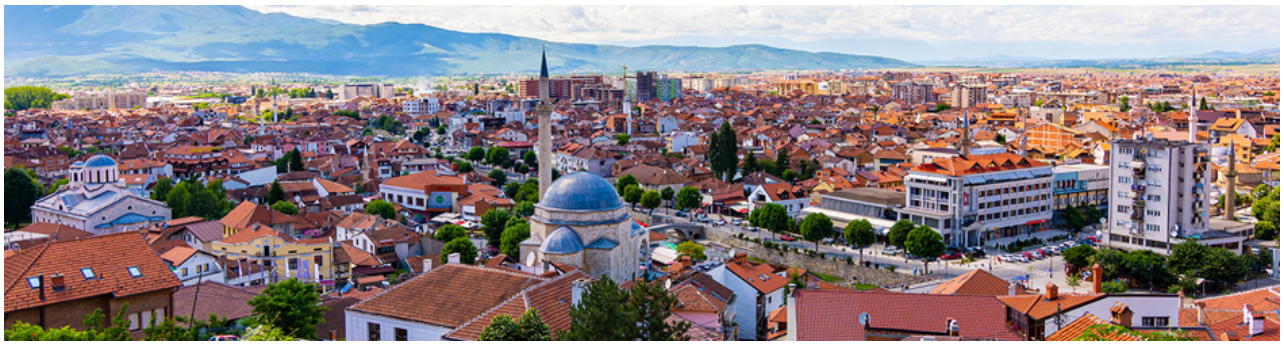
DATA PROTECTION LAWS OF THE WORLD

Kosovo

KOSOVO



Last modified 11 January 2024

LAW

The Law on Protection of Personal Data No.06/L-082 (“**LPPD**”) is the Kosovan law which entered into force and became applicable on 13 February 2019. The LPPD transposes the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (“**GDPR**”).

Scope of application

The LPPD has a wide scope of application. Namely, the LPPD applies to (Article 2):

- processing activities by private as well as public bodies;
- processing of personal data in diplomatic and consular offices, including any representative office of Kosovo abroad.

The LPPD has extraterritorial scope in that it applies to data controllers not established in Kosovo, which for the purposes of processing personal data make use of automatic or other equipment in Kosovo; nevertheless, the LPPD will not apply if such equipment is used only for transit purposes through the territory of Kosovo (Article 2(2)).

In addition to LPPD, in 2023 Kosovo has adopted Regulation no.02/2023 on Processing of Personal Data Obtained from Drone Use (“Regulation 02/2023”) which aims to define and establish specific responsibilities and measures related to processing of personal data by the drone owner or operator.

DEFINITIONS

Definition of Personal Data

“**Personal Data**” is defined as *“any information related to an identified or identifiable natural person (‘ data subject’).*"

An identifiable natural person is defined widely as any person *“who can be identified directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.*

Definition of Sensitive Personal Data

“**Sensitive Personal Data**” is defined as “*personal data revealing ethnic or racial origin, political or philosophical views, religious affiliation, union membership or any data related to health condition or sexual life, any involvement in or removal from criminal or offence records retained in accordance with the law. Biometric characteristics are also considered sensitive personal data if the latter enable the identification of a data subject in relation with any of the abovementioned circumstances in this sub-paragraph. ”*

Genetic data, biometric data and data concerning health are also considered as sensitive category of personal data within the meaning of the LPPD.

NATIONAL DATA PROTECTION AUTHORITY

The competent national data protection authority in Kosovo is the Information and Privacy Agency (“**IPA**”) which is established as an independent agency, responsible for the supervision of implementation of the legislation on personal data protection, as well as access to public documents, in order to protect the rights and fundamental freedoms of natural persons in relation to the personal data processing and ensuring the guarantee of access to public documents.

IPA is divided into two organisational structures, namely (Article 58 (4)):

- access to public documents;
- protection of personal data.

IPA is charged with the following tasks (Article 64 (1)):

- supervision of the implementation of the LPPD;
- advising of public and private bodies on issues related to data protection;
- informing the public on issues and developments in the area of personal data protection;
- promotion and support of fundamental rights;
- deciding on complaints submitted by the data subjects;
- advising the Assembly, the Government and other institutions and bodies on legislative and administrative measures with regards to the protection of fundamental rights and freedoms of natural persons in terms of data processing;
- carrying out inspections with regards to the implementation of the LPPD;
- on its own initiative or upon request, providing opinions for public and private bodies, as well as publishing on any issues related to personal data protection.

