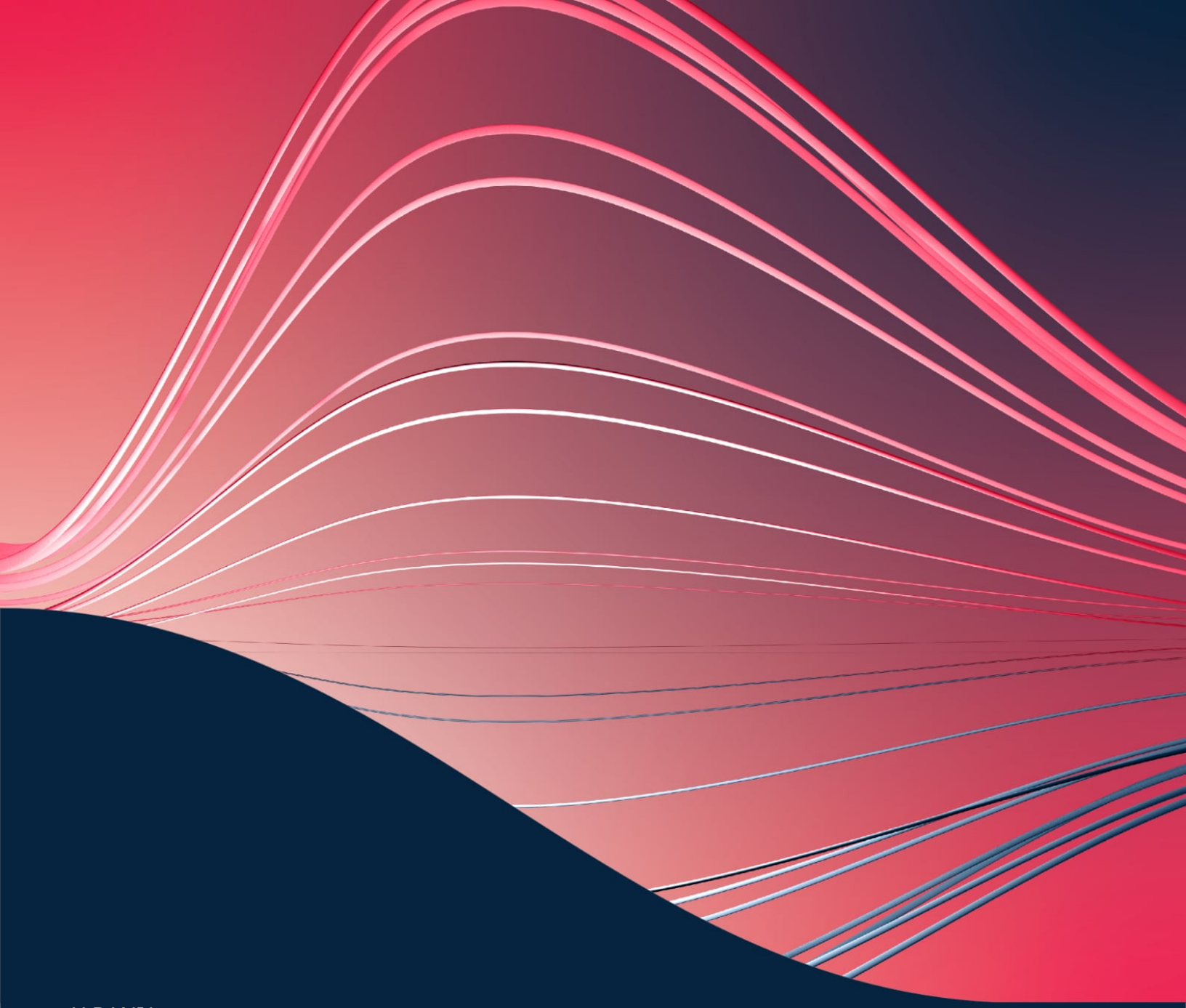


ALBANIA

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.

