JANUARY 2026

Ius Laboris Workplace Data Privacy Update

No 6, January 2026

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.

As we start 2026, it's time for a new year update on workplace privacy, where employee rights remain a priority and regulatory activity shows no signs of slowing down. This edition provides a round-up of the most significant developments shaping compliance and employer obligations across the globe.

Employee monitoring continues to attract attention, with Denmark's regulator taking a strong stance on covert recording practices and issuing a decision on when audio or video monitoring can and cannot be justified in the employment context. Enforcement trends also remain strong within the EU. Polish courts have issued multiple fines for inadequate security measures when handling employee data, alongside a ruling that held a former employee criminally liable for misusing client data for personal business purposes. Germany's Federal Labour Court has also weighed in, clarifying how fines should be reached following data breaches and the factors that aggravate or mitigate liability.

Cyber and data security remain under the spotlight worldwide. In Singapore, a substantial penalty was imposed on a company following a breach that exposed personal data, reinforcing regulators' expectations around timely safeguards, breach response, and accountability in high-risk environments. Meanwhile, the EU has unveiled its Digital Omnibus package, proposing legislative changes spanning cybersecurity, AI, and data laws - an early signal of the more integrated compliance landscape employers will need to navigate.

Elsewhere privacy reform is gathering pace. New Zealand has introduced the Privacy Amendment Act 2025 and issued the country's first Biometric Processing Privacy Code 2025. Further afield, Chile is moving forward with significant updates to personal data and labour regulation, and we provide an employer focused overview of what these changes mean and how employers should prepare. In India, the rollout of the new digital data protection law continues to reshape obligations; Sweden has proposed aligning national rules with EU AI Act; and Ireland has published an overview of its designated competent authorities under the EU AI Act, a key step in shaping governance and oversight.

Finally, this edition also explores current practices around processing employee personal data, the legal framework for background checks, and regimes governing the public display of employee details (including names and ID numbers). Monitoring and surveillance remain recurring themes, but so too do proportionality, transparency, and data minimisation.

You'll find full details on these developments and more below.

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

Chile

Marcela Salazar
CHILE
msalazar@munitaabogados.cl

Court orders supermarket to stop printing employee personal data on receipts

In October 2023, an employee of a supermarket chain reported that customer receipts displayed employees' personal data, specifically the full name and national ID number (RUT) of the cashier who handled the sale. The receipts also identified the treasurer and/or the sales floor operator in charge. The complaint asserted that this practice constituted processing of personal data without complying with the Chilean Data Protection Act (Law No. 19.628), particularly because the employees had not provided express, prior, informed, and written consent.

The investigation confirmed that there was no uniform criterion in how the name appeared, and that the receipts listed the cashier's or treasurer's full name and RUT. The company acknowledged including the name on receipts as a way to identify the seller, invoking industry custom and the use of name badges, but failed to demonstrate valid consent in accordance with the law.

Court's decision

The court upheld the fundamental rights action (known as a tutela) for violation of employees' right to protection of personal data (Article 19 No. 4 of the Constitution and Law No. 19.628), holding as follows:

- There is no sufficient justification to process employees' personal data by including it on receipts without their consent.
- Under Law No. 19.628, consent must be expressed in writing and given after the person is properly informed about the purpose of storage and potential public disclosure of their personal data, requirements that were not met.

The company was ordered to cease this practice as of the date of the judgment, if it was still ongoing.

Accordingly, the court determined that including employees' names and RUT on receipts constitutes a processing and disclosure of data to third parties that requires a legal basis or valid consent, which was absent. The judgment was issued on 30 October 2023, by the Labor Court of Valdivia (RIT T-63-2023).

Practical takeaway

Companies must review and adjust processes that involve handling or disclosing employee data, especially when such data is visible to customers or the public. Exposure to risk is high when there is no lawful basis or informed, written consent; seemingly standard industry practices do not replace legal requirements, nor mitigate liability for violations of fundamental rights.

Personal data and labour regulation set to take effect in Chile later this year

On 13 December 2024, Law No. 21.719 (the "Law") was enacted. The Law will take effect 24 months after its publication, on 1 December 2026. Its objective is to regulate the manner and conditions under which personal data processing is carried out, and to enhance the protection of data subjects' rights, including provisions reflected in employment contracts, Internal Rules of Order, Health and Safety, and security measures – anticipating future regulatory guidelines and oversight by the competent authority.

This new Law, which governs the Protection and Processing of Personal Data and creates the Personal Data Protection Agency, introduces a series of obligations for all entities that process personal data. From an employment standpoint, companies access and process the personal data of their employees; therefore, the Law applies fully to employers.

Key obligations introduced by the Law include the following:

- **Information and Transparency:** The data controller must make specific, detailed information permanently available to public on its website or any equivalent medium. This includes the company's personal data processing policy, the identification of data controller and its legal representative, and the designation of the compliance officer.

- **Data Protection by Design and Default:** Employers are required to implement data-protection measures from the design stage and by default, limiting processing to the personal data strictly necessary for labour-related purposes.

- **Contracts with Data Processors:** If the employer outsources data processing to a third party (e.g. human resources service providers, payroll software companies etc), it must enter into a contract regulating the purpose, duration, objectives, type of data, categories of data subjects, and the obligations of the parties, ensuring that the processor complies with all legal requirements.

