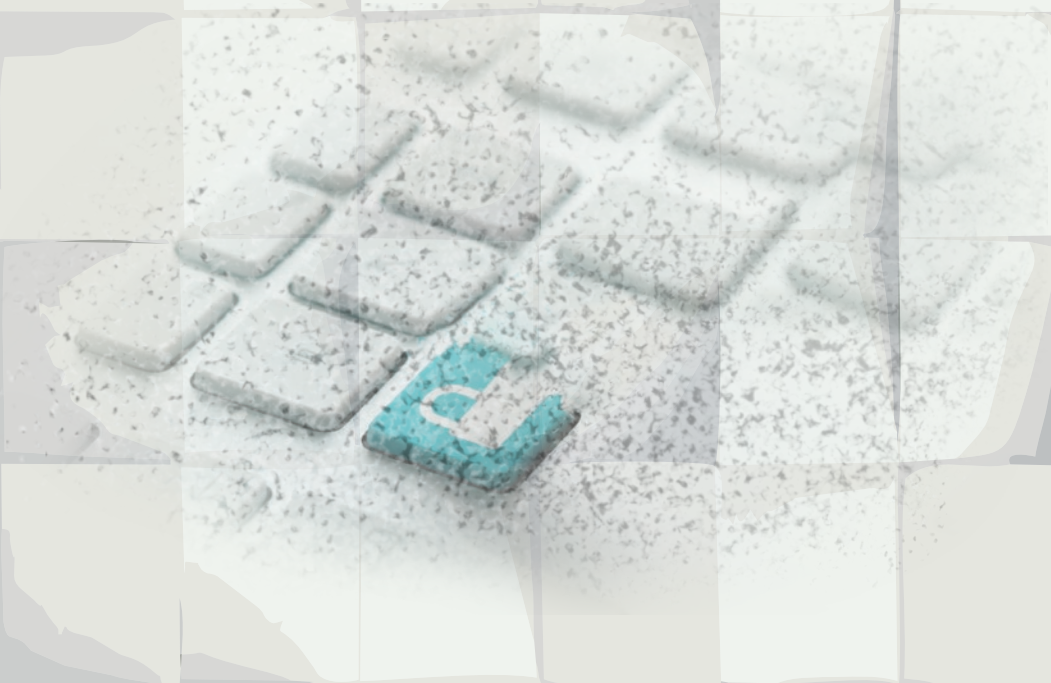
PERSONAL DATA PROTECTION AND THE MEDIA

Guidelines



Directorate for Personal Data Protection
This project is funded by the European Union

altair asesores
human dynamics public sector consulting
A project implemented by Altair Asesores SL and Hulla & Co Human Dynamics KG

PERSONAL DATA PROTECTION AND THE MEDIA

Guidelines

Data protection and the media

Publisher

Directorate for Personal Data Protection

Author

Nataša Pirc Musar, PhD

Translation

Congress Service Center - Office in Skopje

Design

Vlado Fidanoski

Printed by

Grafoservis

Edition

400 copies

This guidelines has been prepared within the project „Data Protection and the Media" EuropeAid/132633/C/SER/multi with reference number IPA TAIB 2012/9.11/LOT7/15 and specific contract number 12-6340/1, financed by the European Union through IPA TAIB 2012 programme and implemeted by Altair Asesores SL from Spain and its consortium partner Hulla & Co Human Dynamics KG from Austria. The contents of this publication are the sole responsibility of Altair Asesores SL and its consortium partners Hulla & Co Human Dynamics KG and can in no way be taken to reflect the views of the European Union.

Table of Contents

The purpose of these guidelines is to clarify the significance of personal data protection, as well as to answer, in a clear, comprehensive and useful way, frequently thought of questions relating to personal data protection and the responsibility of those who control personal data together with those who express their opinion in public and are mandated to provide information. Guidelines are specifically useful for journalists, media owners and individuals whose personal data is (ab)used by the media.

Introduction

The field of human rights and fundamental freedoms has seen an intense development since the 17th Century, whilst the notion has witnessed an expansion since the Second World War, in an era when various international organizations have endeavoured to uphold – through the adoption of legal statutes – various aspects of the rights of the individual. States have committed themselves to respect the rights of the individual in a way that authorities shall not unjustifiably encroach upon such rights as the right to life, freedom, privacy, and title to property. Further, the rights of the individual also need to be protected against encroachment by other individuals, and especially against impingement by organized concentrations of power, such as companies and organizations, including the media.

In Macedonia, the protection of human rights is provided at various judicial levels, by public authorities as well as by the criminal and civil justice system. Protection at the level of public authorities is provided principally by respecting and upholding the Constitution of the Republic of Macedonia as well as international agreements adopted globally by the United Nations (UN) as well as regionally, and in Europe particularly those prescribed by the Council of Europe. Legal protection under criminal law is provided by the state, which, in the public interest, imposes a range of sanctions for offences which are against the law; even attempts to commit an offence are penalized. Protection under civil law protects the interests of an individual and seeks to balance their personal interests with those of others. It considers the cause of the issue between parties as well as the culpability of those involved; penalties are predominantly of financial nature and sanctions dependent upon the consequences of the perpetrator's offence, namely on the damage caused or the benefits gained by the offence. The prohibition of actions is warranted only when it is still possible to prevent or ameliorate the damaging consequences of such actions.

Some General Issues in Relation to the Protection of Human Rights

Legal bases for the protection of human rights in the Republic of Macedonia

The protection of human rights is guaranteed in the Constitution of the Republic of Macedonia, where the individual rights and general rules pertaining to their protection are set forth. Among the international laws, ratified by the Republic of Macedonia, which are, in pursuance of Article 118 of the Constitution, part of the internal legal order, the following are of significance:

- UN treaties, namely: The Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights (both Official Gazette of the Socialist Federal Republic of Yugoslavia, No. 7/1971 – MP), whereas in the field of the protection of personal data, the UN General Assembly's 1990 Guidelines for Computerized Personal Data Files shall apply;
- among the European treaties, the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) is particularly important, also germane is the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data (ECPIAPPD - Treaty 108) as are various Council of Europe (CoE) Recommendations.

Individual rights and freedoms are described in a more general manner in the abovementioned treaties, conventions and statutes. Broad and unclear definitions can lead to certain doubts as to interpretation, since provisions tend merely to set forth certain guidelines as to the implementation of legal standards.

It is possible to prescribe a more exact manner of exercise and protection through the legal provision. Accordingly, Macedonia's parliament has adopted a more precise regulation through the adoption of various acts and statutes. Among such laws, the following are pertinent:

- Criminal Code, which defines individual criminal offences and prescribes penalties;
- Civil Code, which foresees general rules on damages as well as on unreasonable acquisition;
- Law on Personal Data Protection (LPDP), which determines what is defined as personal data, who can control such data, as well as the prevention of unlawful encroachment into the privacy and dignity of an individual in the processing of personal data;
- Law on Free Access to Information of Public Character regulates the conditions, manner and procedure of exercising the right to free access to information of

public character disposed by state administration bodies and other bodies and institutions established by law;

- Law on Media, which sets forth the rights, obligations and responsibilities of legal entities and individuals as well as public interest in the field of media. Critical situations that might be precipitated by a too broadly implemented right of expression are limited by a more precisely defined right to correction and reply to published information which is guaranteed to the affected party by Article 16 of the Constitution.

When deciding on individual cases, the application of rules is frequently supplemented by case-law. In such cases the jurisprudence of the European Court of Human Rights (ECtHR), which interprets the European Convention on Human Rights (ECHR), is of importance.

Right to privacy

A fundamental human right, the right to privacy is protected by Article 25 of Macedonia's Constitution which guarantees the respect and protection of the privacy of his/her personal and family life and of his/her dignity and repute. The notion of the right to privacy is broad and only defined in a general sense. Therefore, the jurisprudence (case-law) of the ECtHR and of the Macedonian's courts is important; namely, they examine each case separately, and try to define the scope of the right to privacy in the hearing of a given case. "Private life" is often defined as the right to that part of life which is not dedicated to the public, and to which third persons, as a rule, do not enjoy access. The meaning of this right is that every individual can live his or her life in accordance with his or her own wishes and is protected from the public eye. To a certain extent, the right to initiate contacts and develop relationships is usually added to the element of secrecy and intimacy, because only in such a way it is possible for a person to realize their own growth as well as the fulfilment of their own individual personality in accordance with their own wishes and is protected from the public eye.

We should also mention the limitation arising from Article 54 which provides that the human rights and fundamental freedoms provided by the Constitution may, exceptionally, be suspended or restricted during a war or state of emergency.

The provision of Article 8 of the ECHR is also important and its first paragraph states that everyone enjoys the right to respect of their private and family life, their home and correspondence; its second paragraph prescribes those circumstances when a public authority can interfere with the exercise of this right, namely:

- if such interference is in accordance with the law,
- and if it is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

According to the jurisprudence of the ECtHR, interference is in accordance with the law if it is based on a provision of domestic law which has certain qualities. The law must be "accessible to the persons concerned and foreseeable as to its effects".[1] A rule is foreseeable "if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct".[2] "The degree of precision required of 'the law' in this connection will depend on the particular subject-matter."[3]

In *Rotaru v. Romania*,[4] the ECtHR found a violation of Article 8 of the ECHR because Romanian law allowed for gathering, recording and archiving in secret files of information affecting national security without laying down limits on the exercise of those powers, which remained at the discretion of the authorities. For example, domestic law did not define the type of information that could be processed, the categories of people against whom surveillance measures could be taken, the circumstances in which such measures could be taken or the procedure to be followed. Because of these deficiencies, the Court concluded that domestic law did not comply with the requirement of foreseeability under Article 8 of the ECHR and that this Article had been violated.

Another example: In *Taylor-Sabori v. the United Kingdom*,[5] the applicant had been the target of surveillance by the police. Using a 'clone' of the applicant's pager, the police could intercept messages sent to him. The applicant was then arrested and charged with conspiracy to supply a controlled drug. Part of the prosecution's case against him consisted of the contemporaneous written notes of the pager messages which had been transcribed by the police. However, at the time of the applicant's trial, there was no provision in British law governing the interception of communications transmitted via a private telecommunications system. The interference with his rights had therefore not been "in accordance with the law". The ECtHR concluded that there had been a violation of Article 8 of the ECHR.

The ECtHR has stated that "the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued".[6]

In *Khelili v. Switzerland*,[7] during a police check the police found the applicant to be carrying calling cards which read: "Nice, pretty woman, late thirties, would like to meet a man to have a drink together or go out from time to time. Tel. no. [...]". The applicant alleged that,

[1] ECtHR, Amann v. Switzerland [GC], No. 27798/95, 16 February 2000, para. 50; see also ECtHR, Kopp v. Switzerland, No. 23224/94, 25 March 1998, para. 55 and ECtHR, Iordachi and Others v. Moldova, No. 25198/02, 10 February 2009, para. 50.

[2] ECtHR, Amann v. Switzerland [GC], No. 27798/95, 16 February 2000, para. 56; see also ECtHR, Malone v. the United Kingdom, No. 8691/79, 2 August 1984, para. 66; ECtHR, Silver and Others v. the United Kingdom, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 March 1983, para. 88.

[3] ECtHR, The Sunday Times v. the United Kingdom, No. 6538/74, 26 April 1979, para. 49; see also ECtHR, Silver and Others v. the United Kingdom, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 March 1983, para. 88.

[4] ECtHR, Rotaru v. Romania [GC], No. 28341/95, 4 May 2000, para. 57; see also ECtHR, Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, No. 62540/00, 28 June 2007; ECtHR, Shimovolos v. Russia, No. 30194/09, 21 June 2011; and ECtHR, Vetter v. France, No. 59842/00, 31 May 2005.

[5] ECtHR, Taylor-Sabori v. the United Kingdom, No. 47114/99, 22 October 2002.

[6] ECtHR, Leander v. Sweden, No. 9248/81, 26 March 1987, para. 58.

[7] ECtHR, Khelili v. Switzerland, No. 16188/07, 18 October 2011.

following that discovery, the police entered her name in their records as a prostitute, an occupation which she consistently denied. The applicant requested that the word 'prostitute' be deleted from the police computer records. The ECtHR acknowledged in principle that retaining an individual's personal data, because that person might commit another offence, might under certain circumstances be proportionate. However, in the applicant's case, the allegation of unlawful prostitution appeared too vague and general, was not supported by concrete facts since she had never been convicted of unlawful prostitution and could therefore not be considered to meet a 'pressing social need' within the meaning of Article 8 of the ECHR. Regarding it as a matter for the authorities to prove the accuracy of the data stored on the applicant, and to the seriousness of the interference with the applicant's rights, the Court ruled that retention of the word 'prostitute' in the police files for years had not been necessary in a democratic society. The Court concluded that there had been a violation of Article 8 of the ECHR.