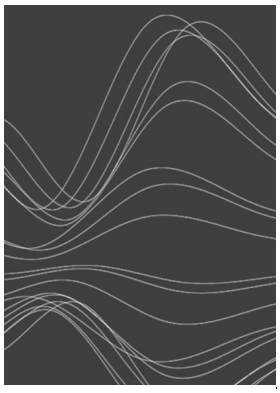
Africa key contact

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

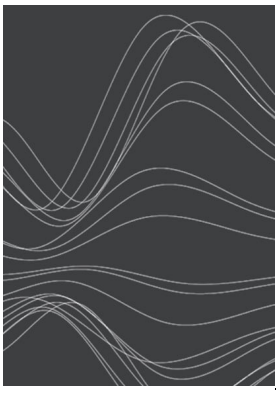
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

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

Albania

LAST MODIFIED 28 JANUARY 2025

Data protection laws

On 19 December 2024, the Parliament of the Republic of Albania passed Law No. 124 /2024, titled "*On Personal Data Protection*" (the "**Data Protection Law**") (Official Gazette of the Republic of Albania No. 9, dated 17 January 2025). This legislation aims to align Albania's legal framework with the European Union's standards, particularly by incorporating Regulation (EU) 2016/679 (the General Data Protection Regulation, or GDPR) and Directive (EU) 2016/680, both of which address the protection of personal data in various contexts, including criminal law enforcement.

The adoption of this law marks the culmination of an extensive process, with the Office of the Information and Data Protection Commissioner pursuing the alignment of Albanian data protection laws with the GDPR since 2018.

The Data Protection Law establishes the rules for safeguarding individuals' personal data and aims to protect fundamental human rights and freedoms, particularly the right to personal data protection.

Scope

The Data Protection Law applies when personal data are processed in whole or in part by automatic means, as well as to the processing of personal data which are part of a filing system or are intended to become part of a filing system where the processing is not carried out by automatic means; however, the law does not cover data processing by natural persons for purely personal or family purposes (Article 3).

Territorial Scope

The Data Protection Law shall apply:

- in the framework of the activities of a controller or processor established in the Republic of Albania, regardless of whether the processing takes place in the Republic of Albania or not;
- of data subjects, who are located in the Republic of Albania, by a controller who is not established in the Republic of Albania, but the processing operations relate to:

i. the offering of goods or services, whether for payment or not, to data subjects in the Republic of Albania; or
ii. the monitoring the behaviour of data subjects, as long as such behaviour takes place in the Republic of Albania;

- by a controller or processor, who is not established in the Republic of Albania, but in a territory where Albanian law applies on the basis of public international law (Article 4).

Definitions

Definition of Personal Data

Data Protection Law defines personal data as any information relating to a data subject (Article 5(3)).

A "**data subject**" refers to any identified or identifiable natural person. A person is identifiable if he or she can be identified, directly or indirectly, by reference to one or more specific identifiers, such as a name, an identification number, location data, an online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity (Article 5(23)).

Definition of Sensitive Personal Data

Data Protection Law defines sensitive data as special categories of personal data that reveal racial or ethnic origin, political opinions, religious beliefs or philosophical views, trade union membership, genetic data, biometric data, data concerning a person's health, life or sexual orientation (Article 5(28)).

"**Genetic data**" means personal data relating to the inherited or acquired genetic characteristics of a person which provide unique information concerning his or her physiology or health and which are obtained, in particular, because of the analysis of a biological sample taken from that person (Article 5(25)).

"**Biometric data**" means personal data resulting from specific technical processing of the physical, physiological or behavioural characteristics of a person which enable or confirm the unique identification of that person, such as facial images or fingerprints (Article 5(24)).

"**Data concerning health**" means personal data relating to the physical or mental health of a person, including the provision of healthcare services, which indicates information relating to his or her state of health (Article 5(26)).

National data protection authority

The Commissioner for the Right to Information and Personal Data Protection (the "**Commissioner**") is the Albanian authority in charge of overseeing and ensuring the implementation of the applicable legislation on data protection, with the primary goal of protecting the fundamental rights and freedoms of individuals in relation to the processing of personal data. The Commissioner is an independent authority, elected by a majority of the Parliament members, based on a proposal from the Council of Ministers, for a seven-year term, with the possibility of re-election.

In carrying out their duties and exercising their powers under the Data Protection Law, the Commissioner operates independently, free from any direct or indirect influence, and does not seek or accept instructions. During the Commissioner's term, they are prohibited from engaging in any activities or professions that may conflict with their duties, whether paid or unpaid.

