BIRN
BALKAN INVESTIGATIVE REPORTING NETWORK | ALBANIA

POLICY BRIEF:
Regulations on data protection and processing for media and journalists in Albania

June 2023

BIRN
BALKAN INVESTIGATIVE REPORTING NETWORK | ALBANIA

POLICY BRIEF

Regulations on data protection and processing for media and journalists in Albania

June 2023

Published by: Balkan Investigative Reporting Network in Albania
Str. Nikolla Jorga, No. 8/8, Tirana, Albania
http://birn.eu.com/

Author: Emirjon Marku

English Editor: Marcus Tanner

Graphic Design: Jurgena Tahiri

Table of Content:

ABBREVIATIONS AND GLOSSARY

Commissioner	Commissioner for Freedom of Information and Personal Data Protection
Convention no. 108	Convention of the Council of Europe *"Convention for the protection of individuals with regard to automatic processing of personal data"* and to the additional protocol thereto of the year 1981
Decision no. 8	Decision no. 8, dated 31 October 2016, of the Commissioner, *"On determination of countries with adequate level of personal data protection"*
Directive 95/46/EC	DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995, on protection of individuals with regard to the processing of personal data and on the free movement of such data
ECHR	European Convention on Human Rights
EFTA	European Free Trade Association
EU	European Union
EU Commission	Commission of the European Union
GDPR	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, and repealing Directive 95/46/EC (General Data Protection Regulation)
Instruction no. 9	Instruction no. 9, dated 15 September 2010, of the Commissioner, *"For the substantial rules regarding the protection of personal data in the print, visual and audiovisual media"*

Instruction no. 31	Instruction no. 31, dated 27 December 2012, of the Commissioner *"On determination of conditions and criteria for the exemption from the relevant obligations relating to processing of personal data for journalistic, literary and artistic purposes"*
Instruction no. 41	Instruction no. 41, dated 13 June 2014, on the Commissioner, *"On permission of some categories of international transfers of personal data to a country without adequate level of personal data protection"*
Law on Personal Data Protection	Law no. 9887, dated 10 March 2008, "On personal data protection"as amended

I. INTRODUCTION

The field of journalism represents a unique microcosm when it comes to data protection and privacy rights of citizens.

Journalism's appetite for voluminous personal information, obtained through daily work (i.e. interviews, investigations, reporting, photographs, etc.), is challenged by the right of the data subjects (citizens) to data protection and privacy.

Indeed, both freedom of expression, embodied especially in journalistic activities, and the right to data protection and privacy represent constitutional imperatives in Albania, provided for respectively under articles 22 and 35 of the Albanian constitution. These rights are also anchored at the same normative level under the ECHR, to which Albania is a party (under articles 8 and 10 thereof).

Everyone has the right to a safe and secure private life and to exert control over the processing of his or her personal data by the relevant controllers (including media organisations and freelance journalists).

On the other hand, journalism plays an indispensable role in the shaping of a well-informed public opinion, and for upholding a democratic society.

Journalists bear responsibility for disseminating information and keeping the public informed about matters of public interest, which the public itself has the right to receive.

However, journalism's crucial role in the life of a democratic society, as public watchdog (as the so-called "fourth estate"), sometimes results in a clash between freedom of expression and the right to privacy.

This collision needs to be addressed in each specific case.

The question of when the right to privacy outweighs freedom of expression, and vice versa, is addressed from a legal perspective – although not exhaustively – in terms of the legislation on personal data protection in Albania (i.e. in the ambit of the Law on Personal Data and its sublegal acts) and GDPR (in the EU).

In light of the above, this document aims to bring to the attention of, and explain to, readers (journalists, editors, media directors, etc.) the boundaries of the co-existence of these constitutional freedoms and rights in Albania – to help them to understand how to achieve the necessary balance between these constitutional rights whilst exercising their profession.

A specific section is also dedicated to legal developments in the EU in the ambit of GDPR.

Please remember, this document primarily aims to offer guidance on approaching principles of data protection legislation, including ethical considerations. It does not provide

exhaustive solutions for achieving legal compliance vis-à-vis freedom of expression and the right to data protection/privacy.

II. ALBANIA'S LEGAL FRAMEWORK

The main piece of legislation in Albania that deals in detail with data protection rights is the Law on Personal Data Protection, along with the sublegal acts issued by the Commissioner, which is the competent authority that supervises the compliance of data controllers and/or data processors with the legislation in force.

The provisions of the Law on Personal Data Protection apply to the processing of personal data of data subjects (citizens/individuals), carried out by relevant controllers/processors through automatic or other means.

The subjects to the law are considered, *inter alia*, data controllers established in the Republic of Albania, as well as data controllers not established in Albania but who make use of equipment situated in this country.