In *Leander v. Sweden*,[8] the ECtHR ruled that secret scrutiny of persons applying for employment in posts of importance for national security was not contrary to the requirement of being necessary in a democratic society. The special safeguards laid down in national law for protecting the interests of the data subject – for example, controls exercised by parliament and the Chancellor of Justice – resulted in the ECtHR's conclusion that the Swedish personnel control system met the requirements of Article 8 (2) of the ECHR. Having regard to the wide margin of appreciation available to it, the respondent state was entitled to consider that in the applicant's case the interests of national security prevailed over the individual ones. The Court concluded that there had not been a violation of Article 8 of the ECHR.

In the case of *Rubio Dosamantes v. Spain*, the ECtHR held that there had been a violation of the right to respect for private life. The applicant, Paulina Rubio Dosamantes, is a pop singer who is very well known in Spain. She complained that her honour, reputation and private life had been harmed by remarks made by the media. The ECtHR noted that in various television programmes, frivolous comments had been expressed about certain aspects of Ms Rubio's private life. Those comments concerned mainly her sexual orientation or her allegedly stormy relationship with her partner, including the claim that she had humiliated him and encouraged him to take drugs. In the Court's opinion, it was clear that the guests on the programme only mentioned and discussed the singer's private life, focussing on details that were lewd.

The ECtHR found that the applicant's fame as a singer did not mean that her activities or conduct in her private life should be regarded as necessarily falling within the public interest. The Court also noted that actual or supposed tolerance of an individual regarding publications relating to her private life does not necessarily deprive her of the right to protection of privacy. The fact that she could have benefitted from media attention did not authorise TV channels to broadcast unchecked comments about her private life. The public had no legitimate interest in knowing certain intimate details about her private life. Even assuming that there had been a public interest, in parallel to the commercial interest of the

[8] ECtHR, Leander v. Sweden, No. 9248/81, 26 March 1987, paras. 59 and 67.

television channels in broadcasting the programmes, the Court found that those interests were trumped by a person's individual right to the effective protection of his or her privacy. The ECtHR also referred to the judgment *Editions Plon v. France*[9] when it reiterated that certain events of private and family life were given particularly careful protection under Article 8 of the ECHR, meaning that journalists had to show prudence and precaution when talking about them. Thus, the spreading of unverified rumours or the limitless broadcasting of random comments on any possible aspect of a person's daily life could not be seen as harmless. The national authorities should have assessed the TV programmes in question, to distinguish between and to weigh in the balance those matters which were intimately part of Ms Rubio's private life and those which might have had a legitimate public interest.

Other precedents in this area are the judgments by the ECtHR in the three cases of *von Hannover v. Germany*. In the first case *von Hannover v. Germany (no. 1)*,[10] Princess Caroline von Hannover had applied to the German courts for an injunction preventing any further publication of two series of photographs relating to her private life in which she appeared with her children in German magazines, because they infringed her right to protection of her private life and of her own image. The photographs were the subject of three sets of proceedings before the German courts, resulting in particular in a landmark judgment delivered by the Federal Court of Justice in 1995 which granted Princess Caroline of Monaco an injunction restraining the publication of photographs. It did so because the children's need for protection of their intimacy was greater than that of adults. However, the German Constitutional Court in 1999 ruled that there was no breach of privacy as Princess of Hannover was undeniably a public figure, specifically a "figure of contemporary society *par excellence*" and had to tolerate the publication of photographs of herself in a public place, even if they showed her in scenes from her daily life rather than engaged in her official duties. The Court referred in that connection to the freedom of the press and to the public's legitimate interest in knowing how such a person generally behaved in public.

The Princess, the applicant, alleged before the ECtHR that those decisions had infringed her right to respect for her private life as they had failed to afford her adequate protection from the publication of photographs taken without her knowledge by paparazzi on the ground that, in view of her origins, she was a figure of contemporary society *par excellence*.

The ECtHR held that there had been a violation of Article 8 of the ECHR (right to respect for private life), finding that the German courts had not, in the present case, struck a fair balance between the interests at stake. It observed that, while the general public might have a right to information, including, in special circumstances, on the private life of public figures, they did not have such a right in this instance. The ECtHR considered that the general public did not have a legitimate interest in knowing the applicant's whereabouts or how she behaved generally in her private life even if she appeared in places that could not always be described as secluded and even if she was well known to the public. Even if such a public

[9] ECtHR, Editions Plon v. France, No. 58148/00, 18 May 2004, para. 47 and 53.
[10] ECtHR, von Hannover v. Germany, No. 59320/00, 24 June 2004.

interest existed, just as there existed a commercial interest for the magazines to publish the photographs and articles, those interests had, in the Court's view, to yield to the applicant's right to the effective protection of her private life. Hence, everyone, including people known to the public, had to have a "legitimate expectation" that his or her private life would be protected. In the ECtHR's view, the criteria that had been established by the domestic courts for distinguishing a figure of contemporary society *par excellence* from a relatively public figure were not sufficient to ensure the effective protection of the applicant's private life and she should, in the circumstances of the case, have had a "legitimate expectation" that her private life would be protected.

In *von Hannover v. Germany (no. 2)*[11] the applicants, Princess Caroline von Hannover and her husband Prince Ernst August von Hannover, complained of the German courts' refusal to prohibit any further publication of two photographs which had been taken during their holiday without their knowledge and which had appeared in two German magazines. They alleged that the domestic courts had not taken sufficient account of the ECtHR's 2004 judgment in von Hannover v. Germany (see above).

The ECtHR held that there had been no violation of Article 8 of the Convention, noting that the German courts had carefully balanced the right of the publishing companies to freedom of expression against the right of the applicants to respect for their private life. In doing so, they had attached fundamental importance to the question whether the photographs, considered in the light of the accompanying articles, had contributed to a debate of general interest. They had also examined the circumstances in which the photographs had been taken. The Federal Court of Justice had changed its approach following the first ECtHR's von Hannover judgment in 2004 (see above), while the Federal Constitutional Court, for its part, had not only confirmed that approach, but had also undertaken a detailed analysis of the ECtHR's case-law in response to the applicants' complaints that the Federal Court of Justice had disregarded the ECHR and the ECtHR's case-law. In those circumstances, and having regard to the margin of appreciation enjoyed by the national courts when balancing competing interests, the Court concluded that the latter had not failed to comply with their positive obligations under Article 8 of the ECHR in the present case.

The *von Hannover v. Germany (no. 3)*[12] case concerned a complaint lodged by the Princess Caroline relating to the refusal of the German courts to grant an injunction prohibiting any further publication of a photograph of her and her husband taken without their knowledge while they were on holiday. The photograph was accompanied by an article about the trend amongst the very wealthy towards letting out their holiday homes. The article went on to describe in detail the von Hannover family villa, located on an island off the Kenyan coast, setting out the furnishings, daily rental cost and holiday pastimes in the area. The article featured alongside several photographs of the villa, as well as one photograph showing Princess Caroline and her husband on holiday in an unidentifiable location ("the photograph"). The photograph had been taken without their knowledge, but they were in the

[11] ECtHR, von Hannover v. Germany, Nos. 40660/08 and 60641/08, 7 February 2012.
[12] ECtHR, von Hannover v. Germany, No. 8772/10, 19 September 2013.

company of other persons and it disclosed no information about the location or how they were spending their holidays.

The Princess complained and succeeded at first instance and on her first visit to the Federal Court of Justice, only to fail in the Constitutional Court, on her second visit to the Federal Court in 2008, the Federal Court of Justice dismissed the applicant's appeal on points of law. It did so because the applicant was a public figure and that, while the photograph did not relate to a subject of general interest, the publisher's freedom of expression should not be overridden by the applicant's right to respect for private life. The report was capable of stimulating discussion on a matter of general interest and could therefore legitimately be accompanied by the photograph. The Federal Constitutional Court declined to consider a further appeal lodged by the applicant.

The ECtHR held that there had been no violation of Article 8 of the ECHR, finding that the German courts had taken into consideration the essential criteria and the ECtHR's case-law in balancing the different interests at stake in the case. Having regard to the margin of appreciation enjoyed by the national courts when balancing competing interests, Germany had not failed to comply with its positive obligations under Article 8.

The German courts, the ECtHR noted, had taken the view that the purpose of the article was to relay the trend among celebrities of renting their holiday homes. This could generate reactions and a dialogue among readers, thereby contributing to a debate of general interest. The ECtHR added that the article gave practically no details relating to the private life of the applicant and husband, but rather focused mainly on the characteristics of the von Hannover villa. It could not, consequently, be claimed that the article was a mere pretext for publishing the photograph and that the link between the two was purely artificial. The ECtHR therefore could accept that the photograph in question, considering the accompanying article, did contribute, at least to some degree, to a debate of general interest.

This decision is consistent with the ECtHR's earlier decision in *von Hannover (no. 2)* insofar as it affirms that where the balancing exercise has been undertaken by the national authorities in conformity with the criteria laid down in the ECtHR's case-law, the Court will require strong reasons to substitute its view for that of the domestic courts. The ECtHR cited as an example a situation where the link between the article and photograph in question would be considered purely arbitrary and artificial.

Where the decision appears to part company with *von Hannover (no. 2)*, however, is in the lack of any need for a link between the subject-matter of the photograph and the article it illustrates. The photograph of the applicant on holiday, considering the article, was found to contribute to a debate of general interest, not because it supported and illustrated the information conveyed, as in *von Hannover (no. 2)*, but because it could not be said that the article was a mere pretext for publishing the photograph.

Right to the protection of personal data

The right to data protection developed out of the right to respect for private life. The concept of private life relates to human beings. Natural persons are, therefore, the primary beneficiaries of data protection. According to the Opinion of the Article 29 Working Party, furthermore, only a living being is protected under the European data protection law.[13]

The ECtHR's jurisprudence concerning Article 8 of the ECHR shows that it may be difficult to separate matters of private and professional life.[14] In Amann v. Switzerland,[15] authorities intercepted a business-related telephone call to the applicant. Based on that call, the authorities investigated the applicant and filled in a card on the applicant for the national security card index. Although the interception concerned a business-related telephone call, the ECtHR considered the storing of data about this call as relating to the private life of the applicant. It pointed out that the term 'private life' must not be interpreted restrictively since respect for private life comprised the right to establish and develop relationships with other human beings. Furthermore, there was no reason of principle to justify excluding activities of a professional or business nature from the notion of 'private life'. Such a broad interpretation corresponded to that of CoE Convention 108. The ECtHR further found that the interference in the applicant's case had not been in accordance with the law since domestic law did not contain specific and detailed provisions on the gathering, recording and storing of information. It thus concluded that there had been a violation of Article 8 of the ECHR.

The right to privacy also extends to data relating to the person. Such rights have developed in relation to the emergence and development of information technology, which has enabled automated data processing. The rapid evolution of technology and unbridled data processing have jeopardized the individual's right to privacy; indeed, this right to privacy in relation to data which pertains solely to them is becoming even more susceptible. The right to protection of personal data is often described as one of the aspects of the right to privacy; namely, the individual's information privacy. Such is also encompassed in Article 8 of the ECHR, as a part of the right of privacy which enables a person to withhold all information about themselves, and proscribes other persons from becoming acquainted with such information. The Constitution of the Republic of Macedonia defines the protection of personal data as a special right; Article 18 states:

The security and confidentiality of personal information are guaranteed. Citizens are guaranteed protection from any violation of their personal integrity deriving from the registration of personal information through data processing.

The protection of personal information is guaranteed to a citizen but not to a legal entity. The citizen is protected against interference from the state and other public sector bod-

[13] Article 29 Working Party (2007), Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007, p. 22.
[14] See, for example: ECtHR, Rotaru v. Romania [GC], No. 28341/95, 4 May 2000, para. 43; ECtHR, Niemietz v. Germany, 13710/88, 16 December 1992, para. 29.
[15] ECtHR, Amann v. Switzerland [GC], No. 27798/95, 16 February 2000, para. 65.

ies and authorities, against commercial companies and other entities in the private sector; citizens also enjoy protection against interference from other individuals based on private or public sector personal data collections. Personal data is namely any data relating to an individual, irrespective of the form in which it is expressed.

