust and reinforce democracy;
9. Mitigate excessive power concentration;
10. Take targeted actions to advance specific future AI benefits.

• *See oecd.ai/en/ai-publications/futures*

Survey on GDPR fines puts Ireland at the top

DLA Piper's *GDPR Fines and Data Breach Survey* of January 2025 reveals that Ireland imposed the highest total amount in fines in the EU. The largest fines were imposed on social media platforms and big tech companies.

Ireland has issued €3.5 billion in fines since the GDPR entered into force in May 2018. This is more than four times the value of fines issued by the second placed Luxembourg Data Protection Authority which has issued €746.38 million (a single fine against Amazon).

"The total fines reported since the application of GDPR in 2018 now stand at €5.88 billion ($6.17 billion/£4.88 billion). The largest fine ever imposed under the GDPR remains the €1.2 billion ($1.26 billion/£996 million) penalty issued by the Irish DPC against Meta Platforms Ireland Limited in 2023."

"In the year from 28 January 2024, €1.2 billion fines were imposed. This was a 33% decrease compared to the aggregate fines imposed in the previous year, bucking the seven-year trend of increasing enforcement. This does not represent a shift in focus from personal data enforcement; the clear year on year trend remains upwards. This year's reduction is almost entirely due to the record-breaking €1.2 billion fine against Meta falling in 2023 which skewed the 2023 figures. There was no record breaking fine in 2024," DLA Piper reports.

• *The survey was published 21 January 2025. See privacymatters.dlapiper.com/2025/01/eu-dla-piper-gdpr-fines-and-data-breach-survey-january-2025/*

Australia stops use of facial recognition in a retail setting

A major Australian hardware chain breached several privacy principles when capturing faces of every individual on CCTV who entered its stores. By **Annelies Moens** of Privcore.

On 29 October 2024, the Office of the Australian Information Commissioner (OAIC) released its long-awaited determination[1] into the use of facial recognition technology (FRT) in Bunnings' stores. Bunnings is a major home and hardware retailer in Australia. The decision is relevant to all retailers with annual turnover greater than three million Australian dollars operating in Australia, as the Federal Privacy Act 1988 has extra-territorial application. The case highlights the importance of ensuring solutions or processes deployed to achieve a particular objective do not create a disproportionate level of privacy risk.

The Privacy Commissioner determined the collection of sensitive information through the FRT system was not necessary. The outcome of the decision is that Bunnings must not continue or repeat the practices the Privacy Commissioner found were in breach of the Privacy Act. Bunnings was also required to publish a statement[2] on its website setting out the decision – to be accessible for a year after publication. Bunnings is seeking a review of the Privacy Commissioner's decision before the Administrative Review Tribunal.

What happened

Bunnings Group Ltd (Privacy) [2024] AICmr 230 (29 October 2024)[3] is a seminal determination by the Office of the Australian Information Commissioner (OAIC) in that it outlines the steps to consider when deciding whether facial recognition technology (FRT) can be rolled out in retailer settings in Australia. Some information was redacted in the OAIC's published decision without providing reasons.

The OAIC's investigation into Bunnings commenced on 11 July 2022 and concluded with the publication of its long-awaited decision on 29 October 2024. In reaching the decision, the *Australian Privacy Principles Guidelines*[4] and the *OAIC Guide to Privacy Regulatory Action*[5] were taken into account.

Bunnings processed facial images of people entering 62 stores over a three-year period to match against a database containing (at its peak) 448 facial images of people whom it considered posed a risk to operations. Risks included individuals, who may impact the safety and security of others, as well as affect Bunnings' stock and facilities.

The FRT system involved the following four steps [para 25]:

1. Video decoding – each frame of the CCTV video was separated into still images.
2. Facial recognition processing – a Gabor filter was applied to each still image to determine whether it contained any images of human faces.
3. Facial feature calculation processing – where a human face was identified from a still image, vector points of the facial features were extracted to create a vector set (the biometric).
4. Comparison processing – each vector set was compared against vector sets previously extracted from the faces of individuals enrolled in the database by calculating the relative differences between the location of the vector points in each vector set.

Where step 4 resulted in a match, an alert was generated containing the information of the enrolled individual and the matched individual (including false positives). Bunnings advised non-matched facial images were automatically deleted within an average of 4.17 milliseconds. As such, its primary argument was it did not collect the personal information of non-matched individuals. The Privacy Commissioner determined there was a collection of the personal information of matched and non-matched individuals.

