MARCH 2025

Ius Laboris Workplace Data Privacy Update

No 3, March 2025

Global HR Lawyers
Ius Laboris

Table of contents

Our experts from around the world have put together an update on data privacy, setting out recent changes to the law, policies and procedures.

Since welcoming the start of the new year, data privacy practitioners worldwide have seen major developments including, key rulings concerning employee data and workplace monitoring, major fines issued for data breaches, emerging legislative changes, and proposed growth opportunities in the realm of artificial intelligence.

The UK has seen government push for the development of AI, recently publishing the AI Opportunities Action Plan to reinforce the country's commitment to a pro-innovation regulatory approach. Additionally, the ICO have reprimanded an NHS Trust for failing to respond to subject access requests promptly, highlighting the importance of prioritising data management practices.

In Belgium, the DPA issued warnings to employers for unlawfully restricting access to their timesheets and failing to promptly close business mailboxes after employment contracts were terminated. The DPA has also provided clarity on the use of cookie banners, confirming that users should be provided with all options in an equivalent manner. In Cyprus, the Data Protection Commissioner ruled against excessive data collection in job applications, reinforcing the principle of data minimisation. France has been active in enforcing data privacy laws, with the CNIL imposing substantial fines for excessive surveillance of employee activity and unsolicited marketing practices.

There has also been a collection of fines levied against major tech enterprises, with Ireland's DPC fining LinkedIn EUR 310 million for unlawful data processing and targeted advertising, the Italian Garante fining OpenAI EUR 15 million for various data privacy violations related to its ChatGPT service, and the Dutch DPA fining Netflix EUR 4.75 million for failing to provide clear and sufficient information to their customers in its privacy policy.

Across the globe, the Indian government has released draft data protection rules to facilitate the implementation of the new data protection law, focusing on notice and consent obligations, information security safeguards, breach reporting, data retention mandates and data subject rights. Whilst in Brazil, we have seen the introduction of new regulations for Data Protection Officers, clarifying requirements and workplace data governance.

In Singapore, the Personal Data Protection Commission clarified the test for defence under the PDPA, and in Türkiye, new guidelines on the transfer of personal data abroad were published. Ukraine saw a rare criminal proceeding for the unlawful use of personal data on the internet, resulting in a fine for the offender.

ALEXANDER MILNER-SMITH

Partner at our UK law firm and Chair of our Expert Group on Data Privacy

alexander.milner-smith@lewissilkin.com

SEAN ILLING

Managing Associate at our UK law firm

sean.illing@lewissilkin.com

Belgium

Inger Verhelst
BELGIUM
inger.verhelst@claeysengels.be

Unlawfully restricting an employee's access to their timesheets (Case no. 14/2025)

In its ruling on 23 January 2025, the Belgium Data Protection Authority (DPA), confirmed that the right to receive a copy of the data is an intrinsic part of the right of access.

In this case, an employee repeatedly requested copies of his timesheets from his employer. Despite these requests, the company failed to provide the copies, offering no valid justification for their inability to do so. The company only offered to let the employee review the documents at the head office.

The DPA ruled that by restricting the employee to merely consulting the timesheets at the head office, the company infringed upon the employee's right of access. As a result, the DPA issued a warning to the employer regarding the handling of future GDPR requests. Additionally, the DPA ordered the company to comply with the employee's request and provide him with the copies of his timesheets.

This case underscores the importance of employers adhering to GDPR regulations, particularly the right of access to personal data. The decision by the DPA serves as a reminder that organisations must not only allow employees to view their personal data but also provide copies upon request. Ultimately, employers should take proactive measures to ensure processes are in place for handling data access requests.

Access to and use of the business mailbox after the employee's departure (Case no. 11/2025)

On 22 January 2025 a decision was issued in response to a complaint about a data controller's failure to promptly close the business mailbox of its employee after their departure. Although the employment contract was terminated, the

mailbox remained open.

In its decision the Belgium Data Protection Authority (DPA) reiterated its well-established position. Employers must implement an out of office message no later than the last day of the actual departure of the employee.

This message must inform all correspondents that this person is no longer working in the organisation and provide the contact details of the person to be contacted or a general email address.

The out of office message should be active for a reasonable period of time. The DPA considers one month to be reasonable but considers an extension up to three months possible depending on the employee's responsibilities and on the condition that the employee consents, or at least has been informed of the extension.

In this case, the DPA established that the employer did not comply with the rules relating to the management of a former employees' e-mail accounts. The DPA has issued a warning to the employer.

The decision underscores the critical importance of adhering to established guidelines for managing former employees' mailbox accounts. Employers must ensure that an out of office message is implemented by the last day of an employee's departure, clearly communicating the change and providing alternative contact details. This practice not only maintains professional communication standards but also aligns with data protection regulations. The DPA's warning in this case serves as a reminder to all organisations of the necessity to comply with these rules to avoid potential repercussions and to uphold the integrity of their data management practices.

Clarity provided on the use of cookies and cookie banners (Case no. 113/2024)

On 6 September 2024 the Belgium Data Protection Authority (DPA) reiterated that the consent to the installation of cookies that are not strictly necessary must be given freely and unambiguously, and that this is not possible if an equivalent choice is not offered at the same level of information. Moreover, the consent must always be easily revoked again.

The use of deceptive design patterns is unlawful and, consequently, the "accept all" button should not be more prominent than other options to encourage the user to click the "accept all" button. Both options must be presented in an equivalent manner and at the same level of information.

The press sites must obtain the user's consent for the installation of cookies that are not strictly necessary and, in the absence of this, another legal basis, such as the legitimate interest, may not be chosen afterwards to allow the installation of the cookies.

The DPA ruled that in this case the company needs to make

the necessary adjustments within 45 days of becoming aware of the decision by modifying the cookie banners and not using misleading button colors. If the adjustments are not made, a penalty of EUR 25, 000 will be imposed for each non-compliant order.

Belgian DPA Upholds Website's Rejection of Salary Erasure Request for Public Company Managers (Case no. 103/2024)

The Belgian Data Protection Authority (DPA) held that a website that publishes the salary of public companies' managers rightfully rejected an erasure request, since the publication of this data is necessary for exercising the right of freedom of expression and information.

In this case, the controller of a website collected pieces of information from the manager of a company owned by the Belgian and French governments and published it. The website provides free information about mandates, management functions or professions held by public mandataries. The manager objected to the processing of his data and filed an erasure request. The controller refused to erase the data, arguing that the publication of this information on its website contributes to the transparency essential to the proper functioning of democracy with regard to the attribution of certain mandates, functions and professions. Moreover, this information was already published on the website of the Court of Auditors and of the Official Journal and that publication on these websites was required by law. The Belgian Law of 2 May 1996 stipulates that a manager of a company is obliged to file a declaration mentioning all mandates, management functions or professions and how much they are earning from these positions.

The DPA followed the reasoning of the controller. The balancing of interests that must be carried out between the manager's fundamental right to the protection of personal data and the controller's right to freedom of expression and information was in favour of the controller.

In the process of balancing these rights, the DPA considered that the manager's salary was already publicly available on official websites, in accordance with the Belgian legislation. The purpose of the processing is also in line with the Law of 2 May 1996, i.e. to increase awareness among the citizenship regarding how public money is spent. A request aimed at removing the disputed information from this website was therefore not justified, and the DPA held that the controller rightly refused to erase the data.