In the same manner, as for the protection of human rights in general, protection under both criminal and civil law is also guaranteed for the protection of personal data. However, in the case of the protection of personal data not collected by an individual, the law also foresees administrative supervision, because it crucially pertains to the issue of human rights, although many are not sufficiently aware of this. Macedonia's Law on Personal Data Protection foresees the protection by the Directorate for Personal Data Protection (DPDP) that helps to protect the data through the reaction on individual incidents; furthermore, and at its own initiative, the DPDP can also exercise supervision over the collection and processing of personal data, as well as instigate penalties for any offences as stated and foreseen by law.

LPDP is the most comprehensive piece of legislation encompassing the principles and general provisions, as well as the rules, on processing of personal data; it also determines the rights of individuals, the institutional protection of personal data, the export of personal data and various field-specific regulations. The LPDP, however, is not the only legislation governing the realm of personal data protection; there is also a series of special statutes protecting personal data in various specific areas, such as medical records and criminal records.

The right to personal data protection is often described as one of the aspects of the right to privacy; namely, the individual's information privacy. The protection of personal information is guaranteed to a natural person but not to a legal person. The individual data subject is protected against interference from the state, other public sector bodies and authorities, against commercial companies and other privately owned legal entities. Personal data is namely any data relating to an individual, irrespective of the form in which it is expressed.

Right to freedom of expression and information

The right to freedom of expression is multifaceted and encompasses, besides the right to disseminate information, the right to receive opinions and information. Freedom of expression is one of the fundamental preconditions for the functioning of a democracy, especially in dissemination of information and the consequent enabling of formation of opinions. Freedom of expression is one of prerequisites for the self-fulfilment of everyone and their autonomy in decision making, whereas at the same time it enables them becoming informed on public matters. The transmission and receipt of information and opinions is thus protected by the Constitution.

Article 16 of the Constitution of RM guarantees the freedom of personal conviction, conscience, thought and public expression of thought, as well as the freedom of speech, public address, public information and the establishment of institutions for public information. The word 'expression' shall be interpreted broadly, in the aspect that it does not merely refer

to the spoken word, but also to images, radio and television broadcasting, electronic media as well as other forms of articulation and action which may express a certain idea (e.g. the way a person dresses). Every person may freely choose, receive and disseminate news and opinions. Such not only encompass ascertainable data regarding facts, but also opinions, critique and speculations; moreover, the notion not only embraces the information and ideas which have been accepted or approved, but also those which are insulting, shocking and disturbing. According to the Constitution of RM, everyone shall also be allowed access to information which is of a public nature.

Article 10 of the ECHR also defines the right to freedom of expression. This right shall include freedom to hold opinions and, regardless of frontiers, to receive and impart information and ideas without interference by public authorities. The Convention also expressly mentions operators in the field of broadcasting, namely radio, television and cinema, whereby it expressly allows states to impose licensing and restrictions as to the exercise of such rights.

All of these liberties, of course, do not mean that the right to freedom of information and expression are absolute and unrestricted. The rights of the media are governed through the necessity to maintain an appropriate balance of interests, and are thus also restricted by law. Article 54 of the Constitution of RM provides that certain human rights and fundamental freedoms may exceptionally be temporarily suspended or restricted during times of war or a state of emergency.

The second paragraph of Article 10 of the ECHR defines those restrictions more broadly and in more detail than it does for the right of privacy; namely: the exercise of these freedoms - since this comes with duties and responsibilities - may be subject to formalities, conditions, restrictions or penalties prescribed by law; these are deemed necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. The case-law of the ECtHR grants states considerable autonomy and leeway in the balancing of proportionality in relation to any assessment as to which legal restrictions may be necessary in maintaining their own (moral) environment.

Where as the ECtHR has not yet explicitly expressed that the state is obliged to provide appropriate information to everyone,[16] Article 16 of the Constitution of RM provides that free access to information and the freedom of reception and transmission of information are guaranteed.

The right to freedom of expression is multifaceted and encompasses, besides the right to disseminate information, the right to receive opinions and information. The word '*expres-*

[16] Note that several judgements have already indicated that this might happen very soon; see the latest Magyar Helsinki Bizottsag v. Hungary, nr. 18030/11, Judgement of 8 November 2016.

sion' shall be interpreted broadly, in the sense that it does not merely refer to the spoken word, but also to images, radio and television broadcasting, electronic media as well as other forms of articulation and action which may express a certain idea (e.g. the way a person dresses). This right includes freedom to hold opinions and, regardless of frontiers, to receive and impart information and ideas without interference by public authorities. Nevertheless, the rights of the media are governed through the necessity to maintain an appropriate balance of interests, and are thus also restricted by law.

Conflicts of interest in the exercise of individual's human rights

The human rights of the individual may be thought of as a free balloon, meaning that each has its own space, content and trajectory; the paths of such balloons may cross in the air; however, if they collide, the body of one may not impinge upon the space of another. The task of the state, as the legislator, is to create a legal order which balances their paths and, within reasonable scope, restricts them. When it comes to more serious conflicts between the rights of individuals, the state should further prevent collisions through appropriate legal means and offer legal protection to the affected party.

Conflict between the right of privacy and the right to protection of personal data on one side, and the right to freedom of expression and information on the other, is frequent. It occurs between individuals, and even more frequently between individuals and the media. The right and the duty of the state is to restrict the right of media when it excessively impinges upon the right of privacy and the protection of personal data. This restriction of rights shall be limited within reason and with consideration of values, whereby the individual should endure certain interferences which cannot be reasonably avoided; namely, individuals may, to a certain extent, be called upon to sacrifice their own rights for those in the common public interest.

The ECtHR, which often decides upon restrictions as to the right to free expression and information, must first - pursuant to Article 10 of the ECHR - assess whether the restriction is set forth by law and whether it is necessary in a democratic society. The expression 'set forth by law' shall not mean that it should only be assessed in a formal way, but requires that it is concordant with the *acquis communautaire*. Three elements should be fulfilled in the process of such conceptual assessment. The first of these requires that the rules of law are accessible and known, namely that citizens have access to information which sufficiently clarifies which rule applies in a certain instance. The second element requires the predictability of same, which means that the rules of law must be formulated precisely enough for an individual to behave in compliance with them. The third element pertains to the legitimacy of the objective which a legal ruling should achieve. The authority of the state shall not be unlimited, and hence the scope and the mode of the exercise of powers shall be determined in a way that an individual is granted appropriate protection against arbitrariness.

When the ECtHR establishes that a restriction is set forth by law, it also assesses whether the intervention is necessary in a democratic society. In this process, the tension between the interests of an individual and the interests of society is brought to the fore, and ECtHR admits that each individual country is best familiar with the circumstances in their own society, and it hence allows a certain degree of discretion to the country in question (the so-called 'wide margin of appreciation'). Nevertheless, the ECtHR reserves the right to supervise the exercise of discretionary power in a signatory state, especially concerning the states' reasoning and considered circumstances. Therefore, in a democratic society, the terms of any necessary restriction must derive from and pertain to one of the restrictions which are clarified in a sufficiently general way in the respective second paragraph of Article 10 of the ECHR (e.g. for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others etc.). The expression: 'necessary' is not interpreted as a synonym for 'indispensable' by the ECtHR, but it rather interprets it more broadly, as a synonym for acceptable, common, beneficial, reasonable or appropriate (required by a 'pressing social need').

The right and the duty of the state is to restrict the right of the media when it excessively impinges upon the right of privacy and the protection of personal data.

This restriction of rights shall be limited within reason and with consideration of values, whereby the individual should endure certain interferences which cannot be reasonably avoided; namely, individuals may, to a certain extent, be called upon to sacrifice their own rights for those in the common public interest.

The media are often confronted with a difficult task of performing a balancing test – balance privacy rights of individuals and the public's right to know.

Questions pertaining to the Right to Privacy and Personal Data and the Right to Freedom of Expression

The media may generally publish any personal data which they receive pursuant to Law on API, however, the purpose limitation principle applies to the use of such data. What personal data is communicated to the media, is the sole responsibility of the competent public sector body.

Do the same standards for limitations of the right to freedom of expression and information apply for everyone?

No, the standards may differ according to the subject concerned. A difference needs to be made between the relation of media towards the state and towards an individual. The state holds a superior position; it thus has fewer rights and can impose fewer restrictions on media which is on a democratic mission of critical supervision in the society – the media is the so-called 'public watchdog'. However, interests of the state also bring restrictions, i.e. measures set forth in the legislation and which are necessary in a democratic society in support

of national security, fight against terrorism, to prevent turmoil or crime, to protect public health, safety or morale, or to protect authority and impartial judicial administration. In case of protection of an individual, the rights of media are far more limited. However, neither the right to privacy nor the right to information has any precedence since they are both equally important. In protection of an individual the difference is made between the protection of an 'ordinary' citizen or a public figure. The requirement for respecting privacy is reduced for as much as the individual himself willingly enters public life or has control or authority over other protected interests. In principle, data on public figures (especially politicians and public function holders) may be published without express consent of the person involved in case there is a strong public interest present. Case law distinguishes between absolute and relative persons of the contemporary life. The first group includes persons who are always under the scrutiny of public eye due to the importance and reach of their role and function in the society (e.g. politicians, public function holders, performing and other artists, professional sportspersons, etc.). Relative persons of the contemporary life are those persons who only temporarily or partially influence the public interest due to their connection with a certain event, role or function (e.g. winners of different competitions or events, lottery winners, serious crime offenders, public officials and such). Data on relative public persons may be published only in case such data is relevant for the public in the context of the event, role or function and in a limited relevant time frame thereof. The afore mentioned also applies for publication related to a criminal offence or facts which have occurred long time ago since in such outdated events there is no public interest. Sensationalism and tasteless quoting of useless information is not allowed neither for absolute nor for relative public figures in order not to encroach upon their right to privacy and not to interfere with their entirely private life. This was decided by the ECtHR which gives the states a substantial amount of freedom to decide pursuant to circumstances and criteria established in a society. However, the European standard dictates that private and family life must be protected also in the case of the so-called public figures. In the case of Von Hannover v. Germany (No. 2),[17] the applicant – the Princess Caroline of Hanover and Monaco was not a politician but a member of an established royal family who participated in cultural and charity events. Newspapers published her photos which were private and showed scenes from her everyday life, private visits to restaurants, her sports engagements, on strolls and holidays. The ECtHR expressed its conviction that in competition of interests of an individual and public, narrower interpretation needs to be applied in such cases and thus protect the right to privacy. Although public figures are exposed to public, reports on their private life which are in no connection to their public presence and have no relevance for the public interest are not allowed.

The requirement for respecting privacy is reduced for as much as the individual himself enters public life or has contact with other protected interests. Sensationalism and tasteless quoting of useless information is not allowed neither for absolute nor for relative public figures in order not to encroach upon their right to privacy and not to interfere with their entirely private life.

[17] ECtHR, Von Hannover v. Germany, Nos. 40660/08 and 60641/08, 7 February 2012.

How is the media obliged to report?

The right and obligation of media in informing the public depends on their authenticity and relevance. People have a right to be informed accurately. Although the speed of information is important in the media, the information may only be useful if we can believe it. This does not mean that only objective facts should be published; however, published facts need to be appropriately checked, information carrier needs to satisfy the obligation of truth. Accuracy check of collected information – prescribed in more detail in the Code of Journalists – is not always necessary. Exception to the afore mentioned is when a journalist receives certain data from the state authority, e.g. at the press conference. In such case, it is presumed that the information is checked and in the event when the information is incorrect or the protection of privacy is violated, the journalist is not held responsible but the state authority conveying such information. The situation is different in the instance of expressing an opinion or comment where strong subjective component is involved and it is hard to establish whether it is genuine or not. The right to express one's own opinion is wider than the right to information and an individual has a right to express his/her opinion, even if such opinions shock and disturb. However, limits exist also in this area. An opinion must not be offensive towards an individual. Each person should lead a discussion in a manner fit for a civilised society and in line with good manners and behaviour. Offensive discussion is not worth being protected since it is unproductive. However, a discussion may be emotional, in particularly as a response to a challenge. There is less tolerance in political discussions and a non-democratic tone which leads to discrimination and violence cannot be supported. A political debate needs to be objective, cultured and needs to respect human dignity.

