Eglė Bilevičiūtė, Katažyna Mikša, Salvija Mulevičienė,
Žydra Klevinskaitė, Justė Bareišaitė, Kamilė Mekšriūnaitė,
Aliona Gaidarovič

Connecting not conflicting:

removing the tension between personal data protection and freedom of expression and information



Eglė Bilevičiūtė, Katažyna Mikša, Salvija Mulevičienė,
Žydra Klevinskaitė, Justė Bareišaitė, Kamilė Mekšriūnaitė,
Aliona Gaidarovič

Connecting not conflicting:

removing the tension between personal data protection and freedom of expression and information

Vilnius, 2023

Mykolo Romerio universitetas

This publication, was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

The content of this publication represents the views of the authors only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

ISBN 978-609-95598-8-9

© Authors, 2023
© Mykolas Romeris University, 2023
© MB „Spalvų kvartetas“, 2023

Content

PREFACE **5**

I. HOW TO MANAGE AND PROCESS PERSONAL DATA ON SOCIAL NETWORKS INTRODUCTION **7**

ABBREVIATIONS **8**

INTRODUCTION **9**

1.THE IMPORTANCE OF PERSONAL DATA PROTECTION ON SOCIAL NETWORKS: WHAT IS IMPORTANT TO KNOW AND .WHY? 11
2.HOW TO KNOW WHETHER YOUR SOCIAL MEDIA ACTIVITIES ARE SUBJECT TO GDPR PROVISIONS ON THE PROTECTION OF PERSONAL DATA? PERSONAL DATA AND HOUSEHOLD EXEMPTION 15
3.THE FUNDAMENTAL REQUIREMENTS OF THE GDPR THAT APPLY IF YOU PUBLISH PERSONAL DATA ON SOCIAL NETWORKS (OUTSIDE OF PERSONAL SPACE) 24
4.BETWEEN THE PROTECTION OF PERSONAL DATA AND FREEDOM OF EXPRESSION AND INFORMATION: HOW TO ENSURE THE BALANCE? 28
5. FREQUENTLY ASKED QUESTIONS 33

II. GUIDELINES ON THE PROVISION OF INFORMATION TO THE MEDIA AND PUBLIC SECTOR REPRESENTATIVES **40**

INTRODUCTION 41
1 KEY GUIDELINES 43
2 BALANCING TEST ALGORITHM AND BEST PRACTICES 47
3 TEMPLATES AND EXAMPLES OF PRACTICAL SITUATIONS 54
4 OBLIGATIONS WHEN PROCESSING PERSONAL DATA FOR JOURNALISTIC PURPOSES 61
5 EXERCISING AND DEFENDING RIGHTS 63
6 RELEVANT CASE LAW 64

III. RECOMMENDATIONS FOR JOURNALISTS AND PUBLIC INFORMATION PRODUCERS (DISSEMINATORS) **80**

INTRODUCTION 81
1 KEY PRINCIPLES 83
2 SAFETY AND SECURITY RECOMMENDATIONS
SAFETY RECOMMENDATIONS 92

IV. HOW TO PROCESS PERSONAL DATA FOR SCIENTIFIC PURPOSES? 107

ABBREVATIONS 108
INTRODUCTION 109
1 DATA PROCESSING FOR SCIENTIFIC RESEARCH PURPOSES 111
2 RIGHTS AND OBLIGATIONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA FOR SCIENTIFIC RESEARCH PURPOSES 120
3 SCIENTIFIC RESEARCH DATA MANAGEMENT PLAN. HOW TO DEVELOP IT PROPERLY? 130
SOURCES 136

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter the 'Regulation', the 'GDPR') imposed an obligation on all European Union Member States to ensure a high level of protection of personal data, at the same time obliging them to reconcile this right with the right to freedom of expression and freedom of information, including the processing of data for journalistic purposes and for purposes of academic, artistic or literary expression.

At first, the introduction of the GDPR did not seem to have brought any particular innovations and changes to the field of expression. However, with time the difficulties of application have become apparent. The challenges faced by those who seek to exercise the right to freedom of expression, in particular by the media, have proven to be of such importance that, at times, there have been questions in the public domain as to whether the right to freedom of expression itself was being restricted.

This is because neither the GDPR nor existing national legislation have provided clear guidance to the media, public administration authorities, users of social networks or the academic community on how to exercise one of the most fundamental rights, i.e. the right to freedom of expression, while at the same time guaranteeing a high level of protection of the right to protection of personal data.

This publication serves as a guide for users of social networks who process data for the purposes of journalistic expression. It recommends what to look out for when sharing information on social networks, what actions can lead to personal data breaches and where to go if you have any doubts.

It also provides practical details on how a public administration authority should deal with requests from journalists or other producers/disseminators of public information to provide material containing personal data. The publication as well sheds light on how to respond appropriately to different types of journalists' queries, how to carry out the balance test, when it is possible to refuse to provide information or to ask for clarification of a query, and when it is compulsory to provide information.

Producers/disseminators of public information and other persons processing personal data not necessarily for their own purposes are advised on ensuring the security of personal data collected or otherwise processed and on the organisational

technical measures to be used.

Members of the academic community who process personal data for the purposes of academic expression will find guidance on how to ensure high standards of personal data protection in research. Among other topics, this publication discusses the rights of the researcher conducting the research, such as the right to access information containing personal data, and the obligations to be respected in order to ensure the protection of personal data. It also provides guidance on how to prepare properly for the processing of personal data in the context of research.

We hope that everyone who processes personal data, regardless of the form of expression that is the purpose, will find answers to the questions on how to process data correctly, which will contribute to ensuring high standards of the right to protection of personal data in Lithuania.

This publication is an integral part of the EU-funded project CONCON: "Connecting not conflicting: removing the tension between personal data protection and freedom of expression and information". This publication contains only the views of the project promoters. They are fully responsible for the content. The European Commission accepts no responsibility for the impact that the information contained in this publication may have.

GUIDELINES:

HOW TO MANAGE AND PROCESS PERSONAL DATA ON SOCIAL NETWORKS?

ABBREVIATIONS

GDPR – Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC and applied since 25 May 2018 (General Data Protection Regulation)

ADTAĮ – Republic of Lithuania Law on Legal Protection of Personal Data

Charter – the Charter of Fundamental Rights of the European Union

EU – the European Union

CJEU – the Court of Justice of the European Union

ECHR – the European Court of Human Rights

MRU – Mykolas Romeris University

ŽEIT – the Office of the Inspector of Journalist Ethics, a supervisory authority

Data subject means a natural person whose personal data is processed.

Controller means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the data processing. Where the purposes and means of such processing are determined by EU or Member State law, the controller or the specific criteria for their appointment may be determined by EU or Member State law.

Processor means a natural or legal person, public authority, enterprise or other organisation that processes personal data on behalf of the controller

INTRODUCTION

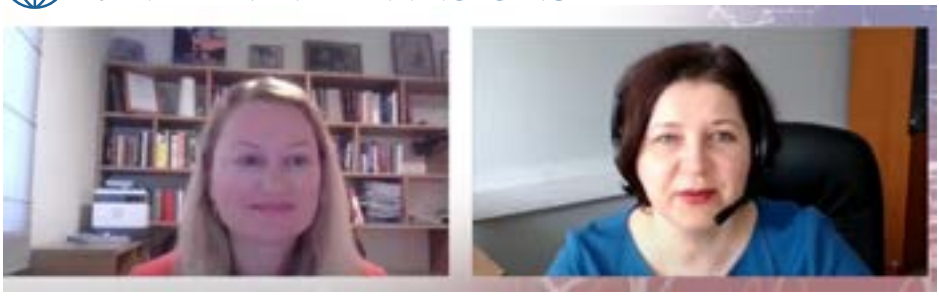
Freedom of expression on social networks has brought new challenges regarding the rights of individuals, especially the protection of personal data. As tendencies of content creators show, users of *Facebook, YouTube, Instagram, Discord, TikTok,* etc. are often not aware of the fact that they can be considered personal data controllers (processors) / public information producers (disseminators) who are responsible for the lawfulness of the processing of personal data published on their social accounts.

The General Data Protection Regulation (hereinafter the 'Regulation'), which came into force on 25 May 2018 throughout the European Union, including Lithuania, obliges all the Member States of the European Union both to ensure a high level of protection of personal data and to reconcile the right to the protection of personal data with the right to freedom of expression and information, including data processing for journalistic purposes. This need to process data for journalistic purposes can be encountered by each of us if we are active members of the public and publish information relevant to the whole public on our social media accounts, i.e. we carry out the activities of the so-called citizens' journalism, which is of crucial importance at the moment.

The Office of the Inspector of Journalist Ethics (ŽEIT, http://www.zeit.lt) is a supervisory authority with powers to act when personal data is processed for the purposes of journalism, academic, artistic or literary expression. The number of complaints addressed to the Office of the Inspector of Journalist Ethics and concerning the publication of personal data on social networks has been increasing. Therefore, we hope these guidelines will benefit all users of social networks.

This publication is an integral part of the EU-funded project CONCON, "Connecting not conflicting: removing the tension between personal data protection and freedom of expression and information ". For more information about the project, click the following link to see the record of the project opening event:

https://www.youtube.com/watch?v=lYGfEp4JlCI&ab_channel=NAME-EVENTPLANNINGAGENCY



Enjoy the read!

Project partners: Office of the Inspector of Journalist Ethics (ŽEIT) and Mykolas Romeris University (MRU).

THE IMPORTANCE OF PERSONAL DATA PROTECTION ON SOCIAL NETWORKS: WHAT IS IMPORTANT TO KNOW AND WHY?

Have you ever re-published information from another person's social network account on your own account, regardless of the personal nature of the given information?

Or, perhaps, someone has posted your photos or information with your personal data on social networks without your consent?

Are you aware of the types of information other people may share about you and the types of information you may share yourself?

How should you assess whether you can publicise or publish (in other words, process) the data of other persons on social networks if you aim to send a message of public interest to the whole of society? (e.g. you have recorded the behaviour of civil servants that is incompatible with the standards of their activity)

These are just some of the questions currently being raised as we all exchange information and opinions on social networks.

In practice, Lithuania is witnessing an increase in cases when people who are not satisfied with social media publications or records turn to the ŽEIT, indicating that this violated their right to the protection of personal data. Their statements are based on the Charter, which provides that every person has the right to the protection of their personal data and that such data must be properly processed and used only for specific purposes and only with the consent of the person concerned or on other legitimate grounds established by law (Article 8) and directly applying the General Data Protection Regulation, that has enshrined strict principles and standards for the protection of personal data across the EU.

THE MAIN SOURCES OF LAW ARE:

The General Data Protection Regulation (GDPR). Introduced in Lithuania on 25 May 2018, the GDPR has established uniform principles and standards for protecting personal data across the EU, and it shall be applied directly.	**Republic of Lithuania Law on Legal Protection of Personal Data** (ADTAI). Adopted on 30 June 2018 by a new version, it entered into force on 16 July 2018.

On the other hand, the Charter, the GDPR and national legislation establish that we have the right to freedom of expression. This right includes the freedom to have our own convictions, to obtain and disseminate information and ideas without hindrance by public authorities and regardless of borders.

The GDPR as well establishes that the right to the protection of personal data under this Regulation must be aligned with the right to freedom of expression and information, including the processing of data for journalistic purposes <...> (Article 85).

So these guidelines are for you if you have your own personal account on at least one social network (Facebook, Linkedin, TikTok, Instagram, Discord, etc.) and engage or intend to engage in at least one of the following activities on your social account at least once:

Activities on the social network	Have you ever conducted it, or have any plans to? (place for the tick)	Why and what is essential to know about properly protecting personal data?
Publishing photos of yourself	☐	It is important to know your rights and how to protect your personal data.
Publishing photos of yourself or other persons, children or other personal data (sensitive data)	☐	Sensitive data: it is important to know the special requirements of the GDPR and the ADTAĮ regarding consent to processing such data and strict restrictions.

Publishing photos of other persons or videos with their images (or other information entailing their personal data)	☐	It is important to know the grounds, principles and conditions for the lawful processing of personal data (consent, legitimate interest or other) and how to set privacy settings so that the so-called household exemption may cover your activities.
Publishing information about a person whose activity you are dissatisfied with (a neighbour who has upset you, a specialist who botched the task, an unfair trader) and indicating specific data such as name, residential address, telephone number or workplace	☐	It is important to know the grounds, principles and conditions of lawful processing of personal data and the practices regarding (not)using the social network as a platform for shaming.
Actively engaging in social networks by publicising information that is of interest to the whole public or by seeking to influence a wide range of people	☐	It is important to know the grounds, principles and conditions for the lawful processing of personal data and how the right to freedom of expression and processing of data for media purposes is to be reconciled with the requirements for the protection of personal data.
Sharing photos or posts on other persons' social accounts	☐	It is important to know the grounds, principles and conditions for the lawful processing of personal data (consent, legitimate interest or other) and how to set privacy settings so that your activities may be covered by the so-called household exemption.
Without indicating the person, sharing photos or videos with visible car plate numbers or a home address, from which one can clearly determine who you are posting information about	☐	It is important to know what is considered personal data and the grounds, principles and conditions of lawful processing of personal data.

You are a professional journalist, but you also post information on your personal social network account	☐	It is important to know the grounds, principles and conditions for the lawful processing of personal data and how the right to freedom of expression and processing of data for journalistic purposes is to be reconciled with the requirements for the protection of personal data.

Thus, if you have checked at least one box, it is crucial for you as a social network user to know:

- basic data protection rules,
- their scope and limits, and
- how to act when faced with two fundamental rights: the right to the protection of personal data and the right to freedom of expression and information.



II. HOW TO KNOW WHETHER YOUR SOCIAL MEDIA ACTIVITIES ARE SUBJECT TO GDPR PROVISIONS ON THE PROTECTION OF PERSONAL DATA? PERSONAL DATA AND HOUSEHOLD EXEMPTION

Usually, you are a data subject. However, in the context of the GDPR, you may as well be considered a personal data controller and obtain all the responsibilities of the controller if you post personal data of other persons (not your own) on your social media accounts in the form of speeches, photographs, audio or video recordings. Thus, are the GDPR provisions on personal data protection applicable to your account records?

Find out by answering the following questions:
The first question for you:

1. DO YOU PROCESS PERSONAL DATA ON SOCIAL NETWORKS?

The discussions in the social networking area and the questions addressed to the ŽEIT have revealed that it is often not clear to social network users what data is or may be considered to be personal data.

For instance, to combat car parking on the lawn, their photos with clearly visible public numbers are published in various social networking groups that unite the inhabitants of certain city areas (e.g. "Šeškinė", "Fabijoniškės" etc.).



As well, there is a tendency to publish photos of lost and found identity cards or other personal documents. Letters with the addresses of individuals are published as well. This reveals a problem – users of social networks, willing to do a good deed and to find the owner of a personal document, disregard potential threats and violate the right of those persons to the protection of personal data, as the data becomes available to an unspecified number of persons.

So – what is personal data?

As defined in the GDPR, "personal" data means

any information about an identified or identifiable natural person (living person).

The term' information' encompasses audio, video, genetic data, fingerprints, etc. This information can be provided in numbers, letters, graphic and photographic images, sound (via phone) and other forms.

A person can be identified:

- **directly**, using identifying data (e.g. by name, personal number, etc.) or
- **indirectly**, i.e. when the data available is not sufficient to identify a specific person, but it is possible to identify the person by using other data, regardless of whether the entity has it (e.g. car registration number, video data, telephone number, etc.).

Thus, even at first glance, information that is not essential but relates to a natural person should be considered personal data.

For clarity, let us analyse the following examples:

There are social networking groups for finding oneself a date, e.g. a Lithuanian group "Pamačiau, patiko, bet neišdrįsau" ("They caught my eye, but I was too shy"). Such groups do not have a direct purpose of disclosing personal data. Still, in a widespread case, a problem of unlawful processing of personal data arises when trying to find the person one liked. These groups encourage us to describe the person as detailed as possible and suggest connecting. For example: "I am looking for a lady I saw yesterday by the shopping centre "Akropolis" in a black Volkswagen Golf, plate number XXX XXX."

Although the name of such a person is not disclosed, the published data is sufficient to identify a particular person. Their presence at a particular time in a particular place becomes known. In this case, personal data are processed without consent and in the clear absence of any public interest.

N. B. It should also be noted that certain categories of data are so important that they are subject to special protection.

Such special categories of data shall entail:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- trade union membership;
- genetic data, biometric data that is processed for the purpose of identifying a person;
- health-related data;

data relating to a person's sexual life or sexual orientation.

According to the GDPR, this is more sensitive data and therefore requires more protection for their processing, as this type of data could lead to a higher risk to human fundamental rights and freedoms. For instance, they could cause a risk of discrimination against individuals.

What is not personal data?

A) anonymous information; personal data, rendered anonymous in such a manner that the data subject is not or no longer identifiable, shall no longer be considered personal data (anonymity must be ensured irreversibly);

(b) information about a deceased person;

(c) information about a legal person separate from its owners or managers (information on public authorities is also not to be considered as personal data. For instance, legal entity code, e-mail address, e.g. info@entity.com, is not personal data.)

The GDPR applies only to the protection of the rights of natural persons and does not apply to the protection of animal data. In practice, however, there have been cases where the protection of the personal data of animals is sought.

For example, the claimant contacted the ŽEIT and claimed that the veterinary clinic had unlawfully disclosed her puppy's personal data, i.e. made the health data of the animal public on their Facebook social network account. The GDPR does not cover animals. In such a case, a possible violation of the processing of personal data could only be considered if information about the puppy's owner was disseminated.

What is personal data processing?

'Processing of personal data' means … "means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

The GDPR therefore applies to the collection, use and storage of personal data:

- **Automatic** – in a digital form (e.g. in the information system, using video cameras, etc.);
- **Non-automatic** – in a structured set in paper form (for example, in card indexes, etc.).

More detailed explanation of the processing of data on a social network account is presented in one of the cases dealt with by the CJEU (Buivids, C-345/17,

https://curia.europa.eu/juris/liste.jsf?num=C-345/17&language=LT):

"Publication on a video website where users can upload, watch and share videos, such as the video in question containing personal data, is the processing of these data in a fully or partially automatic manner.

Without imposing access restrictions, S. Buivids published the video on the video website in question, where users can upload, view and share it, making personal data available to an indefinite number of persons, thus the processing of personal data at issue in the main proceedings is not merely a personal or household activity."

CONCLUSION: Therefore, any sharing of your notes, photos, videos or audio recordings containing personal data by making them available on social networks will be considered as processing of personal data.

Second question to you:

DOES A HOUSEHOLD exemption APPLY TO YOU?

Under the General Data Protection Regulation, individuals may share certain personal information when it is a personal or household care activity that is not related to a professional or commercial activity. Personal or household care activities may include, *inter alia*, correspondence, storage of addresses, or use of social networks and online activities carried out in the course of such activities. Such purely personal activities would not be subject to the strict data protection requirements of the GDPR.

Thus, in cases where you post information on social networks, whether in a closed group or on your personal account if the information relates only to your private life, interests, personal photos or videos, the disclosure of personal data is subject to the household exemption and the GDPR does not apply to such activities.

Here is an example.
on Facebook, a user posts holiday photos, where he is the only one captured, and shares it only with his "friends". GDPR requirements do not apply.

However, the household exemption cannot be applied to the information published on social networks without thinking – the household exemption depends on each case and its circumstances. The processing of personal data by a natural person when transferring such data ***to an unlimited number of addressees***, e.g. via the Internet, cannot be regarded as the processing of personal data by a natural person "engaged solely in personal or household activities"[1].

Therefore, it is very important to understand that this so-called "household exemption" applies only in rather rare cases, when your activity on the social network meets all of the following conditions:

1 Judgment of the Court of Justice of 6 November 2003 in case No. C-101/01

The application of the household exemption depends on several conditions:

- **content and the circle of persons about whom the information is published**. The posts published on the social network should be of a purely personal nature, where they are shared only between family and friends and only contain information about the posting persons themselves or those closest to the household/family circle.

- **purpose. The household exemption can only be applied if the purpose of sharing personal information** is not to achieve any commercial or professional benefits (for example, the household exemption would not apply to LinkedIn blogs of a professional nature, weblogs for marketing, sales of goods, advertising, etc.).

- **accessibility.** If your posts reach beyond the personal circle of you and your close ones and become available for an unlimited number of persons or a large circle of so-called "friends", the household exemption no longer applies (the number of members of the closed group is also important).

Thus, if you post information on your personal account for an unlimited number of persons or a very large number of so-called "friends" or in a closed group with hundreds or thousands of members and disclose personal data of other persons in it, you cannot be considered to process personal data in the social network exclusively for household activities. Therefore, the household exemption cannot be applied. This rule has also been established in the case-law of the CJEU:

The [household] exemption must be interpreted as providing only for activities which private individuals engage in within the limits of their private or family life, which is clearly not the case when processing personal data made available on the Internet and accessible to an indefinite number of persons. [CJEU, Lindqvist case, C-101/01].

Here are a few examples of distinguishing when the household exemption applies and when to obey all GDPR requirements.

Examples:

1) On Facebook, a closed group of up to 50 members was created for relatives to share relevant information about family life, events, share photos of family holidays. On this group, information about grandmother's illness and opportunities to visit her in the hospital is published. Although this disclosure of health data is carried out, in this case, after assessing the purpose for which the information is disseminated and its accessibility, it should be considered that only personal or household activities are carried out.

2) The personal Facebook account contains information about the person who unlawfully parked a car. This information is publicised for an unlimited number of persons and calls for the post to be "shared". In this case, the purpose of the publication of personal data and their accessibility to an unlimited number of persons does not allow to state that such publication of personal data is carried out only in personal or household activities.

3) The use of a system of video surveillance for making video recordings of individuals to be stored on a permanent recording device (such as a hard disk), given that this system has been installed by a natural person on their family house to protect the property, health and life of the owners of the house: when this system is also monitoring the public space, it shall not constitute processing of personal data carried out only for personal or household activities within the meaning of the GDPR. [CJEU, Rynes case, C-221/1

It is important to note that by using the privacy settings of Facebook and other social networks, it is possible to control the visibility and accessibility of the information posted on your accounts, i.e. whether anyone besides the account manager will see, whether the published information will be seen by friends of the given account or by any other person, which can even be not a registered user of the given social network.

For more information on the meaning of your account's privacy settings, see the following live event posted on the ŽEIT account on Facebook:

https://www.facebook.com/100069113293971/videos/123070759983533



In summary, if you process personal data on your personal account and the household exemption does not cover you, it means that your activities are subject to the GDPR and its requirements regarding the principles of personal data protection, the terms of processing and the rights and obligations of other persons. We will discuss this in the next part.

