ANALYSIS OF THE EUROPEAN MODELS OF THE INDEPENDENT OVERSIGHT AUTHORITY IN THE FIELD OF DATA PROTECTION AND ACCESS TO PUBLIC INFORMATION

prepared by
Dijana Šinkūnienė, Lilia Oleksiuk, Oleksandr Shevchuk

This publication was produced with the financial support of the European Union and the Council of Europe. The views expressed herein can in no way be taken to reflect the official opinion of either party.

Cover design and layout: K.I.S. Ltd.

Cover photo: © Shutterstock

Council of Europe Publishing
F-67075 Strasbourg Cedex
(http://book.coe.int)

TABLE OF CONTENTS

1

INTRODUCTION

The topic of personal data protection is of particular importance for Ukraine.

The Association Agreement between Ukraine and the European Union requires bringing the legislation of Ukraine in line with European standards, which also applies to personal data protection.

Section III of the Association Agreement provides for cooperation in the field of justice, freedom and security. According to Article 15 of the Association Agreement, "Ukraine and the European Union have agreed to cooperate in order to ensure an adequate level of personal data protection in accordance with the highest European and international standards, including relevant Council of Europe documents."

One of the key tasks of Ukraine is approximation of Ukrainian legislation to European standards in the field of personal data protection through the implementation of the Regulation (EU) 2016/679 in accordance with paragraph 11 of the Action Plan No. 1106 for the implementation of the Association Agreement approved by the Cabinet of Ministers of Ukraine on October 25, 2017.

The main problem in the field of personal data protection in Ukraine is the lack of an effective national system of personal data protection, a proper organizational and legal mechanism for regulating relations and responsibility for committing offences in this area.

In this regard, it is important to create an effective institutional mechanism for personal data protection in Ukraine: an independent supervisory body responsible for developing guidelines, monitoring and oversight of the compliance with legislation in the field of personal data protection.

The purpose of this Report on the Analysis of the European Models of the Independent Oversight Authority in the Field of Data Protection and Access to Public Information is to describe the results of the analysis carried out by the team of the Council of Europe experts and to provide recommendations on the most appropriate model or specific features to be taken into consideration by the Ukrainian authorities while establishing an independent oversight mechanism in the field of data protection in Ukraine. Art. 15 of the Convention 108+ assigns the Parties the obligation to establish one or more authorities to be responsible for ensuring compliance with the provisions of this Convention, which shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions. Art. 52 of the GDPR explains that the member (-s) of supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

The scope of the analysis carried out by the experts covers the following areas:

- place of the institution within the system of state authorities;
- scope of supervision;
- guarantees for independence (institutional, functional, financial);
- powers of investigation, intervention, complaints handling;
- regulatory powers;

- powers to engage in legal proceedings;
- advisory powers; and
- raising public awareness.

The primary basis for the analysis were the Council of Europe and European Union standards, in particular the modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session of the Committee of Ministers (Elsinore, 18 May 2018), and 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), as well as relevant decisions of the Court of Justice of the European Union.

Although the data protection supervisory authority is not a new concept, in order to explore how the principles of independent functioning of supervisory authorities are implemented in practice after the reform of the EU data protection framework, the team of experts has carried out a survey regarding functioning of the data protection supervisory authorities in the countries of European Union and European Economic Area. The questionnaire that was offered them is presented in Annex 1 to this report. In total, 20 answers were received and used to illustrate practical implementation of the requirements for independent functioning of the supervisory authority.

The experts have also analyzed publicly available information on the status, tasks and powers of data protection supervisory authorities as well as previous research materials prepared by the EU agencies, scientists, experts.

The recommendations provided in this report aim to help find the most consistent way to implement international principles in Ukraine, therefore they take into account the mentioned Council of Europe and European Union standards, practices found in the EU Member States, as well as provisions of the Constitution of Ukraine and legal principles relating to establishment of the state institutions in Ukraine.

The authors of this report are Dijana Šinkūnienė, Lilia Oleksiuk and Oleksandr Shevchuk, Council of Europe experts.

2

LIST OF ABBREVIATIONS

Convention 108+	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108), adopted on 28 January 1981 in Strasbourg, as amended by the Protocol CETS No. 223
FRA	European Union Agency for Fundamental Rights
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
CJEU	Court of Justice of the European Union
DPA (-s)	Data Protection Authority (-ies)
Explanatory Report	Explanatory Report to Convention 108+ endorsed by the Committee of Ministers in its 128th Session (Elsinore, 18 May 2018)
Report	This Report on the Analysis of the European Models of the Independent Oversight Authority in the Field of Data Protection and Access to Public Information

3

PLACE OF THE INSTITUTION WITHIN THE SYSTEM OF STATE AUTHORITIES, SCOPE OF SUPERVISION, GUARANTEES FOR INDEPENDENCE

3.1 Status and place of the institution within the system of state authorities

The independent data protection supervisory authority is an essential component of the data protection supervisory system in a democratic society aimed at ensuring the right to personal data protection. The CJEU in its decision of 9 March 2010 in *European Commission v. Federal Republic of Germany C-518/07* held that: „The supervisory authorities provided for in Article 28 of Directive 95/46 are therefore the guardians of those fundamental rights and freedoms, and their existence in the Member States is considered, as is stated in the 62nd recital in the preamble to Directive 95/46, as an essential component of the protection of individuals with regard to the processing of personal data."[1]

Art. 15 of the Convention 108+ obliges the Parties to establish the authority (-ies) to be responsible for ensuring compliance with the provisions of this Convention. Convention 108+ and the GDPR do not set requirements for the composition of the authority (i.e., a single commissioner or a collegiate body), and there are various practices among the European countries. In some countries one can find a single commissioner (Croatia, Cyprus, Estonia, Ireland, Latvia, Lichtenstein, Lithuania, Norway, Romania, Slovakia, etc.), while in others a collegiate body is responsible for the supervision of implementation of the data protection legislation (France, Greece, Italy, Luxembourg, Portugal, etc.). Icelandic supervisory authority has indicated that the daily work is led by a Commissioner, but the authority also has a Board that issues decisions in major cases, including fines.

