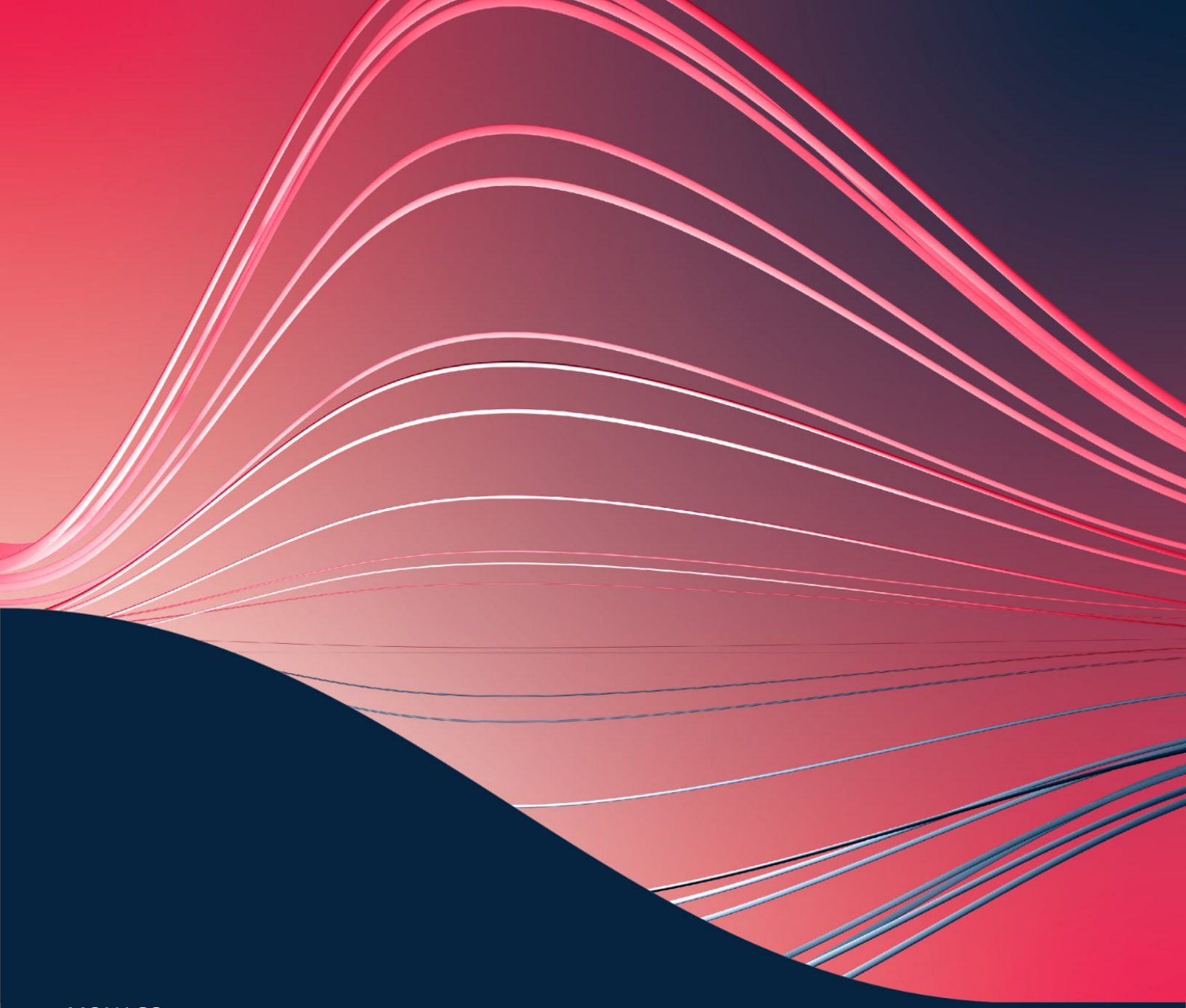


MONACO

Data Protection Laws of the World

DLA PIPER

Introduction

Welcome to the 2025 edition of DLA Piper's Data Protection Laws of the World Handbook. Since the launch of our first edition in 2012, this comprehensive guide has been a trusted resource for navigating the complex landscape of privacy and data protection laws worldwide. Now in its fourteenth edition, the Handbook has grown to provide an extensive overview of key privacy and data protection regulations across more than 160 jurisdictions. As we step into 2025, the global landscape of data protection and privacy law continues to evolve at an unprecedented pace. With new legislation emerging in jurisdictions around the world, businesses face a growing need to stay informed and agile in adapting to these changes. This year promises to bring new developments and challenges, making the Handbook an invaluable tool for staying ahead in this ever-changing field.