III. THE FUNDAMENTAL REQUIREMENTS OF THE GDPR THAT APPLY IF YOU PUBLISH PERSONAL DATA ON SOCIAL NETWORKS (OUTSIDE OF PERSONAL SPACE)

If, however, you, as the controller of personal data, have decided to publish on social networks information containing personal data, it is important to keep in mind the general rule: the processing is lawful only if it is justified by at least one of the conditions provided for in Article 6 of the GDPR (the same rules apply to all users of social networks):

1. **Consent of the data subject**
2. **For the performance of a contract to which the data subject is a party**
3. **Legal obligation**
4. **The person's vital interests**
5. **Public interest**
6. **Legitimate interest**

In practice, the following two conditions are relevant for social network users: either consent or the processing of personal data for journalistic purposes (for example, in the case of citizens' journalists' personal accounts, the condition of lawfulness is public interest).

CONSENT AND ITS TERMS

One of the conditions for the lawfulness enshrined in the GDPR is consent. Since the form of consent is not provided for by law, it can be expressed orally, in writing, and predictable from the conduct. However, it is essential that the controller can demonstrate that the data subject has given consent to the processing of their personal data.

It is important to note that when the data is published on social networks based on the data subject's consent, the person having given their consent has the right to withdraw the consent at any time, rendering their personal data no longer

allowed to be processed based on this consent.

For example, case-law has established that the consent to take photographs does not imply the consent to reproduce, sell, display, print a photograph in any way, as the fact that a person could agree to be photographed does not mean that they also give their consent to show the photo (ruling of the Supreme Court of Lithuania of 02 February 2003 in case No. 3K-3-294/2003). It is important to note that even a person in a public place has the right to express their unwillingness to be photographed, and their will must be respected, because being in a public place does not deprive them from their individuality and privacy.

Social media users often ask how to behave in such situations:

I was photographed by a photographer on the street, I posed and agreed that they would take pictures of me. After I saw my photo on Facebook, I decided that I don't want it to be published there. Can I withdraw my consent after a while and ask the photographer to remove the photo from the social network?

Although you have given your consent to take photographs by means of conduct, i.e. by posing, you can also withdraw such consent at any time.

As a teacher of first-graders, can I post photos with my students from the first day of the school year on my account?

Particular care should be taken when publicising the images of minors. Therefore, to publish photos of events at school or another place, you should obtain the consent of at least one of the parents/guardians.

Is it necessary to obtain the consent of the person to re-publish their photo or other information that they themselves posted on their public Facebook account?

Yes, it is necessary. Such information is related to the protection of private life, so further use of it requires the consent of that person. The fact that the person themselves has published their photo or disclosed other information related to it does not mean that it can be further published without consent. (Content on the public person's account revealing the circumstances or personal characteristics of the private life of this person that have a social significance could be re-published without consent.)

Can I post a photo on a social network showing a neighbour throwing rubbish in an inappropriate place?

You may not. It may be a legitimate interest for you and other neighbours, but such information would not be in the public interest.

I have information that one influencer, well-known in society, has undergone rhinoplasty. Can I share this information in public social networking groups?

You cannot because such information satisfies the public's curiosity and is about the private life of that person, which can only be published with their consent.

The evidentiality of consent and the possibility of withdrawal of consent raises some questions. The GDPR does not provide for the form in which consent to the processing of personal data must be given, but the controller (processor) must be able to prove that the consent has been given.

For example, the person addressed the ŽEIT, claiming that they did not understand that their data would be made public during the filming of a television broadcast and pointed out that they had not given written consent to such publicity. However, the public information producer (disseminator) explained that the claimant was aware in advance of the participation in the filming process, had a pre-agreed script, and had a microphone attached to them during the filming. It was explained as well that the filming was carried out by two cameras of professional operators; therefore, the claimant demonstrated, by not protesting against such actions and by their own conduct, clear consent to the collection and dissemination of data in the television program.

However, it is important to note that a mere conversation with a journalist without the purpose of giving an interview does not itself imply consent to the disclosure of the data learned during the interview.

Very often, people who have agreed to be filmed change their minds before the publication of the program and withdraw their consent in writing (for various reasons, such as unexpected filming and fright). However, public information producers (disseminators) are often not in a hurry to respond to such letters, claim that the program has already been designed and there is no possibility to quickly replace it with other content, so the information regarding whose publicising consent has been withdrawn, is still made public. It should be noted that the GDPR provides that the data subject has the right to withdraw their consent at any time. The withdrawal of consent must be as easy as giving it.

Before making information (such as a photo, where there are other persons besides you) publicly available on social networks, posting photos of other person's documents etc., you must evaluate whether the purpose of the information you want to publish cannot be achieved by other means.

For more information on the requirements for the processing of personal data on social networks, see the following record of a live discussion of the ŽEIT and MRU representatives:

https://www.youtube.com/watch?v=x0LEv1iqjsk&list=LL&index=4&t=1857s&ab_channel=NickPro

Thus, before posting the personal data of another person on social networks, make sure that the person agrees with such processing of their data and that you can prove the consent in case of a dispute. Because if you still plan to publish personal data of other person on social networks without consent or meeting other conditions of lawfullness set out in Article 6 of the GDPR (explained in detail in the next paragraph), you may become subject to the GDPR's liability.

IV. BETWEEN THE PROTECTION OF PERSONAL DATA AND FREEDOM OF EXPRESSION AND INFORMATION: HOW TO ENSURE THE BALANCE?

The GDPR explicitly states that the Regulation aims to reconcile two fundamental rights:

> the right to the protection of personal data under this Regulation shall be aligned with the right to freedom of expression and information, including the processing of data for journalistic purposes.

Article 4 of the ADTAI also explicitly provides for exemptions in cases where personal data are processed for the purpose of exercising freedom of expression and information:

> "where personal data are processed for the purposes of journalism or academic, artistic or literary expression, articles 8, 12-23, 25, 30, 33-39, 41 to 50, 88 to 91 of the Regulation (EU) 2016/679 shall not apply."

Thus, in Lithuania, as in all other EU Member States, the right to the protection of personal data under the GDPR must be aligned with the right to freedom of expression and information, **including the processing of data for journalistic purposes** and the purposes of academic, artistic or literary expression.

How to recognise when your social media activities are carried out for journalistic purposes, and what GDPR rules apply in that case?

First of all, according to the GDPR, each of us can carry out journalistic activities, regardless of the fact that we have not obtained a journalistic education and do not work in any of the media. Anyone of us can be a citizen-journalist as long as we are actively interested in the issues of society and seek to share information relevant to society as a whole on our social networks. Thus, to carry out the activities of a citizen-journalist, it is enough to have the opportunity to disseminate one's information to an unlimited number of persons on the Internet.



This is also emphasised in the case-law of the CJEU, in the aforementioned Buivids case specifically:

> Journalistic activity is an activity aimed at disseminating information, opinions or ideas to the public by any means of communication. The fact that S. Buivids is not a professional journalist does not mean that the production and publication of the video in question on a video website where users can upload, watch and share videos cannot be subject to this provision.

In the case-law of the CJEU, the processing of personal data for the journalistic purposes entails activities aimed at disclosing information, opinions or ideas to the public. Thus, when a public post containing personal data is published on a social network for the purpose of disclosing information to the public, such actions are regarded as processing of personal data for the journalistic purposes.

> N.B. However, it cannot be said that any information published on the Internet containing personal data falls within the concept of 'journalistic activities'. If the purpose of the information is not to disclose information, opinions or ideas to the public, it cannot be said that the processing of personal data was carried out solely for journalistic purposes (for example, this applies to information disseminated solely to satisfy curiosity).

It is also important that, even if we publish the knowledge that is important to society as a whole and thus wish to benefit from the 'journalism exemption', it is further necessary to assess whether such use of personal data is necessary for the dissemination of our message (necessity test) and whether it is a proportionate measure (balance test), i.e., whether the public interest and the public right to know in a particular case outweigh the right of natural persons to the protection of their personal data.

N.B. If you act as a citizen-journalist **on a regular basis**, keep in mind**: the public interest, necessity and balance test must be performed every time.**



Also, in order to reconcile the right to protection of private life and the right to freedom of expression, several criteria that the European Court of Human Rights established in its case-law should be taken into consideration:

- contribution to the discussion in general interest,
- the visibility and reputation of the person concerned,
- the purpose of reporting,
- prior behaviour of the data subject,
- the content and form of the publication,
- the manner and circumstances in which the information was obtained,
- and its compliance with reality.

Thus, the right to inform the public is not absolute and must always be aligned with other rights, including the right to privacy and data protection. The mere satisfaction of public curiosity is not a sufficient basis for the publication of personal

data on social networks.

You can find more about the activities of citizens-journalists and the protection of personal data on social networks in the following video of the discussion of the representatives of the ŽEIT and the MRU:

https://www.youtube.com/watch?v=WeByWJw4eLk&list=LL&ab_channel=MykolasRomerisUniversityLive



V. FREQUENTLY ASKED QUESTIONS

How to protect your personal data on social media?

The personal data of each person belongs only to them and cannot be disposed without an appropriate legal basis. The legal basis may be the permission of the person to disseminate the material, or public interest.

As well, information about private life may be published without the consent of the person in cases where it helps to reveal violations of laws or criminal acts, when the information is made available to the public in the course of the proceedings.

On social media accounts one may share the information they want without the permission of the persons concerned, given that information is not seen by a large group of people. In other words, given that you don't have more than 150 connections on your account, as well as if you have set up your privacy settings.

You can set them up in the personal account settings section of each social network. These settings will ensure that the information you post will only be visible to you and your friends. Also, you have the opportunity to publish individual posts and select settings for them – to choose whether the post will be visible to the public or only to your circle of friends.

Can I share photos of my friends/relatives from the event?

This question should be asked before the photos are published. If these photos contain only the people you know and they do not object to publication, you can share the photos.

However, if there are strangers in the photographs, they cannot be made public without the consent of those people.

The exemption applies in cases where the information is shared via private channels, for personal purposes or within a so-called household. These categories may include social media accounts that have their privacy settings set up, and the number of friends they have is not high.

When is it possible to share other people's private data publicly?

Private data of other people can be shared in the public space only with the consent of the person.

This information should not be shared without consent:

- Photos, videos published by individuals for personal use. The visual material published in their choice does not entitle other persons to freely share the material. Such a right arises only if this natural person is public, and circumstances of their life may have a public meaning.

- Person's workplace. This is personal information that cannot be made public without person's consent. There are cases when certain personal data of a person as an employee of the company can be made public for a reasonable purpose. However, such cases are analysed individually. Some data of employees working in public and state institutions may also be disclosed, provided that their disclosure is based on public interest.

- Family status and circumstances. This personal data may in no case be disclosed without the consent of the person, be it a public or private one.

Private personal data is defended and protected by legislation such as the General Data Protection Regulation, Republic of Lithuania Law on Legal Protection of Personal Data. Within the field of competence of ŽEIT, data is defended in accordance with the Law on Provision of Information to the Public.

The cases of violation are analysed by the responsible authorities and, if there is a presumption, may end up in law enforcement institutions. Offenders are required to take corrective action, i.e. remove the information, and may also be subject to an administrative fine.

How to recognise when personal data is processed for journalistic purposes?

In the case-law of the CJEU, the processing of personal data for the journalistic purposes entails nothing else but the activities aimed at disclosing information, opinions or ideas to the public.

What to do if you notice a photo (video) with you in it posted on the Internet without your consent?

First of all, contact the author or the account manager a specific social media account, requesting the material to be removed. The ŽEIT also recommends informing the specific social network that a photo of you has been posted without consent. The next step would be addressing ŽEIT or the court.

What if a former spouse places photos of a minor child on a social network without your permission?

First of all, discuss the use of the image with the former spouse. In the event of failure to have a fruitful discussion, request the former spouse to delete the photos in writing. If they do not respond, you can go to court (by the way, Facebook has embedded a special tool for parents, which can be used in similar situations). In this case, you should notify the social network about the violation of your rights or your child's rights and wait for a response. The social network must respond to your appeal and provide an answer.

Every person has a right to their image in publicly published photographs and videos. Does it always apply?

People are photographed/filmed during public events: if the video material does not specifically emphasise specific people, its publicity is allowed. However, if the captured specific people express their will to prevent the material from being shared publicly, the author of the video material must respect this desire.

Video material with children (minors) shall be made available to the public only with the consent of both – the children themselves and their parents or guardians. It should be noted that ŽEIT recommends obtaining a written consent. In the event of a dispute concerning the existence of the fact of consent, written consent would constitute a reliable evidence to support a particular position.

The protection of the right of image applies not only to the media, but also to social networks. The consent of the persons to be published must be obtained.

Do I have the right to share photos of other person on my social networks?

You have this right only if you have obtained that person's consent. The publicising of such information is related to the protection of private life. The photos publicised or information disclosed by the person themselves do not in any way imply that anyone can further share and publicise them on their accounts.

The exemption applies to photographs and information on public persons, provided that their life circumstances have a social significance.

Does personal data protection also apply to publishing information on a private social network account or in a closed group?

Under the General Data Protection Regulation, individuals may share certain personal information when it is a personal or household care activity that is not related to a professional or commercial activity.

The application of the household exemption depends on several conditions:

- Content. The social media records may be of a purely personal nature, shared with family and friends, or, conversely, entail published information about other persons.
- Purpose. Whether the purpose is to share personal information or to pursue commercial and professional benefits (for example, Linkedin blogs, video blogs).
- Accesibility. Whether the records are accessible for an unlimited number of persons or only for family and friends. The number of members of a closed group is also important.

Is it possible to publicise images of private persons (migrants) without their consent?

Consent is not necessary for the filming or taking photos of general nature. In other cases, the protection of privacy is applicable; therefore, the consent of the person is required.

Consent can also be expressed through conduct when the person clearly agrees to be filmed or photographed.

We recommend producers and disseminators of public information get the

person's written consent. In the event of a legal dispute or a person complaining to the Office of the Inspector of Journalist Ethics about a breach of privacy or personal data, the public information producer and disseminator should prove that the consent has been obtained.

What functions does the Office of the Inspector of Journalist Ethics (ŽEIT) perform?

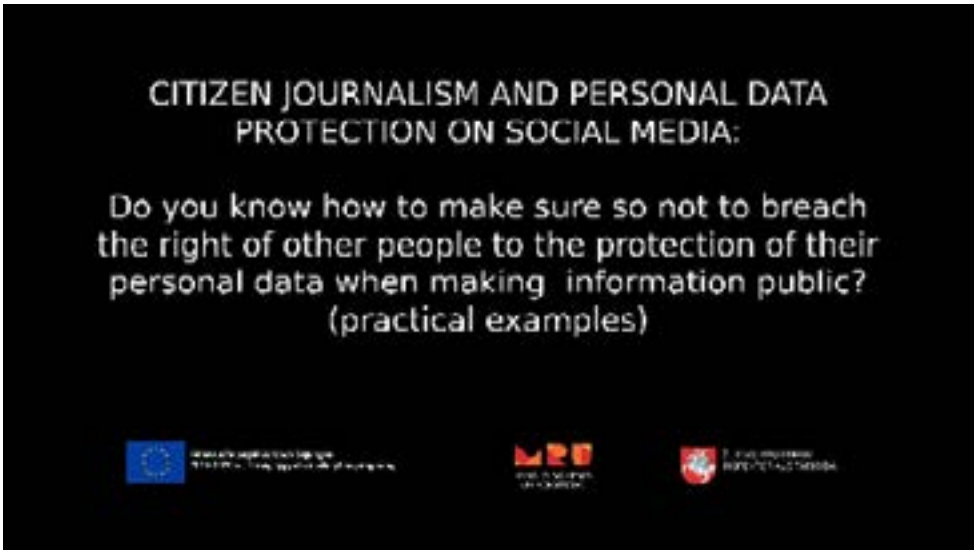
As the name implies, the ŽEIT is an institution primarily concerned with supervising journalists and assessing their ethics. However, the role of the ŽEIT is much broader.



The Inspector of Journalist Ethics supervises the dissemination of virtually all public information in the media, regardless of who is its producer (disseminator), and examines complaints of stakeholders concerning the violation of their honour and dignity in the media, the right to protection of private life and the violation of the processing of personal data. Each situation is unique in the subjective perception of moral rights and realisation of freedom of expression, thus, it as well differs when it comes to the search for the balance of rights and priority determination.

Thus, one of the main functions of the ŽEIT is to deal with complaints by interested parties about violation of their honour and dignity in the mass media, the right to protection of private life, as well as complaints by data subjects under the GDPR concerning the processing of personal data for the purposes of journalism, academic, artistic or literary expression.

The handling of complaints shall be carried out in strict compliance with the requirements laid down in Law on Provision of Information to the Public and Law on Legal Protection of Personal Data. They provide for the function of the activities of the ŽEIT, i.e. ensuring the proper implementation of the public interest – freedom of expression and freedom of the press, as well as provision of information to the public.



In what situation are individuals found in breach of GDPR provisions?

- Photos of personal identity documents being uploaded to inform about unreliable sellers, professionals who do not perform work on time, persons who have not repaid their debts;
- Publication of improperly parked cars with visible public numbers;
- Informing about specific persons having been infected with COVID-19, although there is no need or prevention of possible infection/contact;
- Disagreements between neighbors and videos with personal data made public;
- Disagreements between divorced parents regarding uploading photos of the child to social networks;
- Publishing information, which does not satisfy the public interest but raises public curiosity, the desire to learn the sensations. Or funny, mocking information.

If you have any further questions, address them on the website www.zeit.lt or the Facebook page of the Office of the Inspector of Journalist Ethics.

Mykolo Romerio universitetas

Projektas finansuojamas Europos Sąjungos Teisių, lygybės ir pilietybės programos lėšomis

ŽURNALISTŲ ETIKOS INSPEKTORIAUS TARNYBA

GUIDELINES ON THE PROVISION OF INFORMATION TO THE MEDIA AND PUBLIC SECTOR REPRESENTATIVES

(Guidelines on the provision of information held by public sector bodies and which contains personal data to the media representatives)

PLEASE PROCESS PERSONAL DATA RESPONSIBLY!

INTRODUCTION

The cases where access to data by journalists is restricted under the excuse of personal data protection standards often hit the media headlines and this harms the right of the public to know information which is of public interest. This problem has become particularly acute in Lithuania following the application of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter also the GDPR). Contrary to its nature, the GDPR is often used by state and municipal authorities and bodies as a cover to avoid unwanted attention from the media on topics of public interest.

As one of the GDPR supervisory authorities, the Office of the Inspector of Journalist Ethics (hereinafter - OJEI) provides advice, explanations and opinions to the stakeholders on issues related to the balance between the journalists'[1] (the public) right to information and the protection of personal data. We note that the number of problematic situations concerning the right of media representatives to receive information from public sector entities (public authorities[2]) is not decreasing, and therefore there is a need for a broader awareness of public sector institutions on the essential criteria and rules to correctly determine the relationship between the right to information and the right to data protection of journalists under the GDPR. This need and the acquired institutional experience have led to the development and publication by the OJEI of practical guidelines for the provision of information held by public sector institutions and containing personal data to the media ('the

1 The term "journalist" is used in the Guidelines in a broad sense: it covers both the concept of a journalist as set out in the Law on the Provision of Information to the Public and other producers and/or disseminators of public information who are entitled to process personal data for journalistic purposes.

2 The term "public authority" is used in its broadest sense and, taking the Council of Europe Convention on Access to Official Documents as an example, covers all public sector bodies (at central, regional or local level), depending on the functions performed by the authority rather than its name, and includes public administration bodies, legislative bodies and judicial bodies, if they perform administrative functions under national law; natural or legal persons, insofar as they act with administrative powers or perform public functions or manage public funds in accordance with national law.

Guidelines').

This document sets out in a clear and coherent manner a specific sequence of actions, an algorithm for responding to (acting upon) a request from a media representative for information containing personal data. Taking into account the most common questions raised by public sector bodies, this document provides ground rules and guidance on the criteria for assessing the provision of personal data. The guidelines explain in more details the definition of the purpose/activity of journalism, the details for determining the eligibility of the subject, the impact of the classification as a public figure and the public interest in the decision-making process for the provision of data, etc. Practical tips, templates, examples of standard answers, analysis of the relevant legal framework and case law should help to apply the GDPR effectively and to remove unjustified barriers.

The culture of public administration is based on the principles of transparency, accountability and openness to the public. Media representatives requesting information containing personal data from public sector bodies must ensure that the further processing of the data is lawful and fair. This interaction between the public sector and the media in the area of data accessibility based on mutual commitments best reflects the importance of freedom of expression in a democratic society. These Guidelines are a guidance document. They do not seek to solve all problems of interpretation of the GDPR or to provide universal answers to all questions. Each data processing situation must be assessed individually, taking into account the details of each case. We hope that these Guidelines will serve as a guide to help public sector bodies to make an informed assessment of the proportionality of the data to be processed/provided, to provide information and personal data to journalists in a transparent manner, and to strike an effective balance between freedom of information and the protection of personal data. The guidelines do not reduce the requirements for the protection of personal data or otherwise restrict the data subjects' rights to control their data. On the contrary, both in its day-to-day work and in these Guidelines, the OJEI aims to uphold the highest standards in the protection of personal data and encourages the proactive assertion of the right to data protection where the violation has occurred as a result of the processing of personal data for the purposes of journalism. The active position of each data subject in seeking redress in cases of a possible violation of his or her right to data protection is a guarantee of both the dynamism of the protection of this right towards improvement and the high standards of journalistic practice.

CHAPTER I
GUIDELINES AND RECOMMENDATIONS

PART I
KEY GUIDELINES

1. Data collection and acquisition is an essential preparatory step in journalism, an integral and part of media freedom that should be protected[3] . A clear distinction must be drawn between the requirements for the collection of data by a journalist for the purpose of producing a publication or other form of work (e.g. a report, a social media post, etc.) and the requirements for publishing an article or some other form of work (i.e. the widespread dissemination of such data). It is up to the journalist to decide what personal data is necessary and to what extent at the stage of article writing or other form of work. The journalist to whom the personal data have been communicated assumes full responsibility for their proper use and for assessing what data he or she will be able to disclose in the publication or other form of work, taking into account their necessity, proportionality, the possibility of anonymisation and the interests of the data subject. Once an article or other form of work has been published, and in the event of a dispute as to the compliance of the published information with the requirements of the protection of personal data, the media outlet/journalist will be required to justify to the supervisory authority and/or in court that it has carried out this assessment in a responsible manner.

2. The law does not prohibit the public sector from providing personal data to journalists, so a refusal to provide information merely stating that the requested information contains personal data and therefore cannot be provided, or cannot be provided under the GDPR, is an unreasoned response in breach of the principle of good administration and therefore, on its own, constitutes grounds for declaring it unlawful. The GDPR applies to the processing of personal data relating to citizens of the European Union by a natural person, undertaking or organisation. It does not apply to the processing of personal data of the deceased or legal persons.

3 ECtHR, *Magyar Helsinki Bizottság v. Hungary,* No. 18030/11, § 165, 8 November 2016 ("Finally, it is well-established that the gathering of information is an essential preparatory step in journalism and an inherent, protected part of press freedom". See also the ruling of the Supreme Administrative Court of Lithuania of 3 February 2022 in administrative case No eA-51-822/2022.