The Commissioner is supported by the Office of the Commissioner, which is provided with the necessary human, technical, financial, and infrastructural resources to effectively perform its functions. The staff operates under the exclusive direction of the Commissioner and reports to them regularly. To fulfil the mission and objectives of the office, the Commissioner may also consult with external advisors on specific matters. The Commissioner has the authority to approve the organizational structure of the Office of the Commissioner.

The Commissioner is seated at:

Rr. "Abdi Toptani", Nd. 5
Postal Code 1001
Tirana
Albania

Registration

A data controller or processor must notify the Commissioner of the contact details of the Data Protection Officer.

If a data controller or processor is not established in the Republic of Albania but engages in processing activities related to data subjects in Albania, the controller or processor must appoint a representative and notify the Commissioner. This notification must include the identity of the representative appointed in the Republic of Albania. The notification must be provided in writing (Article 25).

This requirement applies when processing involves:

- the offering of goods or services, whether for payment or not, to data subjects in the Republic of Albania; or
- the monitoring of the behaviour of data subjects, as long as such behaviour takes place in the Republic of Albania.

This requirement shall not apply:

- to processing, which is incidental, does not involve the processing of sensitive data or criminal data on a large scale and is not likely to result in a risk to the fundamental rights and freedoms of natural persons, taking into account the nature, context, object and purposes of the processing; or
- to public authorities.

Data protection officers

Obligation to designate a Data Protection Officer ("DPO") (Article 33)

The controller and the processor must designate a DPO if:

- The processing is carried out by a public authority or body, excluding courts, in the course of judicial activities;
- The core activities of the controller or processor involve processing operations that, due to their nature, scope, or purpose, require regular and systematic monitoring of data subjects on a large scale;
- The core activities of the controller or processor involve processing sensitive data or criminal data on a large scale.

A group of companies may appoint a single DPO, who should be easily accessible to each member of the group. In the case of a public authority, one DPO may be designated to cover multiple authorities, considering their organizational structure and size.

In situations not covered by the first paragraph above, the controller, processor, associations, or other bodies representing a category of controllers or processors may, or in some cases must, designate a DPO, as required by law.

Duties and position of the DPO (Article 34)

The DPO has the following duties:

- Provides advice, upon request, to the management bodies of the controller or processor on all matters related to data protection;
- Participates in data protection impact assessments;
- Informs and advises the staff of the controller or processor on data protection, including raising awareness and training staff involved in processing operations;
- Monitors compliance with the Data Protection Law, other applicable data protection provisions, and the policies of the controller or processor, including the assignment of responsibilities, awareness-raising, staff training, and relevant audits;
- Cooperates with and serves as a point of contact for the Commissioner;
- Gives due attention to the risks of infringing fundamental rights and freedoms that may arise from personal data processing, considering the nature, context, circumstances, and purposes of the processing.

The DPO must be appointed based on certified professional qualifications, particularly with sound knowledge of data protection law and practices, and the ability to perform the tasks outlined in the paragraph above.

The DPO may be an employee of the controller or processor, or someone under a service contract. The DPO may hold other responsibilities, but the controller or processor must ensure these duties do not conflict with the role of the DPO.

The controller and processor must ensure the DPO is involved in a timely manner in all matters related to data protection and has the necessary resources to carry out their duties. The DPO must also maintain confidentiality regarding their duties.

The controller and processor must ensure the DPO is not given instructions regarding the performance of their duties and cannot be dismissed or penalized for carrying out their responsibilities. The DPO reports directly to the highest level of management of the controller or processor.

Collection and processing

The Data Protection Law provides the following definitions:

A "controller" means the natural or legal person and any public authority which, alone or jointly with others, determines the purposes and means of the processing of personal data (Article 5(8)).

A "processor" means the natural or legal person and any public authority which processes personal data on behalf of the controller (Article 5(18)).

Principles for the lawful processing of personal data (Article 6)

Personal data shall be:

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

> The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle").

Lawfulness of processing of personal data (Article 7)

Processing shall be lawful only if and to the extent that at least one of the following applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Lawfulness of processing of sensitive data (Article 9)

Processing of sensitive data is prohibited.