Back to top ↑

Brazil

José Carlos Wahle
BRAZIL
jose.wahle@veirano.com.br

Fábio Pereira
BRAZIL
fabio.pereira@veirano.com.br

The Role of the Data Protection Officer in Brazil: Recent Developments and Workplace Compliance

With the growing enforcement of Brazilian Data Protection Law ("LGPD"), organisations must strengthen their data governance strategies—especially in the workplace. A key component of compliance is the Data Protection Officer ("DPO"), who is responsible for serving as the primary liaison between data subjects, the company, and the Brazilian Data Protection Authority ("ANPD"). The DPO can be a natural person, who may be an employee of the Controller or external to the organisation or a legal entity (for example, a company that provides DPO as a Service).

On July 2024, the ANPD published today the Resolution CD/ANPD No. 18/2024, which approved the Regulation on the role of the DPO ("Regulation). The Regulation aims to establish complementary rules regarding the role of the DPO within an organisation, such as the requirement to (i) appoint a DPO and a Surrogate DPO, who will step in during absences, impediments, or vacancies; (ii) formalize the appointment of the DPO and Surrogate DPO by a Term of Appointment (i.e. a written, dated, and signed document clearly and unequivocally stating the processing agent's intent to designate the respective DPO and Surrogate DPO); (iii) disclose the identity and contact information of the DPO in a clear, objective, and easily accessible manner (e.g. through the privacy notice); and (iv) ensure that the DPO is able to communicate clearly and accurately in Portuguese with data subjects and the ANPD, has expertise in data protection legislation, and does not hold concurrent roles that could create a conflict of interest.

Later in 2024, the ANPD published the Guidance on the DPO's Role ("Guidance"), aiming to provide additional clarity and support organisations in

Giulia Volante
BRAZIL
giulia.volante@veirano.com.br

interpreting the Regulation. The Guidance emphasises that Processing Agents must ensure the DPO has the technical and administrative conditions to fulfill their role effectively. It also recommends that the DPO possesses expertise beyond data protection laws, including risk management, information security, compliance, and auditing.

Furthermore, the Guidance clarifies that conflicts of interest may arise if the DPO simultaneously holds executive or managerial positions, particularly those responsible for determining the means and purposes of data processing. To mitigate potential conflicts, the ANPD recommends the establishment of an "independent organizational unit" within companies, ensuring that the DPO's decisions are not influenced by competing interests.

The appointment of the DPO remains mandatory for all Controllers, except for small-scale Processing Agents, who are only required to appoint a DPO when they carry out high-risk data processing, as stipulated by Resolution CD/ANPD No. 2/2022. Nevertheless, even in cases where a DPO is not mandatory, small-scale Processing Agents must still provide a communication channel for data subjects.

On the other hand, the appointment of a DPO by Processors is optional but is considered a best practice for good governance. From an operational perspective, it is uncommon for a Processor not to also act as a Controller. Therefore, this exception is unlikely to have a significant impact on organisations.

The responsibility for ensuring compliance with the LGPD lies with the Processing Agent. The performance of the DPO's activities does not confer personal liability for the compliance of the Controller's data processing activities before the ANPD. However, the DPO may still be held personally liable under the Brazilian Civil Code if they act unlawfully, causing damages or losses.

Recently, the ANPD initiated an enforcement action targeting 20 large companies in Brazil that failed to disclose the contact details of their DPOs or provide a communication channel for data subjects. This demonstrates the authority's commitment to ensuring compliance with LGPD's

governance requirements. The investigations highlight the importance of transparency and accessibility regarding data protection practices within organisations.

With ANPD ramping up enforcement, businesses must prioritise compliance with DPO requirements and workplace data governance. The DPO is no longer just a regulatory requirement—it is a strategic role that ensures organisations align with legal obligations, mitigate risks, and foster a privacy-conscious culture. By structuring their data protection programs effectively, companies can demonstrate compliance, avoid penalties, and build trust with employees, customers, and stakeholders.

Back to top ↑

Cyprus

Vasilis Charalambous
CYPRUS
vasilis.charalambous@gzg.com.cy

Data collection in a job application

An anonymous complaint was made to the Office of the Commissioner for Personal Data Protection ("DPC") through the Department of Labour Relations, regarding the collection of excessive data in a job application from a company and specifically the information text included in the application. The company had the same job application form for all job applications, requesting salaries of previous work experiences.

During the examination of the complaint, the DPC had instructed the company to amend its job application, however, it did not remove the field regarding the salaries of previous work experiences.

The DPC ruled that there was a breach of article 5(1)(c) of the GDPR since the company as a controller did not adhere to the data minimisation principle and issued an order to the company on 21 February 2024 to:

- amend and/or format the job application form so as to collect data on the salary that applicants had in previous jobs, only in cases of recruitment for managerial and/or senior positions, not at the initial stage or stages of the recruitment process, proceeding for each such procedure, to balance the necessity of processing the data in question; and
- inform the DPC of its actions within two months of the adoption of the DPC's decision.

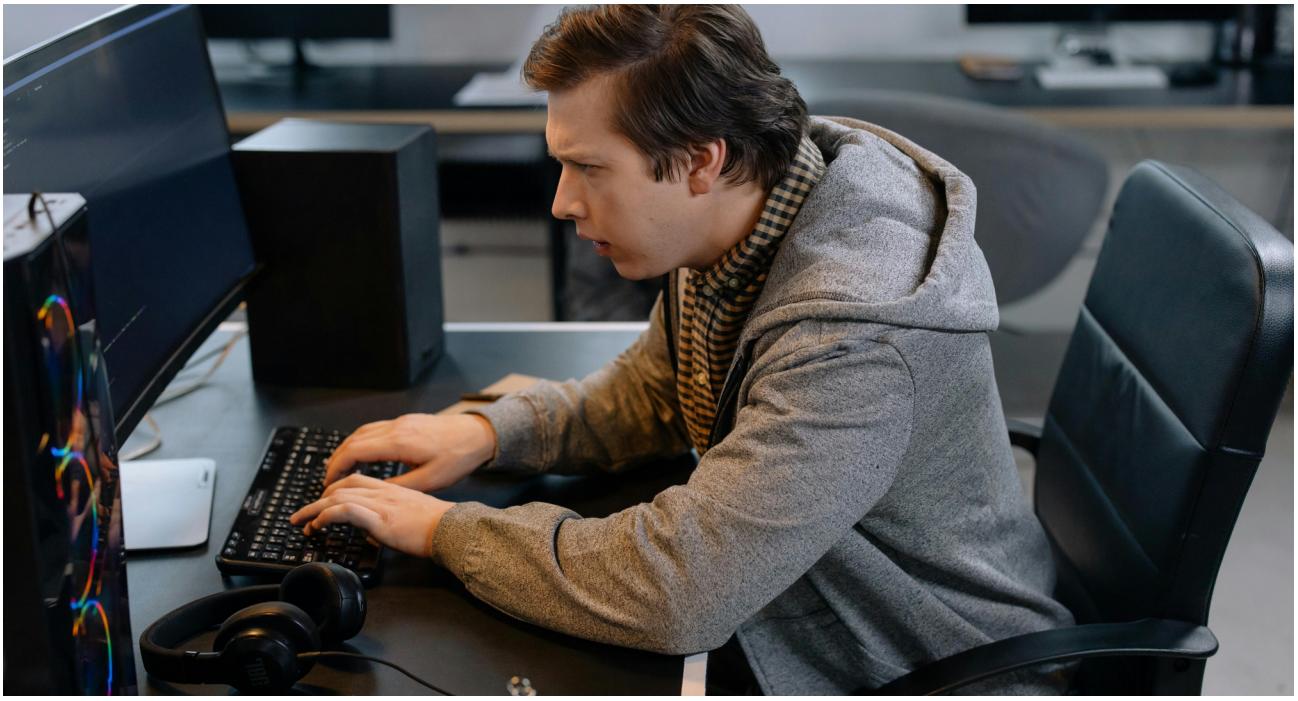
Rights of the data subject

The DPC found a prima facie violation of article 12(4) of the GDPR by a company that did not inform the complainant and former employee of the company, of the reasons for not acting and not fully satisfying his request from the outset, as well as of the possibility of submitting a complaint to a Supervisory Authority and

of the right to judicial remedy.