REGISTRATION

Considering that the LPPD transposes the GDPR, same as the latter, it provides meticulous and protective measures to which the Controllers and the Processors must comply, and as such does not impose restrictive registration or notification requirements to be undertaken with the IPA. Accordingly, in general, LPPD does not contain mandatory provisions requiring registration of processing activities.

However, certain notification requirements apply in cases where a data protection impact assessment suggests a high risk without adequate protection measures (Article 36.1). Further, controllers or processors must report their appointed data protection officer to the IPA, where such appointment is required by law (Article 37.7). In the private sector, controllers or processors using biometric data for their activities must inform the IPA beforehand. This includes providing a detailed description of safety measures for processing biometric data (Article 83).

Additionally, controller and processor, including entities which process personal data based on the LPPD, are required to obtain the certification to perform work related to personal data (Article 43(1)). In practice, the certification procedure is not applicable in Kosovo, and its implementation is subject to the adoption of a sub-legal act (Article 43 (2)).

DATA PROTECTION OFFICERS

Controllers and Processors must appoint a data protection officer in the following cases (Article 37 (1)):

- The processing is carried out by a public authority or body, except in cases of courts acting in their judicial capacity;
- The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and / or their purpose, require regular and systematic monitoring of data subjects on a large scale;
- The core activities of the controller or the processor consist of processing, on a large scale, of sensitive personal data, and processing of personal data related to criminal convictions and offences.

A group of undertakings has the option to appoint a joint data protection officer, provided that the officer remains easily accessible to every entity within the group (Article 37.2). The appointment of a data protection officer is based on their professional knowledge and experience in data protection laws (Article 37.5).

The LPPD outlines the following tasks for data protection officers (Article 39.1):

i. Informs and advice controllers and / or processors on their obligations when processing personal data;
ii. Where required, provides advice on the data protection impact assessment and monitor its performance;
iii. Cooperate with IPA;
iv. Act as the contact point for the IPA on issues relating to processing of personal data.

COLLECTION & PROCESSING

LPPD adopts a wide definition of processing. Namely, processing includes *any operation or set of operations performed to personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction* (Article 3(1)(2)).

For the purposes of LPPD, data controller is defined as *any natural or legal person, public authority or other body which, alone or jointly with others, determines the purpose and means of personal data processing* (Article 3(1) (11)), whereas the processor is defined as *a natural or legal person, from public or private sector which processes personal data for and on behalf of the data controller* (Article 3(1) (14)).

When collecting and processing of personal data, Controllers must abide to the basic principles of data processing set forth in the LPPD. Namely, personal data must be collected and processed based on the following principles (Article 4):

- **Principle of lawfulness, justice and transparency**: personal data must be collected and processed in an impartial, lawful and transparent manner, without infringing the dignity of the data subjects.
- **Principle of purpose of limitation**: personal data must be collected and processed only for the specified, explicit and legitimate purposes and cannot be further processed in a manner which is incompatible with the stated purposes. However, in cases of further processing for archival purposes in the public interest, scientific or historical research, as well as statistical purposes, will not be considered to be incompatible with the initial purpose.
- **Principle of data minimisation:** the personal data should be adequate, relevant and limited to the purpose for which they are further collected or processed.
- **Principle of accuracy:** personal data should be kept accurate at all times, and kept up to date. In this line, every reasonable measure should be taken to ensure that inaccurate personal data are rectified or erased without delay.
- **Principle of storage limitation:** personal data may be stored insofar as necessary to achieve the purpose for which they are processed or collected; after which, the personal data should be erased, deleted, destroyed, blocked or anonymised, unless otherwise foreseen by another relevant law.
- **Principle of integrity and confidentiality:** personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by using appropriate technical and organisational measures;
- **Principle of accountability:** the controller is responsible for, and be able to demonstrate compliance with all the principles mentioned above.

Legal basis for processing of personal data (Article 5)

With reference to the list above, processing of personal data shall be considered lawful if one of the following criteria is met:

- The data subject has given consent for the processing of his/her personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the data subject is a contracting 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 subjected;
- 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 the 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. This provision does not apply in cases where the processing is carried out by public authorities in the performance of their tasks.