The freedom of expression is thus limited, however, the more it proves to be important for the public interest, fewer restrictions apply (this also in the case of conveying facts and opinions). Adverse opinions interesting only to an individual and not the entire public, which serve pure entertainment, contentment or pure curiosity, are not allowed. Therefore, the media may publish news and opinions carefully checked and holding an objective public interest even if they encroach upon individual's privacy. More these news and opinions encroach upon the right to privacy, less space the media has for publishing it. "There is a wide difference between what is interesting to the public and what is in the public interest to make known" – keep in mind this quote from the decision of the UK Information tribunal in Guardian Newspaper Ltd and Heather Brooke v The Information Commissioner and BBC of 8 January 2007 (nr. EA/2006/0011 and 0013) as the lead mantra.

The right and obligation of media in informing the public depends on their authenticity. People have a right to be informed accurately. The media may publish news and opinions carefully checked and holding an objective interest even if they encroach upon individual's privacy. The more these news and opinions encroach upon the right to privacy, the less space the media has for publishing it.

The competencies of the Directorate for Personal Data Protection

The supervisory authority in the field of data protection is The Directorate for Personal Data Protection (DPDP). It is managed by a Director who is appointed and dismissed by the Assembly of the Republic of Macedonia upon the proposal of the Commission for Election and Appointment Matters of the Assembly of the Republic of Macedonia, through an open announcement, for a period of five years.

Competencies of DPDP are the following (Art. 41 Para. 1 of LPDP):

- prepare and adopt by-laws referring to personal data protection,
- develop policies and give directions related to personal data protection,
- perform inspection supervision in accordance with the provisions of this Law,
- asses the equitability and legality of the personal data processing,
- keep a Central Register,
- issue prior approval for personal data processing in accordance with the provi sions of this Law,
- issue prohibition to the controller for further processing of the personal data,
- issue an approval for personal data transfer in other countries,
- give opinion on the draft regulations in the field of personal data protection,
- give opinion on drafts codes of conduct referring to the personal data protection,
- conduct misdemeanour procedure through the Commission for deciding on a proposal, in accordance with law,
- act upon the requests of the supervision bodies in the field of personal data protection of other countries, related to the performance of their activities on the territory of the Republic of Macedonia,
- perform training for the interested controllers, i.e. processors,
- achieve international cooperation in the field of personal data protection and participate in the work of the international organizations and institutions for personal data protection and
- perform other activities determined by law.

Inspection supervision over the implementation of LPDP and the regulations adopted on the basis of this Law, are performed by the DPDP via the inspectors for personal data protection (hereinafter: inspectors). The inspection supervision may be on a regular basis, an irregular basis and as control type. Regular inspection supervision is performed according to annual program adopted by the director of the DPDP. Irregular inspection supervision is conducted based on initiatives submitted by a state administration body, legal entity or natural persons, as well as in the case when the inspector considers there is a violation of LPDP. The control inspection supervision is conducted upon the expiration of the deadline stipulated within the determination for removal of the stipulated deficiencies.

The inspectors have strong competencies within the supervision procedure – pursuant to Art. 44.c of the LPDP they may:

- enter any premises where personal data are being processed and conduct an inquiry in their processing;
- request for written or oral explanation and call and interrogate persons regarding the personal data processing;
- request for an inquiry in the documentations and any other data regarding the personal data processing;
- examine the equipment for personal data processing and the equipment where the personal data are being preserved, with an authorized representative of the controller, i.e. processor;
- use technical equipment intended for taking photographs;
- request to prepare an expert analysis and opinion related to the conducted inspection supervision and
- use the communication devices of the controller, i.e. processor due to meeting the goals of the same.
- Pursuant to Art. 45 Para. 3 the supervision procedure may result in the inspector's decision for removal of the determined violations, thereby stipulating:
- completion, update, correction, revealing or provision of personal data secrecy;
- implementation of additional measures for personal data protection and organizational measures for securing secrecy and protection during the personal data processing;
- prohibition for further personal data processing;
- freezing of the personal data transfer in other countries;
- provision of data and their transfer to other entities,
- block, deletion or annihilation of the personal data,
- deassembly, transfer or removal of equipment, devices, installations and systems used for data processing,
- deadline for adoption of the regulations in accordance with the provisions of this Law, and
- deadline for violation removal.

The same competences apply for the media when processing personal data for journalistic purposes. The DPDP is competent to supervise when media are processing data which are part of any data filling system controlled either by private legal entity or a public one.

If, during the inspection supervision, the inspector determines that there has been a violation of LPDP, he/she submits a request for initiation of a misdemeanour procedure before a Misdemeanour Commission.

The practice of the Directorate for Personal Data Protection

In 2011, the Directorate for Personal Data Protection (DPDP) decided there was a violation of Article 23, paragraph 1 and 3 of the LPDP, when a document clearly showing the name, surname, address and personal identification number of a person was published on TV news.

The same document was posted on the TV's website. Although the TV station promised the individual the document would be removed, the document nevertheless remained on the TV's website. Therefore, the TV failed to apply appropriate technical measures to ensure confidentiality and protection of personal data, thus committed a violation of the LPDP by allowing an unauthorized disclosure of personal data.

In 2012, the DPDP received a complaint of TV reporting about a case of domestic violence with full names and home addresses of the victims. The DPDP found the TV should not process and publish personal data and should not carry out inequitable processing of personal data or process personal data which is too excessive having in mind the purposes for which personal data were collected and processed. The respondent should apply appropriate technical and organizational measures to ensure confidentiality and protection of personal data of the individuals. DPDP also received a request about a publication of video material on the TV news and on YouTube showing the face and body of the person. The video material was taken by the Ministry of Interior affairs during a search of private premises. The building, the apartment, the furniture, the face and body of the complainant were recorded. Furthermore, the person who was recorded, the complainant, was in custody/jail the next day. The DPDP concluded the procedure relating to the request should be stopped, as there was no violation of the right to personal data protection. The inspector found no violation because the person could not be identified on the grounds of the camera footage.

In 2013, the DPDP decided the right to personal data protection was violated in the following case. On a web-newspaper texts were published along with comments of humiliation, personal insults and lies about the person and his family. The DPDP decided the media is obliged not to process and publish personal data, not to carry out inequitable processing of personal data or processing of personal data which is too excessive having in mind the purposes for which the personal data was collected and processed. The respondent should have applied appropriate technical and organizational measures to ensure confidentiality and protection of personal data of the individuals, in this case it should have anonymized the data. In 2014, the DPDP considered several similar cases concerning an editorial, which published extracts from the Central Register of RM. Moreover, an application additionally stated that also their addresses of residence were published, which according to the applicants are not information of public interest. The procedure for determining a violation of the right to protection of personal data was stopped due to a formal defect of the request.

In 2016, a lot of requests were filed before the DPDP. The first one concerning three web portals publishing a photograph of monthly salary calculations together with details of work experience, pension and disability insurance, health insurance, contributions to supplementary health insurance, contributions for employment, Chamber of Commerce and collective insurance, and another photograph was attached to the text that contained defamatory allegations. The initiative for determining a violation of the right to personal data protection was denied as in the previous case. Having in mind that the data were of a director of a public enterprise established by the municipality, the inspector concluded that in

this case the public interest about the disclosure of the salary calculation prevailed over the interest of an individual.

There were also a few requests submitted by the employees of an NGO against several web portals and TV stations, because they published the data of their executives' salaries. Additionally, they wanted the DPDP to perform an extraordinary supervision in the Public Revenue Office since it has as a state body all the relevant data on the personal income of the applicants. The DPDP ruled that the media should remove the articles because they included personal data of executives which are not holders of public function and no other significant public interest could apply. There were several accusations as to the DPDP censorship, however, we believe the decision was justified and proportionate to the aim of data protection.
In the following case the DPDP concluded that there was no violation of the right to personal data protection. A TV station announced information on the news as well as on their official website about a job position of a person without his consent, announcing "Mr. NN, an employee in the company MM representing himself as representative of the company…" The TV station responded to the initiative stating that the same personal data have been previously already made publicly available through social and professional networks as well as through public registries. Additionally, the TV noted that it was in public interest to publish the information about the issue at hand and that the information was published only in the context of public interest. The DPDP affirmed the personal data was fairly processed and in accordance with the Constitution and the relevant Law. After the DPDP's decision, the applicant submitted a complaint to the Administrative Court and the procedure is still ongoing.

Another case concerned an allegation of infringement by a web portal which published false data for a private company (the owner is an Albanian) saying that "all data for products are only in Macedonian language". The owner of the company sent a pre-litigation claim to the web portal requesting the portal to apologize and to withdraw the information. Subsequently, the web portal just published the claim, without any apology, publishing personal data of the owner of the company (address, personal identification number). The DPDP decided there was a violation of the right to personal data protection, since the data was not processed in accordance with the law.

A web portal published on their public Facebook profile a photograph of a child (minor) along with comments, without prior knowledge and consent of the child's parents. The publication of data violated the right to personal data protection according to the DPDP. The DPDP furthermore stated that it was prohibited to process (publish) personal data (photos) on the web portal and on Facebook profile without the knowledge and consent of the data subject.

The DPDP also decided there was a violation of the right to personal data protection when a daily newspaper in the section "Black Chronicle" published the name, address, employment data and health data, which referred to and were a result of the damage caused. In this

case, the public interest did not prevail over private interest, as the same objective could be achieved with anonymization of the data.

A request in 2016 concerned a TV station publishing in one of its programs material revealing identity of a person, without its knowledge and previous consent. A violation of the right to personal data protection was found and the DPDP used the same reasoning as in the before mentioned case. Another similar case regarding a web portal and a printed media was brought before the DPDP where the DPDP decided in the same manner.

The DPDP also wrote an Indication to the Agency for audio and audio-visual services regarding the publishing of license plates of vehicles by the media. The DPDP noted that the data relating to the vehicle (registration number) are indicators of an identification of an individual, and such data are consequently personal information. Thus, when publishing the license plates of vehicles, it is necessary to take appropriate measures to make those numbers invisible, to blur them for instance.

The DPDP's Indication to a daily newspaper (chief editor) refers to a photograph of the Mayor of Skopje published on the cover of a daily newspaper. The photograph was taken on the beach during the Mayor's summer vacation. The DPDP indicated to the editor-in-chief that in this case public interest on publishing the photo does not prevail over private interests of the Mayor, and, at the same time, there was no consent of the Mayor for the photo to be published. The Chief editor reacted to the Indication stating that it is a rude attack on the freedom of speech and censorship, prohibited by the Constitution, and represents an interference in the editorial policy of the newspaper.

Questions related to the publication of personal data

What is personal data and what is the difference between the identified and identifiable individual?

Pursuant to Point 1 of Article 2 of the LPDP personal data is defined as any information pertaining to an identified or identifiable natural person, the identifiable entity being an entity whose identity can be determined directly or indirectly, especially as according to the personal identification number of the citizen or based on one or more characteristics, specific for his/her physical, mental, economic, cultural or social identity. So, personal data is not only a name, surname or individual's address, but also his/her medical data, picture, voice recording and other biometrical data (i.e. physical, physiological and behavioural characteristics unique to everyone, e.g. finger or hand print, form of an earlap, colour and pattern of iris, body posture, etc.). Email address, unique personal identification number, tax number and such have become even more important data with the development of IT.

In other words, personal data is data which in any way defines whether the data relates to a specific individual or a specific individual can be identified using such data. Identified individual is a natural person directly defined (identified) by data, e.g. Angela Merkel, Jovan Ilievski,

Queen Elizabeth II etc. For instance, for public figures it may be enough to refer to the position of the person, such as President of the European Commission, whereas certain more common names, such as John Smith, may need additional data for the data subject to become identified or even identifiable. Identifiable individual is a natural person who may be identified with indirect referencing to one or more characteristics which enable recognition without excessive efforts, time or costs. In Macedonia, Aleksandar Stojanovski is recognised as an identifiable person due to the frequency of the name in the country. If data on function performed by this person is added to the said person, these data become personal data, because for example there is only one Supreme Court justice in Macedonia named Aleksandar Stojanovski.

The ECtHR has also repeatedly stated that the notion of 'persoal data' under the ECHR is the same as in CoE Convention 108, especially concerning the condition of relating to identified or identifiable persons.

Personal data is data which in any way defines whether the data relates to a specific individual or a specific individual can be identified using such data. Personal data is not only a name, surname or individual's address, but also his/her medical data, photo, voice recording and other biometrical data. Email address, unique personal identification number, tax number and such have become even more important data with the development of IT. However, LPDP applies only to personal data that is included in a data filing system.

Does the Law on Personal Data Protection allow publication of personal data and when?