- **Appointment of Data Protection Officer:** Employers may designate a data protection officer or delegate, who will be responsible for overseeing compliance with the Law and serving as the point of contact for data subjects and the Agency.

- **Data Protection Impact Assessments:** Where data processing may pose a high risk on employees' rights (for example, systematic and comprehensive profiling of personal aspects of data subjects, including processing or automated decision-making), the employer must carry out a Data Protection Impact Assessment (DPIA) prior to initiating the processing activity.

- **Adoption of Policies and Security Measures:** Once the required policies have been developed, companies will need to amend certain provisions of their Internal Rules of Order, Hygiene and Safety (RIOHS) to incorporate the relevant security measures and regulate new obligations and prohibitions applicable to employees. Additionally, if the

company voluntarily adopts an "Infractions Prevention Model" under article 49 of the Law, the obligations arising from such model must be incorporated into employment contracts and into the RIOHS.

Employers will also need to update employment contracts to record the employee´s consent for personal data processing and to establish the employee's responsibility to keep such data updated.

» **Notification of Security Incidents:** In the event of a breach of security measures that poses a risk to data subjects' rights, employers must notify the Personal Data Protection Agency, and, in certain cases, the data subjects affected.

As noted above, the Law will enter into force on 1 December 2026. Its implementing regulations, which further develop and supplement key aspects, are still pending enactment. Accordingly, new regulations and interpretative guidance from the authority may arise, and employers should remain attentive to prepare and implement the necessary updates in a timely manner.

Back to top ↑

Croatia

Andrej Žmikić
CROATIA
andrej.zmikic@dtb.hr

Processing of Employee IDs and certificates of no ongoing criminal proceedings by a data controller found unlawful

In November 2025, the Croatian Data Protection Agency (DPA) issued a decision by which it determined that a data controller infringed several provisions of the GDPR. The infringements concerned, among others, that the controller excessively processed personal data of its employees by collecting copies of their identity cards, contrary to Article 6(1), and in connection with Article 5(1)(c) and (2) GDPR.

The DPA identified as an aggravating factor the controller's failure to heed the DPO's warning that the data collection could be unlawful and excessive in relation to the stated purpose.

Similarly, the controller collected certificates of criminal proceedings for its employees, which the Croatian DPA found to be contrary to Article 6(1), and in connection with Article 5(1)(b) and (2) GDPR.

Practical takeaways

- Always identify and document a lawful basis under GDPR before collecting personal data.
- Adhere to data minimisation, collecting only what's strictly necessary.
- Follow and document DPO guidance to bolster internal compliance.
- Provide clear employee notices regarding data processing intent, legal basis, and retention periods.
- Implement strong security and appropriate retention policies for sensitive documents.

Back to top ↑

Denmark

Elsebeth Aaes-Jørgensen
DENMARK
eaj@norrbomvinding.com

Selma Carøe
DENMARK
sca@norrbomvinding.com

Employers' covert audio recordings of conversations with employees results in DPA criticism

The Danish Data Protection Agency (DPA) issued serious criticism of a dental practice for unlawfully making several covert audio recordings of conversations with an employee during the course of the employment relationship. According to the dental practice, the audio recordings were intended to document discussions with the employee, with whom it had ongoing clashes. Those discussions primarily concerned the employee's behaviour towards patients and staff, the quality of the employee's work and patient complaints. The dental practice also stated that the audio recordings would be crucial in any legal proceedings concerning the employment relationship. However, the employee did not initiate legal action until more than three years after the first audio recording was made.

The DPA acknowledged that making audio recordings to protect against potential claims can, in principle, constitute a legitimate interest under Article 6(1)(f) of the GDPR. In this case, however, there were no concrete indications that the employee intended to bring a claim at the time of the recordings. The DPA also emphasised that an employer's recording of a conversation with an employee is such an unexpected processing activity that, according to the principle of transparency, information about this activity must be provided, to the employee, prior to starting the audio recording. On this basis, the DPA found grounds for issuing serious criticism of the dental practice for making the audio recordings without the necessary legal basis and for acting in violation of the principle of transparency by failing to inform the employee that the conversations were being recorded.

Practical takeaway

The case illustrates that employers may have a legitimate interest in making audio recordings of conversations with employees in order to protect themselves from claims if there are specific indications that such claims will be made. In this situation, the employer must inform the employee about the audio recording in advance.

Back to top ↑

European Union

Alexander Milner-Smith
UNITED KINGDOM
alexander.milner-smith@lewissilkin.com

Bryony Long
UNITED KINGDOM
bryony.long@lewissilkin.com

An overview of the EU's Digital Omnibus Proposals

Positioned as a *"first step"* towards optimising compliance and competitiveness, the proposal includes a set of *"technical amendments"* to *"digital legislation"* with a focus on *"unlocking opportunities in the use of data, as a fundamental resource in the EU economy"*. To support this objective, the proposal includes targeted updates to "data protection and privacy rules" contained within Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR) and Privacy and Electronic Communications Directive 2002/58/EC (e-Privacy Directive).