Paragraph 1, article 3, of the Law on Personal Data Protection says personal data means any information related to an individual, identified or identifiable, directly or indirectly, especially by referring to an identification number or one or more factors that are specific to his/her physical, physiological, mental, economic, cultural or social identity.

By way of example, personal data are, without limitation, a person's name, surname, address, image/photograph/video footage, age, fingerprint, voice, phone number, email, curriculum vitae (CV), internet protocol (IP), or social media account, etc., of a data subject/individual.

The processing of personal data includes, but is not limited to, the collection, registration, organisation, retention, adaption or change, transmission, disclosure, erasure or destruction of personal data, etc.

Each of these actions constitutes a personal data processing in itself.

Personal data processing is performed by the data controller and/or the data processor.

A data controller is a natural person or legal entity that determines the scope and manner of personal data processing, in accordance with the legislation in force, being bound to comply with the provisions of such legislation. Media companies/organisations or freelance journalists might be considered controllers.

A data processor is any natural person or legal entity that processes personal data in the name of a data controller. Hired journalists might be considered data processors who act on the instructions of the controller (i.e., the media organisation) that employs them.

Any controller/processor should notify the Commissioner by means of a standard form on their processing activity, either before starting it, or whenever such processing activity is changed (article 21 of the Law on Personal Data Protection). This is *the notification obligation*.

Principles

To comply with the applicable legislation on personal data, a data controller/processor should act in compliance with the principles laid down under article 5 of the Law on Personal Data Protection.

- *'Lawfulness and fairness'.*

Lawful processing of personal data means that a controller may process personal data only under a specific legal basis. That might be the consent of the data subject, the conclusion of a contractual relationship, a legal obligation, legitimate interest, etc. (i.e., see letters (a) to (f) below).

Special emphasis when coming to the lawful processing of the personal data has to be put on the legal basis of processing sensitive data, as well as children's data; they enjoy special protection in legislation.

On the other hand, fair processing of personal data means taking into account the privacy expectations of the data subjects while collecting/processing their data, without misleading them to such an end, or by collecting/processing personal data in a way that causes unjustified harm to the data subject/individual.

This means the controller must ensure that data subjects are treated fairly when they seek to exercise their rights; these include right to access, block, correct, erase, object processing, etc.).

- *'Purpose limitation'.*

This principle implies that the collection of personal data should be done for specific purposes that are clearly determined and lawful, as well as the (further) processing in compliance with such purposes.

For example, if personal data are processed within the ambit of a journalistic purpose (during an interview, etc.), these data cannot be further processed if the *new* purpose differs from the *first* one (i.e. for direct marketing purpose) – so-called "*function creep*".

If the new purpose is not compatible with the previous one, the further processing of data should be based again on a new legal basis (i.e., consent, legitimate interest, etc. – see letters (a) to
(f) below).

By providing transparency about the purpose behind the use of personal data, individuals can gain a clear understanding of the intentions and actions surrounding their information. This clarity empowers them to make informed decisions, including on whether or not to share their data with you.

Moreover, it enables individuals to exercise their rights and exert greater control over the

handling of their data.

- *'Data minimization'*

This principle means that in order to achieve the purpose of processing, the controller should process only those personal data that are sufficient to such an end. Such personal information/data should relate to the purpose of their processing and not be excessive in relation to it.

If you collect personal data beyond what it necessary to fulfil your intended purpose, individuals may exercise their right to request the deletion of their data (*right to erasure*). Conversely, if you hold insufficient data, you may face challenges in obtaining a comprehensive understanding of the relevant facts. In such cases, individuals have the right to request completion of any incomplete data (*right to rectification*).

- *'Accuracy'*

The accuracy principle means that personal data should be accurate, complete and, where necessary, kept up-to-date; every reasonable step must be taken to erase, complete or rectify any inaccurate or incomplete data, having regard to the purposes for which they are collected or for which they are further processed. Apart from being a crucial legal principle for data protection purposes, the accurate exploitation of data is crucial for journalistic work as well. Maintaining public trust by using accurate personal information protects the important public interest inherent to journalism itself and may increase the reputation of a media outlet as a reliable source of news. It is especially important for maintaining accuracy to distinguish between facts and opinions when disseminating information about individuals; significant attention should be paid to the source of the information (the use of internet sources, social media and other user-generated content carries a potentially elevated level of risk as regards accuracy).

- *'Storage limitation'*

Personal data should be kept in a form which permits the identification of individuals for no longer than is necessary for the purposes for which the data are collected or further processed.

Data protection legislation does not provide explicit time limits for different categories of data. It is therefore incumbent on the controller to assess the purpose for which they are processing personal data and reasonably determine the appropriate period for retaining that data.

When deciding on a suitable retention period, it is essential to consider the specific purpose behind the processing of the personal data. By conducting a thorough assessment, you can determine a reasonable time frame for retaining the data that aligns with your purpose and ensures compliance with data protection principles.