Bunnings had enrolled a relatively low number of individuals into the database (compared with the number of visitors to its stores). It enrolled people whom it deemed posed a risk to its operations. Bunnings appeared not to have a policy or guidance for the six relevant staff to determine whether to enrol an individual in the database to match against. It sourced facial images from its own CCTV system and state police.

Prohibition on the collection of sensitive information

APP 3.3 prohibits the collection of sensitive information (which includes biometrics), unless the individual consents to that collection or an exception in APP 3.4 applies. Bunnings sought to rely on APP 3.4(b) – that a permitted general situation under section 16A of the Privacy Act existed – in circumstances where it was found to have collected personal information. In particular, Bunnings argued it reasonably believed the collection of personal information was necessary:

1. For it to take appropriate action in relation to suspected unlawful activity, or serious misconduct that relates to its functions or activities; or
2. To lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

The Privacy Commissioner decided the following is relevant to determining whether the collection was necessary in the above exceptions [para 99]:

a) The suitability of the FRT system, including its efficacy in addressing the relevant activity or conduct.
b) The alternatives available to Bunnings to address the relevant activity or conduct.
c) Whether the use of the FRT system was proportionate, which involves balancing the privacy impacts resulting from the collection of sensitive information against the benefits gained by using the FRT system.

In relation to exception one above,

the Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 states at p.67: "The provision, by specifying that the unlawful activity or serious misconduct must relate to an entity's functions or activities, intends that the exception will apply to an entity's internal investigations." This is also reflected in the APP Guidelines and section 6 of the Act in relation to the definition of serious misconduct. As such, it would appear this exception relates to the processing of, for example, employees' personal information, not customer personal information. However, the Privacy Commissioner interpreted this exception broadly to allow the "unlawful activity" exception to apply to Bunnings' customers' personal information [para 107]. The Privacy Commissioner then considered the suitability, alternatives and proportionality points outlined above in relation to collection of sensitive information to take appropriate action to deal with suspected unlawful activity.

In relation to suitability of the FRT system, its effectiveness was predicated upon recidivism and not single acts of unlawful activity. In other words, a person had to be enrolled in the database. Further, enrolled individuals didn't know they were enrolled in the database, therefore it had no deterrent effect. Bunnings had considered a number of alternatives to address suspected unlawful activity. Unfortunately, the FRT system was the option which impacted the broadest cohort of individuals.

In terms of proportionality, the number of enrolled individuals in the database at its peak was 448 individuals. The Privacy Commissioner made the point that "of the significant volume of personal information collected via the FRT system, the respondent could only rely on the FRT system to take appropriate action in respect of unlawful activity on a relatively small number of occasions and in respect of a relatively small number of individuals" [para 144].

The Privacy Commissioner therefore determined the collection of sensitive information in relation to suspected unlawful activity through the FRT system was not necessary.

In relation to exception two above, in terms of suitability, in addition to the points raised above, the serious threat situations Bunnings was seeking to address could not be assisted by the FRT system, for example, someone wielding a weapon or someone wearing a face mask. Likewise, in terms of alternatives, the FRT system was the option which impacted the broadest cohort of individuals. In terms of proportionality, the FRT system, as with suspected unlawful activity, could only be relied upon to take appropriate action in respect of a relatively small number of incidents.

The Privacy Commissioner therefore determined the collection of sensitive information in relation to serious threats through the FRT system was not necessary.

Consent is another basis on which sensitive (biometrics) information can be collected. However, valid consent in these contexts is extremely difficult to obtain. The Privacy Commissioner, for completeness, found there was no consent from individuals for the collection of their personal information. "In order for consent to be valid, it must be informed, voluntary, current and specific, and given by individuals who have the requisite capacity" [para 85] and as outlined in B.38 of the APP Guidelines[6].

Notification of collection

The Privacy Commissioner also found it was reasonable for Bunnings to take steps under APP 5.1 to notify individuals of some or all of the matters outlined in APP 5.2. Further, the privacy notices displayed at entry points in stores did not meet the requirements of APP 5.2. The Bunnings' privacy notice shown between November 2018 and May 2021 at entries to stores indicated video surveillance was utilised. Bunnings considered it was unreasonable to expressly state it was using FRT in its privacy notice as it would undermine the efficacy of the FRT system. In fact, in the author's opinion, transparency would have increased the efficacy of the FRT system, as it would have provided a deterrent to some individuals behaving in ways Bunnings was trying to prevent. This type of strategy is seen in transparency reporting, adopted by some corporations such as, TradeMe[7] in New Zealand. TradeMe lists second hand goods for sale online and curbs the sale of stolen goods through its transparency reporting. The Privacy Commissioner supports this view in paragraphs 215 and 267 of the decision.