The former employee alleged that he was unjustly dismissed from the company and requested some documentation from the company which was related to the reason for his dismissal. Although, the company satisfied the former employee's complaint to the extent it could, it didn't proceed to satisfy the request to the extent requested, since the rights of others could have been affected.

On 19 July 2023, the DPC imposed the administrative sanction of reprimand to the company in relation to the violation of article 12(4).



Back to top ↑

Denmark

Elsebeth Aaes-Jørgensen
DENMARK
eaj@norrbomvinding.com

Selma Carøe
DENMARK
sca@norrbomvinding.com

Obtaining passport information and criminal records in recruitment processes (Case no. 2023-431-0025)

On 5 September 2025, the Danish Data Protection Agency (DPA) issued an opinion about a stadium that asked job applicants to upload passport information, residence permit when needed, and criminal records when uploading job applications.

The stadium stated that the passport information and residence permit, if necessary, were only collected at this early stage in the recruitment process in cases where casual workers were hired immediately based on the uploaded applications and to ensure that they could legally work in Denmark.

As regards the processing of criminal records, the stadium said that it had a very special risk profile in relation to the risk of terrorism and other crimes associated with large sports and entertainment events and that the stadium employed a very large number of people, often on a short-term basis.

Further, the stadium had specifically assessed the necessity of obtaining the information in question for the individual job categories at the stadium.

On this basis, the DPA found that the collection of passport information and criminal records in connection with the recruitment process was in accordance with the GDPR.

The ruling shows that there may be special circumstances that justify obtaining and processing information about applicants earlier in the recruitment process than is generally the case. However, it is important to be aware that the employer must make a concrete assessment of the necessity of obtaining the information in question.

Back to top ↑

France

Stéphanie Poussou
FRANCE
spoussou@capstan.fr

Guillaume Bordier
FRANCE
gbordier@capstan.fr

Excessive surveillance of employee activity

On the 19 December 2024, the French DPA (CNIL) fined a real estate company EUR 40,000 for excessive employee surveillance.

The decision of the CNIL was the result of an investigation after it had received numerous complaints that the company were filming employees and tracking activity.

The filming surveillance system captured both audio and video recordings of employees at the premises with an aim to prevent theft. These recordings were viewed by managers on mobile applications in real time. The CNIL confirmed that such monitoring consisted of an excessive infringement of employees' rights and was contrary to data minimisation principles (Article 5(1)(c) GDPR).

Furthermore, the activity monitoring software placed on employee devices used to track employee work performance, take regular screenshots of computers, and record periods of inactivity, particularly of those employees working from home, was found to be disproportionate. The system was not an accurate measure of working hours, and the software could not effectively determine if an employee had been productive or not. On this basis, an infringement of Article 6 of the GDPR (i.e. no legal basis for processing personal data) had been found.

The company had also failed to provide adequate information to its employees, ensure data security, and did not conduct a Data Protection Impact Assessment (DPIA) (Article 35 of the GDPR). The CNIL emphasised that the company should have conducted a DPIA before implementing such monitoring measures due to the high risk to employees' rights and freedoms.

The basis of the fine was determined on the violations and the company's financial situation and its small size, aiming for a deterrent but

proportionate penalty.

The violations included:

- Excessive employee surveillance.
- Continuous video and audio recording in the workplace, which violated the principle of data minimisation (Article 5(1)(c) of the GDPR).
- The use of monitoring software to measure working hours and productivity, which was deemed unreliable and disproportionate.
- Inadequate written information provided to employees about the monitoring, in violation of Articles 12 and 13 of the GDPR.
- Shared access to an administrator account, which compromised data security, violating Article 32 of the GDPR.
- Failure to conduct a Data Protection Impact Assessment (DPIA) for the monitoring software, violating Article 35 of the GDPR.

The decision serves as a reminder to protect individual rights in the workplace. Any form of employee surveillance must comply with data protection regulations, ensuring the practices are necessary and proportionate.

Unlawful processing of personal data, by KASPR, collected from LinkedIn pertaining to users who had restricted their visibility on the platform.

On July 28, 2022, the French Data Protection Authority (CNIL) conducted a compliance check on KASPR. KASPR operates a Chrome browser extension that enables users to obtain the business details of individuals whose LinkedIn profiles they have visited.

The investigation revealed that KASPR's database contained approximately 160 million contacts, including various personal and professional details.

KASPR collected data from LinkedIn users who had made their details visible to all (Option two) as well as from those who had limited visibility to first and second degree connections (Options three and four).

Four years after implementing the KASPR tool, the company notified data subjects via email, offering them the option to object to the processing of their data.

KASPR argued that their processing was based on legitimate interest to facilitate professional connections and that users should reasonably expect identity verification on a professional networking service.

However, the CNIL found several violations including:

- No legal basis under Article 6 GDPR for processing data from users who limited

Back to top ↑

their visibility.

- No clear data retention period, violating Article 5(1)(e) GDPR.
- Inadequate transparency and information provision under Articles 12 and 14 GDPR.
- Failure to provide access to data under Article 15 GDPR.

As a result, the CNIL imposed a fine of EUR 240,000 and ordered KASPR to rectify its data processing practices within six months, including stopping the collection of data from users who have limited visibility, ceasing the automatic renewal of the storage period, informing data subjects in a language they understand, and adequately responding to access requests.

Orange fined EUR 50 million for unsolicited marketing practices

The French Data Protection Authority (CNIL) issued a substantial fine of EUR 50 million to France's main tele-communications operator, Orange, for displaying advertisements in users e-mail inboxes and operating cookies on user devices without consent.

Orange provides an email messaging service to its users called "Mail Orange". This service is provided to approximately 7,800,000 users.

During an investigation conducted by the CNIL between 7 and 12 June 2023, it was found that advertisements and marketing messages were embedded in users' inboxes without obtaining consent. Additionally, the company had continued to use cookies across user devices to track activity even after users had withdrawn consent.

Orange argued that the obligation to obtain users' consent for advertising fell on the advertiser, not on them, as they merely transferred the advertisers' emails to users. They also explained that they used a system that allowed them to disseminate advertising emails without processing users' email addresses. However, the CNIL did not accept this defence and stated that the company had direct control over the ads and sold the spaces to advertisers. There was a clear infringement: "the company has derived a definite financial advantage from the infringements" as "advertising is not at the heart of the company's activities". In reaching its decision, the CNIL had also cited the CJEU judgment C-102/20, concluding that promotional emails required users' consent, according to Article L. 34-5 of the Postal and Electronic Communications Code (CPCE).

Regarding cookies, the CNIL held that their persistent functioning after consent was withdrawn was prohibited by Article 82 of the Informatics and Freedoms Act (Law no. 78-17). The mere reading of cookie data fell under this prohibition. Orange had been "highly negligent" and should have been aware of its duties given its "position on the market and the means at its disposal."

For violations of Articles 82 of the Law no. 78-17 and Law no. 34-5 of the CPCE, the CNIL imposed a fine of EUR 50 million and ordered the cessation of the unlawful operation of cookies within three months, subject to a penalty of EUR 100,000 per day in case of delay.

This decision acts as a "warning for other operators" to ensure compliance with direct marketing and cookie laws as failure to do so will result in administrative actions and penalties.