Legal bases

For the processing of personal data to be considered lawful, according to article 6 of the Law on Personal Data Protection, it should be carried out only in accordance with the legal criteria/bases below:

(a) If the data subject has granted his/her consent to personal data processing;

(b) If the personal data processing is substantial for the fulfilment of a contract entered into by the data subject, or for the purpose of discussions or amendments to a project/ contract on the proposal of the data subject;

(c) To protect the vital interest of the data subject;

(d) To fulfil a legal obligation of the data controller;

(e) For the performance of a legal task of public interest or exercising an authority of the data controller, or third party, to which the personal data have been disclosed;

(f) If the personal data processing is substantial for the protection of legitimate interest of the data controller, data receiver or other interested persons, provided that such legitimate interest is not overridden by the data subject's right to the protection of their personal and private life.

In practice, the lawful bases commonly applicable to processing personal data for journalism purposes are:

- *Consent*: When individuals have provided explicit and informed consent for the processing of their personal data for journalistic purposes, this can serve as a lawful basis. It is important to ensure that consent is freely given, specific, and can be withdrawn at any time.
- *Legal obligation*: Compliance with a legal obligation, to which the media organisation is subject, can serve as a lawful basis for processing personal data. This could include obligations imposed by laws or regulations on media activities.
- *Vital interests*: Processing personal data may be justified if it is necessary to protect someone's vital interests, such as in situations involving life-threatening emergencies or protection of individuals' physical integrity.
- *Legitimate Interests*: This requires careful assessment of the interests and rights of the data subjects and ensuring that the fundamental rights and freedoms of the individuals do not override the legitimate interests of the media organisation. To such an end, a

balance test is needed to assess whether the legitimate interest (i.e. the public interest) over a certain publication of a news should prevail over the right of the individual to privacy.

Sensitive data

A special treatment is reserved to the processing of sensitive data, as set out under article 7 of the Law on Personal Data Protection. This comprises any information related to an individual concerning his/her **racial or ethnic origin**, **political opinion**, **membership of a trade union**, **philosophical belief or religion**, **criminal background**, as well as data related to **health and sexual life**.

The processing of sensitive data might take place, *inter alia*: if the data subject has granted his or her written consent; if it is in the vital interest of the latter or of another person (where the data subject is physically or mentally incapable of giving consent); if it is authorized by the competent authority for reasons of public interest; if it relates to personal data manifestly made public by the data subject or is necessary for the exercise or defence of a legal claim; or if it is required for purpose of preventive medicine, healthcare, etc.

Without prejudice to the above, when processing sensitive data for journalism purposes, the lawful bases most likely to be relevant are as follows:

- *Explicit Consent*: Obtaining the explicit consent of the data subject is generally the most reliable and straightforward lawful basis for processing sensitive data. Journalists should ensure that consent is obtained freely and that individuals are fully informed about the purpose and scope of the data processing.
- *Substantial public interest*: Processing sensitive data may be justified if it is necessary for reasons of substantial public interest, such as investigative journalism or reporting on matters of public concern. This also requires suitable safeguards to protect the rights and interests of the subjects whose data are being processed.

It is important to note that when processing sensitive data for journalism purposes, additional safeguards and considerations should be in place to ensure the protection of individuals' rights and interests.

Journalists and media organisations should adhere to the relevant data protection legislation, professional codes of conduct and ethical guidelines specific to their jurisdiction/industry. Additionally, implementing appropriate security measures and ensuring data minimization are crucial to safeguarding sensitive data.

International transfer

As a rule, the international transfer of personal data is allowed to take place with countries that have an adequate level of personal data protection, as determined by Decision no. 8 and Instruction no. 41 of the Commissioner in harmony with article 8 of the Law on Personal Data Protection.

The list of countries that have an adequate level of personal data protection include, among others, Member States of the EU, the member states of EFTA, the parties to Convention no. 108, as well as the countries determined on decision of the EU Commission.

The international transfer of personal data to countries without adequate levels of personal data protection is allowed (article 8 of the law), among others: on consent of the data subject; for the protection of vital interest of the latter; for reasons of public interest or protection of a legal right; or if the data are processed from a register accessible for consultation purposes and that provides information to the public in general. In other cases, the transfer of personal data may be carried out only on the authorization of the Commissioner (article 9 of the law).