Unlike the authority composition, various aspects of independence of the data protection supervisory authorities are reflected in the Convention 108+ and the GDPR. Art. 15 (5) of the Convention 108+ establishes that the supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers. Similar provisions are set up in Art. 52 (1) of the GDPR, which also specifies other aspects important for the independent functioning (functional independence - member (-s) of the supervisory authority shall remain free from direct or indirect external influence, they shall neither seek nor take instructions from anybody; as well as financial and organizational independence).

Place of the data protection supervisory authority within the system of other state authorities plays an important role, as it is closely related to functional independence. The issue of external influence is especially sensitive and relevant when a member (-s) of the supervisory authority is appointed by the

1 CJEU decision of 9 March 2010 in *European Commission v. Federal Republic of Germany*, C-518/07, [2010] ECR I-1885, para. 23.

government, and therefore the authority is embedded within the structure of executive power of the state. However, it should be noted that participation of the government in the procedure of appointment is not excluded. Art. 53 (1) of the GDPR states that each member of the supervisory authority shall be appointed by means of a transparent procedure by the government, as well as by the parliament, the head of the State or by an independent body entrusted with the appointment under Member State law. According to recital 121 of the GDPR, "the general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law". The survey carried out by the team of experts has disclosed various combinations of the appointment procedure existing in the European countries. Although cooperation between the data protection supervisory authority and the government might seem challenging in terms of independence of the authority, the survey showed that the government alone or together with the parliament or the head of the State takes part in the appointment procedure of the member (-s) in many European countries (see Table 1).

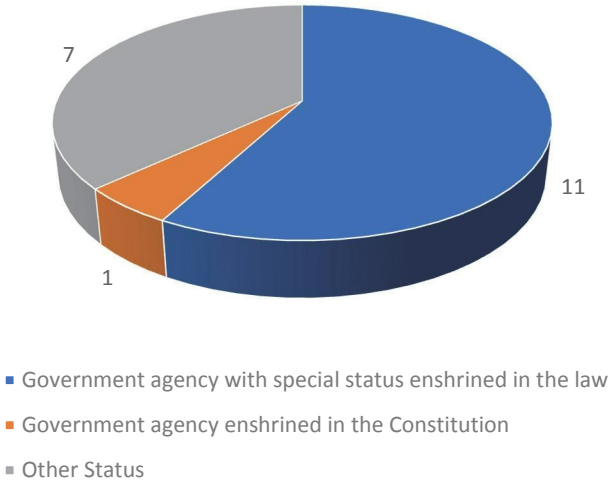
Table 1. Appointment of the member (-s) of data protection supervisory authority

Members appointed by: / Country	Government	Parliament / Government	President / Government	Parliament, or President / Parliament
Austria			+	
Czech Republic				+
Croatia		+		
Cyprus	+			
Greece				+
Iceland	+			
Italy				+
Estonia	+			
Latvia	+			
Lichtenstein		+		
Lithuania	+			
Luxembourg			+	
Norway	+			
Poland				+
Portugal		+		
Romania				+
Slovenia				+
Slovakia		+		

As shown in Table 1, the government takes part in the appointment procedure in 12 countries.

Participants of the survey were asked to indicate the status of the supervisory authority: whether it is a government agency reporting to a ministry; a government agency with a special status enshrined in the law; a government agency established in the Constitution; or it has another status. The responses indicated that in most cases the supervisory authority status is regulated by the law, while in one case the status is enshrined in the Constitution (see Figure 1):

Figure 1: Status of the Data Protection Supervisory Authority



No participants of the survey indicated that the supervisory authority is a government agency reporting to a ministry. It is not surprising, as being subordinated to any other state institution (not necessarily a ministry) would lead to the infringement of the independence requirement. Among the responses indicating another status, the following information has been provided by respondents: it is a public authority with legal personality, autonomous and independent in relation to other public authorities, as well as to any natural or legal person from the private sector; an independent public body (separate from the government, similar to the Ombudsman); a constitutionally established independent public authority; etc. It could be observed that establishing the independent status of the supervisory authority in the legislation is important, however it is not sufficient for ensuring real independence unless guarantees are in place regarding the allocation of resources, ability to make its own decisions about organization of its work, protection from any kind of external influence, etc.

Participants of the survey were asked to indicate whether the supervisory authority has a legal personality, or it is embedded within the structure of another institution, or it is subordinated to a ministry or another state institution. The vast majority – 18 respondents – said that the institution had a legal personality, which is an indispensable precondition for independence, and only one indicated that it is subordinated to a ministry or another state institution.

According to the survey results, no European data protection supervisory authorities are embedded within the structure of other institutions. Again, it is not surprising, as staying within the structure of another institution would be incompatible with the requirements for independence. It is also worth mentioning that not only embedding the supervisory authority within the structure should be avoided, but also subordinating it to a ministry or another state institution as it could lead to restriction of other guarantees aimed at ensuring the independent status of the supervisory authority (e.g., budgetary arrangements, setting up internal regulations and organizational structure, etc.).

To sum it up, the member (-s) of the data protection supervisory can be appointed by the government, the parliament, the head of the State, or with participation of several of them. No matter who appoints the members, the authority should have its own legal personality and not be embedded within or subordinated to a ministry or another state institution.