Key takeaways

Personal data: a narrower, context-based definition

The proposal narrows the definition of personal data by making it relative (i.e. information is not personal data for an organisation that cannot reasonably identify the individual from the data it holds). This departs from the current, more absolute approach where data may be treated as personal if anyone else could reidentify the person using available means. It also aligns with the Court of Justice's position (Case EDPS v SRB C-413/23 P) that pseudonymised data is not always personal and that identifiability must be assessed at the time of collection and from the controller's perspective. The direction mirrors that of the Information Commissioner's Officer (ICO), the UK's Data Protection Authority, signalling a shift that reduces GDPR obligations where linkage to an individual is not realistically possible.

Pseudonymisation: scope and risk criteria

The proposal empowers the European Commission and the European Data Protection Board to set EUlevel criteria for: (1) when pseudonymised data still counts as personal data;

Zahra Laher
UNITED KINGDOM
zahra.laher@lewissilkin.com

and (2) how to assess reidentification risk. This embeds a contextual, riskbased approach and harmonises practice across Member States.

Targeted exceptions around processing special category data.

Under Article 9 GDPR, processing special category data is generally prohibited unless a specific exemption applies. The proposal introduces two additional exemptions to that list namely:

» **Biometric verification under user control** - An exemption to the *"general prohibition"* where biometric verification is *"necessary"* and the data subject stays in *"sole control"* of the process (e.g. app access), with biometric data held solely by the user or by the controller in *"stateoftheart"* encrypted form, and full GDPR principles observed.

» **Use in AI development** - The proposal introduces an exception to the general prohibition on processing special category data where such data forms part and remains in the *"training, testing or validation data sets"* of the AI system or model, and subject to the controller implementing *"appropriate technical and organisational measures"*. This exception will not apply in situations where the processing of special category data is *"necessary for the purpose of processing"* within the AI system or model.

Training AI Models

The proposal sets out that *"legitimate interest"* will be explicitly codified as a lawful basis for processing personal data to train AI models, provided that appropriate safeguards are in place.

This means controllers must still conduct a GDPR balancing test and respect individuals' right to object (opt-out). However, this does not override stricter requirements in other EU or national laws, which may still mandate consent for certain types of data or contexts. Special category data remains subject to Article 9 safeguards (with the exceptions set out above), and additional conditions apply when processing for bias detection or correction.

Tackling "abusive" data subject access requests (SARs)

The proposal seeks to amend Article 12 GDPR by clarifying that the right of access under Article 15 GDPR must not be subject to *"abuse"* by the data subject for obtaining information about their personal data for "*purposes other than the protection of their data*".

To further support controllers, the proposal also sets out to establish a *"lower burden of proof"* to show a request is excessive rather than to show it is manifestly unfounded. It also adds that *"overly broad and undifferentiated requests"* should be considered as *"excessive"*, giving organisations a clearer ground for refusal.

There are again similarities here with ICO guidance about the scope of manifestly excessive or unfounded SARs.

When you may not need to provide a privacy notice

The proposal lightens the load on businesses when it comes to informing individuals about how their data is processed. Where a controller collects data directly from a data subject it permits organisations to skip this requirement if *"there are reasonable grounds to assume that the data subject already has the information"* unless the data is being shared with others, sent outside the EU, used for automated decision making or the processing could pose a high risk to the data subjects' rights.

Requirements for automated decision making (ADM)

The proposal aims to clarify Article 22 GDPR in order to provide *"greater legal certainty"* for decisions made through ADM. It clarifies that when deciding if an automated decision is necessary for *"entering into, or performance, of a contract"* it does not matter if the decision could be taken otherwise than by solely automated means.

This change is notable when compared to the UK's approach under the Data (Use and Access) Act 2025 (DUAA), which goes even further towards a more innovation-friendly, permission-based regime, subject to safeguards, rather than maintaining the EU's prohibition with exceptions model.

Breach notifications and incident reporting

The proposal introduces a more risk-based approach to breach notifications. Controllers would only need to notify the Data Protection Authority if the breach is likely to pose a high risk to individual rights, reducing unnecessary reporting for low-risk incidents. Importantly, this *"higher threshold"* for notification *"does not affect the obligation of the controller to document the breach"* (Article 33(5) GDPR). The proposal also gives organisations extra breathing room by extending the notification deadline from 72 to 96 hours.

In addition, the proposal creates a *"single entry point"* for reporting incidents, a model spanning the GDPR, the e-Privacy Directive, NIS2 Directive, DORA, and the Critical Entities Resilience Directive. In practice, this means a simpler, more streamlined process for compliance across multiple regulatory frameworks.

Harmonising DPIA practices

Existing obligations require organisations to conduct a data protection impact assessment (DPIA) when the data processing is *"likely to result in a high risk to the rights and freedoms of individuals"*. Currently, each EU member state maintains its own list of activities that require a DPIA, creating complexity for businesses operating across borders. The proposal seeks to harmonise these lists at EU level, thereby *"replacing existing national lists"* and reducing fragmentation and uncertainty. In addition, the European Data Protection Board will create a *"common template and common methodology for conducting"* DPIAs making it easier for organisations to understand when and how to perform them. The result, clearer more consistent guidance for assessing high-risk data processing.

Expanding the scope of scientific research

The proposal aims to extend the definition of what constitutes as scientific research *"clarifying the conditions"*. In addition, it proposes *"to extend the exceptions from the information obligation for processing"*, meaning that when data is processed for scientific research purposes, organisations may benefit from relaxed transparency rules.