Europe

Established data protection laws in Europe continue to evolve through active regulatory guidance and enforcement action. In the United Kingdom, the UK government has proposed reforms to data protection and e-privacy laws through the new Data (Use and Access) Bill ("**DUAB**"). The DUAB follows the previous government's unsuccessful attempts to reform these laws post-Brexit, which led to the abandonment of the Data Protection and Digital Information (No.2) Bill ("**DPDI Bill**"), in the run-up to the general election. Although the DUAB comes with some bold statements from the government that it will *"unlock the power of data to grow the economy and improve people's lives"*, the proposals represent incremental reform, rather than radical change.

United States

In the United States, legislation on the federal and in particular state level continues to evolve at a rapid pace. Currently, the US has fourteen states with comprehensive data privacy laws in effect and six state laws will take effect in 2025 and early 2026. Additionally, at the federal level, the new administration has signaled a shift in enforcement priorities concerning data privacy. Notably, there is a renewed focus on the regulation of artificial intelligence (AI), with an emphasis on steering away from regulation and promoting innovation. This includes the revocation of previous executive orders related to AI and the implementation of new directives to guide AI development and use.

In the realm of children's privacy, many of the new administration's supporters in Congress have indicated a desire to make the protection of children on social media a top priority, and new leadership at the Federal Trade Commission (FTC) appears aligned on this goal, albeit with a willingness to take another look at the recently adopted amendments to the Children's Online Privacy Protection Act (COPPA) Rule. Health data

privacy remains a critical concern, with a handful of states following Washington state's lead in enhancing or adopting health data privacy laws. On the international data transfer front, Executive Order (E.O.) 14117 " Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" as supplemented by the DOJ's final Rule will impact companies transferring data into certain jurisdictions, such as China, Iran and Russia. Another area of focus for companies with an EU presence will be the Trump administration's approach to the Privacy and Civil Liberties Oversight Board, as it is a critical pillar of the EU/UK/Swiss-US Data Privacy Framework.

Asia, the Middle East, and Africa

Nowhere is the data protection landscape changing faster – and more fundamentally – than in Asia, with new laws in India, Indonesia, Australia and Saudi Arabia, as well continued new data laws and regulations in China and Vietnam. The ever-evolving data laws, as well as the trend towards regulating broader data categories (beyond personal data), in these regions continue to raise compliance challenges for multi-national businesses.

Emerging trends in data governance

Unlocking data, regulating the relentless advance of AI, creating fairer digital markets and safeguarding critical infrastructure against the ever growing cyber threat, continue to impact and overlap with the world of data protection and privacy. Perhaps most notably, the EU have introduced a raft of new laws forming part of its ambitious digital decade, which will bring huge change to businesses operating within the EU. With the rapid adoption of artificial intelligence enabled solutions and functionality, data protection supervisory authorities have been closely scrutinising the operation of AI technologies and their alignment with privacy and data protection laws. For businesses, this highlights the need to integrate date protection compliance into the core design and functionality of their AI systems. In the midst of this, the privacy community found itself at the centre of an emerging debate about the concept of 'AI governance'. This is not a surprising development – AI systems are creatures of data and the principle-based framework for the lawful use of personal data that sits at the heart of data protection law offers a strong starting point for considering how to approach the safe and ethical use of AI. As AI technologies advance, so will regulatory expectations. It is expected that regulatory scrutiny and activity will continue to escalate and accelerate in tandem with the increase in integration of powerful AI models into existing services to enrich data. Whilst privacy professionals cannot tackle the AI challenge alone, expect them to continue to be on the front lines throughout 2025 and beyond.