Rights of data subjects

Especially important in the context of personal data processing are the rights of the data subject as laid down under articles 12-18 of the Law on Personal Data Protection. They include:

(i) *Right of access*. Data subjects are entitled to obtain, free of charge, from the data controller (upon written request), confirmation of whether their personal data are being processed, information on the purposes of processing, as well as on the categories of processed data and the recipients to whom personal data are disclosed/disseminated. However, this right may be exercised only, among others, if it is in line with the freedom of expression/press and professional secrecy. When denying right of access, the controller should within 30 days explain the reason of such a denial and inform the data subject about his/her right to file a complaint to the Commissioner, who is entitled to check (on request of the data subject) whether the access denial is justified by the aforementioned reasons;

(ii) *The right to request blocking, rectification or erasure of data*. The data subject has the right to request blocking, rectification or deletion of his or her data, free of charge, whenever he or she becomes aware that data relating to him or her are inaccurate, false and incomplete, or have been processed in violation of the law's provisions;

(iii) *The right to object to processing*. The data subject has the right to object to processing

of data related to him/her carried out by the data controller, if the basis for such processing is either the public interest or legitimate interest of the controller or a third party. To this effect, the data subject should rely on the relevant provisions of the applicable legislation that entitle him/her to object to such processing;

(iv) *The right to file a complaint*. Any person who claims that their rights, freedoms and legal interests concerning their personal data have been violated has the right to lodge a complaint or notify the Commissioner and request its intervention to remedy the violated right.

Data subjects may address the courts and seek damage relief in cases of unlawful processing of personal data.

Moreover, according to Article 18, when collecting personal data, the data controller is obliged to inform the data subject about, among others: the name of the controller; the purpose of personal data processing; the person that will process the personal data and the means of such processing; the persons or categories of persons to whom the personal data will be transmitted/disclosed; their right to access and rectify the personal data; the personal data retention period, etc.

The right of information of the data subject corresponds to the obligation of the controller for information. The iinformation of the data subject precedes his/her consent to personal data processing (i.e., informed consent).

II.1 Processing personal data for journalism purposes

Considering the importance of freedom of expression and, especially, that journalism as an instrument in ensuring it, the Law on Personal Data Protection pays specific attention to the processing of personal data for journalistic purposes, considering it a special processing activity.

In this view, according to article 11 of the law, the Commissioner determines, by virtue of a specific instruction, the terms and conditions when controllers (media organisations/ freelance journalists) are exempted from the mandatory requirements of the law in relation to the principles of processing (article 5), the legal bases of processing (article 6), the processing of sensitive data (article 7), the international transfer of personal data (article 8), the obligation for information of the data subject (article 18), as well as the obligation for notification of the processing activity to the Commissioner (article 21).

These exemptions are allowed to the extent that they reconcile the right to personal data protection with the rules governing the freedom of expression.

To such an end, article 11 (point 3) of the Law on Personal Data Protection implies that media organisations are obliged to have in place specific (compulsory) self-regulatory acts, such as codes of ethics/conducts, for purpose of defining and determining policies

and rules around processing activities for journalism purposes.

In the light of the above, the Commissioner has approved Instruction no. 9 and Instruction no. 31. These are mandatory sublegal acts that aim to define and clarify the perimeter of exemptions set out under article 11 of the law, as well as provide legal certainty for both controllers (media organisations/freelance journalists) and data subjects, in the ambit of processing activities for journalistic purposes.

II.1.1 Instruction no. 9

The scope of this instrument is to determine the rules on the processing of personal data by public and private media outlets (i.e., printed, visual and audiovisual media).

Instruction no. 9 emphasizes that the right to data protection should not appear as a secondary obstacle to the journalists' right to freedom of expression.

To this effect, media outlets should take care not to publish inaccurate, misleading or distorted information, including photographs (i.e., *accuracy principle*).

A journalist, apart from providing the essence of the information, should not provide news or photographs of people involved in events that harm the dignity of a citizen. The journalist also should not dwell on details of violence unless he/she considers it news or an image of public interest. The journalist must not take or produce images and photographs of people in a state of arrest without their consent, unless they are of significant public interest, or for justified justice and police purposes.

Media outlets should take into consideration the right of an individual to a private and family life, and to correspondence (including digital communication). No intrusion into a person's private life is allowed without the consent of that individual. Additionally, publication of photographs of individuals in private places without their consent is prohibited. Journalists may not force their way into someone's home, or take images from a private space.

While collecting personal/sensitive data, for journalistic purposes, journalists must evaluate – keeping in mind the rules on the protection of personal data – which information may violate the dignity and personality of the citizen, in order not to publish them. The publication should not contain extensive information unless it is in the public interest. In any case, the responsibility for achieving a balance between privacy and public interest falls on the journalist who publishes the data.

In addition to the general rules, Instruction no. 9 places specific attention on the processing of the personal data of minors, as well as criminal investigations, covert surveillance, health data, publication of photographs, public persons, and lists the circumstances that determine the public interest.

Minors

Minors, as the most vulnerable and least protected individuals, face a high risk of having their fundamental rights violated – including their right to privacy.

A minor under the age of 16 should not be interviewed or photographed for matters involving their own welfare or behaviour, or that of another child, unless the custodial parent gives consent. Pupils should not be photographed or interviewed at school without the permission of school authorities. Journalists should also not use the fame or position of a parent as an excuse to publish details of a minor's private life.