The processing of sensitive data is permitted if appropriate measures are implemented to protect the fundamental rights and interests of data subjects and only in cases where:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where the applicable legislation provides that the prohibition on processing sensitive data cannot be waived by consent from the data subject;
- processing is necessary for the fulfilment of a specific obligation or right of the controller or of the data subject in the field of employment, social security and social protection, including obligations and rights arising from a collective agreement, in accordance with the applicable legislation in these areas, provided that the fundamental rights and interests of the data subject are guaranteed;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is incapable of giving consent due to his / her health condition or when his / her right to act has been removed or restricted;
- processing is carried out in the course of the lawful activity of a not-for-profit political, philosophical, religious or trade union organization, provided that the processing relates only to members or former members of the organization or to persons who have regular contact with it in the context of its activity, and that the personal data are not disseminated outside the organization without the consent of the data subjects;

- processing relates to personal data which are manifestly made public by the data subject and the processing is necessary for the pursuit of a legitimate interest;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- procesecessary for archiving purposes in the public interest, for historical, research, scientific or statistical purposes, subject to legal provisions.

Lawfulness of processing of data related to criminal offences and convictions (Article 10)

Processing of personal data relating to criminal convictions and offences or security measures related thereto is carried out only under the control of competent authority or when the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects. The judicial status register is maintained under the control and supervision of the Ministry of Justice, in accordance with the legislation in force.

Processing of data for specific purposes:

Processing of personal data and freedom of expression (Article 43)

To balance data protection with freedom of expression and information, exceptions to the Data Protection Law can be applied for journalistic, academic, artistic, and literary purposes, provided:

- The data is necessary for preparing journalistic, academic, literary or artistic materials for publication;
- The data is only used for the specified purpose;
- The publication serves the public interest;
- Applying the Data Protection Law would hinder the purpose;
- The processing does not harm the fundamental rights of data subjects.

If these exceptions are applied, personal data should only be retained for as long as needed for the publication and can be shared with those involved in its creation, other potential publishers, or for legal purposes.

Additionally, when publishing, the controller must ensure minors, crime victims, or individuals claiming harm are not identifiable without consent or court approval, except when the victim is a public figure related to their role

Exceptions do not apply to processing data about minors or certain other legal provisions.

Processing of personal data and access to information in the public sector (Article 44)

The right to personal data protection is balanced with the right of access to official documents and information, as outlined in the applicable legislation. Public access to information, is not restricted by personal data protection laws for public authorities or

individuals exercising state functions, unless other fundamental rights (such as the right to life or physical integrity) require specific protection of their data.

Processing of personal data for archiving, research, and statistical purposes (Article 45)

The processing of personal data, including sensitive and criminal data, for archiving in the public interest, or for historical, research, scientific, or statistical purposes, is considered a legitimate interest of the controller, unless the data subject's interests or fundamental rights and freedoms, which require protection of their personal data, take precedence.

Personal data collected for any purpose may be further processed for archiving purposes, historical research, or scientific and statistical purposes.

This processing must be carried out with appropriate safeguards to protect the rights and freedoms of the data subject. These safeguards include, but are not limited to:

- Technical and organizational measures taken by the controller in compliance with Data Protection Law, especially principles of data minimization or pseudonymization, to achieve the processing purpose. If the purpose can be achieved by processing anonymized or pseudonymized data, that method should be used;
- Pseudonymization of data, and where possible, anonymization before transferring data for further processing;
- Specific safeguards to ensure that data is not used for decisions or actions concerning the data subject, unless the data subject has expressly given consent.

Exemptions from certain data subject rights may apply if exercising those rights would significantly hinder or prevent the achievement of the processing purpose. The controller bears the burden of proving that the exercise of these rights would cause such an obstacle to the purpose.

Processing of personal data and direct marketing (Article 46)

See Electronic marketing.

Transfer

General principles (Article 39)

Personal data that is being processed or will be processed after transfer may only be transferred to a foreign country or international organization or further transferred from one foreign country or international organization to another, if adequate protection for the data is guaranteed at the destination, or if specific safeguards are in place specifically for such transfer.