Back to top ↑

Germany

Jessica Jacobi
GERMANY
jessica.jacobi@kliemt.de

Jakob Friedrich Krüger
GERMANY
jakob.krueger@kliemt.de

GDPR requirements for works agreements on employees' personal data

On 19 December 2024, the European Court of Justice (ECJ) issued a ruling following a submission from the German federal labor court (BAG) on data protection rules in works agreements.

Article 88(1) GDPR allows EU member states to adopt 'more specific rules' on the processing of employees' personal data, including through collective agreements. According to Article 88(2) GDPR, these rules must include suitable measures to safeguard employees' fundamental rights.

In this case, a works agreement permitted employees' data processing that would have been unlawful under the legal justifications in the GDPR.

The BAG posed the questions whether data processing in works agreements must only be compatible with Article 88 (2) GDPR or comprehensively with all provisions of the GDPR (in particular Articles 5, 6 (1) and 9 (1) GDPR) and whether the parties to the works agreement have room to negotiate the scope of the regulations that apply, which can only be reviewed by the courts to a limited extent.

The European Court of Justice has ruled that works council agreements on the processing of personal data must comply with the lawfulness and limits of the GDPR (in particular, Articles 5, 6(1) and 9(1) and (2) GDPR must be taken into account), but has not conclusively outlined the relationship with the German regulations. Accordingly, it remains to be seen how the national courts will implement the decision.

Claims for damages in connection with Art. 15 GDPR, if this is not fulfilled

On 17 October 2024, the Federal Labor Court (BAG) issued a

ruling regarding the claims for damages due to a failure to provide information and the resulting feelings of anxiety.

The BAG clarified that claims for non-material damages under Article 82 GDPR cannot be based solely on the plaintiff's fears triggered by a violation (in this case, the unlawful seizure of a USB stick in combination with the failure to provide information). The court emphasised that uncertainty about data processing does not automatically constitute damage. This is significant as it limits the scope for compensation based only on concerns or fears, ensuring that actual damage must be proven.

The plaintiff requested information about his personal data stored by the defendant in accordance with Art. 15 GDPR. The request also related to data stored on a USB stick used privately by the plaintiff, which the defendant had seized on suspicion of unlawful storage of member data. The plaintiff claimed that the right to information had not been fulfilled. The plaintiff feared that the defendant could misuse the data and pass it on to third parties.

The court ruled that the plaintiff also bears the burden of proof for the damage when asserting claims for damages. Negative feelings (fears) can in principle constitute damage. The court's examination focuses on whether these feelings can be considered "justified" in view of the specific circumstances. This involves assessing the overall situation and ultimately the plaintiff's credibility on the basis of a substantiated factual submission. The court takes the view that the uncertainty about the scope of the data processing lies in the nature of the failure to provide information. If reliance on such fears were sufficient to justify damage, any breach of Article 15 GDPR - which could theoretically give rise to a claim under Article 82(1) GDPR - would in practice lead to damage. In this case, the plaintiff's description was not sufficient.

Non-material damages for unlawfully disclosing personal data to thousands (ArbG Duisburg - 3 Ca 77/24)

On 26 September 2024, the Duisburg labour court issued a ruling regarding the claims for damages for breach of data protection law in connection with a circular email.

The data subject, an employee of an air sports association, shared details of his health in an email to 24 people, including the association's president, on 11 May 2023. A month later, the association's president sent an email to almost 10,000 association members, claiming the data subject had made unfounded allegations and had been on sick leave since November 2022. The data subject felt his reputation damaged by the email, especially when he met new people at the affiliated airports and clubs. The data subject demanded EUR 17,000 in damages because the president's actions disclosed his

sensitive health data and falsely created the impression that he was harming the association by feigning illness.

According to Article 82(1) GDPR, the court decided that the data subject was entitled to EUR 10,000 in damages. The President unlawfully processed health data via the email without the data subject's consent, and the processing was not justified by another legitimate purpose. The court clarified that the data subject's email did not contain consent to the sharing of his health data, even though some recipients of the data subject's email and the president's email overlapped.

The court based its decision on the fact that health data was unlawfully processed by the email without the data subject's consent. The court clarified that the data subject's email did not constitute consent for the disclosure of his health data, even though some recipients of the data subject's email and the controller's email overlapped.

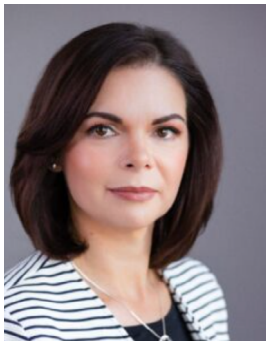
Back to top ↑

Hungary

Hédi Bozsonyik

HUNGARY

hedi.bozsonyik@bozsonyikfodor.com



Dalma Portik-Bakai

HUNGARY

dalma.portikbakai@bozsonyikpartners.com

Changes to the rules and practices of document retention

As of 1 January 2025, Act LXXXI of 1997 on Social Pensions was amended, changing the obligation of employers to keep records.

Previously, employers were required to keep employment records for five years after the insured person reached retirement age. From 1 January 2025, this obligation will be phased out and employers will only be required to retain documents created by 31 December 2024, for a period of five years after the insured person reaches the applicable retirement age.

As a result, employers will need to change their record-keeping practices and, in the case of retention beyond the statutory period, be able to justify the processing on the basis of legitimate interest through a balancing of interests test.

Back to top ↑

India

Stephen Mathias
INDIA
stephen.mathias@bgl.kochhar.com

Arun Babu
INDIA
arun.babu@bgl.kochhar.com

India's new draft data protection rules

Sixteen months after India's new data protection law was enacted, the government has released draft rules to facilitate its implementation. These rules provide necessary details and an actionable framework for businesses to comply with various requirements under the new law, including notice and consent obligations, information security safeguards, breach reporting obligations, data retention mandates, obligations of controllers notified as 'significant data fiduciaries' by the government, facilitation of data subject rights, and parental consent mechanisms for processing children's data. The rules also indicate potential restrictions on cross-border data transfers and establish a framework for consent managers.

Specifically, the rules confirm that consent would need to be obtained through a privacy notice in granular/itemised form, listing each personal information collected, the purpose of the same and the specific product or service it is meant for.

The rules also require a two-stage breach notification: (1) to the proposed data protection authority; and (2) notification to the data subject in every case of a data breach.

The rules also require every data controller to meet several data security requirements "at a minimum".

Another major concern with the rules is the broad authority granted to the Indian government to demand information from data controllers without sufficient

Gayathri Poti
INDIA
gayathri.poti@bgl.kochhar.com

safeguards, potentially complicating data transfers from the EU to India.

Overall, the rules are considered to be fairly onerous compared to global standards.

For now, the rules remain in draft form, and the government is undertaking public consultations and accepting feedback on the rules until 5 March 2025.

Back to top ↑

Ireland

Linda Hynes
IRELAND
linda.hynes@lewissilkin.com

DPA fine of EUR 310 million to LinkedIn for unlawful processing of personal data for behavioural analysis and targeted advertising

This inquiry was launched by the DPC, in its role as the lead supervisory authority for LinkedIn, following a complaint initially made by a French non-profit organisation to the French Data Protection Authority.

The inquiry examined LinkedIn's processing of personal data for the purposes of behavioural analysis and targeted advertising of users who have created LinkedIn profiles. The decision concerns the lawfulness, fairness and transparency of this processing. The decision includes a reprimand, an order for LinkedIn to bring its processing into compliance, and administrative fines totalling EUR 310 million.

The DPC found that LinkedIn had breached the overarching principles of fairness and transparency (Article 5(1)(a) GDPR) all throughout the course of the processing.