Where the legal basis for processing is not based on the consent of the data subject or on the relevant legislation in force, in order to comply with the LPPD and lawfulness principle when processing personal data for purposes different from the initial purpose of the data collection, the following should be considered (Article 5(2)):

- Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- The context in which the personal data have been collected, in particular regarding the relationship between the data subjects and the controller;
- The nature of personal data being processed, especially in cases of processing of sensitive personal data or data related to criminal convictions;
- Possible consequences for the data subjects of the intended further processing;
- The existence of appropriate safeguards, which may include encryption or anonymisation.

Conditions for consent (Article 6)

Where the collection and processing of personal data is based on the consent of the data subject, the Controller must be able to demonstrate that the data subject has consented to process his/her personal data. In this line, when consent is given as a written declaration, the latter must be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language (Article 6(2)).

Processing of special categories of personal data (Article 8)

As a principle, LPPD prohibits the processing of special categories of personal data. Special categories of personal data within the meaning of the LPPD are used synonymously with sensitive categories of personal data.

Notwithstanding the above, exemptions to prohibition of processing of sensitive personal data include the following circumstances (Article 6(3)):

- The data subject has given his/her explicit consent to the processing of those personal data for one or more specific purposes, except where the relevant legislation in force provides that the general prohibition on processing of sensitive personal data cannot be lifted by the data subject;
- Processing is necessary for the purpose of carrying out obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, in so far as it is authorised by the relevant legislation in force or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- Processing is necessary to protect the vital interests of the data subjects or other natural persons, where the data subject is physically or legally incapable of giving consent;
- If the data subject has made the sensitive personal data public, without limiting their use, in an evidenced or clear manner; processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest, on the basis of the relevant legislation;
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of relevant legislation or pursuant to contracts with a health professional when such data are processed by a professional or under his/her responsibility subject to the obligation of

professional secrecy pursuant to respective legislation, established rules by national competent bodies or by another person subjected to professional secrecy;
- Processing is necessary for reasons of public interest in the area of public health, such as protection against serious cross-border threats to health, or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of the relevant legislation;
- Processing is necessary for archiving purposes in the public interest, as well as scientific or historical research purposes, or statistical purposes.

Except in cases where the data subject has made his/her sensitive personal data public, special categories of personal data should be protected in a special manner and be classified for the purpose of preventing unauthorised access or use (Article 8(4)). Classification of sensitive personal data refers to marking of personal data to indicate their sensitive nature (Article 3(1) (4)).

TRANSFER

In the context of transfer of personal data, the LPPD addresses two situations:

- Transfer of personal data to countries and international organisations which ensure an adequate level of data protection, and
- Transfer of personal data to countries and international organisations which do not provide adequate level of data protection.

With regards to the transfer of personal data to countries or international organisations that ensure proper and adequate level of data protection, as per a Decision adopted by the IPA, the list of countries and international organisations providing proper data protection, the latest being adopted on 13 September 2021 (“**the Decision**”) includes the following countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Iceland, Lichtenstein, Norway, and Switzerland.

Moreover, the LPPD expressly allows the IPA to rely on the decisions adopted by relevant EU bodies with regards to the transfer of personal data when drafting the list of approved countries providing adequate level of personal data protection (Article 46.2). Accordingly, based on the Decision, IPA considers some countries (including those outside the EU) ensuring proper level of data protection, in accordance with the EU Commission Decisions (Argentine, Andorra, Canada, Guernsey, Isle of Man, Jersey, Faroe Islands, Israel, New Zealand, Uruguay, Japan and United Kingdom).

With reference to the countries listed above, when transferring personal data, no special authorisation or permission is required from the IPA, provided the data subject is aware and informed that the personal data are being transferred, as required by the LPPD (Article 12.1.6).

In case of transfer to third parties located in other countries, such application will depend on whether such countries are included in the list of the IPA Decision or decisions of the EU Commission.

With regards to the transfer of personal data to international organisations, the Decision of the IPA does not specifically identify or address international organisations providing adequate level of personal data protection.

However, as a general principle, when deciding on the adequate level of data protection of another country or international organisation, the IPA shall firstly take account of the following elements (Article 47.1):

- The rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectorial, including public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another country or international organisation which apply within that country or international organisation, case-law, as well as effective and enforceable data subject right and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
- The existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data

protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities;
- The international commitments the third countries or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data;
- The type of personal data to be processed;
- The purpose and duration of the proposed processing;
- The legal arrangement in the country of origin and the recipient country, including the legal arrangement for protection of personal data of foreign citizens;
- The measures to secure personal data used in such countries and international organisations.