Transfers required by foreign court or administrative authority decisions will only be recognized or enforced if they are based on an international agreement, such as a

mutual legal assistance treaty, in effect between the requesting third country and Albania, and without violating the other transfer criteria outlined in the Data Protection Law.

Transfer of data based on an adequacy decision (Article 40)

Personal data may be transferred to foreign countries or international organizations if the recipient is located in a country, territory, or sector within a foreign country, or belongs to an international organization that ensures an adequate level of data protection. The adequacy of the data protection level for a country, territory, sector, or international organization is determined by a decision of the Commissioner.

Pursuant to the Decision of the Commissioner No. 8, dated 31 October 2016 the following states have an adequate level of data protection:

- European Union member states;
- European Economic Area states;
- Parties to the Convention No. 108 of the Council of Europe "For the Protection of Individuals with regard to Automatic Processing of Personal Data", as well as its 1981 Protocol, which have approved a special law and set up a supervisory authority that operates in complete independence, providing appropriate legal mechanisms, including handling complaints, investigating and ensuring the transparency of personal data processing;
- States where personal data may be transferred, pursuant to a decision of the European Commission.

Transfer of data in the absence of an adequacy decision (Article 41)

In the absence of an adequacy decision, a controller or processor may transfer personal data to a third country or international organization only if appropriate safeguards are in place, and if enforceable data subject rights and effective legal remedies are available for the data subjects.

If appropriate safeguards are not in place, the transfer may only occur if one of the following conditions is met:

- the data subject has explicitly consented to the proposed international transfer, after having been clearly informed of the possible risks of such transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request, or the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically incapable of giving consent, or their right to act has been removed or restricted;
- the transfer is necessary for important reasons of public interest;

- the processing is necessary for the establishment, exercise or defence of a right, obligation or legitimate interest before a court or public authority;
- the transfer is made from a register that is open for consultation by law and provides information to the general public, provided that the transfer includes only certain information and not entire sections of the register.

Where a transfer could not be based on any of the above, a transfer may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the Commissioner and the data subject of the transfer and on the compelling legitimate interests pursued.

Security

General responsibility of the controller (Article 22)

The Data Protection Law requires controllers to implement appropriate technical and organizational measures, based on the nature, scope, context, and purposes of the processing, as well as the potential risks to individuals' rights and freedoms. These measures must be regularly reviewed and updated as necessary.

Data protection by design and by default (Article 23)

Controllers should consider technological developments, implementation costs, and the specific circumstances of the processing when determining safeguards, such as pseudonymization, to protect data subjects' rights.

Controllers must ensure that, in a predetermined manner, only the personal data necessary for each specific purpose is processed, including limiting the data collected, its accessibility, and storage period. Security measures must prevent unauthorized access to personal data and maintain the confidentiality, integrity, availability, and resilience of processing systems and services.

Measures to ensure the security of processing (Article 28)

The controller and the processor implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, *inter alia*, where applicable:

- Pseudonymization and encryption of personal data;
- The ability to ensure the confidentiality, integrity, availability, and resilience of the processing systems and services;
- The ability to restore the availability and access to personal data within a reasonable time in the event of a physical or technical incident;
- A process for regularly testing, reviewing, and assessing the effectiveness of the technical and organizational measures to ensure the security of the processing.

The level of security shall be in compliance with the nature of personal data processing. The Commissioner has established additional rules for personal data security by means of Decision No. 6, dated 05 August 2013 "On the Determination of Detailed Rules for the Security of Personal Data".

Breach notification

Controller's notification to the Commissioner (Article 29)

In the event of a personal data breach, the controller must notify the Commissioner as soon as possible, and no later than 72 hours after becoming aware of the breach. Notification is not required if the breach is unlikely to result in a risk to the rights and freedoms of data subjects. If the notification is not made within the 72-hour timeframe, the controller must provide an explanation for the delay.

The notification to the Commissioner must include, at a minimum:

- A description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected, as well as the categories and approximate number of personal data records involved;
- The name and contact details of the DPO or another relevant contact point;
- A description of the likely consequences of the personal data breach;
- A description of the measures taken or proposed to address the breach, including, where applicable, measures to mitigate its potential adverse effects.

If all of the required information is not available at once, it may be provided in stages, as soon as possible.