The inquiry found that none of the legal basis invoked by LinkedIn justified the data processing at hand. Specifically, the consent of the LinkedIn users to this processing had not been freely given, sufficiently informed, specific or unambiguous. Further, LinkedIn's legitimate interests were overridden by the interests and fundamental rights and freedoms of data subjects and LinkedIn could not rely on contractual necessity for the processing.

In addition, the inquiry found that the information provided to data subjects by LinkedIn regarding the lawful basis it claimed to rely on was insufficient.

The DPC held that LinkedIn could not rely on consent under Article 6(1)(a) GDPR, legitimate interests under Article 6(1)(f) GDPR nor contractual necessity under Article 6(1)(b) GDPR for

its processing.

Comment: This decision highlights that the processing of personal data without an appropriate legal basis outlined in Article 6(1) GDPR is a clear and serious violation of data subjects' fundamental right to data protection.

The GDPR requires that processing is carried out in accordance with the principle of fairness, which requires that the personal data may not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject.

Compliance with transparency provisions ensures that data subjects are fully informed of the scope and consequences of the processing of their personal data in advance and are in a position to exercise their rights.

DPA fined a County Council EUR 29,500 for the excessive processing of CCTV footage of public and private areas and the failure to conduct a DPIA DPC (Ireland) - 07/SIU/2018 - GDPRhub

The controller, a local County Council, had installed CCTV cameras at bottle banks and housing estates stating that they were to enforce the Irish Litter Pollution Act 1997 and detect anti-social behaviour.

These cameras filmed both public and private areas continuously, and the footage was stored without clear records or a defined retention period. The cameras also captured passers-by and individuals using nearby facilities, with some monitoring screens accessible to unauthorised persons due to lack of security measures.

The DPC found that the use of CCTV cameras at bottle banks was not justified under the Litter Pollution Act 1997 or the Waste Management Act 1996. It noted the Law Enforcement Directive did not provide for such a broad scope of CCTV footage processing.

The DPC identified 14 issues, including unlawful processing and failure to conduct a Data Protection Impact Assessment, leading to violations of the GDPR and the Irish Data Protection Act 2018.

Key violations identified by the DPC:

- Security of Monitoring Screens: Breach of Article 5(1)(f) and Article 32(1) GDPR due to inadequate security, allowing unauthorised access.
- Excessive Monitoring: Breach of Article 5(1)(c) and Article 25 GDPR for excessive monitoring of public spaces without implementing privacy masking.
- Data Retention: Breach of Article 5(1)(e) GDPR for retaining data longer than necessary.
- Records of Processing: Breach of Article 30 GDPR for failing to maintain records of data processing.

- Signage and Transparency: Breach of Article 13 GDPR for failing to inform individuals about the processing.

The DPC issued a fine of EUR 29,500 and ordered the controller to comply with data processing regulations

Comment: This decision highlights the importance of oversight and adhering to proper data protection principles. The level of the fine was determined at a level that the DPC considers would be dissuasive to the extent that is necessary to avoid future infringements.

DPA issued a EUR 251 million fine to Meta for failing to prevent a data breach compromising the data of millions of Facebook users as well as its failure to adequately document the breach

In September 2018, the DPC initiated two inquiries into Meta Platforms Ireland Limited's data processing activities. This followed a significant data breach involving Facebook's "View-as" function, which allowed users to see their profiles as others would. This feature included a video upload function that created "user tokens," coded IDs used to verify users and control access to features and personal data.

Between 14 and 18 September 2018, third parties exploited these tokens to access other users' accounts, affecting approximately 29 million users globally, including 3 million in the EU/EEA. Meta employees detected the breach due to an unusual spike in video uploads and subsequently removed the function.

Decision One: Documentation Concerning the Data Breach

- The DPC found that Meta violated Article 33(3) GDPR by failing to include necessary information in their data breach report, resulting in a reprimand and an EUR 8 million fine.
- The DPC also found that Meta violated Article 33(5) GDPR by not properly documenting the breach and remedial actions. For obstructing the supervisory authority's ability to verify compliance, the DPC issued a reprimand and a EUR 3 million fine.

Decision Two: Privacy by Design

- The DPC determined Meta violated Article 25(1) GDPR by not embedding data protection principles into the feature's design, resulting in a reprimand and a EUR 130 million fine.
- The DPC also found that Meta violated Article 25(2) GDPR by not ensuring that only necessary personal data was processed by default, leading to a reprimand and a EUR 110 million fine.

Comment: As highlighted by the Data Protection Commissioner, this decision highlights how the failure to build in data protection requirements throughout the design and development cycle can expose individuals to very serious risks and harms, including a risk to the fundamental rights and freedoms of individuals.

Back to top ↑

Italy

Paola Pucci
ITALY
spp@toffolettodeluca.it

Mauro Gallo
ITALY
mauro.gallo@toffolettodeluca.it

Italian Garante fines OpenAI for EUR 15 million (Case no. 755/2024)

In 2023 a series of news stories emerged on the existence of bugs regarding the Chat GPT service, run by OpenAI. On this basis, the Italian DPA (Garante) imposed on OpenAI a well-known temporary limitation to data processing of subjects established in Italy, as an urgency measure, and started an ex officio investigation regarding the issues above.

At the end of the investigation, the Garante fined OpenAI for EUR 15 million due to a series of data privacy violations. An additional measure has also been imposed on the data controller, requiring it to perform a six-month public campaign to raise awareness about ChatGPT's data processing practices and user rights under the GDPR. Among the main breaches identified by the Garante, the fact that the data processing was not transparent (the data privacy notice was in English only and not easy to reach from the controller's website), an adequate age-verification mechanism was lacking and that the controller failed in identifying the legal basis before starting the data processing.

Comment: This decision is noteworthy as it highlights the Garante's significant focus on data processing related to AI. It concludes a prolonged investigation and a series of measures implemented by the Garante to enhance both compliance and awareness concerning this issue.

What is clear is that a legal basis must exist prior to processing personal data and AI systems must not cost a data subject their privacy.

At the end of January 2025, the Garante had also initiated an investigation into DeepSeek and decided to impose a limitation to their data processing.

Italian Civil Supreme Court considers lawful the recording of conversations with managers, without their consent, if the data are used as evidence in an employment law proceeding (Case no. 24797/2024)

The Italian Supreme Court held that an employee can lawfully record a business meeting, in the absence of an attendees consent, where such information was to be used as evidence in an employment law proceeding. According to the court, the right to a defence in legal proceedings takes precedence over an individual's right to privacy.

In this case, which forms part of a broader dispute, an employee had recorded a conversation between some managers, without the managers being aware of this. Some years later, another employee used this recording as evidence in an employment-law proceeding.

The employer filed a complaint before the Italian Data Protection Authority (DPA) that was rejected.

The decision of the DPA has been challenged before the relevant Tribunal that upheld the data subject claim and considered the data processing unlawful. The decision was mainly based on the fact that, at the time of the recording, there was no defence needs.

The decision was brought before the Italian Civil Supreme Court (Corte di Cassazione) by the employee. The Corte di Cassazione firstly pointed out that, at the time of the recording (2016), the GDPR was not in force. According to the legislation in place in 2016 the recording must be considered lawful because the consent of the managers is not needed provided that the processing was necessary to assert or defend a legal claim, provided that the data is processed exclusively for such purposes and for no longer than is necessary for the pursuit of those purposes. Secondly, the Court added that it is not relevant that the recording is made by a different person from the one that is using it in the labour trial. Lastly, the Court also stated that in the case of application of the GDPR, the conclusion would have been the same.

Comment: This decision is relevant because it confirms a principle that had been previously stated only by criminal courts in Italy: employees can record, without consent or previous notice, conversations at the workplace if the recording is only used as evidence in a trial.