In its second privacy notice used between May and November 2021, Bunnings updated its notice to mention that "video surveillance, which may include facial recognition, is utilised".

None of Bunnings' company-wide privacy policies (which is a separate requirement to APP 5) mentioned its use of FRT, therefore Bunnings' breached APP 1.3.

The Privacy Commissioner determined Bunnings failed to notify individuals at or before the time of collection, or as soon as practicable after collection, of the collection of their sensitive information as required under APP 5.

Practice, procedures and systems

More broadly, the Privacy Commissioner found Bunnings had failed to meet the requirements of APP 1.2. This APP requires entities to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities to ensure the entity complies with the APPs, and will enable it to deal with inquiries or complaints from individuals about compliance with the APPs.

The Privacy Commissioner determined, in the circumstances, this necessitated the conduct of the following:

1. A Privacy Impact Assessment (PIA) prior to the implementation of the FRT system (or at the very least a privacy threshold assessment documenting the reasons why Bunnings believed a PIA was not necessary in the circumstances).
2. Written policies and procedures governing the use of the FRT system prior to its implementation.
3. Staff training for those receiving alerts from the FRT system and senior managers in stores using the FRT system.
4. Periodic review and reporting of privacy risks.

Prior to implementing the FRT system, Bunnings had obtained legal advice (which it did not share with the OAIC during the investigation), a

presentation delivered to senior management with passing reference to privacy, selection of a software product by considering its functionality against privacy risks, training by the biometrics vendor to the six staff using the FRT system to advise how to enrol individuals and perform back-ups. The Privacy Commissioner found the steps Bunnings took prior to implementation and during the operation of the FRT system did not meet the requirements of APP 1.2.

Conclusion

Biometrics carry high privacy risks as they involve unique data elements that are difficult to change if compromised (such as a face, iris or fingerprint).

The Privacy Commissioner at paragraph 5 of the determination encourages "all APP entities to proactively consider whether and how their current and future acts and practices align with their obligations under the Privacy Act, particularly when those acts and practices involve the use of technology which may have an impact on the privacy of individuals. In particular, it may be prudent for APP entities currently deploying FRT to reassess their compliance with the Privacy Act in light of the guidance provided by this determination, including by, inter alia, undertaking a Privacy Impact Assessment."

AUTHOR

Annelies Moens is Managing Director at Privcore.
Email: moens@privcore.com

REFERENCES

1 www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2024/230.html
2 www.bunnings.com.au/about-us/facial-recognition-technology
3 www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2024/230.html
4 www.oaic.gov.au/__data/assets/pdf_file/0030/40989/app-guidelines-combined-December-2022.pdf
5 www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action
6 www.oaic.gov.au/__data/assets/pdf_file/0030/40989/app-guidelines-combined-December-2022.pdf
7 www.trademe.co.nz/c/trust-safety/transparency-reporting

Australia: Meta settles $AU50 million for Cambridge Analytica case

The Australian Information Commissioner has agreed to a 50 million Australian dollar (about 31 million US dollars) payment program as part of an enforceable undertaking (EU) received from Meta Platforms, Inc. (Meta) to settle civil penalty proceedings in the Cambridge Analytica case.

This landmark case's payment scheme will be open to eligible Australian Facebook users impacted by the Cambridge Analytica matter, the Commission says.

The mediation started in February 2024 and the settlement was announced 17 December 2024. Meta is to set up the payment scheme, which will be run by an independent third-party administrator. The Commissioner anticipates that individuals may be able to start applying to the payment program in the second quarter of 2025.

"The payment scheme will be structured into two tiers of payments. The first will permit individuals to apply for a base payment if they believe they experienced generalised concern or embarrassment because of the matter. The second category will provide for specific payment, likely to be higher than the base payment, to those who can demonstrate they have suffered loss or damage. The third-party administrator will also establish a timely internal review avenue for individuals in relation to the payment scheme," the Commissioner says.

• *See www.oaic.gov.au/news/media-centre/landmark-settlement-of-$50m-from-meta-for-australian-users-impacted-by-cambridge-analytica-incident*

events diary

What's right for children and their data? Keeping on the right side of the law

11 March 2025
Host: A&O Shearman, London, UK
PL&B in-person and online conference
CPE Credits: up to 4
Register at early bird rates by 18 February at www.privacylaws.com/children2025/
Some free places available for subscribers to *PL&B* UK and International Reports.
Session 1: Identifying child users: Exploring age assurance methods.
Session 2: Navigating and managing risks: Framing consent and parental controls around the best interests of children.
Session 3: Design: Making data rights understandable and accessible for children.
Session 4: What is right for children and their data? Recommendations.
Speakers from: Lego, TikTok, Google, BBC, k-ID and VerifyMy/The Age Verification Providers Association.