Firstly, it is important to emphasise that the LPDP does not apply for data processing which is performed exclusively by individuals for their personal use, family life and domestic needs. If such persons publish or otherwise transfer personal data without necessary legal base, they may be subject to penal and civil liability.

As for personal data processed by any other so-called controller[18] or processor[19] he or she must have a relevant legal base to perform any personal data processing.[20] The LPDP prohibits publication of all kinds of data as a general rule, however publication is allowed pursuant to Articles 5 and 6 in the following cases:

- if the data subject gives his informed consent to such publication;
- if such publication is prescribed by law;

[18] According to LPDP a controller is any natural or legal person, a state or other body, who, independently or together with others, determines the purposes and the ways of personal data processing; when the purposes and the ways of personal data processing are determined by law or any other regulation, the same law or regulation determines the controller or the special criteria for his/her selection.

[19] While GDPR and other relevant legal text in English refer to this as a "processor", unofficial English translations of Macedonian LPDP refer to it as "personal data collection handler, however this is a natural or a legal person or a legally authorized state body processing the personal data on the behalf of the controller.

[20] According to LPDP processing of personal data is every operation or a number of operations performed on personal data, automatically or otherwise, such as: collection, recording, organizing, storing, adjusting, or altering, withdrawing, consulting, using, publishing through transmitting, revealing or making otherwise available, aligning, combining, blocking, deleting or destroying. Even insight into personal data is understood as personal data processing.

- if publication of data is necessary for the execution of certain competences, tasks and obligations of a body or organisation, unless such processing encroaches upon data subject's rights and freedoms;
- if publication of data is necessary for realization of a contract in which the personal data subject is a Contracting Party or upon a request by the personal data subject prior to his/her accession to the contract
- if publication of data is necessary for the fulfilment of legal obligations of the Controller
- if publication of data is necessary for the protection of life or physical and moral integrity of the personal data subject.

What is the procedure regarding the consent of the person whom the personal data relates to?

Consent or approval must be given by the person to whom the personal data relates to (the so-called data subject) or his or her legal representative (e.g. in case of minors, consent should be provided by the parents or other legal guardian). The consent needs to be given voluntarily without the use of force, threat or fraud. A valid consent can only be given if the data subject has all relevant information relating to data processing available – the data controller therefore must provide him or her with all relevant information prior to the consent is given (especially information on who is the data controller, what data, for what purposes and for how long will be processed and in what sorts of manners, as well as information on consequences of refusal to give consent and rights of the data subject to access and correct one's data; if appropriate regarding the intensity, volume or means of data processing, other relevant information should be provided to the data subject). According to the GDPR, consent or approval may generally be given in a written, verbal or other appropriate manner sufficiently stating the true will of data subject or his or her legal representative, however according to the Macedonian LPDP the consent is a free and expressly given statement of the will of the personal data subject that agrees with the processing of his personal data for predefined purposes.

A valid consent can only be given if the data subject has all relevant information relating to data processing – the data controller must provide him or her with all relevant information prior to the consent is given. In Macedonia, the consent is a free and expressly given statement of will of the personal data subject, which agrees with the processing of his personal data for predefined purposes.

Which acts represent a legal base for publication of personal data?

Several laws exist and since many refer to public data not all can be listed. Therefore, a review as per group should suffice. Personal data contained in public records may generally

be published without consent to the extent the sectoral law allows it, as long as the purpose of publication remains in the context of the purposes for which the records are made public by the law - for example *Land Register data* in the context of real estate market safety, *Register of Companies, Shareholders Register, Register of Freelance Journalists and Cultural Professionals and Register of Attorneys* in the context of market transparency, *Court proceedings* in the context of legal certainty, etc.

What do different Codes of practice for journalists say about protection of personal data by the media?

For example, the *Croatian Code for Journalists* states that journalists should respect human rights. A journalist must protect people's privacy from unreasonable or sensational discovery in public. A journalist is obliged to respect everybody's right to private and family life, home, health and correspondence. Moreover, in Article 16 the Code notes that publishing data that violates someone's privacy without permission must be justified by public interest. Using means to photograph people from a distance in their private surroundings and on their private property without permission is unacceptable. Editors may not publish material of journalists who do not obey these rules. Special attention and responsibility are required when reporting on accidents, family tragedies, sickness, children and minors, trials. The assumption of innocence, integrity, dignity and the sensibilities of all parties in a trial must be respected. In political conflicts, a journalist must respect the civil rights and freedom of all participants and try to be neutral. In addition, Article 17 of the Code provides that a journalist must not take photographs or interview children (under 14 years) concerning issues about their lives without their parents' presence or other responsible adult. It is not allowed for a journalist to talk with pupils or take pictures of them without the permission of the school. It is not allowed to pay children and minors for information (14 to 16 years) nor their parents or guardians, unless it is in the interest of the child.

The *Code for Journalists in Slovenia* notes the journalist should respect the individual's right to privacy and avoid sensationalistic and unjustified disclosure of anyone's privacy to the public. Intrusion into an individual's privacy is only permissible if there is an overriding public interest. With public officials and others seeking power, influence and attention the public's right to be informed is greater. The code points out that the journalist should be aware that gathering and publishing information and photographs may cause harm to individuals not accustomed to media and public attention. Furthermore, when reporting on judicial matters, the journalist should take into consideration that no one is guilty until legally found so. The journalist should exercise caution in publishing names and photographs of perpetrators, victims and their relatives when reporting on tragedies and pre-trial proceedings. Additionally, the journalist should be tactful when gathering and reporting information, publishing photographs and transmitting statements on children and minors, those affected by misfortune or family tragedy, the physically or mentally disabled and others having severe handicaps or illnesses. The journalist may also decline to testify and disclose his source. In Slovenia, should the journalist be invited to a session of the Journalists' Ethics Council, he/she

is obliged to attend it and to abide by its decisions. The Ethics Council or Tribunal in Slovene is a very important decision-making body where one can appeal about the content or title of an article whether it is written or oral. Slovene courts consider the decision of the Ethics Council when deciding on unlawfulness and on possible damages awarded to the plaintiff in lawsuits. *Britain's Code of conduct* provides that the journalist does nothing to intrude into anybody's private life, grief or distress unless justified by overriding consideration of the public interest. Moreover, the journalist should protect the identity of sources who supply information in confidence and material gathered during her/his work.

Another example could also be an *Italian Code of practice* which notes that a journalist must not publish images and photos of people involved in daily episodes which are particularly terrifying or prejudicial to people's dignity, nor may he dwell upon details of violence or brutality unless for a prominent reason of social interest. The Code also states that the journalist should respect the right of secrecy of every person and she/he may not publish news about someone's private life, unless they are transparent and relevant to the public interest, however, he must always reveal his own identity and profession when he gathers such news. Additionally, the names of the relatives of people involved in such daily events cannot be published unless they are relevant to the public's interest; they can be neither made known in case of danger to people's safety, nor can they publish other elements that can reveal people's identity (photos, images). The names of victims of sexual violence can be neither published, nor can a journalist give details that can lead to their identification unless it is required by the victims themselves and it is in general interest. Moreover, a journalist must proceed with great caution when publishing names or elements that can lead to the identification of members of a legal team or of the police, when they may provoke the risk of inquilinity for themselves or their families. A journalist also must undertake the maximum caution in spreading news, names and images of accused people for minor offences leading to mild punishments, except in cases of particular social interest.

According to the *Macedonian Principles of Journalistic Conduct* the journalist shall respect the privacy of every person, except in cases when this is contrary to public interest. The journalists shall not consciously create or process information that jeopardizes human rights and freedoms and is obliged to respect the personal pain and grief. The manner of informing in case of accident, natural disaster, war, family tragedy, sickness, court proceedings must be free from sensationalism. The principle of presumption of innocence, reporting for all involved parties in the legal dispute without pre-empting a verdict, will be applied when reporting on court proceeding. Similar to Croatia, in Macedonia, the journalist must not interview or photograph children under 16 years of age without the consent of the parents or legal guardians, unless that is in accordance with the children's rights. The same applies to people with special needs, who are not able to decide rationally.

What are the procedural guarantees in relation to personal data required by the ECtHR?

The ECtHR has delivered judgments on the states' obligation to protect the right of an individual against excessive encroachment of state bodies during an investigation

in criminal proceedings; particularly, in relation to the supervision of correspondence and telephone tapping. Hence, for example in the case of *Klass et al. v. Germany*[21] the ECtHR ruled that secret supervision did not infringe the right to privacy and correspondence since procedures for supervision were envisaged in sufficient detail and rigorously enough. The ECtHR deemed the need to ensure state security and prevent disorder or crime as an act necessary in a democratic society. Differently, the ECtHR ruled in the case of *Malone v. the United Kingdom*[22] in which the permissibility of police telephone tapping and managing a "register" of outgoing phone numbers were reviewed. The ECtHR found an infringement of the right to privacy since the possibility of telephone tapping in the United Kingdom was excessively arbitrary. Regarding the list of outgoing calls the ECtHR assessed that such action is legal and common in the business world, however, transmission of such data to the police represents an unjustified encroachment upon the right to privacy since no legal authorisation or consent of the affected parties existed.

The case of *Sciacca v. Italy*[23] related to the publication of a photograph of a person in criminal proceedings. The case addressed suspicion of a criminal act performed by several persons who were suspected of blackmail, fraud and forgery at a private school in Sicily. Among them a teacher was reported to the financial police and later held in a house arrest. At the time, the police took his photo and fingerprints. At the press conference, the public prosecutor circulated his photo to the journalists who published the said photo in different newspapers. Although the suspect was later imposed a prison sentence and a fine, the publication of the photo was deemed an encroachment of privacy. Since the applicant failed to obtain satisfaction at the Italian judiciary system, the ECtHR ruled that the publication of the photo represented a breach of the right to privacy given that the publication of the photo was not necessary in a democratic society and the photo was taken at the police station for different purposes.

In *Uzun v. Germany*,[24] the applicant and another man were placed under surveillance via a global positioning system (GPS) device fitted in the other man's car because of their suspected involvement in bomb attacks. In this case, the ECtHR held that the applicant's observation via GPS represented an interference with his private life as protected by Article 8 of the ECHR. However, the ECtHR held that GPS surveillance had been in accordance with the law, was proportionate to the legitimate aim of investigating several counts of attempted murder and necessary in a democratic society, therefore, it did not amount to a violation of Article 8 of the ECHR.

Rights and obligations of states are not only limited to the constraints on public sector bodies not to encroach upon the rights of individuals (i. e. negative obligations), but they also apply in respect that states are responsible for adopting measures to ensure adequate judicial protection of individuals, when other private entities violate their rights (i. e. positive obligations). The ECtHR had thus ruled on the misuse of internet before the opposite EC recommendations, UN resolutions and the EU Directive no.: 2006/24/EC, amending the Di-

[21] ECtHR, Klass et al. v. Germany, No. 5029/71, 6 September 1978.
[22] ECtHR, Malone v. the United Kingdom, No. 8691/79, 26 April 1985.
[23] ECtHR, Sciacca v. Italy, No. 50774/99, 11 January 2005.
[24] ECtHR, Uzun v. Germany, No. 35623/05, 2 September 2010.

rective no.: 2002/58/EC, were adopted. The EU Directive no.: 2006/24/EC imposed on the states to adopt sufficient measures for oppressing cybercrime. Comparative study carried out by the ECtHR established that many countries enacted the obligation of the telecommunications providers to submit the computer data (also that on subscribers) regardless of the nature of the criminal offence. Consequently, the Court granted the appeal of a father of a 12-year-old in the case of *K.U. v. Finland* since neither national Court of First Instance nor appellate court succeeded in protecting psychological and moral interest of an individual (in particular an adolescent or deprived person) who became a target of paedophiles, for they did not manage to enforce mechanisms to identify the perpetrator. In this case, an unidentified person published an internet advertisement indicating that a 12-year-old boy wishes to have intimate contacts with a boy of the same height or taller who would "show him the way". The person detailed the adolescent boy's personal data, including the date of birth, description of his physical characteristics and added a link to his internet page which contained his photo, email address and telephone number. The Court demanded the state to ensure actual and efficient measures to identify the person who published the add and thus enable criminal prosecution.

Pursuant to the first paragraph of Article 6 of the ECHR the ECtHR decided also on the public nature of court proceedings. The Court ruled that the public nature of court proceedings is not only interesting for parties involved but also for the public in general. Public nature of the proceedings ensures a fair trial to all parties involved, in particular when standing against the state (mainly in criminal procedures).