Simplifying cookies and device level personal data

The proposal aims to simplify the interplay of the GDPR and e-Privacy Directive. It suggests that *"processing of personal data on and from terminal equipment"* (i.e. connected devices such as phones and personal computers) should be governed only by the GDPR, removing overlapping obligations under the e-Privacy Directive.

The proposal also clarifies the consent requirements for accessing personal data stored on terminal equipment, bringing these activities squarely within the GDPR's scope. Importantly, the proposal mentions a list of exemptions where access and processing of personal data stored on terminal equipment will be lawful without consent to the extent it is necessary for:

- *"carrying out the transmission of an electronic communication over an electronic communications network;*
- *providing a service explicitly requested by the data subject;*
- *creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;*
- *maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service".*

Additionally, the proposal aims to tackle *"consent fatigue"* by updating the rules to ensure users have provided meaningful consent and introduces a six-month cooling off period, meaning if a user rejects consent an organisation cannot reapproach them for at least six months.

Again, elements of this mirror changes at the UK level via the DUAA, i.e. increasing the exemptions from consent for low-risk analytics cookies.

Implications for workplace data compliance

- **Greater Legal Certainty** - Clearer definitions of personal data, pseudonymisation, and automated decision-making reduce ambiguity in GDPR compliance. This helps organisations and HR teams understand their obligations with more confidence.
- **Consistent Rules Across the EU** - Harmonised templates and methodologies (e.g. for DPIAs and pseudonymisation) aim to eliminate national variations. For employers operating in multiple EU countries, this means simpler, more predictable compliance processes.
- **Reduced Administrative Burden** - Streamlined breach reporting, flexibility in privacy notices, and targeted derogations for certain technologies ease compliance without lowering data protection standards. This can free up resources for HR and compliance teams.
- **Support for Innovation and AI** - By addressing AI development within the GDPR framework, the proposal balances strong safeguards with enabling technological progress. Employers can adopt AI tools for recruitment, workforce analytics, and other HR functions with clearer legal guidance.

Back to top ↑

Germany

Jessica Jacobi
GERMANY
jessica.jacobi@kliemt.de

Jakob Friedrich Krüger
GERMANY
jakob.krueger@kliemt.de

A decision on the limits of employee data use during HR software testing

After both the Labour Court and the Regional Labour Court had dismissed the claim, the German Federal Labour Court (BAG) in its decision of 8 May 2025, awarded EUR 200,00 in non-material damages to an employee whose personal data had been unlawfully processed during the testing phase of a new cloud-based HR software.

The employer had transferred more sensitive personal data to its parent company for processing than a prior works council agreement had permitted. The employer claims that this was only done for testing purposes and that it was agreed with the works council. The works council has a right of co-determination in accordance with s87(1) No. 6 of the Works Constitution Act (BetrVG) when introducing IT systems that are suitable for measuring behaviour and performance.

The BAG, after the preliminary ruling of the CJEU (C-65/23), clarified that such processing of personal data not covered by the works council agreement for testing purposes can only be justified under Article 6(1)(f) GDPR if anonymised "dummy" test data would not suffice. The court also ruled that s26(1) of the German federal data protection act (BDSG) does not meet the criteria of a "specific provision" under Article 88 GDPR due to the lack of safeguards for employee rights and thus cannot serve as a legal basis for such processing.

Practical takeaway

The decision highlights the limits and risks of data processing in employment contexts and warns against broad reliance on national law without GDPR-compliant safeguards. Notably, the court did not have to decide on the requirements for works council agreements that justify the processing of personal data under Article 88(1) GDPR.

Employers must ensure that any test-phase data

processing is necessary, backed by GDPR-compliant legal bases and where applicable limited to agreed categories. Overstepping these bounds even without intent can trigger liability for immaterial damages.

A decision on the legality of employee surveillance by a private investigator regarding suspected feigned incapacity to work

In its decision of 24 July 2024, the BAG held that an employer violated the GDPR by covertly surveilling an employee suspected of feigning illness.

The surveillance, conducted by a private detective, included observation and documentation of the employee's physical condition and activities who claimed to be sick. The BAG found that this constituted the processing of health data under Article 9(1) GDPR. The employee was awarded EUR 1,500 in damages for breach of privacy.

The Court ruled that such processing is only lawful if necessary, under Article 9(2)(b) GDPR in conjunction with s26(3) of the German federal data protection act (BDSG). This requires that the evidentiary value of a medical certificate be seriously undermined and that no less intrusive means (e.g. review by the statutory medical service) are available. In this case, the employer failed to meet these thresholds.

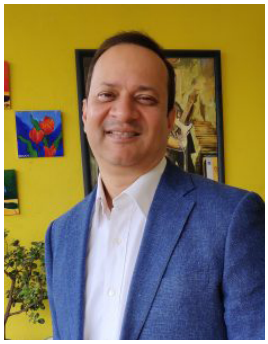
Practical takeaway

The decision reinforces the high bar for lawful surveillance in employment contexts, especially when health data is processed. The latter can be assumed if the employee's visible health status is documented by investigators as part of the observation.