3. A public authority, upon receiving a request from a journalist to provide information held by a public institution which contains personal data ('the information request'), must in all cases carry out a balancing test between the protection of personal data and the right to freedom of expression and freedom of information (the 'balancing test'). However, the application of the balancing test in cases where information is requested for journalistic purposes in order to exercise the right to freedom of expression and freedom of information **has specific features compared to other requests for information**. These peculiarities arise from the special role of the media in ensuring the respect and preservation of democratic values. In accordance with the provisions of Article 7(2) of the Law on the Legal Protection of Personal Data, the Inspector of Journalists' Ethics supervises the processing of personal data for journalistic purposes and for the purposes of academic, artistic or literary expression. **This means that in cases where a media representative requests a public authority information containing personal data, the legal relationship resulting from such a request falls within the scope of supervision of the OJEI**. When investigating the lawfulness of the processing of personal data, the OJEI will check whether the public authority from which the data was requested has carried out the test for the protection of personal data and the balancing test between the right to freedom of expression and the right to information and whether the media representative has abused his or her right to collect and disseminate information.

4. The essential feature is that, on receipt of a request for information from a media representative (meaning only written requests), and in the context of the balancing test, the public authority has only to get assurance:

that a request for information refers to the exercise of freedom of expression and information as a condition for the lawful processing of personal data, where the personal data are needed for the purposes of producing a publication or other form of work for the purpose of informing the public about matters of importance to the public (to provide the public with socially relevant information, opinions or ideas), i.e. where there is a legitimate interest.[4] . This processing condition does not have to be described in legal language, but it is important that the public authority is able to draw the reasonable conclusion from the request that the data are requested

4 "The right to freedom of expression and freedom of information may qualify as a legitimate interest within the meaning of Article 6(1)(f) of the GDPR." Ruling of the Supreme Administrative Court of Lithuania of 3 February 2022 in administrative case No eA-51-822/2022.

for journalistic purposes and not for personal, commercial or other purposes[5] . A journalist can properly indicate a legitimate purpose if he or she indicates that the data are needed for journalistic purposes, for example for producing a publication, or if he or she refers to Article 6(1)(f) of the GDPR, or if he or she indicates that he or she is exercising freedom of expression and information;

that the request for information has been filed by an appropriate entity, i.e. a journalist or other producer and disseminator of public information (e.g. a non-governmental organisation working in the field of human rights or anti-corruption and disseminating information to the public). If there is a doubt whether the eligible entity has requested the information, the institution may request the clarification of the status. The journalist[6] is an eligible entity. Where an entity other than a journalist files a request (e.g. a social media account manager, vlogger, blogger), the institution must get assurance that the entity is a producer and/or disseminator of public information (see more in Part II);

that the information requested is necessary for a legitimate purpose; however, this requirement is applied in the case of the media in a particular way: where the data are requested by an eligible subject with a legitimate purpose, namely the use for journalistic purposes, **it is presumed that the criterion of necessity is met**, provided that no special categories of personal data are being requested (on health, on sexual orientation, etc.[7]). In other words, the fact whether the information requested is necessary for a publication or other form of work in the public interest can only be assessed by the media representative himself.

Requiring a public authority to disclose in advance the content of a publication or other form of work that is still in preparation, or to question its necessity or relevance to society, would constitute censorship, which is prohibited in democratic societies. It is not for the public authority, but for the media themselves to decide

5 Even if a person is a well-known journalist, he or she has the right to ask for non-journalistic data, but then his or her request does acquire any special status - it has to be subject to an ordinary, comprehensive balancing test.

6 A journalist is a natural person who professionally collects, prepares and submits material to a producer and/or disseminator of public information on the basis of a contract with that producer and/or disseminator and/or is a member of a professional organisation of journalists (Article 2(85) of the Law on the Provision of Information to the Public).

7 Article 9 of the GDPR specifies that special categories of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data used for the purpose of specifically identifying a natural person, data concerning health, or data concerning a natural person's sexual life and sexual orientation.

what is important to report to the public. Only media supervisory authorities, as well as the courts and the pre-trial dispute resolution bodies, can decide whether the media have taken the right decision to publish certain data and only to the extent necessary, i.e. whether the published information complies with the requirements for the protection of personal data, by assessing the content of the published publication or any other form of work.

The media representative is solely responsible for ensuring that the personal data are used exclusively for the purpose for which he or she has indicated, i.e. to produce, for example, a publication on a matter of public interest, once he or she has received the information. Failure to publish does not make the collection unlawful. Only after the data have been obtained and checked against other information can it become apparent both the content of the publication and the absence of a message of public interest. Some journalistic investigations may last for years, and no one has the right to require a journalist to identify, for example, the title of the publication, the substance of the content, or to indicate when and where he or she intends to publish his or her investigation.

In order to ensure a balanced application of the legal framework, the responsibility of the media itself for the improper use of personal data in publications or other forms of works needs to be clearly communicated, and decision-makers need to assess whether the remedies available to a person whose data may have been published in violation of the requirements of the legislation on the protection of personal data are effective and appropriate. The journalist/media outlet is under an obligation to put in place, from the moment of receipt of the data, technical organisational measures to ensure the security of the personal data it receives, collects or otherwise processes. It is the journalist/media outlet that has the obligation to ensure that the data processed are not 'leaked', lost or otherwise compromised. Moreover, personal data obtained for the purpose of journalism can only be processed for this purpose.

A public authority cannot be held liable for non-compliance with the requirements for the protection of personal data if it has complied with a journalist's request to provide information containing personal data, having duly carried out this balancing test, which is tailored specifically to the specific role of the media in a democratic society and to ensure the balance between the protection of personal data and freedom of the press.

In cases where a public authority is not able to provide certain information because of personal data protection requirements, but on the basis of other legitimate

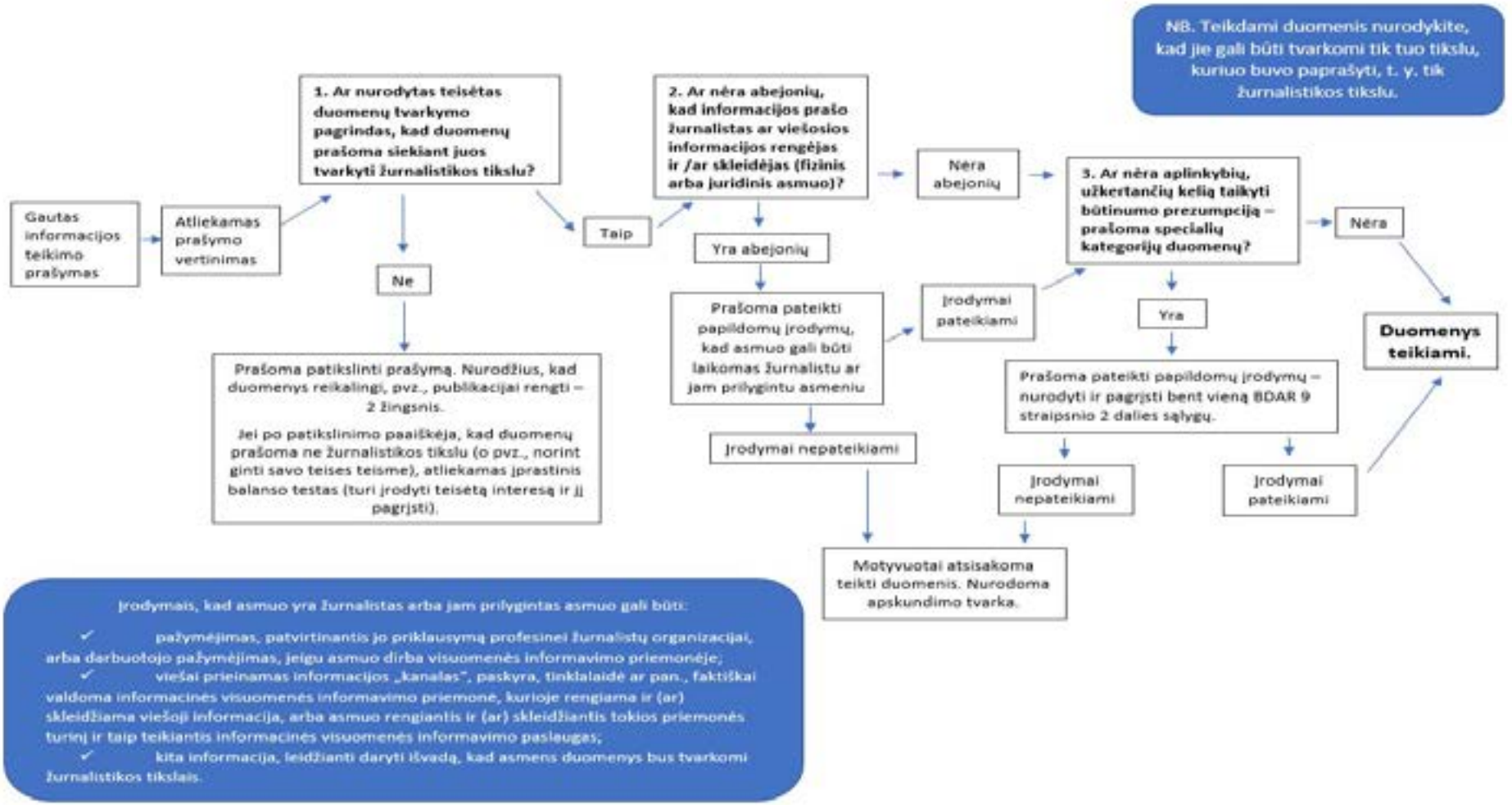
grounds for refusal, such as professional secrecy, compliance with the requirements of the legislation on legal proceedings or prosecution, etc., the specific ground for refusal should be specified and should not be based on a general reference to the GDPR, since the GDPR does not contain any general prohibition on the provision of information to journalists containing personal data.



PART II

BALANCING TEST ALGORITHM AND BEST PRACTICES

Below, we outline the recommended actions and explain how to carry them out in a step-by-step manner, with practical examples.


NB. Teikdami duomenis nurodykite, kad jie gali būti tvarkomi tik tuo tikslu, kuriuo buvo paprašyti, t. y. tik žurnalistikos tikslu.
Gautas informacijos teikimo prašymas
Atliekamas prašymo vertinimas
1. Ar nurodytas teisėtas duomenų tvarkymo pagrindas, kad duomenų prašoma siekiant juos tvarkyti žurnalistikos tikslu?
Taip
Ne
Prašoma patikslinti prašymą. Nurodžius, kad duomenys reikalingi, pvz., publikacijai rengti – 2 žingsnis.
Jei po patikslinimo paaiškėja, kad duomenų prašoma ne žurnalistikos tikslu (o pvz., norint ginti savo teises teisme), atliekamas įprastinis balanso testas (turi įrodyti teisėtą interesą ir jį pagrįsti).
2. Ar nėra abejonių, kad informacijos prašo žurnalistas ar viešosios informacijos rengėjas ir /ar skleidėjas (fizinis arba juridinis asmuo)?
Nėra abejonių
Yra abejonių
Prašoma pateikti papildomų įrodymų, kad asmuo gali būti laikomas žurnalistu ar jam prilygintu asmeniu
Įrodymai pateikiami
Įrodymai nepateikiami
3. Ar nėra aplinkybių, užkertančių kelią taikyti būtinumo prezumpciją – prašoma specialių kategorijų duomenų?
Nėra
Yra
Prašoma pateikti papildomų įrodymų – nurodyti ir pagrįsti bent vieną BDAR 9 straipsnio 2 dalies sąlygų.
Įrodymai nepateikiami
Įrodymai pateikiami
Duomenys teikiami.
Motyvuotai atsisakoma teikti duomenis. Nurodoma apskundimo tvarka.
Įrodymais, kad asmuo yra žurnalistas arba jam prilygintas asmuo gali būti:
✓ pažymėjimas, patvirtinantis jo priklausymą profesinei žurnalistų organizacijai, arba darbuotojo pažymėjimas, jeigu asmuo dirba visuomenės informavimo priemonėje;
✓ viešai prieinamas informacijos „kanalas", paskyra, tinklalaidė ar pan., faktiškai valdoma informacinės visuomenės informavimo priemonė, kurioje rengiama ir (ar) skleidžiama viešoji informacija, arba asmuo rengiantis ir (ar) skleidžiantis tokios priemonės turinį ir taip teikiantis informacinės visuomenės informavimo paslaugas;
✓ kita informacija, leidžianti daryti išvadą, kad asmens duomenys bus tvarkomi žurnalistikos tikslais.

Applying the algorithm to specific situations and practical examples

The authority receives a request for information from a journalist. After an initial assessment it is established that the information requested contains personal data (e.g. the request to indicate who has won the competition to become the Director of Finance Department of the Institution and whether he or she has a family or other close link to the Head of the institution, and if so, the nature of that relationship).

Step 1

It must be verified that the request for data states the lawful basis and/or purpose of data processing.

As the request is filed by a journalist, we first check that he or she indicates that the data is needed for journalistic purposes. The purpose of journalism is not to provide news to the public in any way, but only to inform the public about matters that are important to them. For example, the purpose of informing the public about a plastic surgery performed by a civil servant (if it was not financed from the state budget), although satisfying the public curiosity, would not be considered a journalistic purpose in the context of GDPR.

The exact wording of the request is not important, nor is the journalist obliged to identify the specific points of the GDPR or other legislation on which he or she relies. What is important is that the request makes it clear to a prudent and reasonable person that the data is needed, for example, for the preparation of an article, to inform the public about issues of importance to them, and not for personal, commercial or curiosity reasons.

Examples of an appropriate wording:

"Please provide me with information on the successful candidate for the post of Head of the Finance Unit of the XX Institution and whether he/she has any family or other close links with the Head of the Institution and, if so, the nature of the relationship. *The information is necessary for the purposes of investigative journalism*".

"Please provide me with information on the successful candidate for the post of Head of the Finance Unit of the XX Institution and whether he/she has any family or other close links with the Head of the Institution and, if so, the nature of the

relationship. *The information is required for the purpose of preparing a publication on a matter of public interest"*.

"Please provide me with information on the successful candidate for the post of Head of the Finance Unit of the XX Institution and whether he/she has any family or other close links with the Head of the Institution and, if so, the nature of the relationship. *We are requesting the data on the basis of Article 6(1)(f) of the GDPR in the exercise of the freedom of expression and information*".

"*For journalistic purposes*, please provide information on the successful candidate for the post of Head of the Finance Unit of the XX Institution and whether he/she has any family or other close links with the Head of the Institution and, if so, the nature of the relationship".

Such a justification is sufficient to support a legitimate interest in receiving the data.

If the request does not specify the purpose for which the data is needed, but the public authority has no doubt that the data are requested for journalistic purposes (e.g, data is requested by a journalist accredited by that institution and who regularly reports on the activities of that institution), the public authority may, in accordance with the principle of reasonableness, provide the data only if it can, in the event of a dispute, provide objective arguments as to why it had no doubt as to the legitimate basis of the journalist's request for the data (e.g., it is clear from previous correspondence what the purpose of the data is, the journalist has communicated in another way that he or she is working on a publication, etc). Even in cases where the journalist is accredited by a particular institution, he or she should be encouraged to indicate the purpose for which the data are collected.

If the request merely states that the data are needed, for example, for a publication, but does not indicate whether the publication relates to matters of public interest (and not merely to satisfy curiosity), this wording is sufficient if the nature of the data requested shows that it relates to matters of public affairs. The legislation does not provide a list of areas of public interest, so in each case it would be necessary either to assess the nature of the information requested and to draw a conclusion that would lead to believe that the publication or other form of work is of

public interest (e.g. where the request is for information related to public finance[8]), or to ask the journalist for a confirmation that the data requested is necessary for the purpose of publishing on matters of public interest.

If the request does not specify the lawful basis and/or purpose of the processing, the request must be returned to provide with more details. If the request is not supplemented with the details or is refused to be supplemented, the public authority shall refuse to grant the request and shall give reasons for refusing to provide the data: if the applicant does not specify the basis and/or purpose of the processing, it cannot be assumed that the data are necessary for journalistic purposes.

NB. The authority receiving the request may not require the journalist to disclose the content of the publication or other form of work, to specify where and when the data will be published, or to question whether the data requested by the journalist is really relevant for the purposes of informing the public. Only the journalist himself/ herself may carry out such a verification. Any attempt by the public sector to tell the media what issues it can collect information on, or a decision of a public authority on what constitutes public interest, would amount to censorship and would be incompatible with the principle of the democratic state and the obligation to reconcile the protection of personal data with the freedom of information and freedom of expression, including the processing of data for journalistic purposes.

Step 2

It must be verified that the information containing personal data is requested by the appropriate subject, i.e. the journalist or other producer and/or disseminator of public information.

According to Article 2(85) of the Law on the Provision of Information to the Public , a journalist is a natural person who professionally collects, prepares and submits material to a producer and/or disseminator of public information on the basis of a contract with that producer and/or disseminator, and/or who is a member of a trade union of journalists.

8 "The case-law makes it clear that the administration of public funds and property is a matter of general interest and ongoing public debate, and that there must be very good reasons for restricting freedom of expression in this area." Ruling of the Supreme Administrative Court of Lithuania of 3 February 2022 in administrative case No eA-51-822/2022.

If there are doubts about whether a person claiming to be a journalist is eligible to act for journalistic purposes, he or she may be asked to produce his or her employee's certificate or a document proving his or her membership in a trade union of journalists, but it is not necessary for a journalist to produce his or her identity document. If there are no such doubts, e.g. if the journalist is an accredited journalist, a well-known journalist, etc., there is no need to ask for proof of his/her status as a journalist.

However, entities other than journalists can act for journalistic purposes. A person, e.g. a social network account manager, a blogger, does not have to have a contract with a specific editorial office or belong to a trade union of journalists to produce and publish information, news or opinions for the public.

Different online TV channels, social network accounts, podcasts, blogs, social network accounts with a lot of followers are all means by which information is constantly disseminated to the public. Although the controllers of such sources of information would not be considered journalists for the purposes of the Law on the Provision of Information to the Public, such persons are, for the purposes of the Law on the Provision of Information to the Public, producers/disseminators of public information, who prepare and/or submit public information for dissemination or disseminate public information to the public and are responsible for the legality of that information in accordance with the provisions of this and other laws.

Moreover, it is not only natural persons who produce and publish information, opinions or ideas for the public - legal persons, such as non-governmental organisations, public bodies, associations, etc., can also engage in such activities.

The actual activities of the one who requests the data (who is not a journalist in the strict professional sense) must be taken into account when deciding whether the data subject is eligible to act for journalistic purposes:

the nature and purpose of its activities to conduct and publicize research in the public interest, and to present information, opinions or ideas of social relevance to the public;

consistency and systematic nature of the activity;

whether it has its own publicly accessible information 'channel', account, podcast, etc., or effectively manages an information society media outlet for the production and/or dissemination of public information or produces and/or disseminates the content of such an outlet and thereby provides information society services;

whether the information produced is publicly available (channels content of

which is only available to subscribers are considered to be publicly available).

Thus, if there is any doubt as to whether a person, e.g. the manager of a social networking account or an employee of an organisation claiming to be acting for journalistic purposes, is a journalist, it is recommended to ask for the publicly accessible information channel, podcast, website or other media outlet actually operated by the person or organisation in question, where the information is published. Failure to provide information shall constitute grounds for a reasoned refusal to provide the requested data.

When a clarification is provided, the circumstances of the individual case are assessed: if there is no doubt about the subject's journalistic activities (e.g. a request for certain family links between persons holding senior positions in the institution is made by a representative of an NGO), the data should be provided.

NB. If it is determined that full disclosure is not possible, disclosure of part of the information should be considered on a case-by-case basis.

Step 3

It must be verified that the data request meets the necessity criterion.

It is presumed that when the data are requested by a journalist, stating that they are needed for journalistic purposes, e.g. for the preparation of a publication, the criterion of necessity is met (for the reasons already mentioned that a different treatment would be incompatible with the safeguarding of the functions of the media in a democratic society and could be considered as censorship).

Requests for data must be complied with where there is no objective evidence that freedom of information and expression may be abused in a particular case, in other words, where there is no reason to believe that the data requested are not needed for journalistic purposes, but for personal, commercial or other interests incompatible with journalism.

The legislation does not provide for cases in which a journalist's credibility can be called into question and the journalist's proper assessment of the data needed for an investigation can be questioned, but it is possible to consider that the presumption of necessity should be waived in cases, for example, where the producer and/or disseminator of the information has had more than two serious professional misconduct offences during the last year, or has been recognised of being of poor

professional conduct amongst producers and disseminators of public information.

The presumption of relevance also applies only in cases where the data requested by the journalist do not include special categories of personal data. Special categories of personal data include personal data disclosing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data for the purpose of specific identification of a natural person, data concerning health, or data concerning a natural person's sex life and sexual orientation (Article 9(1) GDPR). This category of data can only be transferred under specific conditions: if the data subject has explicitly consented to the transfer of the data to the journalist (legitimate ground - consent); if the data are data that the data subject himself has already published or if the journalist presents arguments that the processing of these data is necessary **for reasons of overriding** public interest[9] . In order to obtain these data, the journalist must provide detailed evidence of the need for the data, the manner in which it will be used, the purpose of its use, and his/her assessment of the substantial public interest in knowing which outweighs the data subject's rights (for example, (e.g. a request to confirm or deny information on a sick leave certificate issued to a public figure and/or his/her trade union membership, to ascertain whether such a person complies with the established rules of conduct, does not abuse his/her rights and legal position, does not have a conflict of interest between public and private interests, etc.).

If all three conditions are met, the data request must be satisfied.

Part III

TEMPLATES AND EXAMPLES OF PRACTICAL SITUATIONS

Given the current lack of clarity and agreement in practice on how to reconcile the requirements of personal data protection with the right to freedom of expression and information, including the processing of data for journalistic purposes, we recommend that, both in journalist inquiries and in the replies of public authorities, standard phrases be used to justify one's position and to understand

9 Article 9(2)(g) GDPR ("processing is necessary for imperative reasons of substantial public interest based on Union or Member State law, which must be proportionate to the purpose pursued, without prejudice to the essential elements of the right to data protection, and which must provide for appropriate and specific safeguards for the protection of the data subject's fundamental rights and interests").

how personal data protection should be reconciled in a given case with the right to process data for journalistic purposes, and who is responsible for what.

1 situation

The journalist N.N. receives anonymous information about possible favouritism and overpriced social housing from "insiders".

In order to verify this information, the journalist asks the administration of the municipality to provide the names of the persons who were involved in the decision on the acquisition of social housing and to confirm or deny their possible links - family ties - with Mr A.N., from whom the municipality acquired the apartment to meet the needs of social housing.

Options for asking:

"Please provide me with the names of the persons who were involved in the decision of social housing X acquisition, and confirm or deny their possible links – family ties - with A.N., from whom the municipality purchased an apartment to meet the needs of social housing. The information is being collected as part of a journalistic anti-corruption investigation."

Comment. The request is appropriate provided that there is no doubt that the request was filed by a journalist. The only reason to return the request for more information is to clarify whether the person is indeed a journalist.

Suggestions on how the journalist's request could be improved:

"Please provide me with the names of the persons who were involved in the decision of social housing X acquisition, and confirm or deny their possible links – family links - with A.N., from whom the municipality purchased an apartment to meet the needs of social housing. The information is collected in the context of a journalistic anti-corruption investigation.