3.2 Scope of supervision

Art. 15 (1) of the Convention 108+ stipulates that more than one authority can be established to ensure compliance with the provisions of the Convention. Several authorities can exist in view of the particular features of different legal systems, for example, in case of a federal state. The Explanatory Report elaborates it: "Specific supervisory authorities whose activity is limited to a specific sector (electronic communications sector, health sector, public sector, etc.) may also be put in place." Art. 85 (1) of the GDPR also obliges the Member States to make sure that one or more independent public authorities are responsible for monitoring the application of the GDPR. In order to safeguard the independence of the judiciary in the performance of their judicial tasks (when rendering decisions, in particular), the supervisory authority should not be authorized to supervise data processing operations of the courts acting in their judicial capacity (see Art. 15 (10) of the Convention 108+, Art. 55 (3) of the GDPR).[2] Such a restriction of supervisory powers should be limited to judicial activities performed within the national law.[3] Therefore it should be noted that court processing of other data not related to the performance of judicial tasks (e.g., processing of personal data of employees, video surveillance for security purposes, etc.) is part of the competence of the data protection supervisory authority.

Particular attention should be paid to the supervision of data processing for national security purposes. As national security falls outside the scope of European Union law, the GDPR is not applicable to respective data processing, therefore the supervisory authority is not authorized to supervise it (see Art. 2 (2a) of the GDPR). However, data processing related to national security and defense is not completely excluded from the scope of the Convention 108+. As regards supervision of data processing for national security and defense purposes, Art. 11 (3) of the Convention 108+ stipulates that each Party can establish legal exceptions to Article 15, (2 a, b, c, and d) only to the extent that it constitutes a necessary and proportionate measure in a democratic society. The Explanatory Report further clarifies that other appropriate mechanisms for independent and effective review and supervision of processing activities for national security and defense purposes may be provided, without prejudice to the applicable requirements in relation to the independence and effectiveness of review and supervision mechanisms (see para. 117, 118).

The Preamble of the Convention 108+ recalls that the right to personal data protection is to be considered in relation to its role in the society, and that it has to be reconciled with other human rights and fundamental freedoms, including freedom of expression, as well as the need to take into account the principle of the right of access to official documents when implementing the rules relating to personal data protection. Para. 11 of the Explanatory Report comments that the right to data protection is not absolute and may not be used as a means to prevent public access to official documents. Art. 85 of the GDPR regulates balancing of the right to personal data protection with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression. Art. 86 of the GDPR also puts emphasis on the need to balance public access to official documents with the right to personal data protection.

It should be noted that specific competences of the independent data protection authorities may not be transferred to other supervisory authorities that do not have the same independent status and are not recognized at the same level in European Union legislation. An overlap of competences of these institutions can also endanger the unity of action required in terms of supervision.[4] Art. 51 (2) of the

2 Recital 20 of GDPR explains that supervision of such data processing operations could be entrusted to specific bodies within the judicial system of the Member State.

3 Explanatory Report, para. 134.

4 See Opinion of the European Data Protection Supervisor on the Commission proposal for a Regulation of the European Parliament and of the Council on trust and confidence in electronic transactions in the internal market (Electronic Trust Services Regulation), para 41. Available at: https://edps.europa.eu/sites/default/files/publication/12-09-27_electronic_trust_services_en_0.pdf , accessed 19 April 2021.

GDPR underlines the role of the supervisory authority in promoting consistent application of the Regulation throughout the European Union. Consistent and uniform application of the data protection rules is important not only within the context of cooperation among different states, but also among different sectors within one state.

Art. 41 of the Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing the Council Framework Decision 2008/977/JHA allows Member States to have the supervisory authorities established under the GDPR to be the supervisory authorities referred to in this Directive, responsible for the supervisory authority functions and for monitoring the application of this Directive, in order to protect the fundamental rights and freedoms of natural persons in relation to data processing and to facilitate the free flow of personal data within the Union (see para. 1 and 3).[5]

In terms of the GDPR, Art. 1(1) foresees that this Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Therefore, it is also important to note that the task of data protection supervisory authorities is not only to supervise implementation of the rules relating to personal data processing, but also to ensure a fair balance between observance of the fundamental rights and the interests requiring free movement of personal data. This dual role has been underlined by the CJEU in the aforementioned decision of 9 March 2010 in case C-518/07: "In order to guarantee that protection, the supervisory authorities must ensure a fair balance between, on the one hand, observance of the fundamental right to private life and, on the other hand, the interests requiring free movement of personal data."[6]

Activities of the data protection supervisory authorities must cover all the aspects relating to the processing of personal data that are regulated by the Convention108+ and the GDPR, therefore it is important to properly define the scope of supervision with regard to the processing of personal data in various sectors and for various purposes. As regards the scope of supervision, results of the survey showed that in many cases the activities of the data protection supervisory authorities cover data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, as well as data processing for journalistic purposes and the purposes of academic, artistic or literary expression. Five authorities also have functions related to public access to official documents.

Results of the survey show that none of the data protection supervisory authorities is authorized to supervise data processing by courts when acting in their judicial capacity.

To sum it up, one data protection supervisory authority can be responsible for supervision of proper data processing in different sectors and for various purposes. Supervision of data processing by courts acting in their judicial capacity should be out of the scope of its activities.

5 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN#d1e2779-89-1

6 CJEU decision of 9 March 2010 in *European Commission v. Federal Republic of Germany*, C-518/07, [2010] ECR I-1885, para. 24.

3.3 Guarantees of independence

Art. 15 (5) of the Convention 108+ stipulates that the supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions. According to the Explanatory Report (see para. 129), among the elements contributing to safeguarding this independence is the composition of the authority; the method for appointing its members; the duration of exercise and conditions of cessation of their functions; the possibility for them to participate in relevant meetings without undue restrictions; the option to consult technical or other experts or to hold external consultations; the availability of sufficient resources to the authority; the possibility to hire its own staff; or the adoption of decisions without being subject to external interference, whether direct or indirect (see para. 129).