Employers must therefore carefully assess the necessity and proportionality of surveillance measures such as private investigators. Unauthorised processing of health-related data, even for investigative purposes, risks GDPR violations and compensation claims.

Back to top ↑

India



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

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

India's new data protection law set to come into force on 13 May 2027

Over two years after introducing India's new data protection law, the Digital Personal Data Protection Act 2023 (the "Act"), the government has finally notified the date from which the Act will come into force. Barring a few provisions relating to the establishment of the data protection authority and the registration of consent managers, the most substantive provisions of the law will come into effect on 13 May 2027.

The government has also finalised the draft rules, which operationalise the provisions of the Act. The final rules are largely the same as the draft rules, with only a few differences.

India's DPDP regime will roll out in phases over an 18-month period, with institutional provisions effective immediately, the Consent Manager framework will follow after one year, and core operational duties (such as consent and notice requirements, data rights, breach obligations) will apply after 18 months. Organisations should use this transition period to prepare systems and processes for compliance.

Back to top ↑

Ireland

Linda Hynes
IRELAND
linda.hynes@lewissilkin.com

Emma Quinn
IRELAND
emma.quinn@lewissilkin.com

Appointment of a new Commissioner for Data Protection takes effect

The appointment of Niamh Sweeney took effect from 13 October 2025, for a five-year term.

In 2022, the Irish government approved commencement of a process to increase the number of Commissioners for Data Protection. A review was undertaken by the Department of Justice which took account of the evolving organisational structure, governance and business needs of the Data Protection Commission (DPC), Ireland's supervisory authority for the GDPR.

The Irish Council for Civil Liberties recently submitted a formal complaint against Ireland to the European Commission over the appointment of Ms Sweeney on the basis that they say Ireland did not provide adequate safeguards for independence and impartiality in this appointment, whom it describes as "an ex-Meta lobbyist". Its complaint argues that the appointment process has infringed Article 4 of the Treaty on the Functioning of the European Union, Article 8 of the Charter of Fundamental Rights of the EU, and Articles 52 and 53 of the GDPR.

The European Commission has affirmed it does not have authority to intervene in the DPC's appointment. The Department of Justice said it was fully satisfied with the appointment process.

Investigation into sale of smartphone location data results in temporary suspension of company operations

The DPC has confirmed that an Irish company at the centre of a recent investigation into the sale of smartphone location data has temporarily suspended operations.

The company, at the request of the DPC, has suspended all services involving location data

relating to Irish users for a minimum of 28 days.

The DPC also said that the activities of two additional companies based in two other EU member states are also being examined, adding that it is liaising with the relevant national data protection authorities in those jurisdictions.

The action follows an investigation by Ireland's national broadcaster, RTE, on 18 September which showed how the precise movements of tens of thousands of Irish smartphones are being sold by brokers in the digital advertising industry.

Ireland designates national competent authorities for oversight and enforcement of the EU AI Act

Ireland has to date designated 15 national competent authorities for oversight and enforcement of the EU AI Act in Ireland and are as follows:

- Central Bank of Ireland;
- Coimisiún na Meán;
- Commission for Communications Regulation;
- Commission for Railway Regulation;
- Commission for Regulation of Utilities;
- Competition and Consumer Protection Commission;
- Data Protection Commission;
- Health and Safety Authority;
- Health Products Regulatory Authority;
- Health Services Executive;
- Marine Survey Office of the Department of Transport;
- Minister for Enterprise, Tourism and Employment;
- Minister for Transport;
- National Transport Authority;
- Workplace Relations Commission.

Looking ahead, a National AI Office will be established by 2 August 2026 to act as the central coordinating authority for the AI Act in Ireland. It will:

- co-ordinate competent authority activities to ensure consistent implementation of the EU AI Act;
- serve as the single point of contact for the EU AI Act;
- facilitate centralised access to technical expertise by the other competent authorities, as required;
- drive AI innovation and adoption through the hosting of a regulatory sandbox, and act as a focal point for AI in Ireland, encompassing regulation, innovation and deployment.

By staying informed of Ireland's designated authorities, employers can navigate the regulatory landscape effectively and confidently deploy AI-driven tools in compliance with evolving EU standards.

Back to top ↑

Luxembourg

Elisabeth Collin
LUXEMBOURG
elisabeth.collin@castegnaro.lu

Sending confidential data to a private email account is serious misconduct justifying immediate dismissal

On 30 September 2025, the Labour Tribunal ruled on the dismissal of an employee who had disclosed confidential professional data to a third party.

The employee had emailed documents containing confidential information to his former supervisor (to both private and professional email addresses). The supervisor had been dismissed a few days earlier.

The employee did not deny the offence but argued that he had sent the documents in good faith, believing that the supervisor remained part of the team. On that basis, the employee sought a finding of unfair dismissal and an award of damages from his employer.

The employer's position

The employer sought confirmation of the validity of the dismissal from the Tribunal arguing that the leak exposed the company, resulted in the loss of a client, and created a risk of fines from the CNPD. The employer also noted that the employee was on holiday on the day of the transmission of the email and therefore should not have been handling such information. Finally, the employer pointed out that the employee's attempt to recall the message sent to the supervisor's professional email address and not his private one, provided evidence of his awareness that his conduct was non-compliant.