I hereby declare that I have read and agree to comply with the requirements for the processing and protection of personal data; personal data will be processed solely for the purposes of publication and/or programme and will be disclosed only to the extent necessary to achieve the journalistic purpose.

I recall that, in accordance with Article 6(1)(f) of the GDPR and the provisions of the Law on the Provision of Information to the Public, journalists have the right to receive information necessary for the achievement of journalistic purposes (the journalist's freedom of expression and freedom of information constitutes a

legitimate interest in obtaining the personal data necessary to inform the public adequately about matters of interest to it).

I would like to remind you that refusal to provide the requested information may result in liability under Article 547 of the Code of Administrative Offences of the Republic of Lithuania, which stipulates that refusal by the heads of state and municipal institutions and bodies to provide information to representatives of mass media, except for the information that is not sensitive according to the laws of the Republic of Lithuania, without stating the grounds for the refusal, or hindering the performance of journalists' professional duties, shall result in a fine for the heads of state and municipal institutions and bodies.

ADDED. A copy of the document certifying that the person requesting information is a journalist."

Possible answers from the authorities:

"Please be informed that your request has been processed. In the exercise of our duty to provide journalists with information relevant for the achievement of a journalistic purpose, and in view of the fact that you have cited Article 6(1)(f) of the GDPR as the lawful basis for processing, we reply that the Mayor's Adviser is related to Mr A.N., from whom the Municipality acquired the apartment for social housing purposes, by <...> the following <...>.

Providing this data does not mean that you can disclose it in a publication and/or report without first checking your compliance with data protection requirements. We remind to you that any further processing of the personal data you have provided, including the use of the data (volume, quantity) in publications and/or reports, must be carried out in compliance with the GDPR and national legislation. Please note that you may only publish personal data to the extent strictly necessary for the purpose of journalism and in the public interest. Otherwise, you may be liable in accordance with the aforementioned legislation.

This reply may be appealed to an administrative court in accordance with the procedure laid down by the Law on Administrative Procedure of the Republic of Lithuania or to the Lithuanian Administrative Disputes Commission in accordance with the procedure laid down by the Law on the Pre-Trial Procedure of the Republic of Lithuania for the Settlement of Administrative Disputes.

You can consult the Office of the Inspector of Journalist Ethics (www.zeit.lt) on the appropriate use of personal data in publications or other forms of work."

Comment. Suitable option.

"Please be advised that your application was received on 01/01/2022. In accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), we refuse to provide you with the information you have requested, because of the presence of personal data in it.

This reply may be appealed to an administrative court in accordance with the procedure laid down by the Law on Administrative Procedure of the Republic of Lithuania or to the Lithuanian Administrative Disputes Commission in accordance with the procedure laid down by the Law on Pre-Trial Administrative Dispute Procedure of the Republic of Lithuania".

Comment. Not a suitable option. Neither the GDPR nor any other legislation prohibits the transfer of personal data to journalists. This response is unjustified and therefore unlawful.

Related situation

If a request of a journalist lacks information, they should be asked to clarify it. For example, the following request is received:

"Please provide me with the names of the persons who were involved in the decision to acquire social housing X, and confirm or deny their possible links – family links - with A.N., from whom the municipality purchased an apartment to meet the needs of social housing. Journalist X.Y."

This request does not indicate the legitimate purpose of the processing of personal data. The request must specify that the information is collected for journalistic purposes, with a view to produce a publication or other form of work on matters of public interest. The authority may also have doubts as to whether a person who claims to be a journalist, but does not provide any evidence, is really a journalist.

Possible answers from the authorities:

a) "Please be advised that your application was received on 01/01/2022. As the information requested contains personal data, we must ensure that you have a legitimate basis for receiving it. You have not indicated in your request the purpose for which you require this information and we cannot conclude from the mere fact

that you identify yourself as a journalist that you are requesting information that is relevant to the pursuit of journalistic purposes. We kindly ask you to clarify the information relevant to your request by 7 January 2022:

provide evidence that you are a journalist (the media outlet you represent, etc.);

specify the purpose of the processing (use) of the personal data requested.

This reply is of a procedural nature and is not subject to an appeal."

Comment. Suitable option.

b) "Please be advised that your application was received on 01/01/2022. In accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), we refuse to provide you with the information you have requested.

Comment. Not a suitable answer.

Situation 2

The journalist N.N. requests information on the period of sick leave of the civil servant V.T. during the first quarter of 2022 and the reason for the sick leave.

Options for a request:

"Please provide information on the period of sick leave of civil servant V.T. during the first quarter of 2022 and the reason for the sick leave. Journalist N. N."

Comment. No legitimate purpose for processing personal data indicated.

"Please provide information on the period of sick leave of civil servant V.T. during the first quarter of 2022 and the reason for the sick leave. The information is being collected as part of a journalistic anti-corruption investigation. Journalist N. N."

Comment. The request is appropriate.

Suggestions on how the journalist's request could be improved:

"Pursuant to Article 6(1)(f) of the GDPR, please provide me the information on the period of sick leave of the civil servant Mr V.T. during the first quarter of 2022, and the reason for the sick leave. The information is collected in the context of a journalistic anti-corruption investigation.

I hereby declare that I am aware of and undertake to comply with the require-

ments for the processing and protection of personal data; the personal data will be processed solely for the purposes of publication and programmes and will be disclosed only to the extent necessary to achieve the journalistic purpose.

I recall that, in accordance with Article 6(1)(f) of the GDPR and the provisions of the Law on the Provision of Information to the Public , journalists have the right to receive information necessary for the achievement of journalistic purposes (the journalist's freedom of expression and freedom of information constitutes a legitimate interest in obtaining the personal data necessary to inform the public adequately about matters of interest to it).

I note that refusal to provide the requested information may lead to liability under Article 547 of the Code of Administrative Offences of the Republic of Lithuania, which stipulates that refusal by the heads of state and municipal institutions and bodies to provide information to representatives of the mass media, except for the information that is not sensitive according to the laws of the Republic of Lithuania, without stating the grounds for the refusal, or hindering the performance of journalists in the performance of their professional duties, shall be punishable by a fine for the heads of state and municipal institutions and bodies".

ADDED. A copy of the document certifying that the person requesting information is a journalist.

Possible answers from the authorities:

Information is provided in full.

Information is provided on the period of the sick leave, but the information on the sick reasons for the sick leave is refused.

More information is requested.

Information is refused.

Comment. Information on the period of a sick leave of a civil servant should be provided in accordance with the provisions of Articles 6(1)(f) and 9(2)(g) of the GDPR and the Law on the Provision of Information to the Public, but clarification may be requested if there is any doubt as to the status of the subject requesting the information.

But information on the reason for the sick leave must not be provided under Articles 14 and 18(1) of the Law on the Provision of Information to the Public.

Possible answers from the authorities:

"Please be informed that your request has been processed. In accordance with the provisions of Article 6(1)(f), Article 9(2)(g) of the GDPR and the Law on the Provision of Information to the Public, we hereby inform you that the period the sick leave of the civil servant Mr V.T. during the first quarter of 2022 was from 15.1.2022 to 18.2.2022.

Providing this data to you does not mean that you can disclose it in a publication and/or report without further data protection compliance checks. We cannot tell you which personal data are relevant to the public interest, but we remind you that any further processing of the personal data you have provided, including the use of the personal data (scope, amount) in publications and/or reports, must be carried out in compliance with the GDPR and national legislation. Please note that you may only publish personal data to the extent strictly necessary for the purpose of journalism and the public interest. Otherwise, you may be liable to the liability provided for in the aforementioned legislation.

We regret to inform you that we cannot provide you with the reason for the sick leave, as this is special category personal data (health data) and therefore disclosure would only be possible in exceptional cases, with the consent of the individual (which has not been obtained in this case), or where you have demonstrated an overriding reason relating to the public interest in disclosing the data. Your request does not contain such data and therefore this part of the request cannot be granted. If you have evidence as to why disclosure of these special categories of personal data is necessary for the protection of the substantial public interest, please provide it and we will process your request.

This reply may be appealed to an administrative court in accordance with the procedure laid down by the Law on Administrative Procedure of the Republic of Lithuania or to the Lithuanian Administrative Disputes Commission in accordance with the procedure laid down by the Law on the Pre-Trial Procedure of the Republic of Lithuania for the Settlement of Administrative Disputes.

You can consult the Office of the Inspector of Journalist Ethics (www.zeit.lt) on the appropriate use of personal data in publications and other forms of work."

Comment. Suitable answer.

"Please be advised that your application was received on 01/01/2022. In accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing

Directive 95/46/EC (General Data Protection Regulation), we refuse to provide you with the information requested.

This reply may be appealed to an administrative court in accordance with the procedure laid down by the Law on Administrative Procedure of the Republic of Lithuania or to the Lithuanian Administrative Disputes Commission in accordance with the procedure laid down by the Law on Pre-Trial Administrative Dispute Procedure of the Republic of Lithuania".

Comment. This reply does not provide the grounds for refusal as the GDPR does not prohibit the provision of information to journalists. The specific grounds for refusal to provide information should be indicated.

PART IV

OBLIGATIONS WHEN PROCESSING PERSONAL DATA FOR JOURNALISTIC PURPOSES

The Guidelines mention that it is up to the journalist requesting the information to decide what personal data is necessary for the preparation of an investigation, publication or other form of work and to what extent. The journalist to whom the personal data are provided takes full responsibility for their proper, lawful and fair processing and use and for assessing what data may be disclosed in the publication or other form of work, taking into account their necessity, proportionality, the possibility of anonymisation, and the interests of the data subject. Once a publication or other form of work has been published, and in the event of a dispute as to the compliance of the published information with the requirements of the protection of personal data, the media outlet/journalist will be obliged to justify to the supervisory authority and/or in court that it has carried out this assessment in a responsible manner.

First of all, according to Article 5 of the GDPR, personal data must be processed lawfully, fairly and in a transparent manner. This provision is in line with the fundamental principles of public information enshrined in Article 3(3) of the Law on the Provision of Information to the Public: public information in the media must be presented fairly, accurately and impartially. Thus, personal data must be processed for a legitimate purpose and on a lawful basis, and must be processed in

a way that reflects only the legitimate and reasonable expectations of journalists, while at the same time meeting the expectations of a democratic society.

According to Article 5(2) of the GDPR, media representatives, as data controllers, are responsible for ensuring compliance with the principles governing the processing of personal data. It should be stressed that journalists not only have to comply with the principles relating to the processing of personal data, but also have to be able to demonstrate compliance with the principles. This means that journalists have the burden of proof that a balancing test has been carried out and that different interests have been taken into account. In other words, the journalist must responsibly assess and prioritise the public's right to know and the right to protection of personal data before publishing personal data - a balancing test.

Data collected for journalistic purposes can and must be processed only for the purpose for which they were collected. In other words, personal data shall be collected for a specified, explicit and legitimate purpose and shall not be further processed in a way incompatible with the journalistic purpose; further processing for archiving purposes in the public interest shall not be considered incompatible with the original purpose (purpose limitation principle).

Journalists are also subject to the principle of data minimisation, which means that personal data can only be processed to the extent necessary to achieve a specific purpose. However, given the specific nature of the work of those involved in journalism and the GDPR's aim to reconcile freedom of expression and information with the right to the protection of personal data, a journalist may also keep other data which are not related to a specific investigation but which may be of use for future investigations.

It should be noted that personal data processed for journalistic purposes must be processed in such a way as to ensure, through appropriate technical or organisational measures, adequate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (integrity and confidentiality principle). Failure to apply appropriate security measures to the processing of personal data for journalistic purposes may lead to problems in ensuring the protection of personal data and to violations of the rights of data subjects in the media field. Therefore, both journalists and media outlets, as data controllers, must ensure the protection of personal data of data subjects processed for journalistic purposes by all available technical and organisational means.

V PART
EXERCISING AND DEFENDING RIGHTS

Journalists and other producers/disseminators of public information have the exclusive right to receive the information they request from state and municipal authorities within 1 working day (Article 6 of the Law on the Provision of Information to the Public).

Authorities that refuse to provide information must inform in writing about the grounds for refusal the next working day. Every journalist or other producer/disseminator of public information has the right to defend freedom of the media.

In the letter refusing to provide the information, the authorities must also specify the appeals procedure and, if necessary, provide a verbal comment on the procedure of appeals of that decision.

Where to consult?

Both public authorities and journalists can consult the OJEI on issues related to obtaining information from state or municipal authorities. The OJEI provides advice to journalists, producers and disseminators of public information, public authorities, and other persons interested in human rights and freedoms of the media and in the dissemination of public information in general. All consultations are on public information, the lawfulness of its dissemination and the lawful collection of information. Although not binding, the consultation of the OJEI may serve as a basis for a decision of the authority following an interpretation by one of the GDPR supervisory authorities.

Practical information on appeals procedures

A media representative who does not receive the requested information from a public administration body or other public authority shall have the right to appeal against such a refusal in accordance with the procedure established by law.

Possible ways of appeal: to the Seimas Ombudsmen's Office (decision - recommendation), to the Lithuanian Administrative Disputes Commission (binding decision), to court (binding decision).

CHAPTER II
RELEVANT CASE LAW

The main purpose of the GDPR is the protection of personal data. At the same time, the GDPR stresses that this right is not absolute and must be balanced with other fundamental rights and freedoms, including the freedom of expression and information. In turn, the freedom to hold opinions, to receive and disseminate information and ideas is one of the foundations of an open, fair and harmonious civil society and a democratic state and cannot be restricted except by law, if necessary to protect personal health, honour and dignity, private life, morals, or to defend the constitutional order (Article 25(3) of the Constitution of the Republic of Lithuania). Restrictions on freedom of expression must always be perceived as an exceptional measure and must be consistent with the objective pursued: to prevent war propaganda, disinformation or incitement to hatred, to protect another important public interest or to protect the rights and freedoms of individuals. This restriction is exceptional as the grounds for restriction laid down in the Constitution cannot be interpreted by broadening them, and the criterion of necessity enshrined in the Constitution implies that in each case, the nature and scope of the restriction must be consistent with the objective pursued.

The Constitution thus guarantees and protects the public interest in being informed. The European Court of Human Rights (ECHR), in its case law, has emphasised the fundamental role of the media in society and the need for exceptional protection of freedom of expression, and has pointed out that the media plays a vital role as a "public watchdog" (ECHR Jersild v Denmark judgment of 24 September 1994, Axel Springer v Germany judgment of 7 February 2012). Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") enshrines the right to freedom of expression, which encompasses the freedom to hold opinions, receive and disseminate information and ideas. However, this freedom, like the right to protection of personal data and privacy, is not absolute.

In accordance with Article 85(1) of the GDPR, the right to the protection of personal data under the GDPR must be reconciled in the law of a Member State with the right to freedom of expression and information, including processing of

data for journalistic purposes and for the purposes of academic, artistic or literary expression. The exceptions under Lithuanian law are set out in Article 4 of the Law on the Legal Protection of Personal Data (*Processing of Personal Data and Freedom of Expression and Information)*. Where personal data are processed for journalistic purposes or for purposes of academic, artistic or literary expression, Articles 8, 12 to 23, 25, 30, 33 to 39, 41 to 50, 88 to 91 of the GDPR do not apply. In most cases, processing of data for journalistic purposes is carried out on the basis of the principle of legitimacy in Article 6(1)(f) of the GDPR: the processing is necessary for the purposes of the legitimate interests of the controller or of a third party, unless such interests of the data subject or the fundamental rights and freedoms of the data subject, which require protection of the personal data, are overridden by such interests, in particular where the data subject is a child.

It is important to note that according to Article 6(3) of the Law on the Provision of Information to the Public, state and municipal institutions and bodies are obliged to provide public information, as well as existing private information, in accordance with the procedure established by the Law on the Right to Access Information and Reuse of Data and other laws, with the exception of the cases stipulated by the law, where private information is not provided. Pursuant to Article 18 of the Law on the Provision of Information to the Public, state and municipal institutions and bodies, as well as other institutions, undertakings and organisations, shall not disclose to producers and/or disseminators of public information, or to any other person, information which by law constitutes a state, official, professional, commercial or banking secret or which is of a private character; information which is prohibited by other laws from being disclosed because its disclosure would undermine the interests of national security and defence, the prosecution of persons, or would encourage the violation of the integrity of the territory of the State or of public order, or because its withholding would be detrimental to the prevention of infringements of the law or would be essential for the protection of human health.

As regards the provision of information to journalists by an institution or body, it should be noted that the balance between the public's right to know and the individual's right to privacy also depends on the specific nature of the activities of the public institution or body and, where appropriate, of the persons working for it. For example, when providing information on pre-trial investigation cases, law enforcement institutions and prosecutor's offices are guided by the principle that the pre-trial investigation data is sensitive data (Article 177 of the Criminal

Procedure Code of the Republic of Lithuania). In this regard, journalists, public information producers (disseminators) cannot expect to receive more data from the aforementioned institutions than the prosecutor will declare admissible before the case is heard by the court. It should be noted that the publication in the media of personal data on suspects, accused, convicted persons or victims who are minors, from which it is possible to determine their identity, is generally prohibited. Where the law expressly and explicitly prohibits the publication of certain personal data, such data shall not be communicated to journalists.

Information that does not require the collection of additional data shall be made available to producers and/or disseminators of public information and to journalists at least within one working day, and information that requires the collection of additional data shall be made available at least within one week at the latest. State and municipal institutions and bodies and other budgetary institutions which refuse to provide public information to a public information producer shall inform the producer in writing of the reasons for refusing to provide the information no later than on the next working day (Article 6(4), (5) of the Law on the Provision of Information to the Public).

Obviously, the work of a journalist is directly linked to one of the most fundamental rights of every person - the right to hold and express opinions (freedom of information). As already mentioned, a journalist has the right to receive information promptly, given his or her status (Article 6(4) of the Law on the Provision of Information to the Public).

In Lithuania, there is an emerging problem: the unjustified reliance on the GDPR in certain cases by state and municipal institutions and bodies, as well as other institutions, companies and organisations, to refuse to provide information for journalistic purposes. The most unclear issue for the authorities implementing the Law to Obtain Information and the Reuse of Data is the status of the increasingly popular freelance journalists and citizen journalists and their right to access information, in particular related to personal data.

Pursuant to Article 4(1) of the Law on the Provision of Information to the Public, everyone has the right to freely express his or her thoughts and beliefs and to freely collect, receive and disseminate information and ideas. The freedom to collect, receive and disseminate information may not be restricted except by law if necessary to protect the constitutional order, human health, honour and dignity, private life, morals. Moreover, according to Article 5(1)(3) of the Law on the Pro-

vision of Information to the Public, the right to take notes, photograph, film, use audio-visual equipment and record information in any other way, except for the cases referred to in Article 13 of this Law, is available to any person (not only to the journalist), and the obligation not to use audio-visual equipment is available to the journalist only in the case when the private person providing the information, and not the public person, does not wish to use it (Article 41(2)(9) of the Law on the Provision of Information to the Public). The controller should objectively assess, upon receipt of the request, whether the recipient of the personal data has the right to receive such information.

Although the Law on the Provision of Information to the Public defines a journalist as a *natural person who, on a professional basis, collects, prepares and presents material to the producer and/or disseminator of public information under a contract with him and/or is a member of a professional journalists' association.* (Article 2(85) of the Law the Provision of Information to the Public), the changing social situation is a clear indication that the definition of a *journalist* no longer corresponds to the current state of affairs, and it should not be understood in a narrow sense.

According to the case law, in order to take into account the importance of freedom of expression for the democratic community as a whole, the concepts involved, including journalism, must be interpreted broadly. The case-law of the Court of Justice of the European Union (CJEU) holds that the processing of personal data for the sole purpose of journalism is considered to be an activity the sole purpose of which is to disclose to the public information, opinions or ideas *(CJEU Judgment of 14 February 2019, Case C-345/17)*. The purpose of journalism is understood broadly and not limited to professional journalistic activities. The exemption for journalistic activities is not linked to the legal relationship of employment with a particular media outlet or to professional membership of a professional organisation of journalists. It shall be granted to any person who engages in journalistic activities. The ECtHR has clarified that in today's society, it is not only the media that can act as a guardian of the public interest, but also different non-governmental organisations, public bodies and associations play a similar role.

Journalistic activities are those activities the purpose of which is to disseminate information, opinions or ideas to the public by any means of communication. The fact that a person is not a professional journalist does not mean that the journalistic exception does not apply.

The Supreme Administrative Court of Lithuania has also established that

the Law on the Provision of Information to the Public must be interpreted broadly, covering not only traditional but also modern, although not directly regulated, forms of electronic media, focusing not on the formal features of the organisation of such media, but on the functions they actually perform.

It is important to note that the purpose of journalism is not exclusively related to the publication of information, but also includes processing of personal data, such as the collection of data for the purpose of disseminating information, opinions or ideas to the public. The mere fact that the personal data collected have not been made publicly available does not mean that the processing of personal data has not been carried out for journalistic purposes. It should be noted that the Law on the Provision of Information to the Public and the Lithuanian Code of Ethics for Public Information oblige journalists to provide to the public only with verified, correct information, and therefore a journalist does not necessarily have to be convinced that the hypothesis of a journalistic investigation will be confirmed before requesting information. It is understood that in the course of a journalistic investigation, there may be situations where the information that is the subject of the investigation is not confirmed by the investigation and is therefore not published. However, such data collection is undoubtedly carried out for journalistic purposes. It is also important to emphasise that the receipt of the requested information does not in itself imply a lawful dissemination of the information to the public in its entirety. The responsibility for the information published lies with the person who published it, the producer/disseminator of public information, who must assess in each case how much and what kind of information is appropriate to publish. In turn, it cannot be argued that any information published on the internet containing personal data falls within the concept of 'journalistic activity' and is therefore covered by the exemptions of the data protection requirements. Not all information published on the internet together with personal data falls within the concept of 'journalistic activities'.

Recital 153 of the GDPR's Preamble states that "in order to take account of the importance of the right to freedom of expression in a democratic society, concepts relating to this freedom, such as journalism, must be interpreted in a broad sense". For example, according to the case-law the concept of "journalistic purposes" must be interpreted in accordance with Article 2(75) of the Law on the Provision of Information to the Public ("information intended for public dissemination") and Article 14(3) of that law ("when it contributes to the disclosure of violations of

the law or of criminal offences, and when the information is given in the course of a public hearing. In addition, information on the private life of a public person may be published without his/her consent if the information discloses circumstances or personal characteristics of his/her private life which are of public importance"), i.e. the processing of personal data for the purposes of journalism is an activity which collects or publishes information of relevance to the public information or public interest.

Taking into account the case law, as well as the nature of activities of specific natural persons - authors of blogs - and the functions performed by them in the provision of public information to the public, it is obvious that they can be recognised as *sui generis* managers of information media, and thus also as producers and/or disseminators of public information, and their blogs - as means of information media in the meaning of the Law on Information Society *(Decision of the Supreme Administrative Court of Lithuania of 20 April 2009 in case No A-444-70/2009).*

According to this interpretation, internet bloggers are the producers/disseminators of public information and must ensure the lawfulness of the information published. Thus, despite the fact that the activities and legal status of such citizen journalists are not specifically regulated by the Law on the Provision of Information to the Public, this does not constitute a reason to claim that the managers of accounts, blogs and information media are excluded from the sphere of legal regulation. Such persons are treated as producers (disseminators) of public information in terms of their activities, and the means managed by them, which provide information to the public with a certain content, are treated as a public information medium.