Disclaimer

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

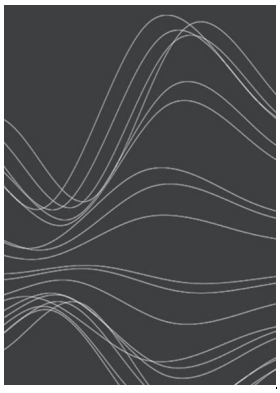
Africa key contact

Monique Jefferson
Director
monique.jefferson@dlapiper.com
Full bio

Americas key contact

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

Asia Pacific key contact



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

Europe key contacts

Andrew Dyson
Partner
andrew.dyson@dlapiper.com
Full bio

Ewa Kurowska-Tober
Partner
Head of Intellectual Property and Technology, Poland
ewa.kurowska-tober@dlapiper.com
Full bio

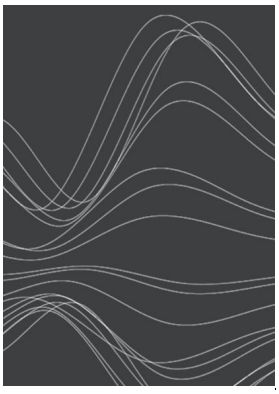
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Middle East key contact

Rami Zayat
Partner
rami.zayat@dlapiper.com
Full bio

Editors

Kate Lucente
Partner
kate.lucente@us.dlapiper.com
Full bio



Lea Lurquin
Associate
lea.lurquin@us.dlapiper.com
Full bio

Monaco

LAST MODIFIED 6 FEBRUARY 2025

Data protection laws

Within the Principality of Monaco (Monaco) data protection law have been recently updated by Data Protection Law n° 1.565 of December 3, 2024 (the "**DPL**"). Article 22 of the Monegasque Constitution still protects the right to privacy and the secrecy of correspondence of every citizen.

Monaco is not part of the EU and did not adopt Data Protection Directive 95/46/EC (hereinafter referred to as the "**European Directive**") or its successor the General Data Protection Regulation (Regulation EU 2015/679) of April 27, 2016 (hereinafter referred to as the "**GDRP**"). However, the new DPL recently adopted offers a strong level of protection similar to GDPR. The aim of the new law was to obtain an adequacy decision from EU.

Monaco is also part of the Council of Europe and entered into Convention n° 108 of the European Council of January 28, 1981 for the protection of individuals with regard to automatic processing of personal data, and into its protocol addendum regarding the controlling authorities and cross-border flows of data, both effective from April, 1st 2009 (through Sovereign Ordinances 2.118 and 2.119 of March 23, 2009).

It is however important to note that, pursuant to Article 3.2. of the GDPR and waiting for this adequacy decision, GDPR is still applicable to companies established in Monaco that process personal data of persons (or "**data subjects**") residing in the EU where such processing is related to:

i. the supply of goods or services to such persons (irrespective of a payment for such supply); and
ii. the monitoring of their behavior taking place within the Union.

It shall be noted that in such a case, the company established in Monaco may be required to designate in writing a representative in the European Union (article 27 of GDPR) and that both GDPR and Monaco DPL will be applicable to these companies.

Definitions

Definition of personal data

Under the DPL, personal data is defined as data enabling identification of a determined or determinable person. Any individual who can be identified, directly or indirectly, notably by reference to an identification number or to one or more factors specific to their physical, psychological, psychological, economic, cultural, or social identity is deemed to be determinable.

Definition of sensitive personal data

While not expressly defined under the DPL, sensitive personal data is considered to be personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health / genetic data, sex life, data concerning morals or social matters.

Definition of data processing

Under the DPL, data processing is defined widely as any operation or set of operations performed on such data, whatever the process used (including collection, recording, organization, modification, storage, extraction, consultation, destruction, as well as exploitation, interconnection or reconciliation, transmission, broadcasting).

Definition of the data processor / controller

Under the DPL, the person in charge of the processing or "Data controller" shall be considered as any person (natural or legal entity governed by private or public law) who alone or jointly with others, determines the purpose and means of the processing and who decides of its implementation.

Definition of the data subject

Any person whose personal data are processed.

National data protection authority

The Monegasque regulator is the Commission for Control of Personal Data (*Commission de Contrôle des Informations Nominatives* or "CCIN") whose composition was recently amended by Sovereign Ordinance n°8.575

The CCIN has different missions and powers, which mainly include (i) a mission of registration and examination of cases (e.g. it receives declarations of processing, expresses advices and opinions, issues authorizations when needed), (ii) a mission of council and proposal (e.g. it makes proposals to the competent authorities and recommendations, informs the data subjects of their rights and obligations, publishes reports) and (iii) a mission of control and investigation.