Art. 54 (1) of the GDPR sets the list of rules relating to the establishment of supervisory authorities that should be provided by law:

- the establishment of each supervisory authority;
- the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;
- the rules and procedures for the appointment of the member (-s) of each supervisory authority;
- the duration of the term of the member (-s) of each supervisory authority of no less than four years;
- whether and, if so, for how many terms the member (-s) of each supervisory authority is eligible for reappointment;
- the conditions governing the obligations of the member (-s) and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

Allocation of resources is another factor that plays a crucial role for ensuring independence of the supervisory authority. Art. 15 (6) of the Convention 108+ requires that the supervisory authorities be provided with the resources necessary for the effective performance of their functions and exercise of their powers. Art. 52 (4) of the GDPR contains a more detailed list of resources stating that Member States shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers. Providing adequate financial, human, technical and other resources is an essential aspect of the supervisory authority independence. Otherwise, its ability to perform its tasks and exercise its powers could be seriously affected.

3.3.1 Term of office of the supervisory authority members

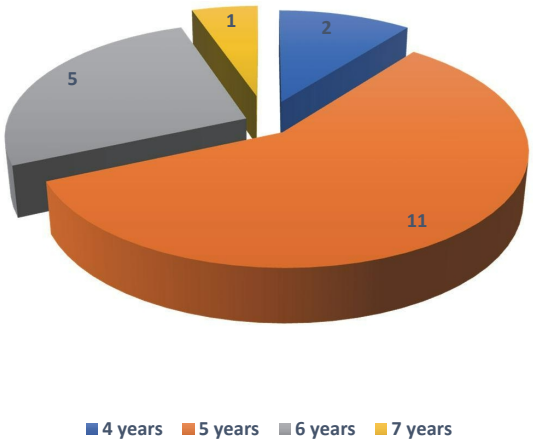
According to Art. 54 (1) of the GDPR, the law shall stipulate the duration of the term of office for the members of each supervisory authority, which could not be less than four years (except the first appointment after 24 May 2016, a part of which may be shorter where that is necessary to protect the supervisory authority's independence by means of a phased appointment procedure), as well as reappointment possibilities and the maximum number of terms a member can hold one's position. The CJEU in its decision of 8 April 2014 in *European Commission v. Hungary* C-288/12 held that in order to ensure the independence of the supervisory authority [under the second subparagraph of Article 28(1) of the Directive 95/46], the government shall allow the authority to serve its full term of office.[7] In the

7 CJEU decision of 8 April 2014 in *European Commission v. Hungary*, C-288/12, ECLI:EU:C:2014:237, para. 60.

same decision, the CJEU underlined that: „If it were permissible for every Member State to compel a supervisory authority to vacate office before serving its full term, in contravention of the rules and safeguards established in that regard by the legislation applicable, the threat of such premature termination to which that authority would be exposed throughout its term of office could lead it to enter into a form of prior compliance with the political authority, which is incompatible with the requirement of independence."[8]

The survey showed that the term of office of the supervisory authority members varies from 4 to 7 years. As shown in Figure 2, the most frequent duration of the term of office is 5 years.

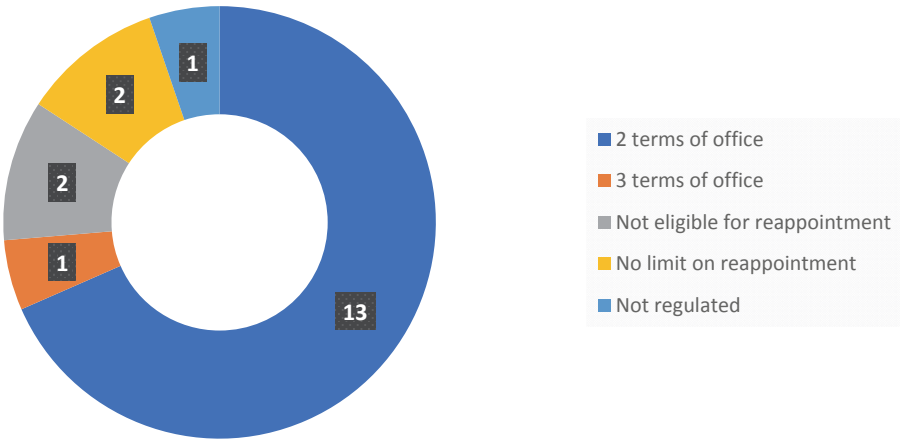
Figure 2: Duration of the Term of Office



According to the survey results, most European countries allow reappointment of the supervisory authority members for two terms of office. In some countries reappointment is not possible, while in others no limit on reappointment is specified (see Figure 3).

As for the relation between the duration of the term of office and reappointment, there is no clear trend in European countries. The Italian authority has stated that a not renewable seven-year term of office was introduced by the law amending the term of office of the inspectors appointed to certain independent authorities, including the data protection authority members. The previous term of office was four years and could be renewed once. The Icelandic authority wrote that the members of the Board were appointed for a five-year term that cold be prolonged twice (up to 15 years in total), while the inspector was appointed for a five-year term with no limit on reappointments.

Figure 3: Eligibility for Reappointment



8 See para. 54.

To sum it up, the duration of the term of office of the supervisory authority members shall not be less than four years. The supervisory authority members can be eligible for reappointment, although the possibility of reappointment is not necessary to ensure independence.

3.3.2 Termination of duties of the supervisory authority members

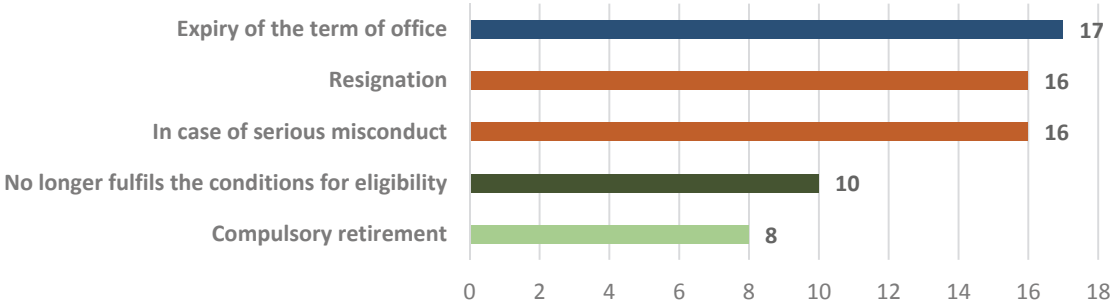
Art. 53 (3 and 4) of the GDPR set forth the main rules relating to the termination of duties of the supervisory authority members:

1) Ending of the duties of a member is possible in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law.