The controller must document all personal data breaches, including the details, impact, and corrective actions taken, to enable the Commissioner to verify compliance. The Commissioner shall respond to the notification in line with their authority. The Commissioner may also instruct the controller to notify the affected data subjects of the personal data breach if the breach is likely to pose a high risk to their rights and freedoms, and if the controller has not already done so, as outlined in the section below.

Controller's notification to the data subjects (Article 29)

The controller must inform data subjects if the risks to their rights and freedoms resulting from the data breach are likely to be high, by providing the information as outlined in the notification to the Commissioner above. However, notification to data subjects is not required in the following cases:

- The controller has implemented appropriate technical and organizational protective measures, such as encryption, which were applied to the personal data affected by the breach;
- The controller has taken additional steps to reduce the risk of harm to the rights and freedoms of data subjects;

- The controller publishes the notice or takes other similar actions to notify data subjects of the breach in a uniform and effective manner, where notifying each individual data subject would impose a disproportionate burden on the controller.

Processor's notification to the controller (Article 29)

The processor shall notify the controller immediately after becoming aware of any personal data breach.

Enforcement

The Commissioner is the competent authority for the supervision and enforcement of Data Protection Law. The Commissioner is responsible, *inter alia*, for:

- Ensuring that data subjects can exercise their rights, including providing them with information and advice on these rights;
- Investigating the compliance of personal data processing activities with the Data Protection Law, either proactively or in response to a complaint;
- Reviewing complaints filed by individuals or non-profit entities, organizations, or associations representing individuals, in cases of alleged violations of the Data Protection Law;
- Evaluating the responses provided by competent authorities to data subjects' requests regarding their rights of access, rectification, or erasure;
- Imposing administrative sanctions and penalties, and overseeing their enforcement.

Administrative offenses related to the processing of personal data may result in a fine of up to ALL 2,000,000,000 (approximately EUR 20,300,000), or, in the case of a company, up to 4% of its total annual global turnover from the previous financial year, whichever amount is greater.

The Commissioner shall issue a directive outlining the rules regarding the imposition of administrative sanctions, which will be based on the guidelines established by the European Data Protection Board.

The sanctioned subject may appeal the fine in court within the deadlines and according to the procedures that regulate the administrative trials.

Electronic marketing

Electronic and direct marketing under the Data Protection Law

The Data Protection Law does not explicitly refer to electronic marketing; nevertheless, it will apply to most electronic marketing activities since they typically involve personal data, like an email address that includes the recipient's name.

Personal data may be processed for direct marketing purposes as a means of communicating with identifiable individuals to promote goods or services. This includes advertising membership in organizations, soliciting donations, and any direct marketing activities, which also cover any preparatory actions taken by the advertiser or a third party to facilitate such communication (Article 46(1)).

The most common legal grounds for the processing of data for direct marketing are:

The legitimate interests of the controller

Processing for direct marketing purposes, whether carried out by the controller or by third parties, may be based on legitimate interests, provided that the interests of the protection of data subjects are not overridden. This also applies to the use of data obtained from publicly accessible sources for direct marketing purposes.

The consent of the data subject

When relying on consent, it is essential to adhere to the requirements set by Data Protection Law. Notably, when personal data is processed for direct marketing purposes, the data subject has the right to object at any time, without needing to provide a reason, to the processing of their personal data for such purposes, including profiling insofar as it relates to them (Article 19(2) and Article 46(4)).

Furthermore, the controller must be able to demonstrate that the data subject has given consent for the processing of their personal data. If consent is provided in the context of a written statement that includes other matters, the request for consent must be clearly distinguishable from the other information. It should be presented in an intelligible and easily accessible format, using clear and plain language (Article 8(2)). In the context of direct marketing, marketing consent forms should include clear opt-in mechanisms, such as checking an unchecked consent box or signing a statement, rather than just accepting terms and conditions or assuming consent based on actions like visiting a website.

The processing of a minor's personal data based on consent, in the context of online goods or services directly offered to them, is lawful only if the minor is at least 16 years old. If the minor is under 16, the processing is lawful only if consent is given or authorised by the minor's parent or legal guardian, and only to the extent that it is given or authorised by them (Article 8(6)).