In order to protect the minor's personality, the journalist should not publish his or her name or provide details that could lead to their identification. The publication and dissemination of details, news or photographs to identify a minor involved in a crime, and/or as victims or witnesses of crimes, including sexual crimes, is prohibited. Especially, while reporting a sexual crime, the journalist may not publish the identification of the minor or imply a relationship between the perpetrator and the minor.

The minor's right to privacy, especially when dealing with a case of abuse, prevails always over any reporting/recording/broadcasting right. This applies even when the identity of the child becomes known from official sources or from sources close to his/her family.

The protection of minors from dissemination of identification data, and from the exposure of sexual life data (i.e., *sensitive data*), is essential and overrides freedom of the press. The latter can be exercised with the same effectiveness without reporting the name and surname, or other identification data of the minor.

Protection in criminal proceedings

When reporting a crime, relatives or friends of persons convicted or accused of a crime should not be identified without their consent.

Journalists are responsible for the complete, accurate and up-to-date information published (*accuracy principle*). In any case, the basic guarantees of the accused person must be respected before all suspicions of guilt until the final court decision (i.e. *presumption of innocence*).

On the other hand, journalists may report, when it is in the public interest, allegations that may come from a third party, even when it is difficult to support his/her claims, from police sources or a police procedure (i.e., arrest). The publication of journalistic materials under these circumstances should not identify the accused person.

Journalists must respect the accused or convicted person's private life, rights, property, health and correspondence.

It is crucial to respect the principle of presumption of innocence, which means that the publication of information on an ongoing criminal proceeding should be done without prejudice to the said principle.

Suspected, accused or convicted persons in principle enjoy a right to privacy, as per article 8 of the ECHR.

The identity of witnesses should not be disclosed, except when (i) these persons have previously given their consent, (ii) the identification of the witnesses is in the public interest, or (iii) the relevant testimony has previously been made public.

Covert surveillance

Instruction no. 9 in principle prohibits the processing of personal data – i.e., including publication of (journalistic) material – obtained through the use of hidden cameras or other covert listening devices, or from private or mobile phone calls, messages or emails, or through unauthorized receipt of documents or photographs that contain personal information.

The publication and/or dissemination – against the will of the interested party – of photographs captured by force by the police for documentation and investigation purposes should not be done without special conditions that fall under public interest perimeter.

On the other hand, even in the presence of a fact of public interest, the publication of data processed from telephone interceptions must respect the parameters of the essence of the information. Items of information containing strictly personal aspects, or related to the sexual sphere of an individual, should not be published. Journalists should not publish texts of messages and/or telephone discussions that concern the private life of the interested parties, their personal reports or professional interest.

Protection of health data

Restrictions on intrusions into private life are particularly important for journalistic publications whose subject are persons who are hospitalized in healthcare institutions. Health data are sensitive data and should not be published without obtaining the consent of the specific subject unless the patient is not identified and details that may lead to his/her identification are not described.

Journalists must respect the dignity and the right to privacy of the individual, especially in cases of serious illness, and thus avoid publishing unnecessary details.

Publication of photographs

During photographic documentation of a fact subject to a specific journalistic chronicle, the journalist/photographer must assess what type of focus should be chosen, avoiding focusing images only on individuals if the dissemination of these data (the images) does not prove to be related to, or exceeds, the purpose of the relevant journalistic chronicle.

Footage/image documenting the arrest of an individual may not be disseminated when it might harm the dignity of that individual. The reproduction of images of people in detention is prohibited, except when this falls under the perimeter of public interest.

Public persons

The private life of prominent or public figures, or those exercising public functions, should be respected. No data on their family members, friends, acquaintances or minors, should be published if the relevant news does not relate to the public life of such public persons.

Moreover, journalists may write about the general health situation/status of a public person without dwelling on the details of the relevant illness, especially in cases of serious diseases, thus avoiding publication of details that are strictly of a clinical nature and do not serve the purpose of the relevant journalistic chronicle/report.

Public interest

Instruction no. 9 does not provide a definition of the public interest. It only lists the circumstances in which a public interest might be inherent (chapter IX of the instruction). Such circumstances include, among others, national security, territorial integrity and public security, prevention of unrest or crimes, protection of health and morals, public prevention of fraudulent actions of individuals, protection of reputation/dignity or the rights of others, etc.

When processing personal data for journalistic purposes, a journalist should take into account the abovementioned circumstances while assessing whether the publication of an information falls under the public interest.

To such an end, the exemption criteria set out under Instruction no. 31 should help journalists to better consider whether the preparation and publication of a story is to be entirely relied on the public interest, or if there is a need to rely on a specific legal basis (i.e., consent, legitimate interest, etc.), in order to comply with data protection/privacy legislation.