2) Dismissal of a member is possible only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

The grounds for ending the duties / dismissal of the supervisory authority members indicated by participants of the survey are shown in the Figure 4:

Figure 4: Applicability of the Grounds for Ending of the Duties / Dismissal of the Members of Supervisory Authority



While the grounds for ending the duties seems to be quite objective, dismissal of a member might be more subjective and can therefore jeopardize independence of the supervisory authority. To guarantee protection from unjustified termination of duties in case of dismissal of a member, the conditions required for the performance of the duties should be clearly established by law. For example, Art. 19 (2) of the Cyprus Law 125(I) of 2018 on Protection of Natural Persons with Regard to the Processing of Personal Data and for Free Movement of such Data stipulates that the person appointed as Commissioner shall possess the qualifications for the appointment of a Supreme Court Judge.[9] Art. 9 (2) of the Law on Legal Protection of Personal Data of the Republic of Lithuania states that a citizen of the Republic of Lithuania of impeccable reputation with a bachelor's and master's degree in law or a professional qualification degree in law (one-level university education) and at least 10 years of legal or legal pedagogical experience and complying with the requirements set up in Art. 53 (2) of the GDPR may be appointed as the Director of the State Data Protection Inspectorate[10]. Para. 4 of the same article obliges the Director of the State Data Protection Inspectorate to suspend his/her membership in a political party during his/her term of office.

Among the things that should be prescribed by law is the exhaustive list of activities that are incompatible with the status of a supervisory authority member. For example, according to Art. 12 (1) of the Law No. 4624 of the Hellenic Republic, a person may not be appointed as President, Deputy President,

9 http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf (unofficial translation). Accessed 22 May 2021.

10 Available at: https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/asr, in Lithuanian. Accessed 22 May 2021.

or member of the Authority if this person is: (a) a minister, state secretary, general or special secretary of a Ministry or of a separate general or special secretariat, and a member of parliament; and (b) a manager or a member of a management body of an undertaking that provides services relating to the processing of personal data or is associated with a project contract of equivalent content.[11] Para. 2 of the same Article stipulates that: „Any kind of professional or other activities relating to the competences of the Authority shall be incompatible with the status of member of the Authority, with the exception of scientific and research activities. The members of the Authority may not appear before the Authority for two (2) years after the expiry of their term of office."

The same could be said about "serious misconduct" – a clear reference to the kind (-s) of the offences should be provided. For example, Art. 21 (3) of the Cyprus Law 125(I) of 2018 on Protection of Natural Persons with Regard to Processing of Personal Data and for Free Movement of such Data establishes that the Commissioner shall be dismissed in the following cases: in the event where the Commissioner, in contravention of the Regulation and of this Law, discloses, in any way, information or personal data to which he/she has access as a result of his or her capacity, or allows anyone to acquire knowledge thereof, commits an offense, and in the case of conviction, is subject to imprisonment which shall not exceed three (3) years or to a fine which shall not exceed thirty thousand euro (€30.000) or to both of these penalties. According to Art. 9 (4) of the same law, the ground for dismissal of the Commissioner is also mental or physical incapacity or physical handicaps rendering him or her incapable of exercising his or her duties.

The procedure of dismissal is also important: it should be provided by law, with due participation of the same institutions as in the appointment of a member (-s).

It should be noted that it is very important to have a limited and well-defined list of the grounds for terminating the duties / dismissal of supervisory authority members, as any dismissal before the end of a member's term of office could pose a danger to the independence of the authority. The CJEU in its decision of 8 April 2014 in *European Commission v. Hungary* C-288/12 held that: "<…> The independence requirement laid down in the second subparagraph of Article 28(1) of Directive 95/46 must necessarily be construed as covering the obligation to allow supervisory authorities to serve their full term of office and to have them vacate office before expiry of the full term only in accordance with the rules and safeguards established by the applicable legislation (see para. 55)."[12]

Members and staff of a supervisory authority when exercising their functions have access to personal data, therefore particular attention should be paid to secrecy obligations. Art. 15 (8) of the Convention 108+ establishes that members and staff of the supervisory authorities shall be bound by obligations of confidentiality with regard to confidential information to which they have access, or have had access, in the performance of their duties and exercise of their powers. Art. 54 (2) of the GDPR clarifies that duty of professional secrecy should be applicable both during and after the term of office of the members and staff of supervisory authorities, particularly emphasizing that during their term of office the duty of professional secrecy shall in particular apply to reporting by natural persons on infringements of the GDPR. Violation of the confidentiality obligation can be the ground for dismissal of a supervisory authority member.

To sum it up, the exhaustive list of the grounds for termination of the duties and dismissal of the supervisory authority members, as well as dismissal procedures should be provided by law, ensuring due participation of the institutions in charge of the member's appointment. The law should also clearly stipulate the qualifications and eligibility conditions, prohibited actions, occupations and benefits

11 Available at: https://www.dpa.gr/sites/default/files/2020-08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF . Accessed 22 May 2021.