Rights and obligations of states are not only limited to the constraints on public sector bodies not to encroach upon the rights of individuals (i. e. negative obligations), but they also apply in respect that states are responsible for adopting measures to ensure adequate judicial protection of individuals, when other private entities violate their rights (i. e. positive obligations).

Rights of data subjects

The right to personal data protection is founded on the premise that each individual should have control over his life and person. The basic right lies in the guarantee that data subject's personal data shall not be processed unless so provided by the law or personal consent of the data subject. In Macedonia, like in most legal systems, the right to data protection includes the right to receive information from the controller (on whether his/her personal data are being processed, on the purposes and legal base for personal data processing and the users or categories of users to whom the personal data are being disclosed, the logic of automatic processing, in case a decision has been made on the automatic processing affecting the personal data subject), to receive his own personal data from the controller, the right to request amendments, corrections and deletion of his/her own personal data, to prevent the controller from processing his personal data (withdraw consent).

The media is not obliged to reveal the source of the information since the protection of the media source is part of freedom of press (expression) which always overrides the right of a data subject to receive the information from the media – data controller.

We can roughly divide personal data protection mechanisms into three groups: 1. Administrative protection (DPDP supervision over LPDP and appeal procedure before the DPDP); 2. Civil liability (damages awarded by civil court); 3. Penal liability (misdemeanour procedure before the Commission pursuant to LPDP and criminal charges brought before criminal court). Administrative protection and misdemeanour procedure applies only in cases where personal data concerned derive from personal data filling system, whereas civil and criminal liability may apply also in cases where personal data concerned did not come from, were not included in nor was there any such intention involved.

As drafted in the chart below media must respect the legality principle when publicizing personal data.

According to LPDP (Article 4a) not only individual's consent or basis in the law are applicable but also a so called overriding public interest applies when the story is in a public interest. Article 4 a namely defines:

"The provisions of this Law shall not be applied to processing of personal data carried out for the purpose of professional journalism, only in the case when the public interest prevails over the private interest of the subject of personal data."

Rights of a data subject

When media publicizes person's personal data - legal ground is needed:

1. Person's consesnt
2. Basis in any law (i.e. Access to Public Information Law)
3. if there is an overriding public interest - freedom of expression prevails over right to privacy and personal data protection

If personal data derives from a data filling system

File an initiative before DPDP (Article 18 of LPDP):

DPDP has to react ex officio and consider the legality of publicizing the personal data taking all 3 possible legal grounds into account

Ex officio - Once the initiative is filled the person cannot withdraw it

If DPDP finds out that persons's rights according to LPDP were violated

then the subject of the personal data can exercise the right to damage compensation caused by the processing of personal data or other activity carried out contrary to the provisions of this Law, by submitting a claim for damage compensation to the competent court (Article 21 of LPDP).

DPDP can independently initiate a misdemeanour prodecure against data controller

If personal data does not derive from a data fillig sytem

File a liability lawsuit for damages before a competent civil court:

Court has to decide upon the case and consider the legality of publicizing the personal data taking all 3 possible legal grounds into account.

The planitiff may withdraw the application at any time

The Media as Personal Data Processors – The Competencies of the DPDP

The Media's Obligation to Abide by the Provisions of the Law on Personal Data Protection

The DPDP is competent merely for the part of the right to privacy which relates to the protection of personal data, and is thus regulated by Article 18 of the Constitution of the Republic of Macedonia. The broader limitations of the media are laid down in Article 25 of the Constitution which provides that each citizen is guaranteed the respect and protection of the privacy of his/her personal and family life and of his/her dignity and repute. These rights are guaranteed under the law and accordingly afforded judicial protection.

In understanding the competences of the DPDP, it is important to appreciate some general notions laid down by the LPDP. According to the provisions of Point 1 of Article 2 of the LPDP, personal data is defined as any information pertaining to an identified or identifiable natural person, the identifiable entity being an entity whose identity can be determined directly or indirectly, especially as according to the personal identification number of the citizen or on the basis of one or more characteristics, specific for his/her physical, mental, economic, cultural or social identity, personal data is defined as any data pertaining to an individual, irrespective of the form in which it is expressed. The fourth point of the same Article further provides that an individual - is any natural person to whom the processed data refer. Pursuant to its Article 1, Macedonia's LPDP regulates the protection of personal data as fundamental freedoms and rights of the citizens, and especially the rights to privacy as related to the personal data processing. With regard to the provision of Point 2 of Article 2 of the LPDP, processing is considered every operation or a number of operations performed on personal data, automatically or otherwise, such as: collection, recording, organizing, storing, adjusting, or altering, withdrawing, consulting, using, publishing through transmitting, revealing or making otherwise available, aligning, combining, blocking, deleting or destroying; it accordingly encompasses any operation or set of operations performed using, or related to, personal data; thus the term embraces both automated and manual processing in relation to a filing or retrieval system. Pursuant to the provisions of Point 3 of Article 2 of the LPDP, a filing system or "Personal Data Collection" is a structured group of personal data available as per specific criteria, regardless if it is centralized, decentralized or dispersed on a functional or a geographical basis.

Most important principles of personal data protection are **purpose limitation**, **data minimisation**, and **proportionality principle** which are envisaged in several LDPD provisions, as well as clearly stated in the provisions and the preamble of the GDPR. Generally, they refer to the following:

- personal data shall be collected for concrete, clear and legally determined (or clearly consented to on the base of relevant information provided) purposes and processed pursuant to those purposes;

- personal data shall be appropriate, relevant and not too comprehensive in relation to the purposes for which they are collected and processed;

- personal data shall be accurate, complete and updated, whereby the inaccurate or incomplete data shall be deleted or corrected, considering the purposes for which they have been collected or processed;

- personal data shall be stored in a form which allows identification of the personal data subject, not longer than necessary to fulfil the purposes for which the data have been collected for further processing

- cases when data processing is allowed by law in the absence of a valid consent all require such processing is necessary for the legitimate aim designated by the law.

If the media publishes personal data, which is part of a certain data filling system or is intended for the inclusion in it, and there is no legal basis (i.e. public interest) or the individual's consent for such, then this could represent an infringement of the provisions of the LPDP.

If there is the publication of data, which merely represents the confirmation of some facts and does not in itself represent personal data emanating from a data filling system, then this shall not be deemed an infringement of the provisions of the LPDP; this, however, does not mean that an aggrieved party shall not be entitled to judicial protection (civil liability).

The publication of personal data in the media, *per se*, does not represent an infringement of the provisions of the LPDP. As arises from the terms stated in the previous paragraph, the publication of personal data could represent an infringement of personal data protection if the data had been illegally supplied from data filling systems of personal data.

In Macedonia, pursuant to Art. 26.a of LPDP controllers are generally required to appoint a data protection officer (hereinafter: DPO) and the media are no exception – same exceptions to the rule apply for them. According to Art. 26.a of LPDP the data protection officer performs the following activities:

- participate in the adoption of decision related to the processing of personal data, as well as the exercise of the rights of entities over their personal data,

- monitor the harmonization of the law and the regulation adopted thereunder, referring to the procession of the personal data, as well with the internal regulations for protection of the personal data and the documentation for technical and organizational measures for the purpose of ensuring secrecy and protection during personal data processing,

- draw up the internal regulations for personal data protection and the documentation for technical and organizational measures for the purpose of ensuring secrecy and protection of during personal data processing,

- coordinate the control of the procedures and guidelines determined in the internal regulations for the personal data protection and the documentation for technical and organizational measures for the purpose of ensuring secrecy and protection of during personal data processing,

- propose training to the employees in connection with the personal data protion, and

- perform other activities determined by law and the regulations adopted thereunder, as well with the internal regulations for personal data protection and the documentation for technical and organizational measures for the purpose of ensuring secrecy and protection of during personal data processing.

Tasks of the DPO pursuant to LPDP are similar to tasks of the DPO pursuant to the GDPR, however, the LPDP provides more specific task, whereas, the GDPR is more goal oriented in designating DPO's duties and tasks. An important difference is also in the position of the DPO. Pursuant to the GDPR, a DPO should be able to execute his tasks and duties in an independent manner, whereas the LPDP includes no such provisions.

A DPO has an important role in an organisation handling personal data. DPO's main tasks and duties involve ensuring data protection regulation compliance in an organisation.

Publication of Personal Data by the Media in Relation to Court Proceedings

Is the publication of a document issued by a law enforcement authority allowed?

Let us take - as an example - an investigation in relation to a suspect, and information which usually includes first name, family name, date and place of birth, permanent residence and citizenship. Based on weighing of the right to privacy against the right of freedom of expression, public interest in current events and the legal interest of a public authority in relation to the protection of law and order, publication of the first name and family name of a suspect not yet captured does not represent an infringement of the right of protection of personal data; as long as such publication can contribute to the capturing of a presumably dangerous suspect publication of some other personal data will be proportionate to the aim pursued. If for example citizenship and birth date and place have no relevance in the search for the suspect they should not be published.

According to the provisions of Point 2 of Article 2 of the LPDP, public processing of personal data as described in the previous paragraph, is admissible in accordance with Article 6 of the LPDP if the permission for such data and its processing are provided by statute, or if the consent of the individual concerned has been provided. One should take into consideration the general principle of proportionality relating to the protection of personal data, as regulated by Article 5 of the LPDP. According to this provision, the personal data being

processed must be appropriate, relevant and not too comprehensive in relation to the purposes for which such data is collected and further processed.

In the process of assessment - in the event of collision of several fundamental rights and/or in the event of prohibition of excessive encroachment into such rights - it is always necessary to assess whether the restriction of such rights or their encroachment are proportional and substantiated with a constitutionally admissible goal which intends to protect or provide some other social or public benefit, and when through the curtailment of such a right they are directly or indirectly protecting the rights of others. This also encompasses the exceptions arising from Article 8 of the ECHR (further see the decision of the ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987) and influencing the rights and interests of the affected parties to the smallest possible degree and/or assessment as to the eligibility of urgent encroachment in relation to the eventual consequences.

From the aspect of general proportionality, which provides that the extent of the interference with a protected right - namely the protection of personal data - must be appropriate and proportionate to the purpose and importance of another constitutionally protected right or public benefit, as is manifested in Article 5 of the LPDP. The publication of personal data must, therefore, also be assessed from the aspect of the constitutionally guaranteed freedom of expression, laid down in Article 16 of the Constitution of RM and enacted through the Law on Media. In relation to the implementation of the provisions of the LPDP the processing of personal data by the media for the purpose of providing information to the public are obliged to respect all provisions of the LPDP. This also means that, when publishing personal data, the media must comply with Article 5 of the LPDP, and employ the principle of proportionality.

Actual implementation of the principle of proportionality in such instances originates from the established practice of the ECtHR, which has, in several cases - e.g. in the case of Von Hannover v. Germany - decided as follows:

1. the media shall only be granted a narrower scope of the right of interference into the privacy of those public persons who are not engaged in politics or who perform an official or political function (i.e. those public figures who cannot be classified as public figures '*par excellence*');
2. the media shall not be granted the right to interfere into the privacy of those public figures who are not public figures '*par excellence*' if the details of their private life are not relevant to the public discussion on the matters which are of general and/or in public interest;
3. the curiosity of the public and media providing public entertainment (such as tabloids) cannot be determined as public interest if it encompasses (illegitimate) interference into the privacy of public figures who are not public figures '*par excellence*';
4. neither the freedom of expression nor the right for privacy are absolute in their character; and, for this reason, they must be appropriately balanced if they collide.

The ECtHR has ordered ECHR signatory states to more precisely define the notion of a public figure. If, in certain cases, the persons cannot be classified as public figures '*par excellence*' then the media is not permitted to interfere with their privacy. In any such case, the detailed personal data is most probably not important or germane to any public discussion on matters which are of general, or in the public, interest. In every individual case, it needs to be assessed whether full disclosure, or merely some personal data from a given document would be sufficient to satisfy the needs of public interest. In the case of a request for investigation, it would, for example, mean solely the publication of the full name of the suspect. The publication of such minimal information would be sufficient to inform the public of current affairs. Other personal data, which may usually be included in a request for investigation, is by no means relevant apropos of public interest or freedom of expression, since an individual - according to point 4 of Article 2 of the LPDP - is fully identifiable from their full name provided in the context of other data arising from a published document.

Publication may be considered as a manifestation of the public's right to know prevailing over the right to protection of personal data; however, it must be in line with the constitutional principle of proportionality. Furthermore, the publication of the date and place of birth, permanent residence and citizenship of a suspect - for which the media have neither appropriate legal basis nor the personal consent of the individual - exceeds what is mandated. Hence this would be deemed unwarranted processing of personal data and an infringement of the provisions of Article 5 of the LPDP.