Recipient means a natural or legal person, public authority, agency or other body to which the personal data are disclosed, whether or not it is a third party (Article 4(9) GDPR).

In the present case, the data recipients could be:

journalists; producers of public information - an audiovisual media service provider, a radio broadcaster, a publishing house, a cinema, sound or video studio, an information, advertising or public relations agency, an editorial office, a manager of an information society media outlet, an independent creator, a *journalist or any other person who prepares or submits public information for dissemination (Article 2(76) of the Law on the Provision of Information to the Public)*; *disseminators of public information* - an audiovisual media service provider, a retransmitter,

a person providing online distribution of television programmes and/or individual programmes to the consumers of the Republic of Lithuania, a video sharing platform service provider, a broadcaster of radio programmes, an *operator of an information society media outlet, or any other person disseminating public information to the general public and being responsible for the legality of such information in accordance with the procedure laid down by this and other laws (Article 2(77) of the Law on the Provision of Information to the Public).*

The right to collect/receive information is an integral part of freedom of expression. Restrictions on freedom of expression may only be imposed if they are lawful, proportionate and necessary in a democratic society. These grounds for restricting freedom of expression follow from the extensive case law of the ECHR on the application of Article 10 of the Convention. Article 10 of the Convention imposes negative and positive obligations on each State Party, which the State must fulfil in order to guarantee freedom of expression. As a general rule for the application of Article 10 of the Convention, any restrictions on freedom of expression are discouraged.

The jurisprudence developed by international courts shows that, in order to reconcile the right to privacy and the right to freedom of expression, the ECHR and the CJEU have identified a number of relevant criteria to be taken into account, namely: the contribution to a debate of general (public) interest, the prominence of the person in question, the subject matter of the report, the previous behaviour of the data subject, the content, the form and the consequences of the publication, the manner and the circumstances in which the information was obtained and to what extent it represents the truth. In addition, account must be taken of the possibility for the controller to take measures to minimise the interference into private life *(ECHR Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, 27.06.2017, CJEU Judgment of 14.02.2019, Case C-345/17).*

As regards the differences between the status of public and private persons, it should be noted that a public person, by virtue of his or her position in the society, does not benefit from the same scope of privacy protection as a private person - the boundaries of the protection of the public person's privacy are much narrower.

Given that a public figure's position in society is partly due to the attention he/she receives from the public, and given that the conduct of a public figure has an impact on the lives of other members of the public, they cannot claim the same protection for their private life as a private individual. On the other hand, a pub-

lic figure also has a right to a private life. Information about a public figure may not be collected and published in an unregulated way. Information about the life of a public person must be collected in a lawful manner *(2012-11-15 Lithuanian Supreme Court (hereinafter - the Supreme Court of Lithuania) ruling in case No 3K-3-481/2012)*.

The Constitutional Court of the Republic of Lithuania, in its Resolution of 23 October 2002 "On the Compliance of Article 8 and Article 14(3) of the Law on the Provision of Information to the Public of the Republic of Lithuania with the Constitution of the Republic of Lithuania", noted that the personal characteristics of persons participating in public and political activities, their behaviour and some circumstances of their private lives may be relevant for public affairs. The public interest in knowing more about these persons than about others is constitutionally justified. That interest would not be safeguarded if the publication of information of public interest concerning the private life of a person involved in public and political activities required the consent of that person in each individual case. Consequently, the media may, without the consent of a person, inform the public about the private life of such a person to the extent that the personal characteristics, conduct and other circumstances of that person's private life may be relevant to public affairs and that the information published is therefore of public interest. A person involved in public and political activities cannot help but expect greater public and media attention (paragraph 8 of the Resolution).

In recent years, the concept of the public person has expanded enormously. This is due to both the amendments to the Law on the Provision of Information to the Public adopted by the legislator and the changes in the case law of the Supreme Administrative Court. *A public figure is: 1) a state politician; 2) a judge; 3) a state or municipal official, a civil servant, a person employed under a contract of employment in a state or municipal institution or body, provided that the decisions or activities adopted by him/her have an impact on the public, as well as a member of working groups, committees, commissions, councils and other collegial bodies established in these institutions or bodies; 4) the head of an enterprise or a body of management or a member of the management body of an undertaking or body of an institution under control of the state or municipality; (5) a member of a political party's governing body or of an election committee; (6) a candidate in an election (the status of a public person shall be retained after the election for a period of time equal to one term of office of the institution for which the person is a candidate); (7)*

the head of a legal person which concludes public procurement contracts and/or performs public procurement contracts as a subcontractor, or a participant holding 1/4 or more of the votes at a meeting of participants; (8) a lobbyist or a person who acts on behalf of legal persons engaged in lobbying activities; (9) the head or a participant holding 1/4 or more of the votes at a meeting of participants of an association or a public body which has received State and/or municipal funding in the last 4 years; (10) a publicly known natural person, a popular social networking personality or a blogger, who shapes the opinion of targeted groups of the public on a range of issues and/or who receives an income from such activities, if their activities are relevant to the public affairs; 11) any other natural person who has public administration powers and/or administers the provision of public services, and/or who has been brought into the public domain by his/her actions or position, if his/her activities are of public interest (Article 2(74) of the Law on the Provision of Information to the Public).

The Supreme Administrative Court has noted that the restriction of the privacy of a former Member of the Seimas, who no longer considered himself a public figure, was found to be proportionate. However, a person's publicity does not automatically cease with the end of his or her office, and the case of a breach of public order (traffic rules) dealt with in the publication satisfied a clear public interest to know. The Court noted that the legislation does not provide for a period of time during which a person may no longer be considered a public figure once he or she has ceased to engage in active public activities, and therefore each situation must be assessed individually, taking into account the person's activities, the public's expectations of the former members of the Seimas, etc., and that it is not possible to determine this in advance for a specific period. The real interest of a certain part of the public in receiving information illustrated by a photograph of a person in order to prevent further actions possibly violating generally accepted rules of good conduct has been highlighted, and the composition of the applicant's photograph is a way of journalists' self-expression *(ruling of the Supreme Administrative Court of Lithuania of 17.03.2021 in administrative case No. eA-323-492/2021)*.

In another case, the Supreme Administrative Court of Lithuania changed the previously developed practice by adopting a decision in an administrative case in which it assessed the legality of the information about the applicant published in the TOP Richest Persons List and expanded the concept of a public person. In the opinion of the Extended Chamber of Judges, the concept of a public person

enshrined in the Law on the Provision of Information to the Public should be interpreted in the light of the ECHR jurisprudence on the matter. In the present case, there was no dispute that the applicant does not have public administration powers, does not administer the provision of public services and, by the nature of her work, is not regularly involved in public or social activities. However, in the view of the Chamber, the country's richest persons occupy a position in society which makes their activities in relation to the management of their wealth of public interest (the creation of many jobs, the business environment, the collection of taxes for the State budget) and which therefore makes them public figures within the meaning of both the Convention and the Law on the Provision of Information to the Public .

In this case, the Court made a very important point that there is no uniform level of publicity for public figures. The Court noted that the right of public persons to keep their private life secret is in principle more extensive when they do not hold any official position and more limited when they do hold such a position *(15 September 2021, decision of the Supreme Administrative Court in administrative case No eA-2066-624/2021)*.

In the aspect of the development of the concept of a public person, it is important to note that in one case the Supreme Administrative Court did not analyse the concept of a public person provided for in the Law on the Provision of Information to the Public (according to which the applicant did not meet any of the criteria of a public person), did not cite any specific case law, on the basis of which the provision of support to a political party could be recognised as a criterion for classifying a person in the category of public persons, However, it formulated the practice that the relevance of the information disseminated about a person to the public automatically determines the recognition of a person as a public person, and established the provision that a person may be recognised as a public person only in one specific case, in one individual situation *(27 October 2021, Supreme Administrative Court ruling in administrative case No. eA-2078-815/2021)*.

The Supreme Administrative Court has revealed a trend to broaden the concept of public person and expressed the necessity to assess whether participation in public procurement is relevant to the classification of a person as a public person. The Chamber of Judges emphasised that the criterion of public resources is one of the essential criteria for determining the category of public persons. In this respect, paragraph 7 of Resolution No 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy establishes that public persons are those

who hold positions in the public service and/or use public resources and, in general, all those who play a significant role in public life (political, economic, artistic, social, sports or in any other sphere) *(Resolution of the Supreme Administrative Court of Lithuania of 17 November 2021 in administrative case No eP-83-602/2021)*.

The Supreme Administrative Court, in interpreting and applying the concept of a public person, emphasised that even in cases where the third party does not have public administration powers, does not administer the provision of public services, and does not, by virtue of the nature of his/her work, regularly participate in state or public activities, the determination of whether that person is a public person also includes an assessment of the relevance of the person's activities to public affairs. "The ECHR itself has repeatedly drawn the boundaries of the public person and its jurisprudence has included not only elected public officials or celebrities, but also business people <...>, journalists and lawyers <....>, distinguished academics <...>, as well as other persons occupying a relevant position in society or involved in the public sphere <...>" *(Decision of the Supreme Administrative Court of Lithuania of 3 February 2022 in case No. eA-51-822/2022)*.

It is worth noting that the change in the concept of the public figure also reflects society's changing social situation and its appreciation of the increasing number of areas where person's actions have a significant impact on, and a legitimate interest for the society.

In the context of data provision, the public interest is particularly relevant, usually in relation to matters that affect the public to the extent that it can legitimately take an interest in them, and that attract their attention or concern in a significant way, in particular because they affect the well-being of the population or the life of the community. The same is true of matters which are likely to give rise to significant controversy, which concern an important social matter or issue about which the public would have an interest in being informed *(ECHR judgment of 27 June 2017, Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland)*.

The Supreme Administrative Court, having examined the administrative case concerning the audio recording of the Government meeting, established that the refusal of the Office of the Government of 4 October 2018 to provide the information recorded in the audio recording violated the right of the applicant journalists to receive, collect and disseminate information. The Court's ruling states that the Government Office, in the exercise of its public functions, made the following made an audio recording of the Government's meeting on 3 October 2018 and had the

information on the activities of the Government at its disposal at the time when the applicants' requests were lodged, on 4 October 2018. It therefore had the opportunity to make it available within one working day, as provided for by the Law on the Provision of Information to the Public .

The ruling of the Supreme Administrative Court noted that the Office of the Government did not provide any evidence in the case that it could not disclose the information about the Cabinet meeting (which is one of the organisational forms of the Government's activities) on the grounds that such a restriction was necessary by law and in a democratic society in order to protect the rights and freedoms of other persons and the values enshrined in the Constitution. The Chamber of Judges noted that the publication of all documents available and generally accessible in the public sector, not only those relating to the political process but also those relating to the legal and administrative process, is an essential means of expanding the right to know, which is a fundamental principle of democracy *(Order of the Supreme Administrative Court of the Republic of Lithuania in Administrative Case No eA-1639-520/2020 of 2020-07237)*.

In another case, the Supreme Administrative Court referred to the practice established by international courts that when a private company chooses to engage in transactions involving substantial public funds, it voluntarily opens its activities to greater public scrutiny. This is particularly so in cases where it is alleged that such transactions have been detrimental to public finances (*ECHR, judgment of 27.11.2007, Timpul Info-Magazin and Anghel v. Moldova, p. 34*) The same is essentially true of a private individual who engages in the public sphere: in a case concerning repairs carried out by a contractor in publicly funded institutions, the Court held that the contractor was thus a recipient of public funds; by engaging in the public sphere, private individuals expose themselves to greater scrutiny, and the proper use of public funds is undoubtedly part of the public interest (*ECHR judgment of 21.12.2010 in Novaya Gazeta v Voronezhe v. Russia, pp. 46-48*).

In another case after the reopening of the proceedings, the Extended Chamber of Judges of the Supreme Administrative Court of Lithuania (SACJ) disagreed with the conclusion of the defendant, the court of first instance and the SACJ College of Judges that the purpose of the Publication could have been achieved without disclosing the data of the third interested party. The Extended Chamber of Judges of the Supreme Administrative Court held that the non-disclosure of the final beneficiary of the benefits of the public procurement and of his links with the contracting

authority would render that part of the Publication essentially meaningless, since the mere provision of abstract information, leaving the public to speculate about the links, closeness and importance of the organisations (and the persons working for them or otherwise directly involved in their activities), would not allow the general public to understand the real situation in the area described, and thus to make a real contribution to the debate on the public interest in the proper use of public funds. In the circumstances, the provision of more limited information would only allow the applicant to exercise his right to information and freedom of expression in a declarative manner.

At the same time, the Court pointed out that, unlike a private person who is not known to the public, a public figure cannot ask for a special protection for his/her private life. Furthermore, Extended Chamber of Judges, taking into account the status of the third party, the content of the Publication, its text and its context, held that, in the present case, the Publication referred to a public figure in the context of a subject of public interest (the issue of public procurement, that is, the allocation and use of public resources), and that the reported facts contributed to the debate in a democratic society. It also stressed that the information published in the Publication about the third interested party - his name and relationship with an employee of another undertaking - was not presented as inducing curiosity, but on the contrary, it was considered necessary and contributed to the public interest debate and informed the public about the subject of public procurement covered by the Publication *(judgment of the Supreme Administrative Court of the Republic of Lithuania of 3 February 2022 in case No eA-51-822/2022)*.

Gathering information is an important preparatory step in journalism and is an integral, protected part of press freedom. Therefore, in the light of the interest protected by Article 10 of the Convention, the law may not permit arbitrary restrictions which may amount to a form of indirect censorship by the authorities by creating obstacles to the gathering of information *(ECtHR judgment of 26.4.2006, Dammann v. Switzerland, Application No. 77551/01)*.

Thus, in the light of the case-law, the question of the provision of information must be based on an assessment of (1) the public interest to know the information requested, (2) the possible negative consequences of providing such information and (3) whether the public interest to know the information outweighs the possible negative consequences.

Legislation:

1. Convention for the Protection of Human Rights and Fundamental Freedoms
2. Council of Europe Parliamentary Assembly Resolution 1165 (1998)
3. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
4. Constitution of the Republic of Lithuania
5. Law on the Provision of Information to the Public of the Republic of Lithuania
6. Law on Legal Protection of Personal Data of the Republic of Lithuania
7. Law of the Republic of Lithuania on the right to access information and reuse of data
8. Law on Public Administration of the Republic of Lithuania

Case law:

European Court of Human Rights case law:

1. Judgment of 8 July 1986 in the case of Lingens v Austria, Application No 9815/82
2. Judgment of 23 May 1991 in Oberschlick v Austria, Application No 11662/85
3. Judgment of 26/02/2002 Krone Verlag GmbH & Co. KG v Austria, Application No 34315/96
4. Judgment of 24 June 2004 in Von Hannover v Germany, Application No 59320/00
5. Judgment of 14 June 2005 in Minelli v Switzerland, Application No 14991/02
6. Judgment of 26 April 2006 in Dammann v Switzerland, No 77551/01
7. Judgment of 17.10.2006 in Gourguenidze v Georgia, Application No 71678/01
8. Judgment of 14 July 2007 in Hachette Filipacchi Associés v France, Application No 71111/01
9. Judgment of 27.11.2007 in the case of Timpul Info-Magazin and Anghel v Moldova, Application No 42864/05
10. Judgment of 15 January 2009 in the case of Reklos and Davourlis v Greece, application No 1234/05
11. Judgment of 23/07/2009 - Hachette Filipacchi Associés (ICI PARIS) v France, Application No 12268/03

12. Judgment of 21.12.2010 in the case of Novaya Gazeta v Voronezhe v Russia, Application No 27570/03
13. Judgment of 7 February 2012 in Von Hannover v Germany, Application Nos 40660/08 and 60641/08
14. Judgment of 8 November 2016 in Magyar Helsinki Bizottság v Hungary, Application No 18030/11
15. Court of Justice of the European Union case law:
16. Judgment of 6 November 2003 in Case C-101/01
17. Judgment of 16.12.2008 in case No C-73/07
18. Judgment of 27 June 2017 Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland, No 931/13
19. Judgment of 14 February 2019 in Case C-345/17
20. Judgment of 22 June 2021 in Case C-439/19

Practice of the Constitutional Court of the Republic of Lithuania:

1. Resolution No 36/2000 of 23 October 2002
2. *Practice of the Supreme Administrative Court of Lithuania*:
3. Judgment of 20 April 2009 in case No A-444-70/2009
4. Order of 28 April 2011 in case No A-62-787/2011
5. Order of 26 July 2012 in case No A-858-2133/2012
6. Order of 10 September 2012 in case No A-525-1460/2012
7. Order of 14 November 2016 in case No A-2115-525/2016
8. 11-12-2019 ruling in case No eA-3316-629/2019
9. Order of 22 January 2020 in case No eA-58-261/2020
10. 2020-06-03 ruling in case No eA-1056-442/2020
11. Order of 23 July 2020 in case No eA-1639-520/2020
12. 2021-03-17 ruling in case No eA-323-492/2021
13. 2021-09-15 decision in case No eA-2066-624/2021
14. 2021-10-27 ruling in case No eA-2078-815/2021
15. 2021-11-17 ruling in case No eP-83-602/2021
16. Judgment of 3 February 2022 in case No eA-51-822/2022
17. Order of 9 February 2022 in case No eA-146-415/2022

Lithuanian Supreme Court case law:

1. Order of 2 January 2008 in civil case No 3K-7-2/2008
2. Resolution of 15 November 2012 in civil case No 3K-3-481/2012
3. 2016-06-21 ruling in criminal case No 2K-206-303/2016

RECOMMENDATIONS FOR JOURNALISTS AND PUBLIC INFORMATION PRODUCERS (DISSEMINATORS)

Introduction

The fact that exemptions under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation") ("GDPR") are applicable to the publishing of information for the purposes of journalism, does not mean that journalists are exempt from the obligation to properly protect personal data. The journalist to whom personal data are communicated in the course of a journalistic investigation takes full responsibility for their proper, lawful and fair processing and use. For these reasons, journalists should consider the sensitivity and confidentiality of the personal data they possess and the harm that could result in cases of loss or misuse of such information. Journalists should take steps to prevent the leakage, loss or use of personal data collected in the course of an investigation without a legitimate purpose.

It is understood that the work of journalists and other professional producers (disseminators) of public information would be impossible without the collection and processing of personal data, and therefore both journalists and media outlets, as data controllers, must aim to ensure the protection of the personal data of the data subjects processed for the purpose of journalism by all available technical and organisational means. Controllers (processors) of personal data, including journalists, must not only ensure that the processing of personal data is lawful, but also that such processing is in accordance with the principles set out in Article 5 of the GDPR. Although Article 4 of the Law on the Protection of Personal Data of the Republic of Lithuania provides for exceptions to the application of the GDPR in cases where personal data are processed for journalistic purposes, the obligation to comply with the principles of processing personal data remains.

In the cyber world, the security and privacy of personal data is fragile. Laptops, tablets, smartphones, different compact data storage devices, cloud computing and wireless data networks have become part of our everyday life. We use these technologies at work, at home, when travelling, to collect, store, process and transmit a wide range of information, including personal data. Without sufficient knowledge and negligent, irresponsible use of technology, there is a high risk not only of data loss, but also of data theft or accidental dissemination.

While every institution/editorial office should follow the rules for safe use

of information technology and data processing set out in its internal procedures, journalists themselves must also take care of the security of the technology they use. Backing up data protects against data loss. When data is lost, there is usually some loss associated with that and that is the end of the data journey. In the case of data leakage, theft or accidental publication, things are much more complicated and the consequences can be very varied and long-lasting, depending on the sensitivity of the data. According to different studies, around half of data security violations are related to the loss of equipment (loss, theft, etc.). We will discuss the basic principles of how to deal with the tools used to collect, process, store and transmit data.

PART I
KEY PRINCIPLES

Principle of lawfulness, fairness and transparency

According to Article 5(1)(a) of the GDPR, personal data must be processed in a lawful, fair and transparent manner in relation to the data subject. This principle includes three different requirements:

Lawfulness. In order for processing to be lawful, personal data should be processed with the consent of the data subject concerned or on the basis of another lawful legal basis set out in the GDPR. Given the specific nature of the journalistic purpose and the exceptions provided for in the Personal Data Protection Act, consent is generally not possible for the collection of information necessary for a journalistic investigation which contains personal data. Therefore, when processing personal data in order to ensure a legitimate and justified public interest, the journalist must be sure at the time of collecting personal data that the journalistic investigation and the subject matter of the investigation are in the public interest, even if the suspicions raised by the collection of the information necessary for the investigation may not be substantiated.

Fairness. The principle of fairness is not defined in the GDPR, but it implies that the processing of personal data must be in accordance with the spirit and meaning of the GDPR, not just its formal provisions. In general, fairness means that personal data must be processed in a way that satisfies the data subject's reasonable expectations. Fairness also means that the media must collect and use information about natural persons in a fair and lawful manner and without causing any unjustified harm. For example, journalists have the right to collect information without the knowledge or consent of the data subject, but it would be unfair to actively mislead individuals as to the journalist's identity or intentions.

Transparency. In applying the principle of transparency, it should be clear to natural persons how personal data relating to them are collected, used, accessed or otherwise processed, as well as the extent to which those personal data are or will be processed. This principle relates in particular to the information of data subjects as to the identity of the controller and the purposes of the processing, as well as to further information to ensure fair and transparent processing in relation to the natural persons concerned, their right to obtain confirmation of the processing of

personal data relating to them, and their right to receive those data. In applying this principle to journalistic activities, it should be noted that the Law on the Protection of Personal Data provides for an exception to the data subject's right of access to the data processed, and that the right to object to processing is not valid. Thus, although the journalist is not obliged to inform the individual about the processing of his/her personal data, nor is he/she obliged to obtain his/her consent to the processing, the principle of transparency requires that personal data be collected in a rational manner and without abusing the rights. For example, a journalist working for one editorial office which has a data contract with the public registers should not use the rights conferred by this contract to use the data collected on the basis of this contract in another editorial office which, for some reason, does not have the right to receive information from the public registers.

EXAMPLE.

A journalist with access to the data of the State Centre of Registers came up with the idea of checking how much and what kind of real estate his neighbour owns for purely personal reasons. Journalists should not collect data which are not the subject of a journalistic investigation, as such collection would not be in the public interest and would be unlawful and unjustified.

Principle of purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes. The processing of personal data for purposes other than those for which they were originally collected should only be permitted if the processing is compatible with the purposes for which the personal data were originally collected. In such a case, a separate legal basis is not required, but the basis on which the collection of personal data is authorised is sufficient. Further processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes should be considered as compatible lawful processing operations. When processing personal data, the journalist must not deviate from the journalistic purpose and use the personal data collected or gathered for other purposes unrelated to the journalistic purpose.