In addition, the above, in its decision-making process the IPA will particularly pay attention on (Article 47.2):

- Whether the personal data to be transferred will be or are used solely for the purpose of which they are being transferred, or whether the purpose may change only on the basis of a permission of the data controller supplying the data or on the basis of personal consent of the data subject;
- Whether the data subject has the possibility of determining the purpose for which his or her personal data will be used, to whom they are being transferred and the possibility of correcting or erasing inaccurate or out-dated personal data, unless this is prevented due to the secrecy of the procedure by binding international treaties;
- Whether the foreign data controller or data processor performs adequate organisational and technical procedures and measures to protect personal data;
- Whether there is an assigned contact person authorised to provide information to the data subject or to the IPA on the processing of personal data transferred;
- Whether the foreign data recipient may further transfer personal data, which may be done only on the condition that another foreign data recipient to whom personal data will be disclosed ensures adequate protection of personal data also for foreign citizens;
- Whether effective legal protection is ensured for data subjects whose personal data were or are being transferred.

In accordance with the above, it is safe to assume that international organisations fulfilling the listed criteria will be considered as providing adequate level of personal data protection. Additionally, international organisations deemed as providing adequate level of personal data protection by the EU Commission, may also be accepted by the IPA (Article 46.2).

SECURITY

LPPD contains general provisions when it comes to safety of processing of personal data. Security of processing of personal data refers to adopting appropriate organisational, technical and logical-technical procedures and measures in order to prevent any accidental, deliberate unauthorised destruction, disclosure, modification, etc. Implementing security measures is carried out by (Article 31 (1)):

- Pseudonymization and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The above measures of security are not sector-specific and apply to the processing of personal data in general.

In addition to implementing appropriate organizational, technical, and procedural measures for the secure processing of personal data, Regulation 02/2023 imposes specific measures on drone users to protect personal data, including (Article 8.1):

- Prohibiting unauthorized access to premises storing processed personal data.

- Restricting data access and prohibiting unauthorized use of archiving tools.
- Requiring authorization from licensed drone users for equipment commissioning and securing tools against unauthorized use.
- Mandating employees to lock computers, lockers, and offices containing personal data when leaving their workplace.
- Ensuring the protection of data from unauthorized access in the presence of non-employees.
- Prohibiting the display of personal data on screens in the presence of unauthorized persons.
- Restricting the removal of devices containing personal data from the office and ensuring data deletion or destruction in unsafe places.
- Prohibiting employees from recording or copying records without permission from the licensed user.
- Restricting the use of drone-collected data for purposes other than its intended collection, unless permitted by relevant personal data protection legislation.

BREACH NOTIFICATION

Breach notification to the IPA

LPPD foresees a mandatory breach notification to the IPA by data controllers not later than seventy-two (72) hours after becoming aware of the breach, unless the personal data breach is unlikely to risk the rights and freedoms of natural persons (Article 33 (1) (1)). When the data controller fails to report the breach after the 72 hours of becoming aware of it, the notification to IPA must also contain reasons on delayed notification.

With regards to the processors, the LPPD states that they should notify the breach to IPA *without undue delay* (Article 33 (2)), however a specific deadline as in the case of controllers is not provided.

Breach notification to the Data Subject

The data subject is notified on any breach resulting in a high risk to his/her rights and freedoms, without undue delay (Article 34 (1)). The obligation to communicate the breach to the data subject will not apply, provided the following conditions are met (Article 34 (3)):

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects (i.e. natural persons) is no longer likely to materialise;
- it would involve disproportionate effort, whereby, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

ENFORCEMENT

Filing a complaint at IPA

The data is subject is entitled to file a complaint with the IPA, while reserving the right to other administrative and judicial remedies (Article 52). IPA is obliged to notify the data subject on the decision of the complaint, as well as inform the data subject on the possibility of judicial remedy to uphold his/her rights with regards to violation of personal data (Article 52 (2)). However, if IPA fails to inform the data subject on a decision with regards to the complaint within three (3) months of its submission, the data subject shall be entitled to an effective judicial remedy (Article 53 (2)).