Tribunal's finding

The Tribunal reminded the employee that he is not supposed to send professional emails, particularly those containing confidential information, to a private inbox, as this breaches basic

IT security requirements. Having more than 35 years of experience in his field, the employee should have known what constitutes confidential information. The Tribunal concluded that this conduct qualified as serious misconduct.

Accordingly, the Tribunal upheld the employer's decision to terminate the employment with immediate effect and rejected the employee's claims.

Practical takeaway

The decision serves as a reminder for the need to set robust IT policies outlining employee's obligations in relation to basic computer use and security. Clear training and regular reminders can help mitigate the risk of similar incidents and the associated legal, client, and regulatory exposure.

Back to top ↑

Mexico

Renata Buerón
MEXICO
rbueron@basham.com.mx

Current regulation and the search for better protection in Mexico

Last October, an initiative to expedite The General Law for the Use and Control of Artificial Intelligence in Public and Private Sectors was proposed. The main purpose was to establish a national regulation concerning the use and application of AI, establishing limits, prohibitions, regulations and mechanisms.

This law considers different practices such as cybersecurity, public administration, education system, healthcare services, private companies, environmental care, intellectual property, military use and public administration; indicating that each of these areas must set constant training and tools for the appropriate exploitation of this technology.

Nonetheless, this is not the only law referring to AI that has been proposed. Multiple reforms to different existing laws have tried to target issues concerning intellectual property, education and violation of sexual intimacy using AI.

Currently Mexico's AI regulation limits itself to decisions without human evaluative intervention. These systems' main use is surrounding employment processes, with many companies using programs such as HireVue, iCIMS Hire, and Skillate to select candidates, analyse curriculums, evaluate skills, and more. Yet, when concerns or problems arise the most the data subject can request is to exercise the right to access (employers must be transparent about automated tools when they are used), correct or object to the use of their data, and challenge decisions that evaluate performance, reliability or behaviour and ask for reconsideration.

As of today, Mexico's regulation is basic, to say the least, although we are hoping for a better future surrounding the regulation of AI so employers should stay vigilant of potential upcoming changes.

Takeaways

- Always identify and document a lawful basis under GDPR before collecting personal data.
- Adhere to data minimisation, collecting only what's strictly necessary.
- Follow and document DPO guidance to bolster internal compliance.
- Provide clear employee notices regarding data processing intent, legal basis, and retention periods.
- Implement strong security and appropriate retention policies for sensitive documents.

Back to top ↑

New Zealand

Peter Kiely
NEW ZEALAND
kiely@ktc.co.nz

Privacy Amendment Act 2025 and the introduction of Information Privacy Principle 3A

In September 2025, the New Zealand Government enacted the Privacy Amendment Act 2025. The key reform of the Amendment Act, which amends the Privacy Act 2020, is the introduction of the new Information Privacy Principle 3A (IPP 3A). IPP 3A expands organisations' notification obligations when collecting personal information indirectly (i.e. from a source other than the individual concerned). IPP 3A will take effect on 1 May 2026, with a lead-in period for agencies to update systems and processes.

Under IPP 3A, when an agency collects personal information indirectly, it must take reasonable steps to ensure the person concerned is informed (unless a specific exception applies) of:

- the fact that their information has been collected;
- the purpose of the collection;
- the intended recipients of the information;
- the name and address of the collecting agency and the agency holding the information;
- whether the collection is authorised or required by law and the relevant legal provision;
- their right to access and correct their information.

Practical takeaways

- Identify all indirect collection points (e.g. checks, platforms, vendors) and ensure standardised notices cover purpose, recipients, agency details, legal authority, and access/correction rights.
- Refresh privacy policies, records of processing, and training.
- Run a gap analysis, prioritise high risk indirect collections, pilot notification workflows ahead of the deadline.

Biometric Processing Privacy Code 2025 takes effect

On 3 November 2025, the Biometric Processing Privacy Code 2025 (the 'Code') came into force, marking New Zealand's first dedicated regulatory framework for the use of biometric technologies such as facial recognition, fingerprint and voice authentication, and behavioural analytics. The Code applies to automated biometric processing for identification, verification or categorisation, and requires organisations to meet strict necessity and proportionality thresholds, provide enhanced pre-collection notification, and implement strong security safeguards.

Highly intrusive uses, such as inferring emotions or sensitive attributes, are largely prohibited. New biometric systems must comply immediately, while those already in use before 3 November 2025 must meet the Code's requirements by 3 August 2026.

Practical takeaway

Employers using biometrics for access control, time/attendance or workforce verification fall squarely within scope and should reassess necessity versus less intrusive alternatives, update employee notices and security controls, and cease any emotion or sensitive attribute inference. Existing deployments will need a compliance plan aligned to the 3 August 2026 deadline, with clear purpose limitation, tight retention, and careful consideration of power imbalance when relying on employee agreement.

HRRT confirms internal sharing of employee data can be unlawful

The New Zealand Human Rights Review Tribunal recently confirmed that improper internal disclosure of employee information can amount to a breach of the New Zealand Privacy Act 2020 (the "Act").

In Cummings v KAM Transport Limited [2025] NZHRRT 8, the Tribunal found that an employer had breached the Act after sensitive employment-related information was shared with a staff member who had no legitimate need to know. The Tribunal emphasised that disclosure within an organisation is still disclosure for the purposes of the Privacy Act.