EXAMPLE

A journalist, who has the right to collect data on real estate owned by natural persons in the Real Estate Register free of charge, should not collect personal data in the Register for the purpose of finding out who the owner of a house is and making an offer based on that information but rather for preparing the publication.

Data minimisation principle

Personal data must be adequate, relevant and only necessary for the purposes for which they are processed. This principle implies that only personal data necessary to disclose the objective of the journalistic investigation should be collected, and that superfluous data which are manifestly irrelevant to the ongoing or any future investigation should not be collected and stored. It should be emphasised that the specific nature of journalism often requires the conduct of investigations of a very wide scope, involving large amounts of information, and that information which is not directly relevant to the publication or other journalistic work being prepared may later on be of broader journalistic interest, and may therefore reasonably be retained in order to prevent the loss of information which has been collected and which may be of value in the future.

EXAMPLE.

In the context of a journalistic investigation, data should not be processed solely to satisfy the public's curiosity rather than to realise the public interest, i.e. the scope of the data published must be proportionate to the aim pursued: if the aim were to publish information on the richest people in the country, the disclosure of their age would be excessive and would not be consistent with the public's interest to know.

Principle of accuracy

Personal data must be accurate and, where necessary, updated; all reasonable steps must be taken to ensure that personal data which are not accurate in relation to the purposes for which they are processed are erased or rectified without delay. This principle is also linked to the fundamental principles of public information enshrined in Article 3(3) of the Law on the Provision of Information to the Public, which requires that information in the media is presented in a fair, accurate and

impartial way. This principle covers not only the publication of personal data, but also the collection of personal data, given that a long-term journalistic investigation must take into account possible changes in the data which may render the subject matter of the investigation irrelevant and no longer in the public interest to publish such information.

Principle of limitation of the duration of storage

Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. In the context of journalism, this means that, once all or part of the information has been collected and published, the journalist has to make certain decisions on how long the information collected must be kept. It should be noted that the obligation to keep a copy of a printed publication, audio-visual works and recordings of radio and/or television broadcasts for at least one year from the date on which the information was disseminated is laid down by the Law on the Provision of Information to the Public. Moreover, there is no statute of limitations for the defence of a person's moral rights, such as honour and dignity, before a court of general jurisdiction, so a journalist must be able to prove the legitimacy of the information published and the truth of the statements made indefinitely. The journalist must therefore have the information gathered in order to be able to prove the legitimacy of the information he/she has published. It should be noted that the GDPR does not stipulate how long the storage of personal data is allowed. The principle of limitation of the duration of retention only indicates that there is a valid reason for retention. Assuming that this reason exists, personal data may be kept indefinitely. However, journalists are advised to regularly review the information retained to ensure that the information held is still up-to-date, relevant and not excessive for the purposes pursued, and to delete any information that is objectively no longer necessary. In addition, the methods and time limits for storing information should be defined in the publishing house data management policy.

EXAMPLE.

A media outlet published an investigation into possible fraud schemes in a private company. The investigation included checks on employees' relationships with other individuals and collected a large amount of personal data that was not intended to be used in the specific publication, but was collected to provide information that could be relevant in the future if new circumstances emerged. However, in the absence of new circumstances, it is recommended to assess whether there is still a valid reason to process the data of the individuals concerned and to delete it if it is considered no longer necessary.

Principle of integrity and confidentiality

Personal data must be processed in such a way as to ensure, through appropriate technical or organisational measures, adequate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Information handled by journalists often contains highly sensitive personal data, and every effort must be made to prevent the loss, theft or misuse of personal data. Personal data must be handled in accordance with the procedures and security protocols established by the company (editorial office). All employees of the media company should be aware of the organisation's policies and procedures and follow them. Information should be locked, password protected and encrypted where possible. Media outlet staff should take special security measures when leaving the premises with documents, phones or laptops containing personal data. At the same time, it should be noted that information containing personal data should only be accessible to media outlet staff who are directly involved in the fulfilment of the journalistic purpose, i.e. access to journalistic investigative data should not be granted to staff performing general or technical functions, such as a financial officer.

EXAMPLE.

A journalist preparing a story on a politician's health to find out whether he can continue to perform his duties successfully gathered a variety of particularly sensitive health data. In this case, it is recommended to store the data in an additional password-protected folder or to give the data pseudonyms (using numbers or letter combinations instead of names) to protect it from leakage.

Accountability principle

The controller is responsible for compliance with Article 5(1) of the GDPR and must be able to demonstrate compliance. Under this condition, the controller is not only responsible for compliance with the GDPR, but must also be able to demonstrate compliance with the GDPR. In the case of a journalistic purpose, it is possible that an exception to the subject's rights has been implemented. In such cases, the media outlet or journalist should be able to explain why compliance with the relevant provisions was incompatible with the journalistic purpose. In this case, the journalist would have to demonstrate that he or she has carried out a balancing test taking into account the different interests involved.

EXAMPLE.

In the event of a complaint by an individual against a media outlet before a court or the Inspector of Journalists' Ethics for potentially unlawful processing of his or her personal data, the media outlet must be able to demonstrate that the processing of personal data was carried out in accordance with the GDPR, by means of the implementation of technical and organizational measures.

So, journalists should:

- Collect and use information about individuals in a fair and lawful manner, i.e. not collect personal data without a legitimate purpose, and in accordance with the principles of legality, fairness and transparency.
- Not to use personal data for any purpose other than journalism - to respect the purpose limitation principle.
- Ensure that the information is relevant, up-to-date and not excessive for the purpose pursued - follow the principle of data minimisation.
- No longer than necessary keep personal data. Consider how long it is mandatory to keep personal data collected - be guided by the principle of limiting the duration of storage.
- Protect information, i.e. not to send or otherwise pass on information to other journalists or media outlets that do not have a legitimate basis for receiving such data.
- Use a password on the computer on which the investigation material is stored to protect the information on the computer from being accessed by third parties.

- Apply an additional security code to folders where the journalist stores sensitive personal data (personal identification number, health data, etc.).

- Regularly update an anti-virus software to protect your computer from possible hacking.

-Ensure the physical security of data in your possession: do not leave unattended mobile devices, documents, dictaphones, hard drives, USB sticks or computers.

The GDPR does not provide for specific security and organisational measures for personal data, but Article 32 lays down a general rule and an obligation to provide for appropriate technical and organisational measures to ensure adequate protection of personal data. The Article sets out the criteria according to which these measures should be implemented:

1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a)	*the pseudonymisation and encryption of personal data;*
(b)	*the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
(c)	*the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
(d)	*a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in

paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

.

According to the Guidelines on the Protection of Privacy in the Media, media outlets should ensure and demonstrate compliance with data protection requirements in all possible ways and by all possible means. For example, the following "accountability tools" are recommended for media outlets:

- appointment of a data protection officer;

- establishment of a register of data protection processing activities;

- developing a privacy policy;

- developing an internal procedure to take into account the impact of data protection at key stages of journalistic activities and to take swift decisions in the event of ethical challenges;

- developing procedures for drafting internal memos, handling complaints from individuals, alerting the organisation's management, contacting the data protection authority, handling security breaches, etc.

It is recommended that editorial offices use personal data protection policy (Article 40 of the GDPR) and that they specify how and in what way personal data collected for journalistic purposes will be handled (stored), i.e. technical and physical security, personnel and organisational measures, training and supervision of staff, and that all staff are made aware of and comply with these policies. It is also recommended to stipulate who in the editorial office may have access to journalistic research material. For example, editorial staff who do not carry out journalistic investigations (HR specialists, administrators, accountants, etc.) should not have access to personal data collected during the course of investigation. It is also advisable to provide that certain categories of personal data, such as health data, should be regularly reviewed to assess whether it is still relevant to process such data. It is recommended that editorial offices should provide regular training to journalists on the basic principles of lawful processing of personal data, security risks, security procedures and so on.


How to balance the journalists right to get the information and the personal data protection requirements?

PART II

SAFETY RECOMMENDATIONS

Computer

Nowadays, one usually chooses a laptop computer for work, it is used not only in the office, but also at home or when travelling, which means that at some point there is a risk that a computer will fall into the hands of unauthorised persons who may misappropriate the data found on the computer. To prevent unauthorised persons from getting hold of the data on a lost computer, a computer intended for use with personal data must be adequately equipped and regularly maintained. Minimum requirements for a laptop computer:

1. The internal drives (data storage media) of the laptop must be encrypted. The easiest way to do this is to use the standard tools offered by the computer's operating system.

1.1. On *Apple* computers, data drives are encrypted using the *FileVault* tool of the *macOS* operating system. To check if encryption is enabled and to turn it on, use Apple menu > System Settings > Security & Privacy > FileVault. When encrypting your data, remember to keep your recovery key in a safe place, as if you forget your computer password, you will not be able to access your data without the recovery key.

1.2. A computer with *Windows* operating system must have at least the TPM (Trusted Platform Module) version 2.0 security assurance module, which is required to encrypt data disks. When choosing a *Windows* operating system, we recommend the following versions of *Windows 11*: *Pro, Enterprise* or *Education*, as they can use the built-in *BitLocker* data encryption tool, which is capable of encrypting not only the computer's internal data drives, but also portable USB data storage devices. *BitLocker* can also be used by the relevant versions of *Windows 7, Windows 8* and *Windows 10*, but these are already outdated operating systems the maintenance of which that have been or are about to be discontinued, which will create additional security problems. Advanced users can use other disk encryption tools such as *VeraCrypt*, etc. When encrypting data, remember to keep the recovery key in a safe place, as forgetting the computer's password will make it impossible to access the data without the recovery key. When disk encryption is enabled, it is indicated by a lock icon next to the disk icon:



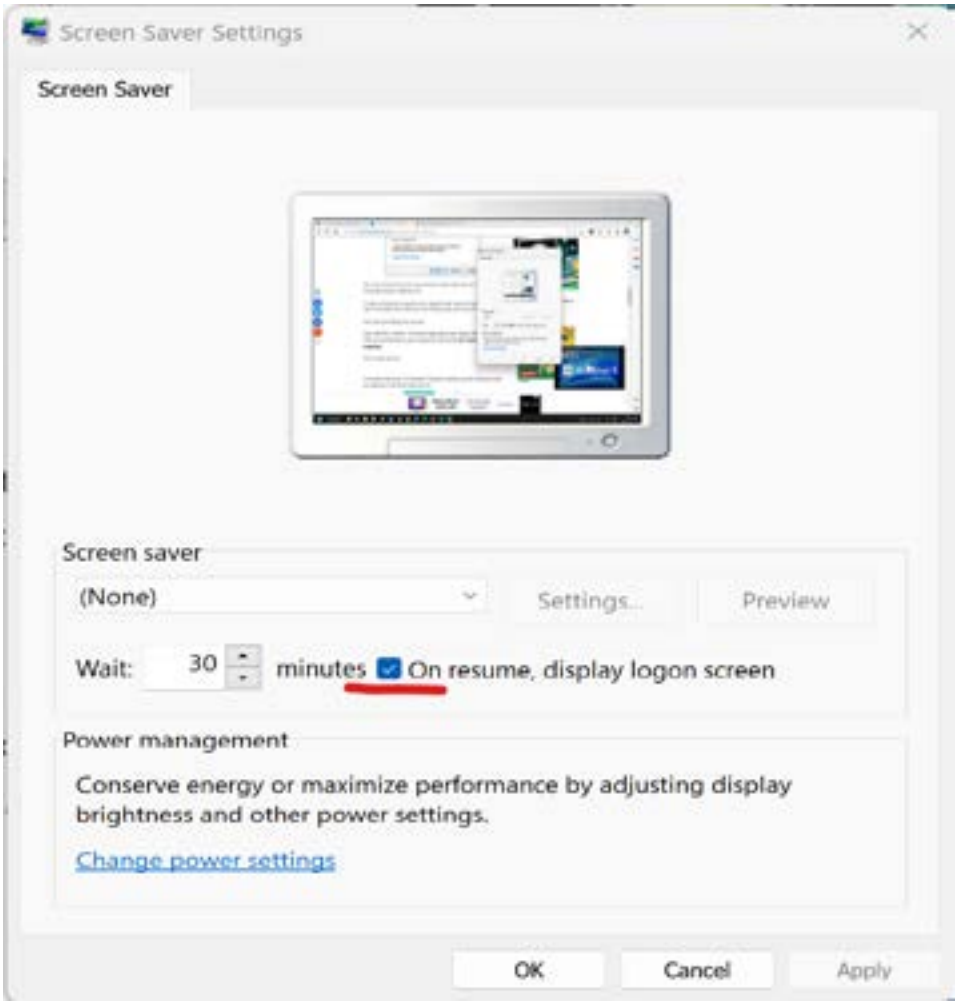
2. Your computer must be password protected. We recommend using a password of at least 11 characters, consisting of upper- and lower-case letters, numbers and special characters. The longer and more complex the password, the harder it is to guess. DO NOT use passwords that are easy to guess (1111, 1234, password, Secret123, etc.), and do not use your own or your loved ones' dates of birth, names or other data that are easily detected in your environment (pet names, car numbers, addresses, company code, your mother's first name, etc.).

3. If your computer is connected to an *Apple* or *Microsoft* account, make sure these accounts are protected with sufficiently strong passwords and two-factor authentication (2FA) is enabled.

4. In addition, you can enable fingerprint or camera face recognition to unlock your computer. This will not only allow you to unlock your computer quickly, but will also protect your computer password from being guessed while you are typing your password.

5. Your computer must have an anti-virus programme installed and kept up-to-date to protect your computer from the many computer viruses and other malware that can spread and steal information. Without proper protection, an intruder can use malware to take over your computer, steal stored data, find out passwords, etc.

6. Never leave your computer unattended with the screen unlocked. Keep your computer screen locked even when you step away for a short time. You can also use the screen saver feature to lock your computer after a few minutes of inactivity (in the search box, search for "*Screen saver*" and select "*Change screen saver*").


Screen Saver Settings
Screen Saver
Screen saver
(None)
Settings...
Preview
Wait:
30
minutes
On resume, display logon screen
Power management
Conserve energy or maximize performance by adjusting display brightness and other power settings.
Change power settings
OK
Cancel
Apply

7. Make sure you have backed up your most important data before you take your computer in for repair. We recommend that you remove your computer's internal data drives or make sure that the data on the drives is encrypted and inaccessible to unauthorised persons.

8. Before you dispose of an old computer that you no longer need, or before you pass it on (sell it, etc.), make sure you remove and destroy the data disks, or, if you are an advanced user and you know what you are doing, at least use special software to securely destroy all the data on your computer. REMEMBER - files that have been deleted by pressing *DELETE* button are very easy to recover and read!

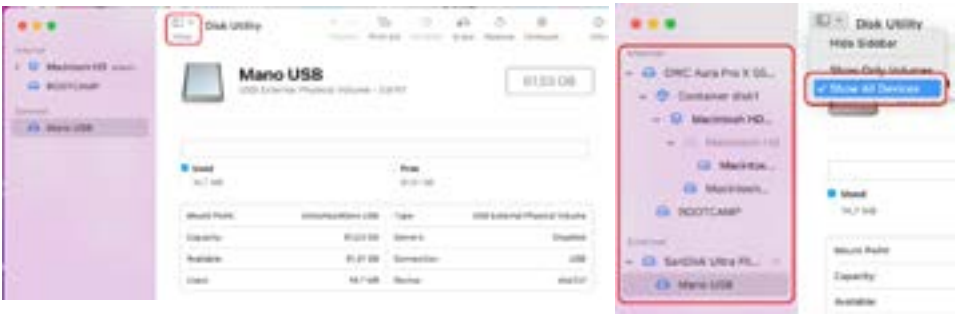
Portable data storage media

Different types of portable storage media are used to store data, such as USB sticks, external USB drives, memory cards (*SD, Micro SD, CF*, etc.), optical storage media (CDs, DVDs, BluRays, etc.), etc. They are small, often lightweight and easy to lose. Data media used to store personal and other confidential data must be encrypted or stored in securely encrypted files - data containers.

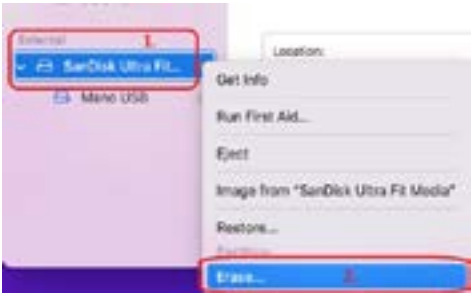
Data encryption techniques for portable data storage:

1. On *Apple* computers, encryption of portable storage media can be done using *Disk Utility* for the *macOS* operating system or third-party data encryption tools like *VeraCrypt*. With *Disk Utility* encryption, only Apple computers will be able to access the data without special applications. During encryption, all data on the media is erased. Portable storage media is encrypted on Apple computers as follows:

1.1. Once the *Disk Utility* application is open, click the *View* button and select *Show All Devices*. The view on the left side of the application window will change.



1.2. Make sure that all the data on the media is saved elsewhere, as it will be deleted. Highlight the media you want to encrypt and click on the *Erase* button in *Disk Utility*, or, put your mouse pointer on the media to be encrypted, tap with two fingers on the touchpad and select the *Erase* command from the pop-up menu. In the pop-up window that appears, select "*Scheme: GUID Partition Map*", then "*Format: APFS (Encrypted)*", in the pop-up window that appears, type in your password twice, enter a name for the encrypted media, and then click on the *Erase* button. That's it - the portable storage medium is encrypted. The next time you connect an encrypted portable storage device to your *Apple* computer, you'll be prompted for the unlock password you just made up.







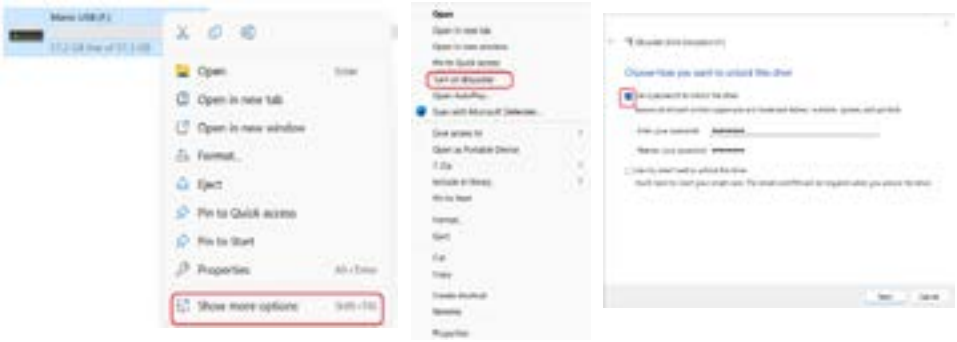


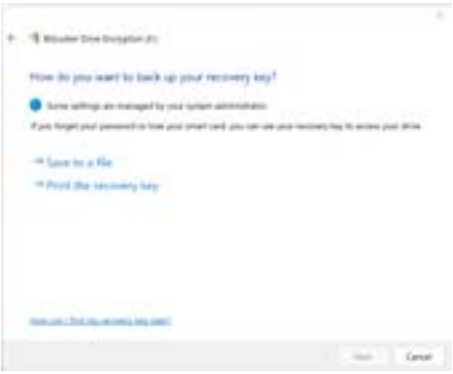
2. On PCs running *Pro, Enterprise* and *Education* versions of the *Windows* operating system, you can encrypt your portable data storage using the built-in *BitLocker* data encryption tool or third-party data encryption tools such as *VeraCrypt*. The *BitLocker* encryption tool is easy to use, is suitable wherever *Windows 7* or later version is used, and has a high level of security (if a complex password is used). With *BitLocker* encryption, data can only be accessed on computers running the *Windows* operating system without special applications. Shouldn't it be like this: portable storage media on computers with *Windows* operating system is encrypted as follows:

3. Put your mouse pointer at the media you want to encrypt, right-click, select "*Show more options*" from the pop-up menu, then select "*Turn on BitLocker*", tick the "*Use a password to unlock the drive*" checkbox, enter the password you've made up twice, and then click "*Next*".

In the window that opens, choose how you want to save the emergency unlock key: save it to a file ("Save to a file") or print it out.

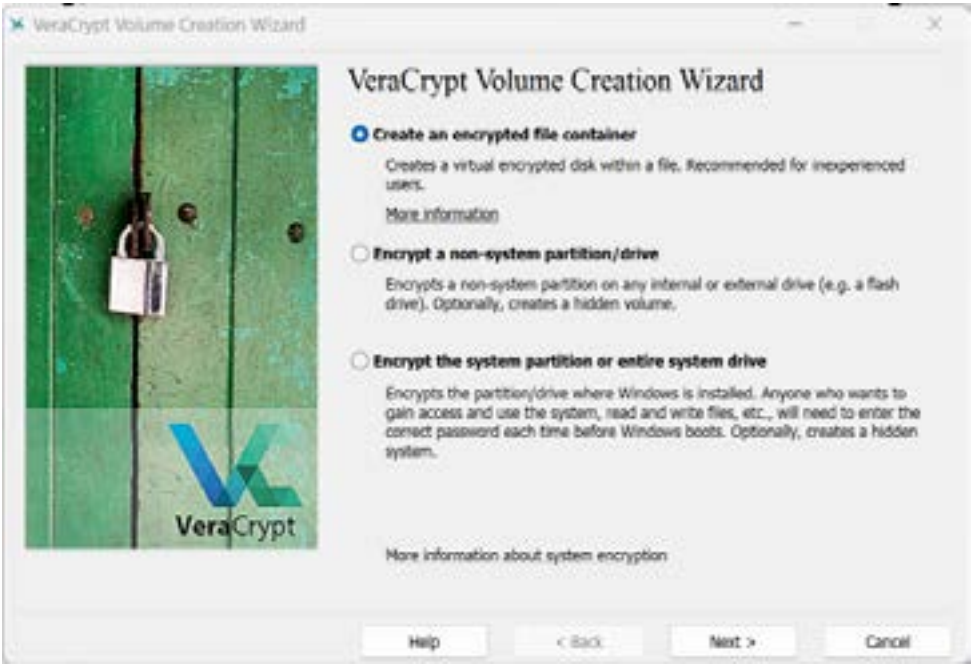
3.2. In the new window, choose whether you want to encrypt only the data footprint or the entire data storage medium. The first choice is for data media that have not yet been used, while the second choice is for encrypting data media that have been used before (more secure). After clicking "*Next*", select "*Compatible mode*" for the portable storage medium and click "*Next*" again. In the next window, click "*Start encrypting*" and wait for the encryption to finish.