Filing a complaint against a Decision of the IPA

Every natural or legal person is entitled to file a complaint at the competent court against a binding decision of the IPA concerning them, by initiating an administrative dispute before the competent court (Article 53).

Right to an effective judicial remedy against a controller or processor

Without prejudice of the right of the data subjects to issue a complaint with the IPA, each data subject shall have the right to an effective judicial remedy in cases where he/she considers that the controllers or processors infringed the rights accorded by the LPPD, as a result of processing of his/her personal data.

With regards to filing complaints as described above, the data subject has the right to engage/mandate a non-profit body, organisation or association which has been established in accordance with the relevant law and is active in the field of personal data protection, to submit the complaint, represent and receive compensation on behalf of the data subject (Article 55 (1)).

Fines

Violations of provisions of LPPD are considered as minor offences/misdemeanours (i.e. *kundervajtje,* in Albanian) and are punishable by fines.

Fines for violation of provisions of LPPD, may be issued to legal persons, the authorised representative of the legal person or to the person exercising independent activities.

The severity of the fine depends on the identity of the offender, the nature of the violation and the extent of the violation.

IPA is authorised to issue fines to legal persons or to a natural person exercising independent activities, in the amount ranging from EUR 20,000 to EUR 40,000, if they fail to process personal data in accordance with LPPD, including but not limited to the following violations (Article 92 (1)):

- he/she processes personal data without any legal basis or without the consent of the data subject as provided by the LPPD;
- he/she entrusts an individual task relating to the processing of personal data to another person, without concluding a written contract as required by the LPPD;
- he/she processes sensitive personal data in violation of LPPD, or fails to provide the required protection to the sensitive personal data.

A fine ranging from EUR 2,000 to EUR 4,000 shall be imposed on the responsible/authorised representative of the legal person or to the person exercising independent activities (Article 92 (2)).

A fine ranging from EUR 1,000 to EUR 2,000 shall be imposed to the responsible person of a state body, in cases of minor offences with regards to personal data (Article 92 (3)).

A fine ranging from EUR 400.00 to EUR 1,000 shall be imposed to an individual, in cases of minor offences with regards to personal data (Article 92 (4)).

Serious and major violations of legal provisions

In cases where IPA finds a serious and grave violation of the provision of processing of personal data, it may impose a fine ranging from EUR 20,000 to EUR 40,000, or in cases of a company or enterprise it may impose a fine amounting to two percent (2%) of the general turnover of the company/enterprise for the previous fiscal year in compliance with the GDPR (Article 105).

ELECTRONIC MARKETING

LPPD applies to direct marketing activities and to automated decision-making including profiling. LPPD allows data controllers to use personal data obtained from publicly accessible sources or within the framework of lawful performance of activities for the

purposes of providing goods, services, employment or temporary performance of tasks, using postal services, telephone calls, e-mails or other telecommunication means (Article 73 (1)). With regards to direct marketing, the data controllers may only use the following personal data(Article 73 (2)):

- personal name
- permanent or temporary address
- telephone number
- e-mail
- fax number.

Other data may be processed only based on the data subject’s consent (Article 73 (2)).

A data subject is entitled to object at any time, the use of his/her personal data for the purposes of direct marketing (Article 74). The objection of the data subject must be submitted in writing, and within eight (8) days of receiving the objection, the controller must cease to use such personal data (Article 74 (1)).

ONLINE PRIVACY

There is no specific legislation with regards to on-line privacy (including cookies and location data). However, the LPPD considers location data and online identifiers as personal data (Article 3 (1) (1)). Accordingly, the processing data which fall within the definition of the LPPD, must be done in accordance with the provisions and principles of the LPPD.

Moreover, with reference to the location data, Law on Electronic Communications No.04/L-109 **(“LEC”)** stipulates that when location data are being processed, such data may be processed **only if they are made anonymous** *or* the users have given their consent for processing. In this line, Article 23 of LPPD provides the following: *“taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Law*" (Article 89 LEC).

KEY CONTACTS

Tashko Pustina Attorneys
tashkopustina.com/

Floran Pustina
Partner
Tashko Pustina Attorneys
T + 383 38 71 77 55
floran.pustina@tashkopustina.com

Mrika Gashi
Senior Associate
Tashko Pustina Attorneys
T + 383 49 61 36 65
mrika.gashi@tashkopustina.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.