The internal leak later contributed to the spread of harmful workplace rumours, and the Tribunal held that the employee had suffered humiliation, loss of dignity and injury to feelings, awarding NZD 30,000 in damages and issuing a declaration that the employer had interfered with the employee's privacy.

This decision highlights the need for employers to maintain strict controls over who has access to sensitive employee information, particularly during disciplinary processes, and to ensure that confidentiality is upheld at all levels of the organisation.

Poland

Michalina Kaczmarczyk
POLAND
michalina.kaczmarczyk@raczkowski.eu

Failing to implement appropriate security measures results in significant fine

The Polish Data Protection Authority (DPA) fined McDonald's Polska PLN 16,932,657 (approximately EUR 3,960,000) and its processor PLN 183,858 for data breaches involving the personal data of employees.

Personal data (including names, PESEL numbers, and passport numbers) of McDonald's and franchisee employees were disclosed in a publicly available catalogue. The data was processed by the processor for managing work schedules.

McDonald's was found to have failed to conduct a risk analysis, implement appropriate safeguards, and properly supervise the entrusted data. In doing so, it breached its responsibilities and failed to comply with the data processing agreement (DPA).

The processor was also fined for its role, as it was responsible for the IT system that exposed the data.

Practical takeaway

This case sends a strong message: merely having a DPA in place is insufficient. Controllers must actively **validate, audit, and monitor** their processors.

(Case no. DKN.5130.4179.2020)

Former employee found criminally liable for data misuse

A Polish court has held a former employee criminally liable for unlawfully processing their former employer's clients' personal data for their own business purposes.

While still an employee, the individual gained access to client data, which was considered a trade secret. After being dismissed, they arranged for another employee to use their (the former employee's) login credentials to unlawfully download this client data and transfer it to them for use in their new, competing business.

The court applied Article 107 of the Polish Data Protection Act, finding that both the former employee and the employee who accessed the data (the accomplice) were criminally liable for processing personal data without a legal basis or authorisation.

The former employee was ordered to pay a total of PLN 2,000 (approximately EUR 470). The court took into account the individual's lack of a prior criminal record as a mitigating factor. The other employee involved was also held criminally liable and ordered to pay PLN 1,000.

Practical takeaway

This case serves as a sharp warning that the consequences of unlawful personal data processing are not limited to administrative fines under the GDPR but can extend to criminal liability for individuals.

(Case no. SR IIK 543/24)

Back to top ↑

Sweden

Petter Wenehult
SWEDEN
petter.wenehult@elmzell.se

Malin Berndal
SWEDEN
malin.berndal@elmzell.se

DPA finds unlawful processing of personal data according to the GDPR

The Swedish Authority for Privacy Protection (DPA) found that the Moderate Party's national organisation unlawfully processed personal data with the distribution of personal video greetings, via SMS or email, ahead of an upcoming election. Amongst other things, the political party failed to inform data subjects about the processing of their data.

Facts

The personalised video greetings were sent to individuals who had no prior membership or active consent to receive communications from the party. The party argued that the messages were sent for political outreach purposes and were in the party's legitimate interest. However, no prior information about the processing of personal data, its purposes, or the recipients' rights was provided, in breach of Articles 12-14 GDPR. The party also attempted to rely on national law and internal policies, but the DPA clarified that these cannot override GDPR obligations.

Legal issues

The central legal issues concerned whether political communications can be justified under the "legitimate interests" basis of Article 6(1)(f) GDPR when recipients have not consented, and whether the transparency and information obligations under Articles 12–14 GDPR had been fulfilled. A further question was the extent to which national law or internal party rules could provide legal cover for the processing of personal data in political campaigns.

Decision

The DPA concluded that the personalised video greetings constituted unlawful processing of personal data under Article 6(1) GDPR. The party had failed to meet the transparency obligations required under Articles 12–14 GDPR. The authority emphasised that

Swedish national law or internal policies cannot replace GDPR requirements, even in the context of political messaging. As a consequence, the Moderate Party received a reprimand. No financial penalties were imposed due to the limited scale of the infringement, but the DPA stressed that privacy rights take precedence over political interests.

Practical takeaway

This decision demonstrates that any sending of personalised communications requires a clear, GDPR-compliant legal basis. The transparency obligations must be fulfilled, and recipients must be informed about the processing, its purposes, the legal basis, and their rights before their personal data is used. Personalisation, such as including names or creating tailored videos, increases the intrusiveness of the communication and thus the need for strict compliance. Furthermore, national law or internal rules cannot override GDPR obligations, and even unintentional unlawful processing can trigger regulatory oversight, reprimands, and reputational risk.

Government proposes national adaptations to the EU AI Act

On 23 September 2024, the Swedish government commissioned an inquiry into the need to introduce national adaptions and supplementary provision to the EU Artificial Intelligence Act ('EU AI Act').

The inquiry was presented on 6 October 2025 (SOU 2025:101) and proposes that the Swedish Post and Telecom Authority (PTS) should act as the market surveillance authority responsible for the EU AI Act and should be able to impose sanctions or fines for certain breaches of the Act. The new supplementary law and regulation, along with other legislative amendments, are proposed to enter into force on 2 August 2026.