The publication of a surfeit of personal data in any request for an investigation should be deemed an unwarranted encroachment into an individual's right to protection of personal data. It could also lead to identity theft or other abuse (e.g. forgery of documents based on the detailed personal data which has been published, or interference with the privacy or family life of the individual, and even a personal attack (retaliation) or other criminal offence against that person) or even interference with the law and the safeguarding of public order.

If, in certain cases, the persons cannot be classified as public figures 'par excellence' then the media is not permitted to interfere with their privacy. In any such case, the detailed personal data is most probably not important or germane to any public discussion on matters which are of general, or in the public, interest. In every individual case, it needs to be assessed whether full disclosure, or merely some personal data from a given document would be sufficient to satisfy the needs of public interest.

Is the publication of autopsy reports pertaining to victims permissible?

Autopsy reports generally include sensitive personal data the processing of which is regulated by Article 8 of the LPDP, which provides that sensitive or so-called special categories of personal data can only be processed if this is authorised by law based on public interest or on a Decision of the Directorate for personal data protection.

The right to freedom of expression by the media is not an absolute right; as with all such rights and freedoms it may be subject to limitation by the rights of others, as well as in the instances specified in the Constitution of RM.

It should be stressed that the right to freedom of expression is already restricted by Macedonia's Law on Media itself, namely by Article 3. Pursuant to the provisions of Article 3, the activities of the media shall be based on freedom of expression, together with the respect of human individuality, privacy and dignity.

While the Macedonian Law on Media does not provide for more detailed provisions, the Slovene Media act for instance clearly provides that the media shall not be entitled to information if this would entail infringement of confidentiality as to personal data in accordance with law, unless publication thereof would prevent a serious criminal offence or avert danger to human life or public property. The provisions of the Slovene Media Act clearly point to public interest in connection with the publication of data that encroaches upon an individuals' right to personal dignity, privacy and protection of personal data: when exercising the right to freedom of expression, the media shall be obliged to respect the inviolability and protection of personality and dignity; the media may only impinge upon such rights in the event that publication would prevent a serious criminal offence or avert danger to human life or public property.

The publication of autopsy reports which pertain to victims of crime necessarily involve the collision of two human rights: the right of freedom of expression and the right of personal data protection; appropriate reconciliation is provided in accordance with the constitutional principle of proportionality as determined in Article 5 of the LPDP which states that the processing of personal data must be appropriate, relevant and in its extent not too exhaustive in relation to the purposes for which they are collected and further processed (more information on this is provided in the answer to the first question herein concerning the implementation of the principle of proportionality).

Through implementation of the provisions of Article 3 of the Law on Media, we could say the media would be entitled to obtain and publish autopsy reports or parts thereof, providing such action would prevent a serious criminal offence or avert danger to human life or public property etc., which will, in practice, very unlikely be the case.

Is the publication of a photocopy of a suspect's ID permissible?

Let us take, as an example, the publication of a photocopy of the ID-card of a suspect, whereby the following personal data is processed: a photograph of the individual, his/her name, surname, date of birth, place of birth, sex, ID-card number, date of issue of the ID-card, date of its expiry, place of issue and signature of the holder.

Pursuant to the provisions of Article 6 of the LPDP, which are also binding on the media, to publish personal data from an ID card, a legal basis for such action must exist, either a personal consent of the individual whose personal data is being published, or overriding substantiation as to the primacy of the public's right to know concerning all personal data on the said ID-card. In this respect, all published personal data must be adequate and in its extent, appropriate in relation to the purposes for which it has been collected and further processed. Failure to do so would infringe the principle of proportionality (for more information on implementation of the principle of proportionality see above). It is evident that prior to publishing a photocopy of the entire ID-card of a suspect, the media is obliged to conceal the following personal data: date of birth, place of birth, sex, ID-card number, date of issue of ID-card, date of expiry of ID-card, place of issue of ID-card and the signature of the holder.

However, not only privacy issues arise in case of ID-card or passport copy publication – also public safety and state security issues arise. For example, in Republic of Slovenia it is forbidden to make or hold electronic copies of personal ID-card or passport – the rational of such explicit ban is more in the protection of ID-cards and passports as authentic and official identification instruments, preventing falsification of such documents which would infringe not only holder's privacy but state security interests as well.

A legal basis for publishing personal data from an ID card must exist, either a personal consent of the individual whose personal data is being published, or overriding substantiation as to the primacy of the public's right to know concerning all personal data on the said ID-card.

Questions Pertaining to the Publication of Personal Data of Employees in the Media

Is the publication of personal data in relation to private sector employees admissible?

If the media - for example - publishes the names and surnames of recipients of the highest gross and net salaries of employees in a company, and had neither the individual's consent or other legal base for such processing of personal data, such action would represent an illegal supply of personal data to the public.

The processing of personal data of private sector company employees is governed by Macedonia's Labour Relations Law. Pursuant to the said Law, as well as with respect for the provisions of Article 6 of the LPDP, the media may only publish the data of the recipients of the highest gross and net salaries in companies if this is necessary in the exercise of the rights and obligations arising from an employment relationship or related to an employment relationship, or if the consent of the individual to whom the data pertains was provided, which is in practice very unlikely to be justified. The public nature of salaries is prescribed only for the public sector. If the media publishes such information, they may not invoke the right to freedom of expression and public interest because pursuant to Article 10 of the ECHR such rights and freedoms are restrict-

ed by the rights of others. Moreover, the right to freedom of expression is restricted by the Law on Media itself, according to which the media would not be entitled to obtain and publish such data, unless publication thereof would prevent a serious criminal offence or avert direct danger to human life or public property, which, in the present example, is probably out of question.

Publication of salaries of the employees working in private sector would encroach upon the right of dignity of the individual, the protection of personality and privacy, as well as the right to the protection of personal data; whereas, the right to freedom of expression would not prevail in collision with these rights.

Which personal data of civil servants is permissible to publish?

Regarding the processing of the name and surname and some other personal data of civil servants, one should consider the provisions of Para. 1 of Article 6 of Macedonia's Law on Free Access to Information of Public Character (hereinafter: Law on API) where personal data is stated as one of the exceptions when the public-sector body may deny applicant's access to requested information. Nevertheless, even personal data may be disclosed pursuant to Para. 3 of Article 6 of Law on API when by the publishing of the information the consequences for the protected interest are smaller than the public interest that would be satisfied by the publishing of the information.

Furthermore, the main objective of the system regulated by the Law on Civil Servants is to provide means for selecting civil servants based on objective criteria of professional competence. Such means of objectivity are provided within the scope of the procedure for the selection of a candidate filling a vacant position. In this regard we should mention Article 9 of the Law on Civil Servants which provides that any individual who meets the following general requirement may be employed as a civil servant, which means that the employment of civil servants shall be implemented so as to guarantee equal access to positions for all interested candidates under equal conditions, and to guarantee the selection of the candidate who is the most professionally qualified for the performance of tasks in relation to the respective post. This principle is applied in relation to each vacant post, at least from the perspective of selecting the most professionally qualified candidate. Through the application of the criteria and implementation of this principle, competition, professionalism and efficiency are introduced into the civil service, while the potential for corruption is diminished.

As regards access to personal data of civil servants, it should be stressed that in accordance with the doctrine of the expectation of privacy - as endorsed by the ECtHR in the cases *Halford v. United Kingdom* and *Copland v. United Kingdom* - civil servants are not entitled to expect privacy as regards their names, title, post, salary, business address and those sections of a successful job application which denote the applicant's qualifications in relation to occupation of a particular work post. Due to this principle of openness, which requires transparent operations of a public-sector body with the objective of achieving a high degree of

participation by citizens in executing the power of state authorities, those employed within Macedonia's public sector thus automatically experience significantly reduced expectations of privacy than those employed in the private sector.

Data related to the employment relationship of civil servants should be examined prior to the publication in the media, to ensure it does not represent an exception from freely accessible public information. The criteria used to carry out such examination are usually laid down in the internal act on the organization and classification of posts of the public-sector body concerned, and/or in a public procurement specification.

All personal data pertaining to civil servants which is not related to their employment relationship such as home address, date and place of birth, names of parents, number and names of children, private telephone number, number of exams passed and average marks during the studies, as well as other qualifications that were not required for the post, etc., should be removed prior to publication. Such data does not represent freely accessible public information, and hence belong to the category of protected personal data.

Media Publication of Recordings and Photographs in Relation to Personal Data

Is it necessary to obtain the individual's consent prior to the publication of their photograph or voice or video recording in the media?

Person's photo is a set of relatively complete and detailed characteristics of an individual since a photo is the carrier which is a type of "technical copy" of individual's visual characteristics. Modern legal theory and case law agree that a photograph of an individual represents his or her personal data as long as the photograph resolution is sufficient to recognise facial, posture, clothing, location or movement features. With modern face recognition technologies (even those less sophisticated and publicly available such as Google image search) any individual is quite easily identifiable through a photograph.

To publish a photo, consent from the photographed person needs to be obtained; such consent needs to be given voluntarily. Permission is then valid only for a person to whom consent is given, and only for an agreed period, manner and purpose of the publication. Publication of a person's photo several times when the consent has been given only for a single publication or publication of a photo by multiple persons (e.g. in several media) is deemed an abuse of consent and consequently encroachment upon privacy of the photographed person. Publication without consent of the person photographed is only allowed when in public interest, which may generally be presumed for photos taken in public places, especially public events (photos from different events, photos of a park, street or square etc.), however explicit consent is required if the person photographed is the main highlight of the photograph and their presence or acting in such public place or event is of no specific public interest. Particularly, public figures should tolerate greater encroachment upon their

privacy in public places. Publication of such photographs is generally allowed unless the photo represents a snapshot of their everyday or intimate life.

When examining encroachments into the right to privacy and personality, it is important to realise that everyone, who attends a public event (as a performer or a spectator) must be aware there is a significant chance they shall be photographed and/or recorded.
An individual may not be photographed as the focal motif of a photograph which is then published. Nevertheless, photographing or otherwise recording a public event, as a record or documentary of that event, may also include an image of an individual. At a public venue, a private individual can expect more encroachment on their privacy and the right to privacy as such.

Publication of the image of an individual can be justified by a higher private or public interest. Such instances need to be decided on a case-by-case basis weighing the opposing interests. A conflict of opposing interests pertains to photos and recordings of contemporary personalities who in themselves evoke public interest. Legal practice has thus identified - and accordingly distinguishes between - two groups of personalities: so-called absolute persons and relative persons, they both enjoy a reduced degree of protection. The absolute group encompasses individuals who are under constant and longstanding public scrutiny, due to their role or function in society (e.g. politicians, public office holders, artists and athletes etc.), among them, some are deemed as public figures "*par excellence*". The relative group includes persons who are only of temporary public significance, most often due to their connection with a certain event or their role in public. Relatively public persons include, among others, perpetrators of crime (kidnappers, murderers etc.), winners of competitions or lotteries, as well as public servants etc. Taking of photos or making other such records of persons from either group without their consent is only permissible to a certain degree, proportionally to the importance of the event or their role and only concerning relevant data relating to that event or role. A relative personality in contemporary life can only be depicted during the period when they are - due to a certain event - deemed to be in the interest of the public, and not after that period. Attention should be paid in relation to both groups insofar that unmitigated or mere sensational or tasteless pursuit of the individual is not permissible, and nor is the publication of images or information which is either irrelevant or encroaches upon the intimate and private domain of the individual, having no relevance to the event, role or public interest.

A precedent in this area is the case of *Von Hannover v. Germany (no. 2)*, where the ECtHR decided the publication of the photos interfered with Princess Caroline's right to privacy. The Court stressed that the Princess often appears in public places where the media have plenty opportunities to photograph her, therefore there was no need to disturb the Princess in her private life. The ECtHR also warned the media that the publication of photos had not contributed to any political or public discussion. In balancing freedom of expression against the protection of privacy, the impact of the publication of the information (in this case photographs) upon the discussion in general should be decisive.

Unjustified visual or audio recording (clandestine surveillance or eavesdropping without the appropriate court order) can respectively represent an offence according to Articles 151 and 152 of the Criminal Code RM, only in the event, however, that such a recording or use of that recording would significantly encroach upon the privacy of an individual. An affected party can file a proposal to initiate a criminal prosecution for a suspected illegal recording at the competent State's Prosecutor's Office. Civil liability may apply as well.