II.1.2 Instruction no. 31

Unlike Instruction no. 9, which has a descriptive content – sometimes even a redundant one – Instruction no. 31 defines the basic criteria by which the processing of personal data for journalism purposes might be exempted from the application of the privacy principles (article 5), legal basis of processing (article 6), processing of sensitive data (article 7), international transfer of data (article 8), obligation for information of the data subject (article 18), as well as the obligation for notification of the processing activity (article 21).

This instrument sets out that the exemption requirements apply to all controllers/natural persons (i.e. freelance journalists) or legal entities (i.e., media organisations), which process personal data in the ambit of their journalistic activity.

In this view, the processing of personal data is exempted from the abovementioned data protection legal obligations if the controller (the media organisation/freelance journalist) fulfills the following cumulative criteria:

(i) The processing is carried out with a view to the publication of journalistic material for which the relevant personal data appear necessary;

(ii) Publication of the journalistic material is in the public interest; and

(iii) Compliance with the specific data protection obligation contradicts the intended journalistic purpose.

However, according to this instruction, the relevant media outlet should fulfill its data protection obligations if it is possible to achieve this without relying on the exemptions mentioned above.

This renders the exemption option a last resort option rather than a principal rule of personal data processing for journalistic purposes.

According to Instruction 31, the controller (in all cases), when relying on the abovementioned exemptions, should also comply with the following obligations:

(a) Personal data should be retained only for as long as they serve the journalistic purpose.

(b) Personal data should not be disseminated in other forms different to the journalistic material or different to receivers helping in its preparation.

(c) Personal data should not be (further) processed for other processing purposes that differ from the journalistic purpose.

(d) No direct or indirect identification information of minors should be contained in the prepared material, unless authorized by the relevant custodial parent/person, or the court.

(e) No identification information of a victim of/person claiming to have suffered from a criminal offence should be contained in the journalistic material unless the victim has given his/her consent to it, it is allowed by the court, or the victim is a public figure and the latter has suffered from the criminal offence due to his/her public function.

In addition, journalists should use effective means to hide the identity of the individuals mentioned under letter (d) and (e) above. In particular, the entire face of the individual and any relative or known close associate of him/her, if they appear in the same image with the concerned individual, or in a separate image that is published simultaneously, must be hidden or otherwise rendered unidentifiable.

II.2 How to understand/use the exemptions

The exemption criteria are cumulative and apply together. It should be noted that processing personal data "*with a view to publication of journalistic material*" does not necessarily mean that a story must be published in order for the publisher to benefit from the exemption rules. There might be cases when personal information is collected and archived for purpose of being used at a later stage for (identified) journalistic purposes.

Exemptions apply only to the processing of personal data for journalistic purposes. This is an imperative.

Therefore, a media organisation/freelance journalist that processes personal data for other purposes than journalistic ones (i.e. for administrative, human resources, or other economic purposes), cannot rely on the said exemptions.

This means that, for the field of personal data processing for non-journalistic purpose, the rules that apply to other (non-media) controllers (i.e., commercial companies, public institutions, etc.) apply to media organisations/freelance journalists as well.

In addition, as the journalistic exemption purpose appears to be a privilege of professional media organisations/freelance journalists, personal information gathered, analyzed and reported/broadcasted/published/etc., by the general public (via blogs/vlogs, social media accounts, etc.) – so-called citizens' journalism – can barely be justified under the exemption rules.

When relying on the journalistic exemption, it is important to carefully weigh the factors that lead the journalist to the reasonable conclusion that a specific journalistic material (of public interest) would be negatively affected in its essentials if the data protection obligations are complied with.

Hence, if there is no other way to account to the (prevalent) public interest than by disregarding data protection obligations, it is recommended that journalists keep records

of any discussions/reasoning and communications with senior editorial staff and/or the data protection officer of the relevant organisation on the subject matter, in order to prove their fair efforts to respect the data protection right of a certain subject of their journalistic material (i.e., a public person). The more intrusive and harmful a journalistic story is, the more formal and material attention from senior editorial staff is needed.

The justified avoidance of a certain obligation while preparing a journalistic story (i.e. publication of data without a legal basis) does not necessarily mean that other obligations are to be avoided, too (i.e. the principles of processing). Hence, exemption has to be carefully considered and evaluated in the light of the whole data protection legislation.

Considering that time is of paramount importance for journalistic works (which means an editorial consultation may not be possible), it would be advisable to have in place appropriate policies and codes of ethics/conducts (within a media organisation or at the industry level) that would help journalists to properly assess and decide on a case-by-case basis whether to rely on the journalistic exemption or to account to all, or only to specific, data protection/privacy obligations.

A general public interest in freedom of expression *per se* should be noted. However, the mere general justification of processing personal data for journalistic purposes is not necessarily sufficient to reconcile freedom of expression with the right to personal data protection/privacy.

Therefore, it is important to consider also the specific circumstances around each processing activity inherent to the preparation of a specific journalistic material – '*special public interest*'.