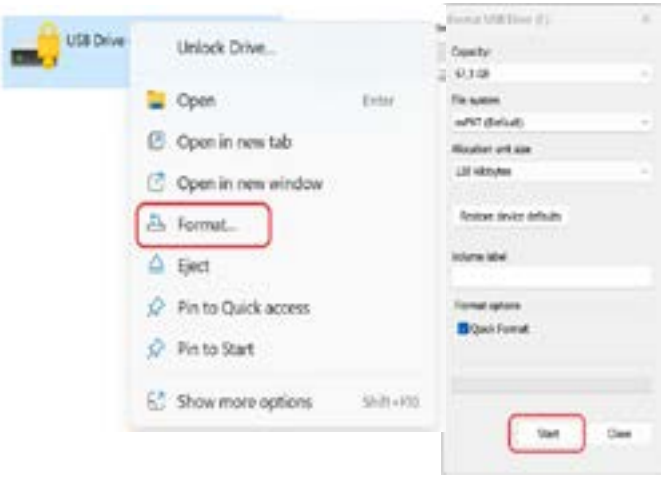
4. Special media and data encryption software, such as the free, open source encryption software *VeraCrypt*, can also be used to encrypt portable data media. It works on most operating systems and can not only encrypt the entire data medium, but also create encrypted files of the required size, i.e. data containers into which data files can be uploaded. *VeraCrypt* is a free and highly secure alternative, but it is more complex to use than *BitLocker*.



5. Use of special encrypted portable USB storage devices. Special encrypted USB sticks and drives using hardware data encryption may be used for data storage and transport. This is one of the most secure ways of transporting and storing data. There are versions with a physical keypad for unlocking and versions without a keypad, which are unlocked from the USB key by launching an unlocking application. Encryptable USB keys with physical keyboard work on any operating system (*Windows, Apple macOS, Android, iOS*, etc.)



6. Dispose of old, defective and unwanted portable data media or securely destroy the data before transferring it to other persons. This can be done by using special applications with secure data destruction functionality or by simply formatting the encrypted data storage medium without unlocking it. Special encrypted USB sticks can also destroy data if you enter the wrong password or PIN code multiple times (some encrypted USB sticks are "destroyed" if you enter the wrong code 10 times or more and can no longer be used). REMEMBER - files that have been deleted by simply pressing the *Delete* button are very easy to recover and read!



Mobile phones and tablets:

It's hard to find anyone these days who doesn't have at least one mobile phone, usually a smart one. We use our phones to make calls, to communicate by text and email, to take photos and videos, to record audio, to browse the internet, to navigate and for many other activities. Telephones are also widely used for authentication when connecting to various e-services portals, for banking, for electronic payments, for unlocking doors or cars, for storing contacts, notes, passwords and other important data. A tablet is usually the same as a smartphone in terms of functionality, but bigger. A smartphone and a tablet are a treasure trove of information for the curious individual or organisation. Therefore, these devices need to be particularly well protected.

Tips to protect your phones and tablets:

1. Your phone and tablet must be protected with a password or PIN. We do not recommend using "*Pattern lock*" as it is quite easy to guess or bypass. A fingerprint or a camera face recognition lock can be used in combination with a PIN or password.

2. Data encryption is turned on by default in all modern smartphones and tablets, but Micro SD memory cards in phones and tablets are usually not encrypted, so you should not use Micro SD cards to store information, or you should also turn on data encryption before using them. A Micro SD card that has been encrypted on your phone or tablet will only be unlocked and used on the phone or tablet that was used to encrypt the card.

3. We recommend that you only register your smartphones and tablets with your own well-secured Google (for *Android* phones) or *Apple* (iPhone, iPad) account, as phones and tablets can be controlled (see location, view and manage your contact list, install apps, lock your phone and tablet, and delete all data on it) through your Google and Apple accounts.

4. For security reasons, we recommend that you regularly update the software on your phones and tablets, and that you install security updates for *Android, iOS* and iPad operating systems to fix security gaps. It is better not to use old phones and tablets that are no longer supported by their manufacturers due to security issues that are no longer solved.

5. Dispose of old phones and tablets that you no longer need, or restore them to their manufacturing settings and delete all data in the process.

Features of creating and storing passwords

A few decades ago, it was enough to remember one or two passwords. But these days, the list of websites and accounts you might want to sign up for is almost endless. Worse still, hackers like users who repeatedly use the same passwords. That's why it's important to make them strong and unique for each website or account. Tips for choosing passwords:

1. Use all symbols. We tend to have multiple online accounts, so many of us take the easy way and create easy-to-remember passwords (e.g. Secret, qwerty, 1234, 1111, Spring, etc.). Unfortunately, these simple passwords are easy to hack. There are databases of commonly used passwords on the Internet that are widely used by hackers. To create a good password, mix uppercase, lowercase letters, numbers and special characters. For example, instead of "**Bingo123**" it is much better to use "**b1Ng01789;**". You can also replace letters in words with similar symbols or numbers, e.g. instead of "**druskininkai**" use "**dru5k!n!nk4!**" etc.

2. Variety is key. Typically, most of us have at least one social network account (Facebook, Twitter), a bank account that we access frequently, various service accounts, a cloud account (Dropbox, Onedrive, iCloud), an email account (Gmail, Outlook.com), an app store (App Store, Google Play) and a few other accounts for online activities. Remembering so many different passwords is not easy, so many people tend to use the same password for several accounts. This is a bad choice, as a hacker always tries to use the hacked password of one account on other accounts of the same person and unfortunately often succeeds in hijacking them (domino effect). Using different passwords for different accounts makes it much harder for hackers to work and protects your data.

3. Personal information is not suitable for a password. Names, surnames, pet names, birthdays or other dates that are important to you, or other information that can be easily linked to you, are not suitable for passwords, as the password will be easily guessed once information about you has been collected.

4. Old passwords are dangerous. Change the passwords of at least your most important accounts and systems periodically - there's a good chance that a password you've been using for a long time is known to someone and even used to log in on

your behalf.

5. Use of Two Level Authorisation (2FA). No online account security is complete without the use of two-factor authentication (2FA). Two-factor authentication uses what you know (answers to questions), what you have (phone, computer, code generator), or who you are (your fingerprint, face, voice). With two-factor authentication, when you log in to your online account, you will be asked not only to enter your password, but also, for example, to enter a one-time code received by SMS, to use your fingerprint, to give an answer to a question that only you know, etc. Many online accounts ask you to provide your phone number for this purpose and then send you a one-time login verification code by text message. You can also use special apps on your smartphone for a two-factor authentication, such as *Google Authenticator, Microsoft Authenticator, Authy* and others. Using two-factor authentication greatly enhances the security of your accounts and data.

6. Using password storage apps. A password manager is one of the most important tools for the modern internet user. When you use it, all your passwords are stored encrypted on your computer, your phone or on the server of the manufacturer of the password storage app. As well as storing passwords, a password storage app can generate passwords, assess the complexity of the passwords you use, notify you if your account logins are found to have been used by hackers, and store other confidential information. It is necessary to protect your password storage application account with two levels of authorisation and a password that is difficult to guess. The most popular password storage apps are *LastPass, Bitwarden, Dashlane, Keeper, 1Password, NordPass and Roboform*. All the most popular web browsers also have the option to store your passwords, but this method of storage is less secure.

7. Keep your passwords safe from prying eyes. It seems like a simple rule, but many people ignore it. However, if you work with confidential data, this rule should not be ignored. So:

7.1. Do not enter your passwords with anyone watching. Many smartphones, tablets and many laptops can be unlocked using a fingerprint or a camera that recognises your face, rather than a password or PIN - use it.

7.2. If you have written your password on a slip of paper, don't write what it's for, or don't write down the whole password. Do not keep your written password within the easy reach of others, do not stick slips with password on screens, keyboards, desks, etc., and do not dispose of your password slip in the trash without destroying it first.

8. The length of the password is also important. As computers get faster and computing power increases, the length of the password also matters: the shorter the password, the faster a powerful computer can "guess" it. Currently, various sources recommend using a password of at least 11 characters, made up of at least numbers and upper and lower case letters, which can take around 40 years to "guess", while 12 characters can take thousands of years, while a 12-character number password can be guessed in seconds.

CAUTION - Phishing

The National Cyber Security Centre (NCSC) provides the following definition of phishing: "Data theft - phishing (from English – password fishing) is a form of fraud against organisations or individuals that uses spam emails or spoofed websites to obtain passwords and other confidential data to access information systems."

These attacks are mostly targeted at bank customers to obtain login credentials to steal money through e-banking, but users of other electronic services can also fall victims of phishing.

Criminals usually use mass emails, SMS or social networking messages containing false information with specially generated links to fake emails, banks, social networks, e-payment systems and other websites, where users are asked to enter their login details, i.e. usernames, passwords, bank card details etc. Usually there are mistakes in such fraudulent websites, but there are also very professionally designed websites, so you should always be vigilant.

Recommendations for protection:

1. Check the sender of the email. No government institution or bank sends emails using email servers such as gmail.com, yahoo.com, outlook.com and the like. If you see that you are being emailed, e.g. policija@gmail.com, prokuratura@outlook.com, swedbank@gmail.com, etc., this is a clear sign that the email is a fake.

2. Never click on links in messages and emails. Especially if the links are in emails you weren't expecting. Manually type the address of the website into your browser and look for the information you need there. Links may take you to fake websites that look very similar to the ones you expected when you clicked on the link. One quick way to check if a link is safe is to put the mouse pointer over it. When you do that, don't click on it, just wait until the actual address appears at the bottom of your browser or next to the mouse pointer. Sometimes the address looks

very similar because some of the letters in the address have been replaced by other very similar letters or numbers, e.g. *Factbook.com ('t' instead of 'e'), swedbank.it ('i' instead of lower case 'L'), etc.*

Destruction of printed information

In addition to digital information media, a wide range of information is stored in printed copies. Printed confidential information should not fall into the hands of persons not authorised to see it. Such documents cannot simply be thrown away in waste bins. There are a number of ways of destroying unnecessary documents, but the most popular way of destroying documents in the office is with special document shredders that can shred unnecessary paper documents or even optical data discs (CDs, DVDs). Document shredders are divided into 7 security classes, denoted by the letter "P" and a number from 1 to 7. The higher the security class number, the finer the document is shredded. The larger the fragment of the document that remains after shredding, the easier it is to recover the document. P1 and P2 shredders cut documents into full-page strips that can easily be re-stapled, making them unsuitable for shredding confidential documents. For this purpose, it is recommended to use P5 or higher class shredders. By comparison, a P4 shreds an A4 sheet into approximately 421 pieces, a P5 into 2000 pieces, a P6 into 6000 pieces and a P7 into as many as 15000 pieces.

The publication contains only the views of project managers. They are entirely responsible for the content. The European Commission accepts no responsibility for any impact that may result from the information contained in this publication.

HOW TO PROCESS PERSONAL DATA FOR SCIENTIFIC PURPOSES?

Guidelines

Abbreviations

GDPR – Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC and applied since 25 May 2018 (General Data Protection Regulation)

ADTAĮ – the Republic of Lithuania Law on Legal Protection of Personal Data

Charter – the Charter of Fundamental Rights of the European Union

EDPB – European Data Protection Board

EU – the European Union

CJEU – the Court of Justice of the European Union

ECHR – the European Court of Human Rights

LAT – the Supreme Court of Lithuania

LVAT – the Supreme Administrative Court of Lithuania

MRU – Mykolas Romeris University

TFEU – the Treaty on the Functioning of the European Union

ŽEIT – the Office of the Inspector of Journalist Ethics, a supervisory authority

Data subject means a natural person whose personal data is processed.

Controller means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the data processing; where the purposes and means of such processing are determined by EU or Member State law, the controller or the specific criteria for their appointment may be determined by EU or Member State law.

Processor means a natural or legal person, public authority, company or other organisation that processes personal data on behalf of the controller

Introduction

The Charter of Fundamental Rights of the European Union (hereinafter the 'Charter') enshrines the right of every person to the protection of their personal data. Following Article 8(2) of the Charter, "such data must be properly processed and used only for specific purposes and only with the consent of the person concerned or on other legitimate grounds laid down by law. Everyone has the right to to access and rectify their personal data collected." It is also worth recalling that Article 7 of the Charter, as well as Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, ensures respect for the private and family life of the individual, their home and communication. This legislation is complemented by Regulation (EU) 2016/679 of the European Parliament and of the Council of 25 May 2018 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which repealed Directive 95/46/EC (General Data Protection Regulation) (hereinafter 'the Regulation' or 'GDPR') and came into force on 25 May 2018 in the entire European Union, including Lithuania.

The Regulation requires very high standards for personal data protection and provides for strict sanctions for non-compliance with these standards. On the other hand, the GDPR provides for exceptions that set out derogations from certain rights relating to the protection of personal data, for example, with regard to the processing of personal data for scientific research purposes. Following the Regulation, the legislation of the European Union or of a Member State can set out provisions for derogations in relation to the rights referred to in Articles 15, 16, 18 and 21. Following the new Republic of Lithuania Law on Legal Protection of Personal Data, which came into force on 16 July 2018, some provisions of Regulation (EU) 2016/679 8 do not apply when data is processed for academic purposes. However, we may often encounter questions, such as: What is data processing for scientific purposes? Is it allowed to disseminate personal data for academic purposes? What obligations stem from the processing of personal data for research purposes? How to process particularly sensitive data, e.g. in the case of health research? How to prepare for the processing of personal data in scientific projects?

We hope these guidelines will help you with the above questions and processing personal data safely, per GDPR requirements.

This publication shall be an integral part of the EU-funded project: "Connecting not conflicting: removing the tension between personal data protection

and freedom of expression and information" — CONCON). For more information about the project, click the following link to see the record of the project opening event:

https://www.youtube.com/watch?v=lYGfEp4JlCI&ab_channel=NAME-EVENTPLANNINGAGENCY



PART I:
DATA PROCESSING FOR RESEARCH PURPOSES
WHAT IS PERSONAL DATA?

The term **'information'** encompasses audio, video, genetic data, fingerprints, traits of mental, economic, cultural or social identity, etc. This information can be provided in letters, numbers, graphic and photographic images, sound (via phone) and other forms.

A person can be identified:

- **directly**, using identifying data (e.g. by name, personal number, etc.), or
- **indirectly**, i.e. when the data available is not sufficient to identify a specific person, but it is possible to identify the person by using other data, regardless of whether the relevant authority has it (e.g. car registration number, video data, telephone number, etc.).

As for the processing of personal data for research purposes, it is particularly important to note that specific processing rules are provided for certain categories of personal data. **Fundamental importance is given to personal data** on a person's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic and biometric data that are processed to specifically identify the natural person; health data or data on the sex life and sexual orientation of a natural person.

"**Genetic data** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question." (Article 4(13) of the GDPR)

"**Biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data." (Article 4(14) of the GDPR)

"**Data concerning health** means personal data related to the physical

or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status." (Article 4(15) of the GDPR)

According to Article 29 Working Party's letter of 5 February 2015 on mHealth, addressed to the European Commission, health data should be understood much more broadly than medical data. Based on the established practice of applying data protection legislation in various EU countries, such information as personal intellectual and emotional abilities and qualities (e.g. IQ), person's height, weight, a fact that the person has injured the leg and is temporarily unfit for work (e.g. Lindqvist case), that the person wears glasses or contact lenses, information on smoking habits, drug and alcohol consumption habits, allergy data disclosed to private entities (e.g. bank, insurance company or airline company) or public sector bodies (e.g. school, state social insurance institution or university hospital); membership of a person in a patient support group (e.g. cancer support group), alcoholics anonymous, group psychotherapy or other self-help and support groups with health-related goals; even information about the fact that someone is sick in the context of an employment relationship – all this is considered to be personal health data.

Similar practices are followed by the the Supreme Administrative Court of Lithuania, in its practice stating that the concept of personal data must be interpreted broadly. On 2 March 2022, the Supreme Administrative Court of Lithuania stated: "The data on a relative of the patient, recorded in the epicrisis of the history of the disease, shall be considered to be the personal data of that relative of the patient, i.e. relatives of patients whose data are indicated in the epcrisis of the history of the disease of the patients, even in the absence of indication of their names, shall be as well considered as data subjects in respect of this data."

Health data can be collected from various sources:

Medical patient history collected in a healthcare institution;

Information that becomes available by linking health data to other data, thereby revealing the state of health or health risks (e.g. the assumption that a person has a higher risk of having a heart attack due to high blood pressure measured

over a period of time);

The information obtained from a self-examination survey in which data subjects respond to questions related to their health (e.g. symptoms);

Information that becomes health data due to its use in a specific context (e.g. information about a recent trip to or presence in a region affected by COVID-19, processed by a medical professional for diagnosis).

Processing of personal data of special categories is generally subject to more stringent safeguards!

What data does GDPR not apply to?

- Information about **a deceased person** is not personal data, therefore, the processing of data of deceased persons is not subject to the GDPR.
- Information about a legal person, separately from its owners or directors, is not personal data and does not fall within the scope of the GDPR. Information about public authorities is also not considered personal data.
- The GDPR shall not apply to **the processing of anonymous information**, including the processing of data for statistical or research purposes. Personal data, rendered anonymous in such a manner that the data subject is not or no longer identifiable, shall no longer be considered personal data. In order for the data to be truly anonymous, anonymity must **be provided irreversibly**. The personal data from which the personally identifiable information is removed, which is encrypted or pseudonymised, but which can be used to re-establish the identity of the person, remains personal data!

What is scientific research and academic self-expression?

The preamble to the Regulation (recital 159) states that "the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health."

In the Law on Higher Education on Research, **research and experimental development** is defined as "systematic creative activity of the study of nature, man, culture and society, and the use of the results of such activity."

In the context of the application of the GDPR, research can be carried out by various public sector bodies, not necessarily only in scientific and study institutions. It is important that research carried out are in line with methodological and ethical requirements and good practices in its field (e.g. health sciences).

For example, data for research may also be collected in a health institution whose main purpose is providing health services rather than scientific activity.

For example, the recital of Directive (EU) 2019/790 of the European Parliament and of the Council states: "Research organisations across the Union encompass a wide variety of entities the primary goal of which is to conduct scientific research or to do so together with the provision of educational services. The term 'scientific research' within the meaning of this Directive should be understood to cover both the natural sciences and the human sciences. Due to the diversity of such entities, it is important to have a common understanding of research organisations. They should for example cover, in addition to universities or other higher education institutions and their libraries, also entities such as research institutes and hospitals that carry out research. Despite different legal forms and structures, research organisations in the Member States generally have in common that they act either on a not-for-profit basis or in the context of a public-interest mission recognised by the State. Such a public-interest mission could, for example, be reflected through public funding or through provisions in national laws or public contracts. Conversely, organisations upon which commercial undertakings have a decisive influence allowing such undertakings to exercise control because of structural situations, such as through their quality of shareholder or member, which could result in preferential access to the results of the research, should not be considered research organisations for the purposes of this Directive."

The guidelines adopted by the Ombudsperson for Academic Ethics and Procedures on 10 December 2020 for the assessment of compliance with research ethics states that "the researcher must follow the principles of reliability, integrity, respect and accountability". Specific requirements for compliance with research ethics are set for biomedical research and research/testing on animals.

For example, the Law on the Ethics of Biomedical Research of 11 May 2000 provides for special ethical requirements for the implementation of biomedical re-

search, defining it as "verification of hypotheses of biomedical sciences by means of methods of scientific research pursuing the aim of developing scientific knowledge about human health, diseases, diagnosis, medical treatment or prevention thereof".

In Sorguç against Turkey case, ECHR stated that academic freedom in scientific research and training should guarantee freedom of expression and action, freedom to disseminate information and freedom to conduct scientific research. and to spread knowledge and truth without any

Processing of personal data for the purposes of **'academic self-expression'** means (1) processing directly related to the freedom of academics to disseminate information, (2) their freedom to freely disseminate knowledge and truth, e.g. through publication, dissemination of research results, and (3) sharing data and methodologies with colleagues and exchange of views and approaches. In its preliminary opinion, EDPB "considers that the specific data protection regime for research shall be applied when all three criteria are met:

1) personal data are processed;

2) appropriate sectoral methodological and ethical standards are applied, including informed consent, accountability and supervision;

(3) scientific research are carried out with the aim of increasing collective knowledge and welfare of society, and not primarily to satisfy one or more private interests."

What exception are applied when processing personal data for research purposes?

Article 89(2) of the GDPR states that "where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes."

Article 4 of the Law on Legal Protection of Personal Data provides that "where personal data are processed for the purposes of journalism or academic, artistic or literary expression, articles 8, 12-23, 25, 30, 33-39, 41 to 50, 88 to 91 of the Regulation (EU) 2016/679 shall not apply."

In other words, the processing of data for academic purposes **is not subject to the GDPR provisions** on the consent of the child to whom information society services are offered; on the rights of the data subject; on records of processing activities; on notifications to the supervisory authority and the data subject about a personal data breach; on the assessment of the impact on data protection and prior consultation; some provisions on codes of ethics and certification; on the transfer of personal data to third countries or international organisations; on the processing of data in an employment context and the obligation of secrecy.

However, the controller and the processor must comply with the fundamental principles of personal data protection established by the GDPR, even when processing data for scientific research purposes!

It should also be noted that, **according to the CJEU case-law**, all restrictions on the rights of data subjects must be applied only to the extent that is strictly necessary.

Thus, the permitted derogation from certain provisions is not absolute! The controller and the processor must:

Ensure measures of data protection, such as pseudonymisation;

Demonstrate that without derogation from before mentioned rights specific objectives may not be achieved or these rights may constitute a serious obstacle to achieving them.

The right to access information for academic purposes

Principles of EU scientific research policy and facilitating data sharing

Under Article 13 of the EU Charter, "arts and scientific research must not be restricted. Academic freedom must be respected."

Following article 179(1) of the TFEU, "the Union shall have the objective of strengthening its scientific and technological bases by achieving a European

research area in which researchers, scientific knowledge and technology circulate freely, and encouraging it to become more competitive, including in its industry, while promoting all the research activities deemed necessary by virtue of other Chapters of the Treaties."

The EU therefore encourages the sharing and reuse of research data. Public funding for research projects shall be provided on condition that their results are disseminated and shared with the public.

Public Sector Information Directive requires **public sector bodies to allow the reuse of all public information**. The Directive requires Member States to "ensure the accessibility of research data" by means of measures to "make publicly funded research data freely accessible (open access policy)". This openness is subject to certain limits: the Commission Recommendation on access to and storage of scientific information States that research data should be "as open as possible, as close as necessary".

Scientific research data includes not only peer-reviewed publications, but also data that underpin the findings so that other researchers can re-apply or rely on the methods. This allows to combine data from several research and build on it instead of replicating existing studies, thus the data can be used for completely different purposes than they were originally collected for!

The ECHR has also shared its opinion on the accessibility of information on several occasions.

"Article 10 shall not entitle a person to access information held by a public authority and shall not oblige the Government to provide such information to a person. However, such a right or obligation may arise where access to information is essential for the exercise of a person's right to freedom of expression, in particular 'freedom to receive and disseminate information', and where refusal to grant it constitutes interference with that right" (ECHR, *Magyar Helsinki Bizottsag against Hungary*).

Threshold criteria for access to state-protected information (ECHR, *Magyar Helsinki Bizottsag against Hungary*):

(A) **the purpose of the request for information**

In order to apply Article 10, it must be ascertained whether the information requested is indeed necessary for the exercise of freedom of expression. In the

ECHR's view, access to information would be considered necessary if failure to receive it would hinder the person from exercising their right to freedom of expression, including the freedom to "receive and disseminate information and ideas", in a manner consistent with such "duties and responsibilities" as may arise from Article 10(2).