CPDP.ai 2025: The world is watching

21-23 May 2025
Brussels, Belgium
A multidisciplinary conference discussing legal, regulatory, academic and technological developments in privacy and data protection.
Early bird fees until 9 March
See www.cpdpconferences.org/

PL&B 38th International Conference: *The Good, the Bad and the Good Enough*

7-9 July 2025
St John's College, Cambridge, UK
Subjects cover a wide range of UK and international policy developments, legislation, enforcement and examples of best practice in compliance.
To register visit www.privacylaws.com/
Sessions include: The global impact of data privacy laws after 50 years;
Debate at the Cambridge Union: This House Believes the concept of 'Special Category Data' needs Reforming; The CNIL's Mobile Apps recommendation; AI Implementation in Practice: Day-to-Day Challenges for Privacy Officers; Navigating the Interplay of the GDPR and Emerging Tech Regulations.

Poland: Landmark ruling on legitimate interests

Poland's Supreme Administrative Court upholds an employer's right to retain rejected applicants' data for defence against potential discrimination claims. By **Xawery Konarski** and **Mateusz Kupiec** of Traple Konarski Podrecki & Partners, Poland.

The Polish Supreme Administrative Court issued a landmark ruling on 20 February 2024 (case no III OSK 2700/22), affirming that employers can lawfully retain personal data of rejected job applicants based on their legitimate interest in defending against potential discrimination claims. This decision provides significant guidance on the interpretation of Article 6(1)(f) of the General Data Protection Regulation (GDPR) concerning the lawful grounds for processing personal data after the conclusion of a recruitment process.

Background

The case originated from a complaint filed by Ms. M.K. to the President of the Polish Data Protection Authority (Polish DPA). Ms. M.K. alleged that A.D.C.P. Sp. z o.o., a company based in G., unlawfully processed her personal data by failing to delete it after the recruitment process concluded and her application was rejected. She also claimed that the company had improperly fulfilled its information obligations under Articles 13 and 15 of the GDPR during the recruitment process.

In January 2022, the Polish DPA issued a decision reprimanding the company for violating GDPR provisions. The authority held that the company had no legal basis to retain Ms. M.K.'s data after the recruitment process ended, stating that data should be deleted immediately unless another legal ground justifies further processing. The Polish DPA argued that the company's reference to potential legal claims was insufficient, as it did not specify any concrete claims or legal proceedings that would necessitate retaining the data.

The company appealed the Polish DPA's decision to the Voivodeship (provincial) Administrative Court in Warsaw. The court overturned the Polish DPA's decision, holding that the company had a legitimate interest in retaining the data to defend against potential claims of discrimination under the Polish Labour Code. The court emphasised that the limitation period for such claims, as specified in Article 291 in conjunction with Articles 183b and 183d of the Labour Code, provided a lawful basis for data retention.

The Supreme Administrative Court's judgment

The Polish DPA appealed the judgment to the Supreme Administrative Court. The Court upheld the decision of the Voivodeship Administrative Court in Warsaw and provided a detailed analysis of the legal grounds under the GDPR for retaining personal data after a recruitment process.

The Court examined whether the retention of the applicant's data was justified under Article 6(1)(f) of the GDPR, which allows processing when it is necessary for the legitimate interests pursued by the controller, except where overridden by the interests or fundamental rights and freedoms of the data subject.

> Employers' need to retain data to defend against potential legal claims is a legitimate interest.

The Court noted that employers have a legitimate interest in retaining data to defend against possible future claims of employment discrimination, as provided for under Polish law. The Labour Code grants candidates the right to seek redress for discriminatory recruitment practices, and employers may need to provide evidence to defend against such claims. The Court emphasised that the employer's legitimate interest must be balanced against the data subject's rights and freedoms. In this case, the Court found that retaining the data for the duration of the statutory limitation period did not disproportionately infringe upon the applicant's rights. The data retention was limited in scope and time and served a specific legal purpose.

Criticism of the Polish DPA's Position

The Court criticised the Polish DPA for not adequately considering the legal framework and for failing to conduct a proper assessment of the legitimate interests involved. The Court pointed out that the Polish DPA did not address the company's arguments regarding the applicable Labour Code provisions and the need to retain data to defend against potential claims. Thus the Court rejected the Polish DPA's assertion that data cannot be processed "just in case" or for hypothetical future claims. The Court clarified that the potential for legal claims is inherent in the employer-applicant relationship, and retaining data for such purposes is recognised under the GDPR when properly justified.