12 CJEU decision of 8 April 2014 in *European Commission v. Hungary*, C-288/12, ECLI:EU:C:2014:237, para. 55.

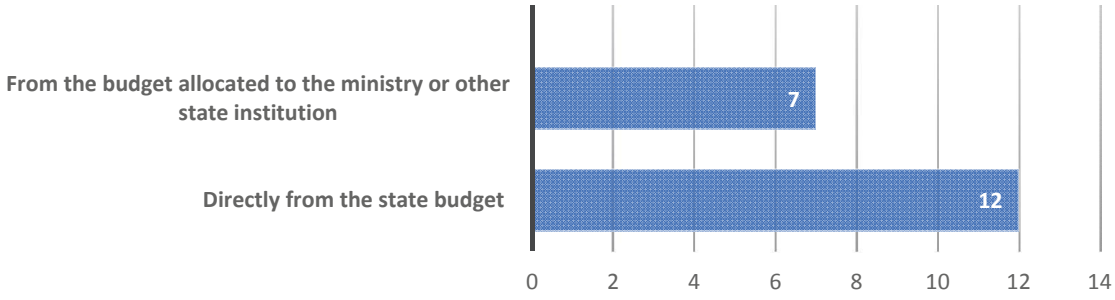
which are incompatible with the status of a member and staff of a supervisory authority during and after the term of office, as well as obligations of the members and staff of the supervisory authorities.

3.3.3 *Financial resources*

A sufficient budget is very important as it significantly affects other aspects, such as remuneration of staff, proper premises, communication systems etc. While Convention 108+ does not expressly regulate budgetary arrangements[13], Art. 52 (6) of the GDPR stipulates that each supervisory authority shall have a separate annual budget, which may be a part of the overall public or national budget. One of the issues relating to the allocation of budget is whether the supervisory authority budget shall be shown in a separate budget line (heading). The CJEU in its decision of 16 October 2012 in *European Commission v. Republic of Austria* C-614/10 held that: "<…> Member States are not obliged to reproduce in their national legislation provisions similar to those of Chapter V of Regulation No 45/2001[14] in order to ensure total independence of their respective supervisory authorities, and they can therefore provide that, from the point of view of budgetary law, the supervisory authorities are to come under a specified ministerial department. However, the attribution of the necessary equipment and staff to such authorities must not prevent them from acting 'with complete independence' in exercising the functions entrusted to them within the meaning of the second subparagraph of Article 28(1) of Directive 95/46."[15] Although there is no obligation to show the supervisory authority budget in a separate budget line (heading), the obligation to make sure that the supervisory authority has its own separate budget remains. It should also be noted that where the budget allocation procedure allows for decisive influence of the state institutions of executive power (e.g., at the stage of budget negotiations), this can lead to external influence on the supervisory authority.

The survey has shown that supervisory authorities receive financial resources either directly from the public budget or from the budget allocated to a ministry or another institution (see Figure 5):

Figure 5: Allocation of Financial Resources to Supervisory Authority



Some respondents stated that even though the supervisory authority budget was a part of the budget of another state institution (e.g., Ministry of Justice), the resources allocated to the supervisory authority would appear in a separate budget line.

According to the survey results, there are other sources of funding in some European countries besides the public budget, however one can conclude that this is not a common practice as only two respondents have indicated other sources: one respondent pointed out that the data protection supervisory

13 It is worth stressing that provisions of art. 15 (6) of the Convention 108+, obliging the Parties to provide supervisory authorities with the resources necessary for effective performance of their functions, also cover financial resources.

14 Article 43 (3) of Regulation No 45/2001 provided that„The [European Data Protection Supervisor's] budget shall be shown in a separate budget heading in Section VIII of the general budget of the European Union." Similar provision is set forth in art. 54 para. 3 of Regulation (EU) 2018/1725 which repealed Regulation No 45/2001: „The budget of the European Data Protection Supervisor shall be shown in a separate budgetary heading in the section related to administrative expenditure of the general budget of the Union."

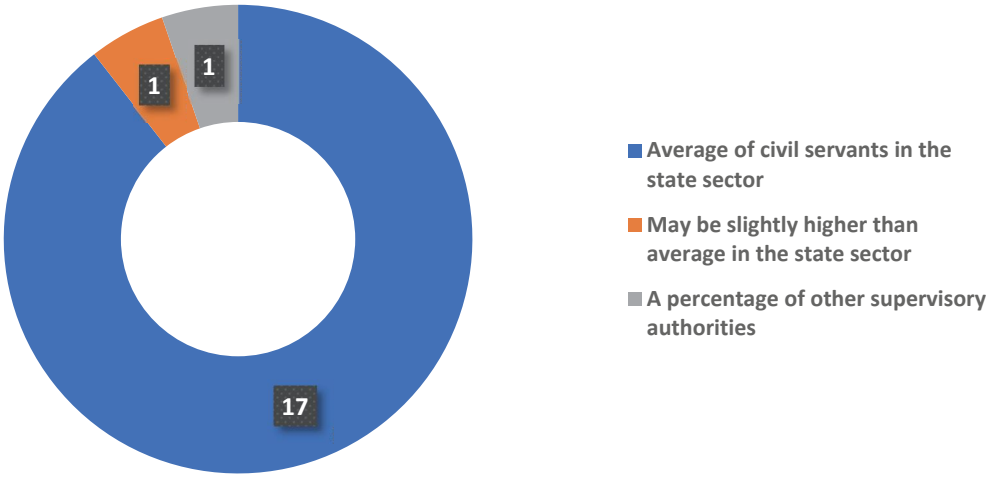
15 See para. 58.

authority received resources from paid services (fees for participation in the seminars organized by the supervisory authority and for data protection officer qualification tests), and another one referred to administrative fines or other monetary sanctions imposed as a penalty for infringements. One supervisory authority indicated that other legally received funds could be used to finance it.