Registration

Data controllers, who process personal data must notify the CCIN and request approval so that their processing of personal data may be registered. Any changes to the processing of personal data will require the registration to be amended. Concerning data controllers who are legal persons governed by public law, public

authorities and bodies governed by private law with a mission of general interest, the decision shall be taken by the competent authorities or bodies following a reasoned opinion from the CCIN. A recent Ministerial Order of 18 March 2021 has brought some changes to this procedure.

Any natural or legal entities governed by private law who intend to implement automated data processing including personal information must first complete the required procedure with the CCIN.

There are four possible procedures to follow:

- Ordinary declaration (all nature or legal persons governed by private law usually fall under the ordinary declaration procedure);
- Simplified declaration (all processing compliant to a referenced Ministerial Order and only when it is clearly established that the processing operations do not adversely affect the rights and freedoms of the data subjects);
- Authorization request (only for automated processing of personal data relating to suspected unlawful activities, offences or security measures or including biometric data required to check persons' identities, or for the purpose of surveillance);
- Legal advisory request (only processing relating to research in the field of health - excluding biomedical research and for processing implemented by natural or legal persons governed by public law, public authorities, organizations governed by private law entrusted with a mission of general interest or a concessionaire of public utility).

The data controller must decide which procedure is the most adapted to the processing he wants to implement. To do so, he needs to analyze the purpose of the processing, and depending on this purpose, complete one of the aforementioned procedures (ordinary request, simplified request, authorization request, or legal advisory request).

The notification to the CCIN should include at least the following information:

- What data is being collected;
- Why the data will be processed;
- The categories of data subject;
- Whether the data will be transferred either within or outside the Monaco.

Data protection officers

There is no requirement in Monaco for organizations to appoint a data protection officer.

However, appointing a data protection officer is viewed by the CCIN as evidence of a company's measure taken in order to ensure compliance with the data protection legislation. In practice however, companies in Monaco do not generally appoint data protection officers.

When appointed in these companies, he is usually responsible for informing and advising the members of the entity on the legal obligations regarding data processing and for cooperating with the CCIN.

Collection and processing

Data processing must be justified by at least one of the following bases:

- The data subject's consent;
- A legal duty imposed to the data controller;
- A public purpose;
- The performance of a contract entered into between the data controller and the data subject;
- The data controller's legitimate interests, unless the data subject's fundamental rights and liberties outweigh the controller's legitimate interests.

If sensitive personal data is processed, at least one of the above bases must be met plus one from an additional list of more stringent conditions (determined in Article 12 of DPL).

Additionally, the data controller must provide the data subject with fair processing information. This includes information about the identity of the data controller, the purposes of processing, the identity of recipients, the right to oppose, access and amend their data and any other information needed under the circumstances to ensure that the processing is fair.

Transfer

Monaco is not part of the EU, so the DPL does not distinguish between EEA jurisdictions and non-EEA jurisdictions.

However, the DPL provides that the transfer of data is authorized for cross-border access, storage and processing of data only to a country which offers equivalent data protection and reciprocity (and in particular circumstances, including for example when the data subjects gave his consent for such transfer or when the transfer of data is necessary to save his life or a public interest).

The CCIN has established a list of the countries deemed to offer equivalent protection and reciprocity.

Data transfers to countries with an adequate level of protection are not subject to the authorization by the CCIN.

The CCIN has adopted a position of principle and decided that all personal data transfers to a country or an organization which does not ensure an adequate level of protection should, in any event, be submitted to the Commission in the form of a

transfer authorization application. Subsequently, the CCIN affirmed that it is necessary to submit a transfer authorization application to the Commission if personal data will be accessed from a country that does not have an adequate level of protection.

GDPR has an impact on data transfers to and from Monaco. Two situations must be distinguished:

- Companies of the European Union that want to send data to Monaco:

  They should no longer have to carry out any specific formalities with their supervisory authority as long as tools to protect the data are put in place between the European data controller and his subcontractor or subsidiary, notably:

  - o An approved code of conduct pursuant to Article 40 of the GDPR;
  - o An approved certification mechanism pursuant to Article 42 of the GDPR;
  - o Standard data protection clauses approved by the European Commission (art.46);
  - o Binding corporate rules (art.47);

- Companies that want to send data from Monaco.

As described above, they are still subject to the data transfer formalities of the CCIN if they wish to send data to a country which does not have an adequate level of protection.