The processing of sensitive data for direct marketing purposes is carried out with the explicit consent of the data subject (Article 46(3)).

The Commissioner has issued an Instruction no. 06, dated 28 May 2010 "On the correct use of SMSs for promotional purposes, advertising, information, direct sales, via mobile phone". This instruction emphasizes the importance of the prior consent given by the data subject.

Electronic and direct marketing under the Electronic Communications Law

According to Law 54/2024 "*On electronic communications in the Republic of Albania*" ("Electronic Communications Law"), natural or legal persons who possess the email addresses of their customers for their products or services may use these addresses for direct marketing of similar products or services only if they have obtained the explicit consent of the customers to be contacted for marketing purposes. Additionally, they are required to provide customers with a simple and free way to opt out of the use of their email address for marketing purposes at any time. It is also prohibited to send SMS or email messages for direct marketing purposes if the sender's identity is

concealed or if a valid address is not provided, through which the recipient can request the cessation of such communications (Article 165 "Unsolicited communications").

Online privacy

Online privacy under the Data Protection Law

The Data Protection Law does not include specific regulations for cookies or location data. However, location data and online identifiers (which include cookies) are considered identifying factors for data subjects. As such, the general data protection provisions outlined in the Data Protection Law also apply to online privacy.

Apart from the general data protection principles applied mutatis mutandis, the Data Protection Law contains few specific provisions regarding online privacy. These include:

Right to rectification and erasure (Article 15(2)(dh))

The data subject has the right to request the erasure of personal data relating to them from the controller. The controller is required to erase the personal data as soon as possible, and in any case, no later than 30 days from the receipt of the request, if the data was collected in the context of online provision of goods or services.

The right to be forgotten (Article 16)

When the controller has made personal data public and is required to erase it, they must take reasonable steps, including technical measures, to notify other controllers processing those data that the data subject has requested the removal of any link, copy, or reproduction of the personal data, considering the applicable technology and implementation costs. Additionally, at the data subject's request, operators of internet search engines must remove outdated information from search results based on the data subject's name if that information, although no longer current, significantly harms the data subject's reputation.

In order to provide some clarifications on the notion of cookies and their use, the Commissioner has defined the cookies in an online dictionary as *some data stored on the computer, which contain specific information*. This rudimentary definition is further complemented by a short explanation which states that cookies *allow any server to know what pages have been visited recently, just by reading them*.

The Commissioner has also released an opinion (which is somewhat outdated and non-binding for data controllers) regarding the protection of personal data on the websites of both public and private entities. In this opinion, the Commissioner highlights the obligations of data controllers under the Data Protection Law, as well as the rights of data subjects, which must also be observed in the context of online personal data collection:

- The right to be fully informed and to give their approval if a website (or an application) processes their data;
- The right to keep their online communications secret (including email, the computer' s IP or modem No.);

- The right to be notified if their personal data are compromised (data has been lost or stolen, or if their online privacy is likely to be negatively affected);
- The right to request that their personal data to be excluded from data processing for direct marketing if they have not given their consent.

Additionally, in this opinion, the Commissioner stresses the importance of public and private controllers drafting and publishing privacy policies on their websites, including, among other things:

- The identity of the controller;
- The information collected from the users, specifying the category of personal data;
- Specific policies regarding cookies and other technologies that allow data controllers to gather information on the users that use the website and to notify the latter about their use.

Online privacy under the Electronic Communications Law

The Electronic Communications Law defines "*location data*" as any data processed in an electronic communications network, indicating the geographical position of the terminal equipment of a user of the electronic communications network.

Location data may only be processed when they are made anonymous or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.

The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service.

Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time. Users or subscribers must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

Processing of location data must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service (Article 163 of the Electronic Communications Law).

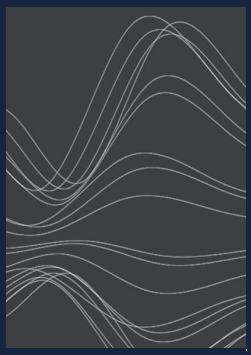
Data protection lawyers

Flonia Tashko
Partner
Tashko Pustina
flonia.tashko
@tashkopustina.com
View bio

Alban Shanaj
Partner
Tashko Pustina
alban.shanaj
@tashkopustina.com

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