It is worth underlining that the notion of „adequate financial resources" is not simple, and there is no unique methodology on setting up adequacy of financial resources. FRA in its paper „Elements of independence of the data protection authorities in the EU" has drawn attention to the fact that the general price level varies among EU Member States as the relative purchasing power of the Euro varies between them, which means that „in some countries, a certain amount of money will go farther than in others – with higher wages, resource costs etc. – distorting any comparison drawn between Member States. <...>" (see p. 16).[16] FRA tried to make the amounts spent by each data protection supervisory authority comparable across the 28 EU Member States by taking into account the population of each Member State, as well as a correction coefficient that takes into account purchasing power across the Member States. The budget of each authority has been divided by the correction coefficient, with the whole sum in turn divided by the population of the Member State, producing the relative amount available to data protection supervisory authority per capita annually:[17]

The question as to how much money is sufficient and should be allocated is always important but not easy to answer. Among the relevant indicators there can be the wage level of the supervisory authority staff. Results of the survey show that in most cases it equals the average pay of civil servants / public sector employees (see Figure 6):

Figure 6: Level of Salary of the Staff



An issue closely related to financial independence is the budget preparation procedure and possible influence by the government or its institutions. Here the data protection supervisory authority could play an important role. Financial independence of the supervisory authority would be significantly strengthened if the authority was closely involved in the budget development, especially as regards assessing the amount needed and conducting consultations throughout the decision-making process. Participation of the supervisory authority would contribute to budgetary stability and independence in the decision-making process on the allocation of funds and minimize the risk of influence by other state agencies and the government.

16 Available at: https://www.asktheeu.org/en/request/2398/response/9765/attach/3/21.FRA%20Focus%20Data%20protection%20authorities%20independence%20funding%20and%20staffing%20ATTACHMENT%20FRA%202013%20Focus%20DPA.pdf . Accessed 24 May 2021.

17 Ibid.

To sum it up, the data protection supervisory authority should have a separate, public annual budget, which may be a part of the overall public or national budget. The supervisory authority could have other sources of funding, however the obligation to ensure sufficient resources lies upon the government. Financial resources should be adequate and enable the authority to be equipped with qualified personnel, necessary premises, technical equipment and infrastructure. The risk of external influence on the supervisory authority during the budget allocation procedure could be significantly minimized thanks to participation of the supervisory authority in the consultations and decision-making process on the allocation of funds.

3.3.4 Human resources

Art. 52 (5) of the GDPR establishes the obligation to ensure that each supervisory authority shall be able to hire its own staff that will only report to the members of the supervisory authority concerned. The possibility for the supervisory authority to hire its own staff is also highlighted in the Explanatory Report (see para.129). The CJEU in its decision of 16 October 2012 in *European Commission v. Republic of Austria* C-614/10 held that the staff of data protection supervisory authorities should not be under the authority or subject to supervision of any other body in terms of hierarchy and remuneration, as well as disciplinary controls. The CJEU underlined that: "It should be borne in mind, in this regard, that paragraph 45(1) of the BDG 1979 grants the hierarchical superior an extensive power of supervision over the officials in his department. That provision enables the hierarchical superior not only to ensure that his staff carry out their tasks in accordance with the law, efficiently and economically, but also to guide them in carrying out their duties, rectify any faults and omissions and ensure that working hours are adhered to, encourage the promotion of his staff in accordance with their performance and direct them to those tasks which correspond best to their capacities."[18] The CJEU has ruled that "<…> such supervision by the State is not compatible with the requirement of independence set out in the second subparagraph of Article 28(1) of Directive 95/46, which must be satisfied by supervisory authorities for the protection of personal data."[19] In the same decision CJEU pointed out the risks to independence due to the organizational overlap with other state authorities, where the supervisory authority members are engaged in other work at the same time: "In view of the work-load of a supervisory authority responsible for the protection of personal data, on one hand, and of the fact that the members of the DSK exercise their duties under paragraph 36(3a) of the DSG 2000 at the same time as engaging in other work, on the other, it must be held that the members of such an authority rely in large measure on the staff made available to them for assistance in exercising the functions entrusted to them. The fact that the office is composed of officials of the Federal Chancellery, which is itself subject to supervision by the DSK, carries a risk of influence over the decisions of the DSK. In any event, such an organisational overlap between the DSK and the Federal Chancellery prevents the DSK from being above all suspicion of partiality and is therefore incompatible with the requirement of 'independence' within the meaning of the second subparagraph of Article 28(1) of Directive 95/46."[20]

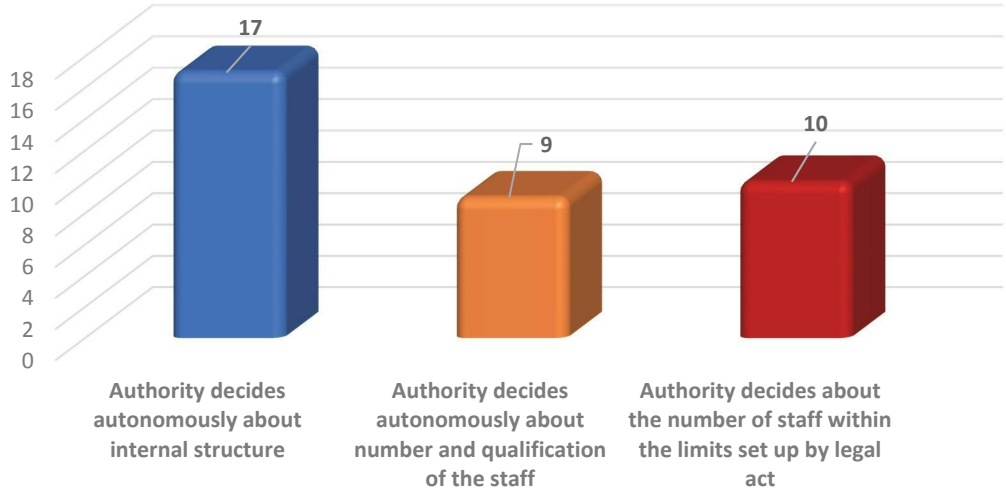
Participants of the survey were asked to provide information on the status of the employees, as well as powers of the supervisory authority regarding internal management (e.g., decisions about the internal structure of the authority, number and qualification of the staff). According to the results of the survey, there are various practices in the European countries as regards the status of the supervisory authority employees: they can have the status of civil servants, be employed under a labor contract, and the approaches can be combined.