For example, in the case of scientists, such information may be necessary for the preparation of a scientific paper or a book. In *Sheks against Croatia*, ECHR stated: "in the Court's view, it is not very important whether the documents were indeed of great importance for its book; it is sufficient that the applicant sought to get to know them in order to provide his readers with a detailed and exhaustive chronology of the events that took place during that period."

(B) **the nature of the information requested**

The ECHR considers that, in order to create a need for disclosure under the Convention, the information, data or documents to which access is requested normally shall have to meet the criteria of public interest. Such a need may exist where, *inter alia*, disclosure ensures transparency on the manner in which public affairs are handled and on issues of public-wide interest, thereby enabling the general public to participate in public governance.

The Court emphasised that the circumstances of each case determine what might be considered a public interest subject. The public interest relates to issues which affect society in such a way that it can legitimately interest them, which attract its attention, or which are of great concern to it, especially because they affect the well-being of citizens or the life of the community. This may include data that is controversial, may be related to an important social issue or a problem that the public would be interested in being informed about. The public interest cannot be reduced to the public's desire to receive information about the private interests of others. In order to determine whether a publication relates to a matter of general interest, it is necessary to assess the entire publication in the context in which it appears.

For example, in the *Sheks against Croatia* case, the ECHR agreed with the conclusion of the Croatian Constitutional Court that "the scientific monograph on the establishment of the Republic of Croatia was a matter of public interest."

(c) **the role of the applicant**

In the judgment of the ECHR in *Magyar Helsinki Bizottsag against Hungary* case, it is stated to be "important to take into account whether a person seeking

access to relevant information does so in order to inform the public as a 'guard dog'. However, this does not mean that access to information should be restricted to NGOs and the press. The Court reiterates that a high level of protection also applies to academic researchers (see judgment in *Başkaya and Okçuoğlu against Turkey* [GC] case").

(D) **the readily available information**

This means that the requested information is "readily available" and that the authority, from which the information is requested, is not required to collect any data. On the other hand, the public authorities cannot refuse providing information on the grounds of difficulty, if such difficulty arises from the practice of the public authority itself.

PART II: RIGHTS AND OBLIGATIONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA FOR RESEARCH PURPOSES

Data processing means "any operation or set of operations which is performed upon personal data or 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, erasure or destruction." (Article 4(2) of the GDPR).

The processing of personal data for research purposes is subject to appropriate safeguards for the rights and freedoms of the data subject as provided for in the GDPR. Those "safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the **principle of data minimisation**." (Article 89(1) of the GDPR). Those measures may include **pseudonymisation or depersonalisation** provided that those purposes can be fulfilled in that manner.

In other words, the purpose of the safeguards is (a) to protect the rights and freedoms of data subjects and (b) to process personal data as little as possible and only to the extent necessary to achieve the research purposes. However, it is not always possible to achieve the research purpose by depersonalising the data, and in such cases other technical or organisational safeguards must be taken.

Personal data which are pseudonymised and which could be attributed to a natural person by means of additional information should **be considered as information about an natural person** who can be identified.

In determining whether a natural person can be identified, it is necessary to:

- take into account all means, **for example** exclusion, which could reasonably be used by the controller or another person to identify a person, directly or indirectly.
- in determining whether certain measures could reasonably be used to identify a natural person, account should be taken of all objective factors, **for exam-**

ple the costs and the time required to identify, given the technological development and technologies available at the time of processing.

- It is also necessary to assess whether the identity of the person could not be established on the basis of data held by third parties.

Thus, even if pseudonymisation methods have been applied, this data is still considered personal data in accordance with Article 4(5) of the GDPR!

It should be noted that the complete depersonalization of genetic data is practically impossible, and therefore the processing of this data should always comply with the requirements of the GDPR!

Depersonalisation of data is particularly important in the publication of research results in scientific publications: personal data for publication or dissemination should be technically processed in such a way that it is not possible to identify the data subject.

The principle of data minimisation enshrined in the GDPR means that the scope of processing of personal data should be minimised in accordance with the principles of proportionality and necessity. It is proposed to define research questions as precisely as possible and to assess what data is needed. If scientific research can be conducted using anonymised data, it should be done.

"Personal data must be (...) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')". (Article 5(1)(c) of the GDPR)

For example, if, in the beginning of the scientific research, it is understood that some of the data collected are excessive and not to be used for scientific research purposes, excess personal data that are not necessary to posses must be destroyed in order to protect data subjects from the potentially improper processing of their personal data. For example, when collecting data on the most common chronic diseases among men of working age in Vilnius, data on their family status were also collected. During research it became clear that data will no longer be used for the

purpose of the scientific research. Such data should therefore be further processed and destroyed.

Technical and organisational measures include:

- pseudonymisation and encryption of personal data;
- the ability to ensure the continued confidentiality, integrity, availability and resilience of data processing systems and services;
- the ability to restore the conditions and access to personal data in a timely manner in the event of a physical or technical incident;
- the verification, assessment and assurance of a regular performance evaluation process of technical and organisational measures to ensure the security of the processing;
- measures shall be taken to ensure that any natural person under the authority of the controller or the processor who has access to personal data does not process them unless the controller has instructed them to be processed, except where that person is obliged to do so in accordance with the law of the EU or Member State.

In addition, Article 32(2) of the GDPR states that "in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

The Regulation also requires to establish **reasonable period for which the personal data shall be stored.** As stated in Article 5(1)(e) of the GDPR, "personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes (...), scientific (...) research (...) purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject." The periods of storage should depend on the duration and objectives of the scientific study.

Other important principles of personal data processing

The controller and the processor must also comply with other principles of personal data processing set out in Article 5 of the GDPR. This is especially important because large amounts of (often particularly sensitive) personal data can be processed for scientific research purposes.

The principle of transparency. The controller and the processor of personal data must comply **with the principle of transparency** – personal data must be processed in a fair and transparent manner in respect of the data subject. It is related to the obligation to **properly inform the data subject** about the processing carried out. Depending on the nature of scientific research carried out, different requirements regarding informing the data subjects may be imposed.

The more significant data (e.g. genetic data) is used for scientific research, the more detailed the information on transparency, such as the specification of types of research and the updated consent, should be.

For example, when personal data is collected from the data subject for biomedical scientific research, the following information is required:

the purpose of biomedical research, the plan, and the methods used;

decisions of the Lithuanian Bioethics Committee or the respective regional biomedical research ethics committee;

the expected benefits of biomedical research for the subject;

research rights, possible risks and inconveniences that the subject may be caused by biomedical research, as well as the procedure for compensation of possible damages caused by biomedical research;

the right of the subject to withdraw in writing the consent of the person to participate in the biomedical research at any time, providing information on the consequences of termination of such biomedical research;

guarantees of confidentiality of information.

Principle of purpose limitation. The controller and the processor must comply **with the principle of purpose limitation**, i.e. data are collected for spec-

ified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes pursuant to article 89(1) shall not be considered incompatible with the original purposes.

The purpose for which the personal data will be processed **must be defined in advance**, i.e. before the person gives their consent to the processing of their personal data. Personal data cannot be collected simply because this data may be useful in the future.

For example, researchers decided to conduct research on lung cancer and collect data from individuals related to their health. Thus, the data collected has to be related to the planned research. The case where the data collected is not needed for a specific study, but where researchers take the opportunity to try to gather as much information (data) as possible for undefined future studies, is not appropriate.

However, "it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose." (recital 2 of the preamble to the GDPR). Thus, even if the controller and the processor are unable to formulate a specific purpose, it must be clear to the data subject that their data will be used for scientific research. In such cases, it is particularly important to give the data subject the right to withdraw consent and to inform them of such possibility.

While recital 33 of the GDPR gives some flexibility in describing the purposes of the research for which the data subject's consent is obtained, the requirements of Article 5 of the GDPR must still be met in order to ensure that the processing is lawful, fair and transparent. It is therefore necessary to narrow down the areas of research, to provide the context in which personal data are collected, and to take into account the reasonable expectations of data subjects.

For example, the European Court of Human Rights emphasises in its jurisprudence that data is essential for the person to be able to exercise their right to respect for private life, as guaranteed by Article 8 of the Convention. National law must therefore provide for adequate safeguards to prevent any use of a person incompatible with that Article's guarantees. National law should, in particular, ensure that such data are relevant and not excessive, taking into account the purposes for which they are stored, and are stored in a form that allows the identification of data subjects for no longer than is necessary for the purpose for which those data are stored. National law must also provide adequate guarantees to ensure that the personal data stored is effectively protected against abuse.

Re-processing or further processing of data

Personal data may **be reused or used for further research** only if appropriate safeguards are complied with in the further processing of data for scientific research purposes. It is important that further processing is consistent with the clearly defined and legitimate purposes for which the data were collected. In case of specific categories of personal data (e.g. personal data relating to health), it is necessary for the further processing to take place with the explicit consent of the subject, unless the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the objective pursued. In addition, further processing of personal data must not violate the essential provisions of the right to data protection, and appropriate and specific measures must be provided for the protection of the fundamental rights and interests of the data subject.

The data collected for scientific research purposes cannot be used for other purposes!

For example, researchers collected data on individuals' habits related to smoking and alcohol consumption to assess the impact of these habits on a person's health. The data collected by researchers cannot be further used, for example, for marketing of manufacturer's medicinal products for giving up smoking or alcohol.

However, data collected for purposes other than scientific research can be used for scientific research!

For example, data collected for statistical purposes can be used for scientific purposes.

The Law on Ethics in Biomedical Research provides: "a decision on whether a person's consent to participate in research is necessary for conducting biomedical research on a person's tissues, organs, embryos, cells and genetic material which has been obtained for the purpose of provision of medical interventions before applying for undertaking research on this person shall be taken by the Lithuanian Bioethics Committee or a regional biomedical research ethics committee issuing an approval to conduct biomedical research."

For example, if personal data were collected when providing the health services in a health institution, this data cannot be used for scientific research unless authorised by the relevant authority. Also, if the data collected for one scientific study (e.g. lung cancer) is to be used for another scientific study (e.g. the influence of smoking on family well-being), a new legitimate ground for such further processing will be required.

Legitimate ground for the processing of personal data

The processing of personal data requires a legitimate ground in accordance with Article 6 GDPR. Article 6 of the GDPR provides for the following grounds for legitimate processing of personal data:

- Consent of the data subject
- For the performance of a contract to which the data subject is a party
- Legal obligation
- The person's vital interests
- Public interest

The main legitimate ground for processing data for research purposes is **consent**. The Regulation defines the consent of the data subject as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Consent is therefore considered appropriate when it is:

- Freely given;
- Specific and unambiguous;
- The expression of the will of the duly informed person by a statement or by a clear affirmative action in which they consent to the processing of personal data relating to them.
- Consent shall be considered freely given if the person is actually given the opportunity to decide to give or not to give the consent to process their personal data and the person does not suffer any negative consequences as a result of such a decision.

Although the GDPR does not provide consent forms, it does establish certain conditions for consent:

- the controller must be able to demonstrate that the data subject has given their consent to the processing of their personal data;
- If the consent of the data subject is given by a written declaration relating to other matters, the request for consent shall be submitted in such a way that it is clearly distinguished from other matters,
- consent is given in an understandable and easily accessible form,
- consent is written in clear and plain language;
- The withdrawal of consent must be as easy as giving it. The person must be informed of the right to withdraw their consent before giving it.

For scientific research purposes, **particularly sensitive personal data** (e.g. related to personal health) may be processed as well; however, this requires consent that meets the specific conditions set out in Article 9(2) of the GDPR and detailed in the Law on Ethics of Biomedical Research:

- The data subject has expressly consented to the processing of such personal data for one or more specified purposes;
- The consent of the person must be given in writing;
- Before giving consent, this person shall be informed (upon signing), in a form that they understand, about the purpose of biomedical re-

search, the plan, the methods used, the decisions of the Lithuanian Bioethics Committee or the relevant regional biomedical research ethics committee, as well as other relevant information related to the research and their rights.

The consent to participate in scientific research activities in clinical trials should be subject to the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council (hereinafter: Regulation on Clinical Trials).

The Regulation on Clinical Trials sets out the following requirements for consent:

- The consent shall be in writing, with a specified date, signed by the subject (or, where the subject is unable to give informed consent, by the representative legally designated by them) during a prior interview with a member of the research group with an appropriate qualification. The person receives a copy of this consent.
- If a person is unable to write, their consent may be given and recorded by other appropriate means, with the participation of at least one impartial witness who signs the document of informed consent and indicates the date.
- The person or their legally designated representative shall be given sufficient time to consider their decision to participate in the clinical trial.

In order to obtain an informed consent, the subject or, where the subject is unable to give an informed consent, their legally designated representative shall be provided with information that:

a) enables the subject or their legally designated representative to understand:

- the nature, objectives, benefits, effects, risks and inconveniences of the clinical trial;
- the rights and guarantees of the subject with regard to their protection, in particular their right to refuse to participate and the right to withdraw from the clinical trial at any time without experiencing any harm or need to provide justification;
- the conditions under which the clinical trial is to be conducted, including the expected duration of the participation of subjects in the clinical trial; and
- possible treatment alternatives, including follow-up measures, if the subject's participation in the clinical trial is terminated;

b) is comprehensive, concise, clear, relevant and understandable to a non-professional;

c) is submitted during a prior interview with a member of the study group who is appropriately qualified in accordance with the legislation of the Member State concerned;

d) includes information on the applicable system of procedure for reimbursement, and

e) includes an EU trial number and information on the possibility of finding out the results of the clinical trial.

Where appropriate, **an informed consent** may also be obtained **under a simplified procedure**. This is allowed under the following conditions:

- The clinical trial shall be conducted exclusively in one country.
- The person is provided with the above information and informed about the possibility of refusing to participate in the study.
- The potential subject after being informed does not object to participation in the clinical trial.
- The simplified procedure for obtaining informed consent shall not conflict with the national law of the Member State concerned.
- The clinical trial methodology requires that, in a clinical trial, different investigational medicinal products are administered to groups of subjects rather than to individual subjects.
- A clinical trial is a low-intervention clinical trial, and investigational medicinal products are used under the conditions set out in the marketing authorisation.
- Only interventions that are standard treatments for the subjects concerned shall be performed.
- The protocol shall justify the reasons for obtaining informed consent in a simplified manner and shall describe the scope of the information provided to the subject and the ways in which it is provided.

Part III: Scientific research data management plan. How to develop it properly?

Most national and international projects require project participants to complete **a data management plan** (hereinafter 'DMP') and specify, among other things, how personal data will be processed. When completing the plan uncertainties often arise, thus we would like to provide some guidelines to make it easier for you to complete the part of the DMP that deals with the processing of personal data.

Legal and ethical requirements, codes of conduct

Before you start processing personal data, make sure that you process them in accordance with the provisions of the General Data Protection Regulation and Republic of Lithuania Law on Legal Protection of Personal Data.

Therefore, before processing of personal data begins, determine how you will ensure the compliance with the applicable legal acts regulating the protection of personal data:

Have you obtained consent to the storage and/or sharing of personal data?

- Please pay particular attention to whether your consent meets the specific requirements set for it!

What personal data will be anonymised?

- Remember: in data anonymisation, *the more* (data) and *the earlier* (time of anonymisation) means the *better*.
- If you believe that anonymisation of data will hinder achieving the purpose of the research, you need to justify this statement in a clear and as detailed manner as possible.
- Guidelines for anonymisation:

https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_nuasmeninimo_metodai_2015.pdf

What personal data will be pseudonymised?

- It is important to remember that even pseudonymisation of data sometimes leaves a possibility to identify individuals, for example, through the data held

by third parties, and therefore such data will continue to be subject to the provisions on the protection of personal data.

Will you encrypt your data? If so, what data will be encrypted? How?

- Make sure that the data is absolutely not understandable to any person who does not have permission to access the given data.

What procedure for managed access to processed personal data is applied to authorised personal data processors and/or controllers?

- Check how the protection of personal data is regulated in your institution, what procedures should be implemented regarding the authorised personal data processors and/or controllers. If there are no specific procedures provided for, it is necessary to do so in the DMP for your scientific research.

Will intellectual property rights apply? What laws will apply and to what extent?

- Check how intellectual property law issues are regulated in your institution. If no regulation is in place, it is necessary to provide for these issues in the DMP for your scientific research.

Who is the data processor and/or the owner of the controller and who will have the right to control access to the data processed?

- It is very important to discuss this issue as specifically as possible – to indicate the specific persons (e.g. project manager, special person appointed only for these issues, third parties, etc.).
- If, for example, staff from other partner institutions have access to the data (for example, if a scientific project is carried out by several institutions), please indicate them. What are the provisions on the right of several partners to control access to data included in a consortium or other type of agreement?

What access conditions will apply to the data? Will the data be open or will access restrictions apply?

- If the data is openly available, make sure that you have the appropriate consents or that the data will be properly anonymised or pseudonymised.
- If restrictions apply, describe them.

- Please indicate if data access and reuse licenses are available.

Are there restrictions on the reuse of third-party data? If there are, what are the restrictions?

- If the data is reused, please specify who can see or use them. How long will the data be stored? – The description of these aspects should be as detailed as possible.

What national and international codes of conduct and institutional ethical guidelines do you follow? Does data collection require an ethical review (e.g. by an ethics committee)?

- If you process particularly sensitive data, pay extra attention to these aspects.

Sharing and long-term storage of data

Data sharing is another important aspect to be discussed in your DMP. Answer the questions below to find out if you have decently prepared.

How and when will data be shared?

Are there any possible data sharing restrictions or prohibitions?

- If yes, please specify the restrictions and the reasons (e.g. for the protection of intellectual property, etc.)

How will the data be accessed and shared?

- For example, by placing the data in a reliable data storage, adding to a directory, using a secure data service, directly submitting data queries, or using another mechanism.

How long will the data be stored?

- Keep in mind that the storage period of the data must be closely related

to the ongoing scientific research, thus it cannot be that the data will be stored for an indefinite period of time. Provide a data storage plan.

When will the data be reported?

- Indicate the estimated time of release.

Will exclusive use of data be required?

- If so, please explain why and how long.
- Please indicate whether data sharing will be delayed or restricted, e.g. to publish, protect intellectual property, etc.

Who will be able use the data?

- Indicate who will be able to use the data for research and/or be consumers. In this case, the best solution is to indicate specific persons, their institutional affiliation, contacts.

Should access be restricted to certain persons or subject to a data sharing agreement?

- If so, please specify why and how access will be restricted.
- Indicate what action will be taken to remove or reduce restrictions.

How will data be collected and where will data be stored for a long time? For example, in the data storage or archive?

- How will it be decided which data to store? Describe the data that needs to be stored for a long time.
- It is recommended to demonstrate that the policies and procedures of the repositories, including all metadata standards and associated costs, have been checked.

What data must be stored or destroyed for contractual, legal or regulatory purposes?

- Particular attention should be paid to particularly sensitive data.

What methods or software tools are needed to access and use data?

- Indicate the specific tools that potential users need to access and (re)use

the data.

- Specify how sustainable is the software required to access data.

Will data be shared through repository?

Will the requests be processed directly or will another mechanism be used?

- How will the application of a unique and permanent identifier be ensured for each set of data?

How can data be reused in other contexts?

- Indicate whether permanent identifiers (PID) will be used to identify the location of the data and direct towards it in a reliable and efficient manner. PID also help to track citations and reuse.

Data processing and management responsibilities and resources

When processing personal data, it is particularly important to properly allocate duties and responsibilities, indicating the specific persons and their areas of responsibility.

Who will be responsible for data management and processing?

- Specify the role, job position, authority, contacts, etc.

Who is responsible for performing specific functions?

- For example, data capture, metadata production, data quality, backup and storage, data archiving, data opening. If there is a possibility to identify specific persons.

If the research (project) is implemented with partners, how will the responsibility for data management and/or processing be divided between partners/institutions?

- How will the responsibilities be divided?
- What is the possible specificity of the data management responsibility of the partners? How will it be coordinated with all partners?

Who is responsible for implementing the DMP? Who will ensure the review and, if necessary, the revision of the plan?

- It is necessary to identify specific persons.

How will a regular update of the DMP be ensured? What is the regular frequency of revision and, if necessary, update?

- For example, at least once a year?

What resources (such as finance and time) will be allocated to data management and to ensuring that data are findable, accessible, interoperable, re-usable?

- Project funding is usually limited in time, but it may also be necessary to store data for longer periods (e.g. due to publication, reuse, etc.). It is, therefore, important to specify how the funding of storage will be ensured after the funding is no longer provided to the scientific project.

How have you assessed the necessary resources (e.g. time) for sharing and storing data?

- The storage and sharing of data must be linked to the objectives of the project and the expected results.

Justify all resources required to provide data:

- e.g., data storage costs, hardware, special equipment, staff time, specialised experience (qualifications), training (if necessary) costs, removal of possible technical barriers, costs required for data preparation input and storage fees).

What additional resources may be needed to prepare the data for storage (e.g. performing data processing tasks)?

- If applicable, specify the storage fee. How much financial resources you will need and how you will cover these costs?

Literature:

Legislation:

1. The Convention for the Protection of Human Rights and Fundamental Freedoms
2. The Charter of Fundamental Rights of the European Union
3. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General data protection Regulation)
4. Republic of Lithuania Law on Legal Protection of Personal Data

Case law:

1. 19 October 2016, the judgement of the CJEU in case C-582/14 P. BREYER, ECLI:EU:C:2016:779.
2. 14 February 2019, the judgment of the CJEU in case C-345/17 S. BUIVIDS, ECLI:EU:C:2019:122.
3. 11 June 2020, the judgment of the ECHR in case *P.N. against Germany*, statement No. 74440/17.
4. 2 March 2022, ruling of the Supreme Administrative Court of Lithuania in case No. A-233-525/2022.
5. 23 June 2019, the judgment of the ECHR in case *Sorguç against Turkey*, statement No. 17089/03.
6. 8 November 2016, the judgment of the ECHR in case *Magyar Helsinki Bizottsag against Hungary*, statement No. 18030/11.

Other useful links:

1. European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, adopted on 21 April 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en

2. EDPB document on response to the request from the European Commission for specifications on the continuing application of the GDPR, using on health research, adopted on 2 February 2021,

https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/edpb-document-response-request-european-commission_en

3. Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research. Final report. EDPS/2019/02-08, 2021,

https://edpb.europa.eu/system/files/2022-01/legalstudy_on_the_appropriate_safeguards_89.1.pdf

4. European Data Protection Board, a preliminary opinion on data protection and scientific research, adopted on 6 January 2020,

20-01-06_opinion_research_en.pdf (europa.EU).

Connecting not conflicting: removing the tension between personal data protection and freedom of expression and information

Eglė Bilevičiūtė, Katažyna Mikša, Salvija Mulevičienė,
Žydra Klevinskaitė, Justė Bareišaitė, Kamilė Mekšriūnaitė,
Aliona Gaidarovič

Edited by Margarita Armalienė
Layout Jovita Jankauskienė

Published by
MB „Spalvų kvartetas“
Laurų 2b Seniava, Kauno r.
www.spalvukvartetas.lt