In this view, a thorough consideration of any pros or cons vis-à-vis a publication, in any specific circumstance, would help journalists to carry out a reasonable balance assessment between freedom of expression and data protection/privacy right.

Such factors include: the probability and severity of any harm to individuals (or other public interests); the status of the individual (i.e., private or public person); the nature of the information processed and its expected contribution to the public interest; and whether such information is already in the public domain (provided that such presence in the public domain is not in breach of personal data protection legislation).

Save for the above, it should be emphasized that some information/data do not fall under the applicability of the legislation on personal data. This legal exemption includes the processing of personal data of public official or public servants, which relates strictly to their public, administrative activity, or to affairs/matters related to their duties/tasks (article 4 (4) (b) of the Law on Personal Data Protection).

In addition, the personal information of deceased persons does not fall under the applicability of the legislation of personal data protection.

However, reasonable attention should be paid to the privacy features/elements of deceased persons which would affect the privacy of their family members, relatives, acquaintances, etc.

III. GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR is the legal instrument that governs the processing of personal data in the European Union. As a regulation, it is a binding legislative act that is directly applicable and enforceable in its entirety across the EU. It represents the most important piece of legislation for each Member State for guaranteeing data protection and the privacy rights of data subjects.

GDPR applies to controller/processors situated in the EU, as well as those situated outside the EU that fulfill one of the following conditions:

- ✓ They offer goods or services to data subject in the EU; or
- ✓ Monitor the behaviour of data subjects in the EU.

Though widely misunderstood, GDPR does not protect only the data protection/privacy rights of EU citizens but also those of non-EU citizens situated/residing in the EU.

In other words, if a controller, established/situated in Albania, monitors (i.e. interacts with or processes personal data unilaterally) the behaviours of a data subject situated/residing in the EU, that controller must comply with GDPR rules (*extraterritoriality principle*).

GDPR has repealed former Directive 95/46/EC, which the Albanian Law on Personal Data Protection[1] is fully aligned with, thus bringing data protection requirements to a considerably higher- quality level.

Some of the most important novelties of GDPR vis-à-vis Directive 95/46/EC (i.e. also: the Law on Personal Data Protection) include the following:

- ✓ Extraterritoriality principle (as explained above).
- ✓ Principle of accountability. This is the core principle of GDPR, according to which any controller should not only comply with GDPR provisions (i.e. principles of lawfulness, accuracy, minimization, storage limitation, etc.), but bear the burden of proof to demonstrate and evidence compliance therewith.
- ✓ Dedicated provisions/rules regarding the processing of personal data of minors (i.e. including criteria for consent).

[1] Albania has started the process of approximation of the national legislation with GDPR. To this effect, the Commissioner, in the ambit of a consultancy project of the EU Delegation, has prepared, circulated and published for public consultation the draft of the new law, which intends to achieve a full approximation of the national law with GDPR provisions. Currently, the draft is under review and evaluation process in the Ministry of Justice.

- ✓ Introduction of new categories of sensitive data (i.e. biometric and genetic data).
- ✓ Introduction of new categories of rights of data subjects (i.e. right to be forgotten and right to data portability).
- ✓ Augmentation of the requirements of information obligations of the controller (i.e. for data processed directly by data subjects and those processed through third parties).
- ✓ Introduction of principles of privacy by design and by default. These principles mean that any system of personal data processing should be designed to address any personal data protection issue (i.e. *data protection by design*), including encryptions/ pseudonymizations, and that these systems should be by default (i.e. automatically) data protection compliant/friendly and not process data more than is necessary to achieve the processing purpose (*data minimization principle*).
- ✓ Introduction of self-regulatory mechanisms, such as certification mechanism, codes of conduct and binding corporate rules that apply only to international transfer of personal data to countries without adequacy level.
- ✓ Introduction of the obligation to carry out a data protection impact assessment before any processing activity, and/or whenever it changes.
- ✓ Introduction of the obligations to keep records of data processing activities.
- ✓ Introduction of the mandatory role of the data protection officer.
- ✓ Tightening the rules for international transfers.
- ✓ Increase administrative sanctions up to a maximum of 20 million euros, or 4 per cent of the annual global turnover of a controller, whichever is higher.

As regards processing of personal data vis-à-vis freedom expression, article 85 (para. 1) of GDPR sets out that it is a responsibility of the Members States to reconcile the right to protection of personal data pursuant to GDPR with the right to freedom of expression and information, including the processing of personal data for journalistic purposes.

By delegating this task exclusively to the EU Member States, GDPR determines also the perimeter of exemption for journalistic purposes, within which the Member States would act in this regard. To such an end, article 85 (para. 1) mentions as eventual derogations, *inter alia*, the principles of processing (Chapter II), the rights of data subjects (Chapter III), relationship between controller and processor (Chapter IV), international transfer (Chapter V), etc.