Back to top ↑

Mexico

Adolfo Athié
MEXICO
aathie@basham.com.mx

Renata Buerón
MEXICO
rbueron@basham.com.mx

New local data protection authority to be defined in 2025

On 28 November 2024, the Mexican Senate approved the "Organic Simplification" bill, which dissolves seven autonomous constitutional entities, including the National Institute for Transparency, Access to Information, and Personal Data Protection (INAI). The INAI has played a key role in ensuring government transparency and protecting personal data.

On 20 December 2024, this bill was published in the Official Gazette of the Federation (DOF). Under this reform, responsibilities for access to information, transparency, and personal data protection will be transferred to the Ministry of Anti-Corruption which will assume responsibility for the protection of personal data held by private parties and obliged subjects.

The Mexican Congress must amend the data protection legislation to, among other changes, formally designate the Ministry of Anti-Corruption as the new data protection authority. This amendment is expected to take place in the first half of 2025.

As the legislation has not yet been amended, it remains uncertain how the new data protection authority will be structured. However, according to government statements, for obligated subjects on data protection, transparency oversight will be divided among authorities per branch of government (executive, judicial, and legislative), as well as autonomous bodies, political parties, and labour unions. And for private entities, the sole data protection authority will be the Ministry of Anti-Corruption.

It is relevant to mention that INAI's past rulings will remain legally valid.

This reform significantly alters Mexico's transparency framework, shifting oversight from an independent body to government-controlled

institutions. Critics argue it marks a return to past decades, where a single dominant political party operated with minimal transparency. Now, the government will oversee itself, raising concerns over accountability and access to information.

Erika Itzel Rodríguez

MEXICO

erodriguez@basham.com.mx

Iván García Argueta

MEXICO

igarcia@basham.com.mx

Back to top ↑

Netherlands

Philip Nabben
NETHERLANDS
p.nabben@bd-advocaten.nl

Ilse Spee
NETHERLANDS
i.spee@bd-advocaten.nl

Netflix fined EUR 4.75 million for not properly informing its customers

On 26 November 2024, almost five years after the complaint had been filed, the Dutch Data Protection Authority (DPA) issued a decision to impose a fine of EUR 4,750,000 to Netflix. The request to investigate Netflix's practices was advanced by noyb, after representing complaints from data subjects that Netflix had failed to provide necessary and sufficient information, in a clear and transparent way, within its privacy statement for customers.

The case was transferred from the Austrian DPA to the Dutch DPA as Netflix's European headquarters are situated in the Netherlands.

The investigation by the DPA spanned a period from 2018 to 2020, specifically relating to concerns with Netflix's privacy statement and helpdesk (which had been established to assist with questions regarding the processing of personal data).

The DPA identified that the privacy statement lacked sufficient information on the purposes of processing personal data in a transparent way. Specifically, the DPA had found the following:

- A lack of sufficiently clear information in the privacy notice for data subjects on access requests.
- Failure to mention the duration of retention periods within the privacy policy. The DPA did not accept a retention explanation of "permitted by laws and regulation" within the privacy policy as a sufficient defence.
- There was also no mention of which countries data subject rights in relation to international data transfers outside of the EEA. There was also no mention of which countries personal data was to be transferred

to, possible adequacy decisions and whether there are appropriate safeguards for the processing.

Furthermore, Netflix had made use of several service providers active in advertising who were likely to receive and process personal data of its customers. These service providers were not identified in their privacy notice.

According to the DPA, Netflix's actions amounted to several violations under the GDPR, including Article 5, Article 12, Article 13 and Article 15.

Netflix's primary defence in this regard was, in short, that the obligations arising from the GDPR contain open norms and that a data controller has a certain degree of freedom in the way they determine the way in which information is provided and the appropriate level of transparency in that regard. This defence, however, could not change the ruling of the DPA.

Since the ruling, Netflix has updated its privacy notice and helpdesk to end the violations.

Comment: This decision is noteworthy, as it underlines the importance of ensuring that all necessary information is included in a privacy notice in a clear, organised and transparent manner.

The complete decision of the DPA can be found on the website of the Dutch Data Protection Authority:

https://www.autoriteitpersoonsgegevens.nl/actueel/boete-netflix-voor-niet-goed-informeren-klanten

Back to top ↑

Poland

Michalina Kaczmarczyk
POLAND
michalina.kaczmarczyk@raczkowski.eu

Processing of personal data by religious organisations concerning former members (Case no. III OSK 769/23)

In its decision on 3 September 2024, the Polish Data Protection Authority (DPA) rejected a complaint of a former member of the Jehovah's Witnesses. The data subject left the organisation in 2020 and wanted to erase her data from the controller's data base. The case was later lodged with the Administrative Court and was decided in favour of the controller. Subsequently, the data subject lodged an appeal with the Supreme Administrative Court.

On appeal, the Polish Supreme Administrative Court did not revisit all the case facts, and ruled that the processing of historical data of a former member of a religious organisation may be lawful under Article 6(1)(f) GDPR and does not have to be based on consent under Article 6(1)(a) GDPR.

The GDPR, specifically Article 17, does not bestow rights upon any enforcement organisations, be it a court or a DPA, to demand a return of documents or copies of documents.

Comment: This case demonstrates that the lawful processing of historical data may be valid under Article 6(1)(f) GDPR, which pertains to legitimate interests, without necessitating consent under Article 6(1)(a) GDPR. It also affirms that the GDPR, specifically Article 17, does not empower any enforcement bodies, including courts or Data Protection Authorities, to mandate the return of documents or their copies. This decision highlights the balance between data protection rights and the legitimate interests of data controllers, particularly within the context of religious organisations.

Unlimited access to data excludes personal nature of processing

On 16 October 2024, the

Supreme Administrative Court ruled that when personal data is shared on social media, this will fall within the scope of the GDPR, where the information is accessible to an infinite number of users.

In this case, an individual, a member of the data subject's family, published the court verdict via their Facebook account. The verdict was published in that way for 11 days and had referred to the data subject.

The data subject filed a complaint with the Polish Data Protection Authority (DPA). The DPA dismissed the complaint as it considered that the personal data was published under Article 2(2)(c) GDPR, i.e. for purely personal activity. Additionally, the individual and the data subject were related. Thus, according to the DPA, the processing fell outside the scope of application.

The data subject brought an appeal with the Administrative Court. The court repealed the DPA's decision, and the DPA lodged a cassation appeal before the Supreme Administrative Court.

The Supreme Administrative Court explained that the notion of purely personal activity was inherently limited. When the personal data was made accessible to an unrestricted number of people, for instance social media users, it excluded the application of Article 2(2)(c) GDPR. The court based its reasoning on Recital 18 GDPR, case C-212/13 and WP29 Opinion 5/2009.

Comment: The verdict is a consequence of the case law of the Court of Justice of the European Union in this area, which has already been shaped over the years. It is important to remember that Article 2 of the GDPR does not tie processing to business or profit-making purposes.

Back to top ↑

Slovakia

Peter Marciš
SLOVAKIA
marcis@nitschneider.com

Marek Bugan
SLOVAKIA
bugan@nitschneider.com

Slovak DPA Rules on GDPR Breach: Auto-Reply Consent

The Slovak Data Protection Authority (Úrad na ochranu osobných údajov Slovenskej republiky) issued a ruling which identified a breach of the GDPR following an employee's complaint against the employer for using an auto-reply message without consent.

The employee was on long-term sick leave and asserted that the employer had decided to write an auto-reply message to be sent from the employee's account with the following wording: "This is an autoreply. Due to [note: my] long-term sick leave, please, contact in work-related matter (...). Name and surname of the [note: concerned] employee".