Commentary

This ruling provides important clarification for employers regarding the lawful basis for retaining personal data of unsuccessful job applicants. Employers can rely on their legitimate interests under Article 6(1)(f) of the GDPR to retain such data for the purpose of defending against potential legal claims, particularly those related to discrimination in hiring practices.

However, the retention must be proportionate, limited to what is necessary, and confined to the duration of the statutory limitation period for

such claims. Employers should also ensure compliance with other GDPR principles, such as transparency, data minimisation, and informing applicants about data retention policies.

Data Protection Authorities should note that legitimate interests can include the need to retain data to defend against potential claims, even if such claims have not yet materialised. The ruling encourages a more balanced approach that respects both the rights of data subjects and the legitimate needs of controllers.

Supporting this perspective, France's Data Protection Authority (the CNIL) also acknowledges that employers may retain personal data of rejected candidates to defend against potential legal claims. The CNIL suggests that while the primary purpose of processing ends after recruitment, data necessary to demonstrate the fairness of the recruitment process can be retained temporarily for evidentiary purposes.

The Court's reasoning is also worth placing in the broader context of the recent CJEU case law. In its judgment regarding case C 621/22, *Koninklijke Nederlandse Lawn Tennisbond*, the CJEU held that a legitimate interest under Article 6(1)(f) of the GDPR must be lawful but does not need to be determined by law. The CJEU clarified that commercial interests could constitute legitimate interests, expanding the scope of what may be considered valid grounds for data processing.

Juxtaposing the CJEU's judgment with the Polish Supreme Administrative Court's ruling, both courts recognise a broad interpretation of "legitimate interest" under the GDPR. While the CJEU acknowledged that commercial interests might justify data processing, the Polish Court affirmed that employers' need to retain data to defend against potential legal claims is a legitimate interest. However, both courts also highlight that the processing must be necessary and proportionate. In the CJEU case, the Court stressed that the processing should be limited to what is absolutely necessary and that data subjects' rights should not be outweighed by the controller's interests. Similarly, the Polish Court emphasised that data retention must be confined to what is necessary for the specific legal purpose and limited in time.

AUTHORS

Xawery Konarski is a Senior Partner and co-founder of the law firm Traple Konarski Podrecki & Partners, Poland, and Mateusz Kupiec is an Associate at the same firm.
Emails: xawery.konarski@traple.pl
mateusz.kupiec@traple.pl

INFORMATION

This article has been previously published by INPLP, a not-for-profit international network of qualified professionals providing expert counsel on legal and compliance issues relating to data privacy, www.inplp.com

US trade organisations advocate federal privacy law

Thirty-nine US trade associations wrote to the US Congress on 28 January calling for a comprehensive national level privacy law. The signatories say that Congress should "adopt a federal privacy framework that fully pre-empts state laws related to data privacy and security."

The trade associations argue that the current situation is challenging for consumers as they have to navigate an inconsistent patchwork of state laws. In addition, technological developments and advances in AI call for timely action, they say.

• *See www.uschamber.com/assets/documents/Coalition_PrivacyDay_SenateCommerceHouseEC_2025-01-28-143316_mbsb.pdf*

EDPB calls for alignment between GDPR and other EU digital laws

The European Data Protection Board (EDPB) says in its December 2024 statement that legal certainty is needed between new digital legislation and the GDPR. The DPA group recalls some of its ongoing initiatives to clarify the enforcement interplay of the GDPR with the AI Act, the EU Data Strategy and the Digital Services Package.

The EDPB says it has already begun to work on this issue within the scope of its competence, including preparation of guidelines on the interplay between the GDPR and some of these new laws. The EDPB may decide to develop guidance together with the EU Commission or other competent authorities.

The EDPB welcomes the Commission's invitation to establish cooperation with other sectoral regulators established under the new EU digital legislation. The EDPB says that it will continue to actively participate in EU-level structures designed to facilitate this cross-regulatory cooperation, such as the Digital Markets Act (DMA) High Level Group and the European Data Innovation Board.

• *See www.edpb.europa.eu/news/news/2024/edpb-calls-coherence-digital-legislation-gdpr_en*

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 180+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked in advance of the free-place deadline. Excludes the Annual Conference. More than one place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

> "An indispensable resource for anyone who has a serious interest in privacy, combining latest news with thoughtful commentary and analysis."
>
> **Richard Cumbley, Partner, Linklaters**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the UK GDPR and related regulatory changes, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.