In this view, GDPR does not contain specific provisions that regulate in detail the derogation of data protection provisions in favour of freedom of expression. It confers this exclusivity onto the Members States, which have embraced different approaches in this regard.

Below is illustrated a general review of the exemption/derogation legal framework in some EU member states:

Italy

Italy has incorporated some principles regarding journalistic exemption through a code of ethics, such as the exemption of the right to information of the data subject, as well as protection of sensitive data without consent. However, the journalist may not go beyond the essentials of the information published, provided that there is public interest in the publication itself. Italian legislation also provides for stringent rules on the processing of the personal data of minors, of people suffering serious or terminal disease, sexual life, etc.

Germany

German legislation exempts the controller from an obligation to erase personal data where erasure is impossible, or only possible with disproportionately high effort and where the data subject has a minor interest in erasure, or when it restricts the data subjects' rights based on certain requirements.

France

French legislation provides for the exemption of data processing for journalistic purposes from the obligations regarding information of data subject, rights of the data subject, retention and the processing of special categories of data (sensitive data), etc.

Spain

Spanish legislation lacks any specific provision that reconciles freedom of expression and data protection.

Sweden

Swedish law sets out that GDPR and the Data Protection Act (national law) shall not be applied to the extent that it breaches laws on freedom of expression. Therefore, GDPR provisions on, *inter alia*, data processing principles, lawful bases, rights of the data subject, international transfer of personal data, etc., are not applicable to the processing of personal data for journalistic purposes.

Special note: United Kingdom

UK legislation sets out that the processing of personal data is not bound by the obligations

of data protection legislation if the following cumulative criteria are met:

- the personal data are being processed with a view to the publication of journalistic material;
- the media outlet reasonably believes that publication would be in the public interest; and
- the media outlet reasonably believes that the application of data protection provisions are incompatible with its journalistic purpose.

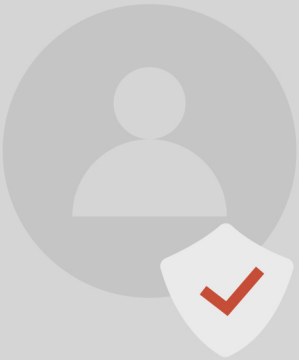
In any case, the public interest should be considered on case-by-case basis, in order to balance the public interest with the level of intrusion into the private life of an individual.

IV. CONCLUSION/KEY TAKEAWAYS

Below are listed some key advice that serves as a summary of important aspects about data protection compliance. It is crucial to keep the following points in mind:

- ✓ Publishing personal data constitutes data processing, so it is essential to ensure that you have the necessary permission or legal basis to disclose such data. Without a valid legal basis, it would be unlawful.
- ✓ If personal data is processed for the journalistic purposes (i.e. for serving the public interest), it may be exempted from certain provisions of the Law on Personal Data Protection and GDPR. Conversely, if personal data is collected, analyzed, or processed for other reasons, the provisions of Law on Personal Data Protection and GDPR will fully apply
- ✓ Publishing sensitive information can potentially harm an individual's private life. It is important to carefully evaluate whether the public interest justifies this harm. This involves balancing the interests at stake and considering the level of intrusion into the data subject's private life. Only when the public interest clearly outweighs privacy concerns can such information be published.
- ✓ Involving senior editorial staff or seeking expert input (i.e. from the organisation's data protection officer) can be beneficial in ensuring compliance data protection requirements. It is important to remember that journalists involved in the preparation of a story may not always be entirely objective when balancing the various interests involved.
- ✓ Collect only relevant data that is in the public interest for your journalistic work/ investigation. For example, if you are investigating a politician for possible corruption, discovering sensitive information about their sexual orientation, which is not relevant to the subject matter of investigation, might constitute a data protection breach. This principle aligns with the data minimization concept, a key element of the Law on Personal Data Protection and GDPR.
- ✓ In particularly contentious cases, when it's unclear if or to what extent the journalistic exemption applies to data processing, seeking consultation from the supervisory authority (i.e. the Commissioner) can provide clarity on data protection considerations.
- ✓ Special precautions must be taken when processing personal data that reveal sensitive data.
- ✓ Data concerning vulnerable persons, particularly minors, should only be processed if there are strong justifications, specific to the journalistic processing in question. It is crucial to ensure that such justifications exist before proceeding with any data processing.

- ✓ Always be able to demonstrate compliance with data protection legislation (*accountability principle*). To such an end, keep track of thoughts, discussions, comments exchanged with colleagues, senior editorial staff and the organisation's data protection officer, about efforts to reconcile the right to freedom of expression with that of data protection/privacy. Use checklists to such an end, and always keep yourself within the perimeter of tolerance and balance provided for under the codes of conduct and other ethics policies applicable to your organisation.


POLICY BRIEF:
Regulations on data protection and processing for media and journalists in Albania

June 2023