Practical takeaways

Any organisation developing, deploying, or placing AI systems on the Swedish market must anticipate that the Swedish Post and Telecom Authority (PTS) will be the primary enforcement authority. High-risk AI systems and certain prohibited AI uses will fall under strict oversight, and entities will be required to maintain clear documentation, risk assessments, and compliance procedures, otherwise it can lead to administrative fines, sanctions, or operational restrictions. Companies should prepare for the 2 August 2026 implementation date, ensuring both EU AI Act obligations and proposed national requirements are fully addressed.

Government inquiry launched into the establishment of an appropriate legal framework for background checks

The Swedish Government has appointed a special investigator to assess the need and conditions for conducting background checks in both the public and private sectors.

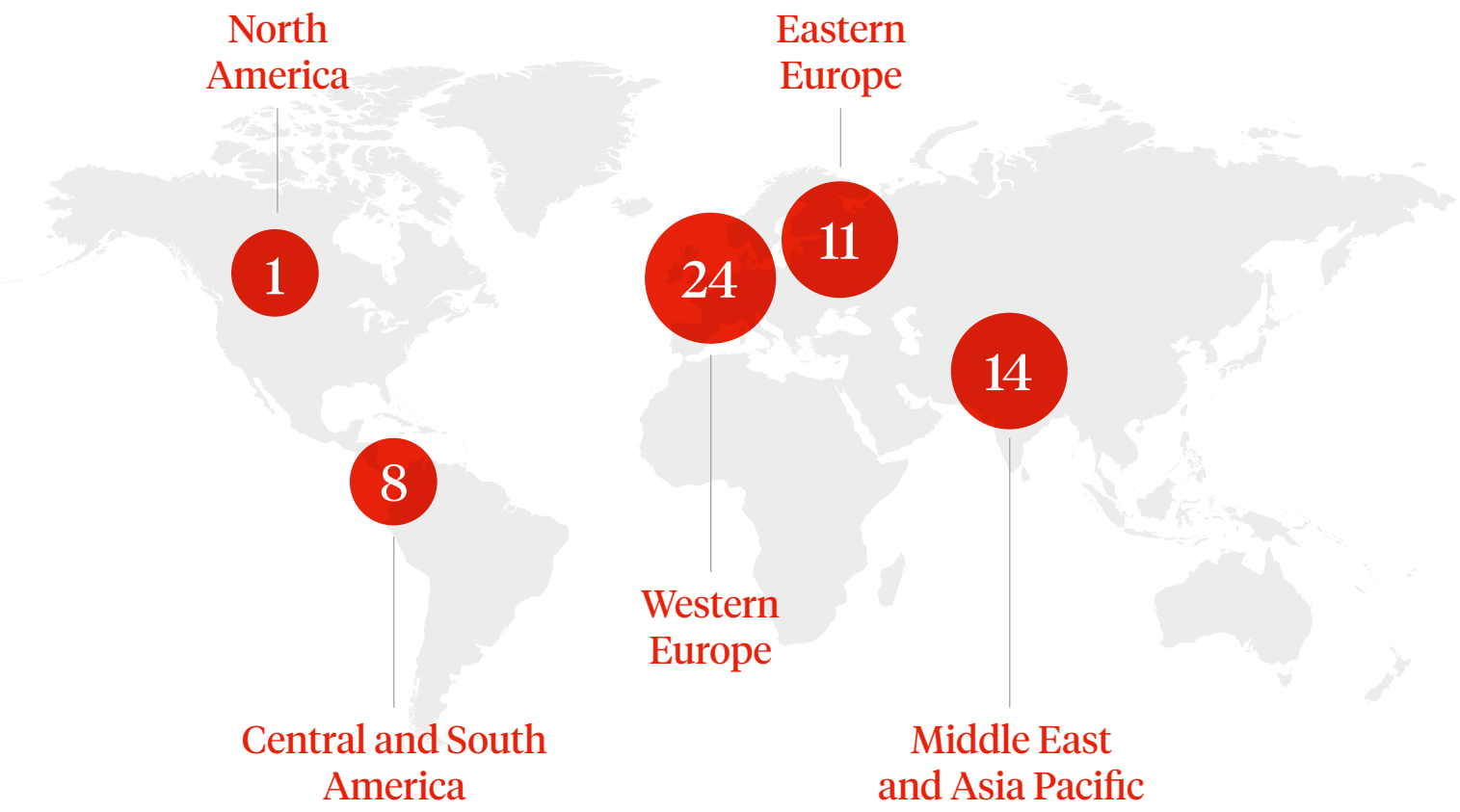
Currently, there is no uniform legal definition of "background check" in Sweden and the inquiry aims to provide organisations with effective tools to prevent risks posed by individuals with criminal or harmful intentions, including infiltration or undue influence. It will consider both pre-employment and ongoing checks while ensuring that personal privacy is protected. The investigator will propose a proportionate framework for follow-up checks during employment or participation in activities. The inquiry will also evaluate whether mandatory checks of the suspect register and the criminal records register should be extended to more sectors.

Practical takeaways

Companies should monitor the development of this inquiry, as it may result in clearer rules that make it easier for certain sectors to conduct background checks in the future, given the current uncertainty about what is legally allowed.

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

Copyright Ius Laboris 2026

Global HR Lawyers
Ius Laboris