Security

Data controllers must take appropriate technical and organizational measures designed to protect against unauthorized or unlawful processing, accidental loss or destruction of, or damage to, personal data.

Measures implemented must ensure an adequate level of security with regard to the risks posed by processing and by the nature of the data to be protected.

Where the data controller or their representative engages a service provider to process personal data, they must ensure that the service provider is able to comply with the obligations laid down in the two previous paragraphs.

The implementation of processing by such service provider must be governed by a written agreement between the subcontractor and the data controller that stipulates specifically that the service provider and his employees work under the sole directive of the data controller, and that he is also accountable for the obligations relating to the security of the processing.

Breach notification

There is no mandatory requirement in the DPL to report security breaches or losses to the CCIN or to data subjects.

Enforcement

The CCIN and Monegasque Courts are responsible for enforcing the DPL. If the CCIN becomes aware that a data controller is in breach of the DPL, it can serve an enforcement notice requiring the data controller to resolve the non-compliance. Failure to comply with an enforcement notice is a criminal offense and can be punished on conviction with imprisonment of one month to one year or a fine of between €9,000 and €90,000 or both.

Sanctions remain rare. The CCIN website only mentions one decision of sanction dated July 18, 2017, which was a warning and the fixation of an action plan to implement corrective measures, against a Monegasque company which didn't submit to the CCIN a request to conduct automated processing of personal data.

Electronic marketing

Prior to implementing any electronic marketing activity the CCIN must be notified, as electronic marketing activities may use personal data. The DPL does not prohibit the use of personal data for the purpose of electronic marketing *per se*. However, when implementing electronic marketing activities a company must respect the provisions of Articles 1, 10-1, 10-2 and 14 of the DPL.

The automated or non-automated processing of personal data must not infringe the fundamental rights and freedoms enshrined in Title III of the Constitution.

When marketing, personal data must be:

- Collected and processed fairly and lawfully;
- Collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes;
- Adequate, relevant and not excessive in relation to the purposes for which it is collected and / or further processed;
- Accurate and, if necessary, updated; every reasonable step must be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.

Processing of personal data must be justified by one of the following bases:

- By consent from the data subject(s);
- By compliance with a legal obligation to which the data controller or their representative is subject;

- By it being in the public interest;
- By the performance of a contract or pre-contractual measures with the data subject;
- By the fulfillment of a legitimate motive on the part of the data controller or their representative or by the recipient, on condition that the interests or fundamental rights and freedoms of the data subject are not infringed.

Data subjects from whom personal data is collected must be informed of all of the following:

- The data controller's identity and, if applicable, the identity of their representative in Monaco;
- The purpose of processing;
- The obligatory or optional nature of replies;
- The consequences for data subjects of failure to reply;
- The identity of recipients or categories of recipients;
- Their right to oppose, access and rectify their data;
- Their right to oppose disclosure to and use of personal data by a third party, or the disclosure for the purposes of the third party's commercial use, including marketing.

Online privacy

Prior to the use of traffic data, location data and cookies the CCIN must be notified. The use of traffic data, location data and cookies will have to comply with the provisions of the DPL.

In its Deliberation No. 2019-083 of May 15, 2019, the CCIN has specified the main principles applicable to the methods of depositing cookies and other tracers on the terminals of network users.

In this recommendation the CCIN insists on the requirement to insert a banner appearing as soon as an Internet user arrives on the visited site. It is also requested that no cookie other than those necessary for the operation be deposited in the user's terminal without its consent.

The banner must not be solely for information purposes but must allow the approval or deactivation of the deposit of cookies directly on the site by a positive action of the user.

According to the CCIN, the employer cannot access the contents of private messages sent or received from the professional e-mail system without the employee presence and agreement.

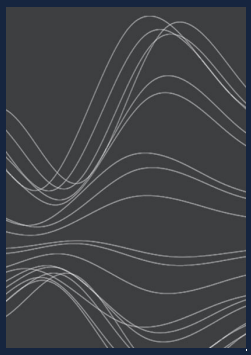
However, in order for messages to be considered private, it is necessary for employees to identify them as such for example by specifying in the message's subject key words such as "private", or "personal".

Data protection lawyers

Gilbert Delacour
CEO
Of Counsel
Gordon S. Blair Law Offices
gilbert.delacour
@gordonblair.com
View bio

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com