Consent from the photographed person needs to be obtained to publish a photo and it needs to be given voluntarily. Permission is then valid only for a person to whom consent is given, and only for an agreed period, manner and purpose of the publication.

Publication without consent of the person photographed is only allowed when in public interest, which may generally be presumed for photos taken in public places, especially public events. Particularly, public figures should tolerate greater encroachment upon their privacy in public places. Publication of such photographs is generally allowed unless the photo represents a snapshot of their everyday or intimate life.

Publication of Personal Data which is the Result of an Analysis of Published Data

Is the publication of the list of 100 richest Macedonians admissible?

Pursuant to Article 16 of the Constitution of RM, freedom of personal conviction, conscience, thought and public expression of thought is guaranteed. The freedom of speech, public address, public information and the establishment of institutions for public information is also guaranteed. The notion of expressing opinion and conscience relates to spoken words as well as to images, the press, electronic media and all actions which have the purpose of expressing an idea or an opinion, or the presentation of news or information. Dissemination of information and opinions as well as receiving and collection thereof shall be guaranteed. This does not, however, mean that the freedom of expression extends merely to ascertainable data and information. The right arising from Article 16 of Macedonia's Constitution also extends to opinion, critique and speculation, which arises as well from the judgment of the ECtHR in the case *Lingens v. Austria*.[25] Moreover, in the case *Thorgeir Thorgeirson v. Iceland*[26] the ECtHR was of the view that the expression of opinion does not include any obligation to prove veracity or truthfulness.

The list entitled the 100 richest Macedonians, published in the media, could be in the domain of the constitutional right to freedom of expression, which represents predominantly speculation and assessment based on estimates, obtained through unarticulated criteria for analysis of public and/or publicly accessible information (e.g. share and securities registers, the Stock Exchange, the annual reports of companies, archives and information known to the media...). Such data is a matter of public record, whilst estimates and calculations and conclusions which may derive from them are to a degree speculative and hence do not represent personal data which would be protected by the LPDP.

[25] ECtHR, Lingens v. Austria, No. 9815/82, 8 July 1986.
[26] ECtHR, Thorgeir Thorgeirson v. Iceland, No. 13778/88, 25 June 1992.

Within the scope of exercising its constitutional right to freedom of expression - which also includes the right to estimate and guess - the media is free to publish a list of the 100 richest Macedonians, as long as this data is not derived from official databases.

In doing so it would not infringe the provisions of the LPDP, since the published material is not protected as personal data, but it is rather an estimation derived from publicly available data. However, certain degree of caution as to the protection of dignity and privacy of individuals in making such lists is advised, for civil liability may apply nevertheless.

The Scope of Personal Data Sources which may Supply the Media

Can a municipality supply the media personal data contained in a citizens' initiative calling for a referendum?

A public initiative calling for a local referendum, which, in accordance with Law on Referendum and Civil Initiative, includes the names of signatories, *is processed by a municipal authority*. The purpose of obtaining such data is to enable verification as to whether enough (genuine) voters have supported the initiative to require the calling of a referendum, as well as to simultaneously prevent abuse (e.g. fictitious or ineligible persons, impersonation etc.). Once it has been established that the initiative calling for a referendum has the requisite *bona fide* support, the names of the voters are no longer relevant as the purpose of the verification of collected votes has been achieved. Consequently, the personal data of those who gave their support for the calling of a referendum should not represent any part of the documentation in the further referendum procedure or the protection of their personal data should be provided in some other way.

Within the context of Article 6 of the LPDP, the abovementioned Law represents the legal basis for the collection of personal data for a single specific and lawful purpose; accordingly, unless otherwise provided by statute, this data may not be further processed in any manner contrary to the purposes for which it was collected – to verify the authenticity of the signatories and their eligibility. Any communication, further processing (e.g. supplying to the media) or otherwise making available data contained in the initiative would not be in accordance of the purposes determined in the Law on Referendum and Civil Initiative and would thus represent contravention of Article 6 of the LPDP. However, in extraordinary cases when serious doubts as to whether the competent authorities' decision on authenticity and eligibility of the signatories was correct, transfer and publication of certain data may be deemed as necessary in a democratic society and proportionate to the pursued legitimate aim of revealing authority's wrong doing.

The personal data of those who gave their support for the calling of a referendum should generally not be a part of the documentation in the further referendum procedure or the protection of their personal data should be provided in some other way.

Can a hospital supply data on the health status of a patient?

Article 8 of the LPDP, as a legal basis for the processing of sensitive personal data, which pursuant to Point 10 of Article 2 of the LPDP also encompasses data on health status, provides that processing may only be carried out if the individual has provided their explicit written personal consent for it.

The fact that the media may already be partially or completely familiar with the personal data, which they have obtained from other sources, does not provide a hospital or healthcare professional with any legal basis for the disclosure and/or supply of data contained in the medical documentation – only consent does.

Can the media publish the names and surnames of pupils which may occur in a document proclaiming parental support for a teacher?

The Law on Media RM does not define public interest within the meaning of Article 6 of the LPDP (for more on this see the answer to the second question in the second point of this chapter of the Guidelines) and hence it provides no legal basis for the processing of personal data in the case in question (listed names and surnames of pupils). The Law on Media's definition of publication in the public interest does not extend to content which is not remotely related to personal data, thus in this context and under this legislation the publication of personal data is unwarranted.

By publishing the names and surnames of pupils the media would, under Article 18 of the Constitution RM, contravene the right to protection of the pupil's personal data; such action would also be in contravention of Article 6 of the LPDP. Encroachments upon the rights deriving from Article 18 of the Constitution RM are not sanctioned in principle; potential exceptions need to be strictly assessed and only permitted if deemed urgent or pressing from the perspective of public interest, whereby the invasion of privacy would have to be carried out to the minimum possible extent. In such instance, it would also be necessary to carry out a strict assessment as to the encroachment of rights pertaining to the protection of personal data.

It is necessary to stress that the notion of public interest - if we regard it as something which is not determined or institutionalized by the legislator, but rather as something which is germane to some specific public - should not merely represent something which is interesting to the public. Popular curiosity and interest of the public is entirely different than an issue or information of public interest. Consequently, the former is no justification for any encroachment of the rights enshrined in Article 18 of the Constitution RM. Furthermore, it may be concluded that the freedom of expression and public interest do not provide a basis for railroading Article 18 of the Constitution RM or the provisions of Article 6 of the LPDP (for more information on the implementation of the principle of proportionality in practice, see the answer to the first question in the second point of this chapter of these Guidelines).

Technical and organisational measures in personal data protection

Every controller is required to implement sufficient technical and organisational measures to ensure compliance with data protection principles and regulations, specifically to ensure that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against un-authorized or unlawful processing and against accidental loss, destruction or damage. The controller should always be able to demonstrate that processing is performed in accordance with the regulation that apply. There are no general rules as to which concrete measures should be implemented – it is a result oriented requirement. However, several standards have been established and applied to personal data protection, ISO/IEC 27001 most common throughout the EU.

When implementing technical and organisational measures controllers should consider 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. A prior privacy impact assessment is advisable, so technical and organisational measures could be tailored considering the complexity and means of data processing (e.g. if processing includes profiling of individuals, automated decision-making and on-line storage, technical and organisational measures should be more restrictive), quality and quantity of data processed (e.g. if processing involves sensitive personal data and large sets of data, technical and organisational measures should be more restrictive) and size and type of the controller (e.g. if the controller is a large multi-national company with many subsidiaries and departments, technical and organisational measures should be more restrictive).

Technical and organisational measures mainly involve IT solutions, internal data processing regulation as to how concretely personal data should be processed, stored and transferred, clear internal responsibility and reaction plan in case of data breach, employees' training and technical and organisational measures revisions and update. Main two data protection principles should be considered – data minimisation and proportionality principle.

Technical and organisational measures for data protection by the media

While the media are somewhat privileged in the context of their important role as public watchdogs providing them with public interest as the legal basis for data processing, they are not in any way privileged in the aspect of providing personal data security.

All the general rules for defining and implementing appropriate technical and organisational measures apply to the media to the same extent as any other controller. Some obligations may be simplified in some countries (e.g. in Slovenia the media are not obliged to pass internal rules on data processing and establish a personal data filling system catalogue), however, the GDPR has no specific provisions concerning the media.
Probably the most important organisational measure for the media is awareness raising among and education of editors, journalists, investigators, photographers and cameramen.

They are the ones who are directly collecting and distributing personal data to the public, so they are the key factors in data processing within the media. They should be provided with sufficient legal support before publishing personal data. They should always act according to data minimisation and proportionality principles when collecting and publishing data, always considering the use of efficient anonymization techniques, especially when reporting about children, sexual abuse, criminal charges and health related topics. They should not build the story around the person, but around an issue or event and, while doing that, make as little as possible if not any collateral damage to the privacy of individuals involved.

Caution is necessary not to reveal personal data even in the process of collecting the data from different sources. They may not collect personal data under false pretences or with covert methods. Journalists should not use personal data in contravention with the purposes for which the data were initially collected.

When handling personal data media personnel should follow the so called clean desk and clean screen policy rules. This means they should never leave documents and other personal data carriers (such as USB keys and other data storage units) unattended or in plain sight for un-authorized persons to be able to get acquainted with personal data. Closets, drawers and offices where personal data is stored should be kept locked when unattended. Computers should be automatically locked after a reasonable period after last use with the use of user name and password. The use of cryptography methods is advised (in some countries, i. e. Slovenia, even required) when transferring sensitive data via telecommunication means or if storing them on the hard drive. Never use public internet connections when transferring personal data. Quality passwords should be generated (no names of pets, children, latest vacation spots or any dictionary words for that matter), passwords should not be shared with anyone or kept stored in obvious places (i. e. written on post-its under the keyboard). A good password includes letters in small and large caps, different symbols (such as &, %, #) and numbers. When disposing of personal data carriers, they should be destroyed efficiently (with the use of paper shredders or with overwriting techniques).

Other technical measures should be provided to media personnel by the management with the IT team support – i. e. firewalls, anti-malware and spyware, password quality and change reminders, backup, etc.

Probably the most important predisposition is to recognise when personal data is being processed ('personal data' means any information relating to an identified or identifiable natural person) and be aware that processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction and even plain insight.

Conclusion

Overall, the right to privacy (together with the right to protection of personal data), as well as the right to expression and information, can be deemed as exceptionally important human rights which can often collide. Journalists, editors, the media, must therefore undertake their work with a great deal of sensibility, while the information they provide must be true, up-to-date and verified. Reporting should not be insulting towards those who are the subject of it, and must not interfere with their privacy. Additional attention should be paid when juveniles or otherwise vulnerable persons are involved.

Notably, the interests of the individual's right to privacy together with the public interest and the right to information always need to be weighed. The general guidance is to weigh the interests, which was also performed by the ECtHR in the case of *Biriuk v. the Republic of Lithuania*,[27] where the court protected the right of privacy over the alleged public interest, when the headlines of a newspaper reported that living in a certain village was a thirty-year-old Gitana Biriuk, a mother of two children and who was infected by HIV virus. Since she was leading a promiscuous life and was looking for male company - which she had until then no problems finding - local wives were supposedly shaking with fear as to the lethal infection their husbands might contract, and hence had bought up all the condoms in the area... The provision of such information may be in the interests of some; however, its main intention was entertainment, titillation and sating public curiosity, which should not be the aim of serious professional journalists.

Nataša Pirc Musar, PhD

[27] ECtHR, Biriuk v. Lithuania, No. 23373/03, 25 September 2009.

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

342.738(497.7)(035)

ПИРЦ Мусар, Наташа
Заштита на личните податоци и медиумите : прирачник / [автор Наташа Пирц Мусар]. - Скопје : Дирекција за заштита на лични податоци, 2017. - 60, 51стр. ; 25 см

Насл. стр. на припечатениот текст: Personal data protection and the media : guidelines. - Обата текста печатени во спротивни насоки. - Текст на мак. и англ. јазик. - Фусноти кон текстот. - Публикацијата е во рамки на проектот "Заштита на личните податоци и медиумите" EuropeAid/132633/C/SER/multi со референтен број IPA TAIB 2012/9.11/ LOT7/15 и договор број 12-6340/1, финансиран од Европската Унија преку ИПА ТАИБ 2012 програмата

ISBN 978-608-4682-27-1

а) Медуми - Заштита на лични податоци - Македонија - Прирачници б) Право на приватност - Македонија - Прирачници
COBISS.MK-ID 103807242