The employee claimed that she had never written the autoreply and that the employer had used her name and surname as a signature under the text without her knowledge or consent.

In its defence, the employer argued that it had requested several times from the employee to draft her own autoreply. However, due to the employee's failure to respond, the IT postmaster was instructed to compose an auto-reply on her behalf.

The DPA ruled that the employer's actions to use the employee's name and surname, to falsely authorise the message, contravened the employee's wishes. In particular, this action was carried out without her consent. The DPA confirmed that the actions violated the fundamental principles of fairness and transparency and failed to meet the requirements for lawful processing under Article 6(1) of the GDPR.

As best practice we strongly recommend (i) employers sign off on communications where they are providing an autoreply email on behalf of an employee; and (ii) employers to avoid disclosing any health data (for example information about sick leave) of an employee in such communication messages.

Back to top ↑

Singapore

Lionel Tan
SINGAPORE
lionel.tan@rajahtann.com

The clarified test for the defence under section 4(1)(b) of the Singapore PDPA (Reed, Michael v Bellingham, Alex (Attorney-General, intervener) [2022] 2 SLR 1156)

Section 4(1)(b) of the Singapore Personal Data Protection Act ("PDPA") provides that "any employee acting in the course of his or her employment with an organisation" is not subject to certain obligations under the PDPA.

The Singapore Court of Appeal in this case examined this defence in detail and laid out the applicable test to be applied to determine if the defence is available to an employee.

It held that the issue of whether in taking a particular action, an employee acted in the course of his employment was a question of mixed fact and law. Evidence had to be adduced of:

- what was done;
- what the employment required the employee to do; and
- in appropriate cases, whether the employee deliberately evaded practices set up by the employer to deter such action.

Only then would the Court be able to determine whether the employee's action should be attributed to the employment or whether the employee was off on a frolic of his own.

This case thus clarifies the test that will be applied when an employee claims that he breached an obligation under the PDPA by virtue of their employment.

Telemarketing violation will not be covered by the employment defence (Wee Jing Kai Leon [2023] SGPDPC 8)

The Do Not Call Registry ("DNC Registry") is a national database kept and maintained by the Singapore Personal Data Protection Commission ("PDPC"), pursuant to section 39 of the PDPA. Persons may register their Singapore telephone numbers with the DNC Registry so as to not receive unsolicited telemarketing calls and messages.

Under section 43 of the PDPA, a person cannot send telemarketing messages to a Singapore telephone number unless that person has, at the time of sending the message, valid confirmation that the Singapore telephone number is not listed in the DNC Registry.

In this case, the PDPC was responding to numerous complaints it had received that one Wee Jing Kai Leon ("Mr Wee") had sent unsolicited telemarketing messages to telephone numbers registered on the DNC Registry. The PDPC found that Mr Wee had breached section 43 of the PDPA.

It also considered whether the defence under section 48 of the PDPA, which provides that section 43(1) of the PDPA does not apply if it can be shown that the sender of the telemarketing material did so in good faith in the course of his employment or in accordance with instructions given to him by or on behalf of his employer in the course of his employment, was available to Mr Wee. The PDPC held that the defence was not available to Mr Wee as in accordance with industry practices, real estate salespersons are not in an "employer-employee relationship" with their agencies.

This case thus clarifies that real estate salespersons cannot invoke the defence under section 48 of the PDPA and claim that they are merely sending out telemarketing materials in the course of employment with the real estate agency that they are registered with.

Back to top ↑

Türkiye

Batuhan Şahmay

TÜRKIYE

batuhan.sahmay@bener.com

Oguzhan Yorulmaz

TÜRKIYE

oguzhan.yorulmaz@bener.com

Announcement Regarding Guidelines on Transfer of Personal Data Abroad

The Guide on the Transfer of Personal Data Abroad Has Been Published!

The Guide on the Transfer of Personal Data Abroad ("Guide") has been published to provide guidance regarding the transfer of personal data abroad within the scope of Article 9 of the Personal Data Protection Law. The guide outlines the principles and implementation requirements for conducting international data transfers in compliance with the applicable regulations. You can access the Turkish version of the Guide at the following link: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/13711235-abb6-4b17-9a6b-0a68c1ad86c5.pdf.

Ukraine

Vitalii Meliankov
UKRAINE
meliankov@vkp.ua

Vladyslav Ivanov
UKRAINE
Ivanov@vkp.ua

Use of other person's personal data to create a Facebook account and publish offensive posts in public groups (Case no. 463/6663/24)

On 23 July 2024, the Lychakiv District Court of Lviv issued a ruling in case No. 463/6663/24 regarding the use of other person's personal data to create a Facebook account and publish offensive posts in public groups.

The Court ruled that the accused was guilty of unlawful collection, storage and usage of confidential personal data of another individual, including their name, date of birth, photographs, and contact information. Using this personal data, the accused created a Facebook account using other person's personal data and published offensive posts in public groups.

The offender was fined UAH 8500 (EUR 192.60).

This case is interesting as unlawful use of personal data, especially on the Internet, is seldom the subject of criminal proceedings in Ukraine.

Back to top ↑

United Kingdom

Lee Ramsay
UNITED KINGDOM
Lee.Ramsay@lewissilkin.com

Zahra Laher
UNITED KINGDOM
Zahra.Laher@lewissilkin.com

The UK's AI Opportunities Action Plan

On 13 January 2025, the UK government introduced the AI Opportunities Action Plan designed to harness the transformative potential of artificial intelligence (AI) across various sectors, with an aim to make the country an "AI superpower".

The action plan is structured around three pillars, each with a specific goal:

- **Lay the foundations to enable AI.** The recommendations in this section focus on continuing with sustained investment in computational power and AI infrastructure. This is expected to drive the creation of high-skilled jobs, increase investment opportunities, and growth of AI based service businesses. Key to this will be access to high-quality data for fuelling "frontier AI progress and high-quality AI applications" whilst "enabling safe and trusted AI development and adoption through regulation, safety and assurance".

- **Changing lives by embracing AI.** The action plan outlines strategies for scaling AI deployment across the public sector positioning the sector as the "largest customer and as a market shaper". Specific goals mentioned include increasing the efficiency of public sector employees through the use of AI assistants to complete repetitive tasks, streamlining report and form drafting with AI tools, leveraging AI to assist with healthcare diagnostics and use of AI to improve threat detection and anomaly identification. This section is pivotal in the government achieving its broader transformative agenda, including the five missions set out in the Plan for Change.

Jessica Dempster
UNITED KINGDOM
Jessica.Dempster@lewissilkin.com

- **Secure the future of homegrown AI.** Building on the above two pillars, this section focuses on positioning the UK as "national champions at the frontier of economically and strategically important capabilities". This section also includes the establishment of a new unit, UK Sovereign AI, aimed at promoting public-private partnerships to maximise the UK's position in frontier AI.

Employment Considerations

The AI Opportunities Action Plan is set to transform working practices by driving economic growth. Certain strategies proposed include:

- Training, attracting and retaining AI talent: train AI professionals across the "technology stack" to meet expected demand. Assist in bridging the skills gap creating new job opportunities and enhancing the workforce skill set to thrive in an AI economy.
- Creating an inclusive workforce by increasing diversity in the AI talent pool.
- Increasing the use of AI resources within the public sector to streamline repetitive processes and administrative tasks freeing up employees time to focus on value add work. This can lead to a shift in responsibilities requiring employees to adopt technologies and workflows in daily practices.
- Supporting AI adoption across the private sector to drive AI adoption across the country and accelerate its use by working throughout supply chains.

Regulatory approach

The action plan reinforces the UK's commitment to a pro-innovation regulatory approach, supporting AI growth and removing any deterrents. Particularly, the action plan includes the following requirements for regulators:

- Publication of annual reports demonstrating how AI innovation has been facilitated within respective sectors.
- Advance AI in priority sectors by collaborating with government and promoting AI initiatives such as regulatory sandboxes.
- Ensure sponsor departments focus on fostering safe AI innovation practices within strategic guidance to regulators, including empowering the Regulatory Innovation Office to drive regulatory innovation for technologies.
- Liaise with government to identify needs required to scale up AI capabilities.
- Align AI governance frameworks with the proposed Data (Use and Access) Bill.

Unlike the EU, the government continue to express little appetite in introducing AI specific legislation and continue to leverage existing legislation (across various areas such as data protection, cybersecurity, employment, online safety etc) to address AI concerns. Several regulators – including the ICO, CMA, FCA and Ofcom – have outlined their strategies for AI regulation to ensure innovation is not stifled when safeguarding rights and freedoms.

Failure to respond to SARs promptly.

The ICO launched an ex-officio investigation into the United Lincolnshire Teaching Hospitals NHS Trust (the "Trust") for failing to comply with the UK GDPR. The investigation scrutinised the the Trust's handling of subject access requests ("SARs") from 1 March 2021 to 31 March 2022.

The Trust, as the data controller, admitted to a significant shortfall in its handling of SARs. Specifically, it failed respond to 32% of SARs within the statutory one-month timeframe, breaching Articles 12(3), 15(1), and 15(3) of the UK GDPR. While 68% of SARs were answered on time, the Trust acknowledged flaws in its logging system, which affected the accuracy of the data provided to the ICO. Consequently, the Trust could not specify the exact number of unanswered SARs.

The investigation revealed that the Trust's SAR management system was inadequate, prompting its transition to a more effective system in 2024. Several deficiencies were highlighted, including data quality issues and the inability to accurately track SARs. The case management system lacked essential functionality, and the data included requests for records of deceased individuals, which are not subject to UK GDPR. Additionally, the Covid-19 pandemic further strained resources and hindered the retrieval of paper records.

To address these issues, the Trust implemented several measures:

- Developing an Information Asset Management Strategy ("IAMS")
- Procuring a new case management system

- Updating its Access to Records Policy
- Providing staff training
- Recruiting additional staff

The Trust aims to digitise patient records by March 2025, in line with NHS England's Plan for Digital Health and Social Care. Despite these efforts, a backlog of SAR cases remains, though improvements have been noted by the Commissioner.

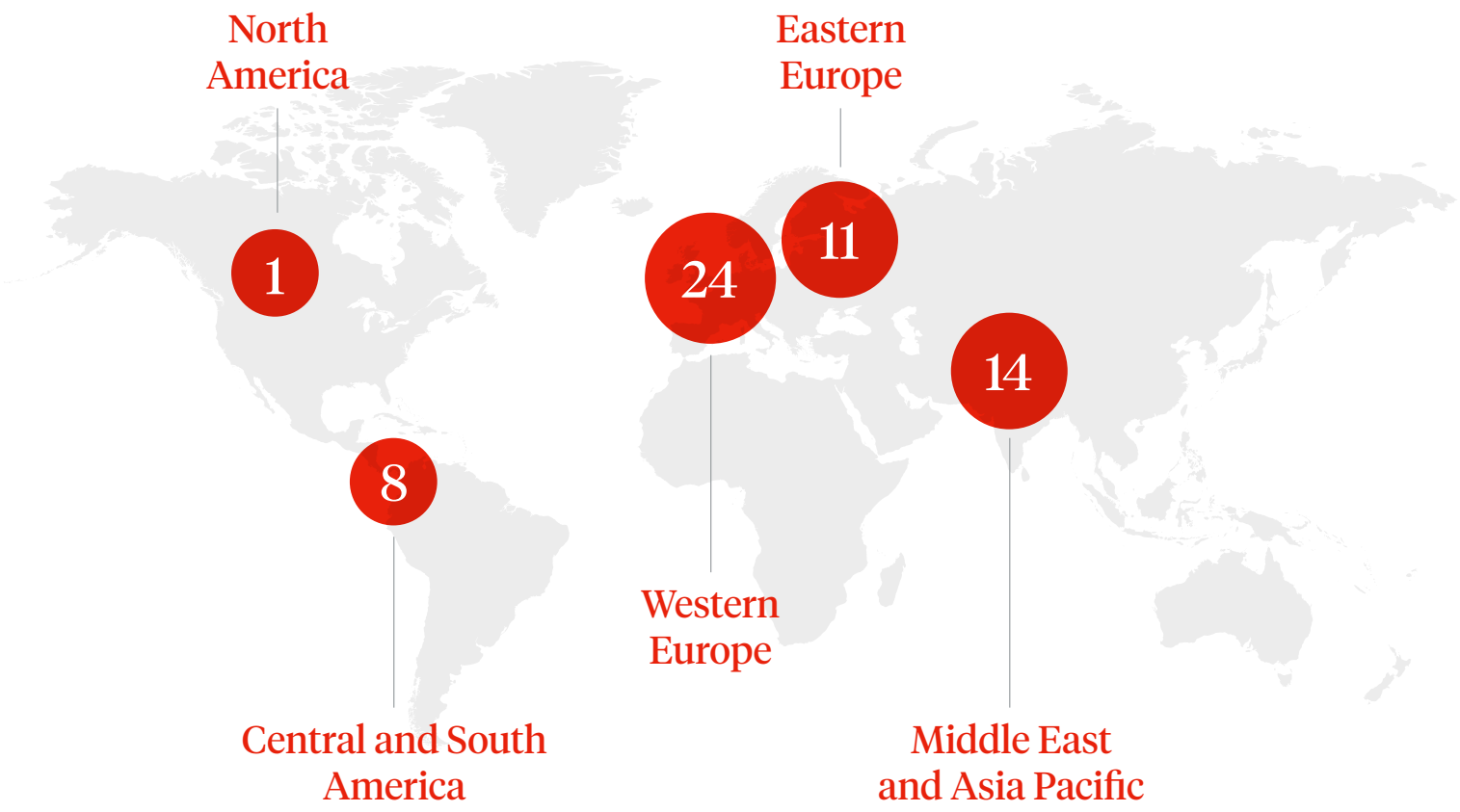
On 13 December 2024, the Commissioner issued a reprimand to the Trust, considering the remedial steps already taken. The Trust was invited to provide representations but chose not to. The Commissioner made several recommendations to improve compliance with UK GDPR, including:

- Adhering to the IAMS
- Maintaining the Records of Processing Activities (ROPA)
- Responding to all outstanding SARs
- Ensuring timely responses to future SARs
- Monitoring compliance
- Ensuring adequate staff resources and training.

Our comment: this reprimand serves as a critical reminder for organisations to prioritise data privacy compliance by implementing robust systems, ensuring timely and accurate responses to SARs, and continuously monitoring and improving their data management practices. The Trust's experience underscores the potential consequences of non-compliance and the importance of proactive measures to safeguard personal data.

Back to top ↑

Ius Laboris
Geographical Coverage



We understand the challenges of managing a national and international workforce

- Ius Laboris is a close-knit alliance of leading employment law firms working together in one global practice.
- Ius Laboris brings together the finest team of dedicated specialists, advising multinational companies in the major commercial centres across the world, from immigration to individual contracts, and from restructuring to pensions, our expertise covers all aspects of HR law.
- We are an integrated alliance, sharing experience, knowledge and training.
- International employment law is our core business.

@iuslaboris
/iuslaboris
iuslaboris.com
info@iuslaboris.com

Global HR Lawyers
Ius Laboris