18 CJEU decision of 16 October 2012 in *European Commission v. Republic of Austria*, C-614/10, ECLI:EU:C:2012:631, para. 49.
19 Ibid., para. 59.
20 Ibid., para. 61.

Despite the status of the supervisory authority staff, guarantees for protection against any influence are important. For example, according to Art. 8 (3) of the Law on the Legal Protection of Personal Data of the Republic of Lithuania, state and municipal institutions and agencies, members of the Parliament, other officials, political parties, public organisations, other legal and natural persons shall not have the right to exert any kind of political, economic, psychological or social pressure or other unlawful influence on the State Data Protection Inspectorate, its director, civil servants and employees working under employment contracts. Interference with activities of the State Data Protection Inspectorate shall entail liability established by laws.

As regards the internal structure, number and qualification of the staff, in most cases supervisory authorities are able to decide autonomously about their internal structure. However, as for the number of employees, ten respondents indicated that the legal acts set up the limit (see Figure 7).

Figure 7: Decisions Regarding Internal Structure, Number and Qualification of the Staff



The independence of a supervisory authority grows when it is empowered to appoint and manage its own staff, remaining free from external influence in the recruitment procedures. In addition to having adequate financial resources, it is important to be able to decide autonomously what proper number of employees the authority should have and to recruit sufficiently qualified staff members in various fields who can use their expertise in all areas of the authority's work (e.g., legal, information and communication technologies, etc.). Fair and transparent recruitment process should be ensured as a guarantee of independence.

Although setting up the limit of the number of supervisory authority staff by legal acts is not rare in the European countries, it should be noted that it can negatively affect the ability to carry out its tasks properly. Regulation of the staff limit can create a situation where even with sufficient financial resources the supervisory authority would not be able to hire.

It is also worth underlining that training is an essential part of ensuring that staff members are able to carry out their tasks properly, therefore the supervisory authority should be given sufficient resources to provide training in relevant fields. Adequate training is especially important considering rapid developments affecting the work of the employees.

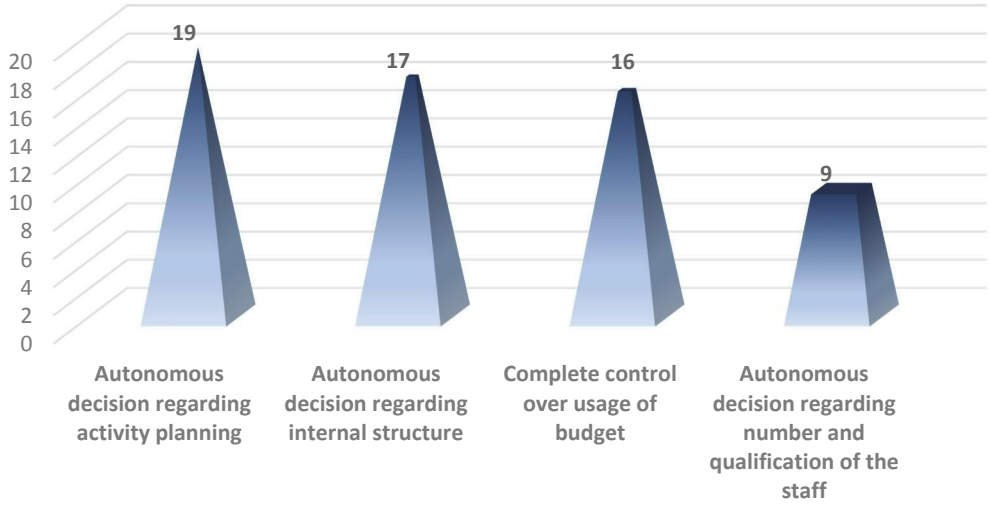
In conclusion, the supervisory authority should have a discretion to select and hire its own staff that will only report to the members thereof. Imposition of external limits on the supervisory authority staff should be avoided. Any organizational overlap between the data protection supervisory authority and any other state institution prevents the supervisory authority from being above all suspicion of bias and is therefore incompatible with the requirement of independence.

3.4. Other safeguards from external influence

3.4.1 Safeguards against control over internal activities and use of resources

Not only the allocation of sufficient resources, but also autonomous usage of them and planning of its activities is of crucial importance when ensuring independence of data protection supervisory authorities. The team of experts has tried to explore how this autonomy is implemented in the European countries, asking participants of the survey to provide information on the usage of the allocated budget (e.g., whether prior authorization / approval / advice from other governmental institution is required), approval of the authority's internal structure, decisions regarding the number and qualification of the staff, as well as activity planning. The results of survey are shown below (see Figure 8):

Figure 8: Autonomy of Usage of the Resources and Activity Planning



According to the survey results, it should also be noted that supervisory authorities are completely autonomous as regards activity planning, as no one has indicated that activity plans should be submitted for review, coordinated or approved by other institutions.

Autonomous usage of the resources does not mean that no type of control exists. Recital 118 of the GDPR explains that the independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review. Art. 52 (6) of the GDPR obliges the Member States to ensure that such financial control does not affect the supervisory authority's independence.

Data protection supervisory authorities must act in complete independence, free from any outside influence, particularly coming from the entities it supervises, as well as from the government. This was clearly stated by the CJEU in its decision of 9 March 2010 in *European Commission v. Federal Republic of Germany* C-518/07, in which the CJEU noted that the State scrutiny, whatever form it takes, in principle allows the government of the respective *Land* or an administrative body reporting to that government to influence, directly or indirectly, the decisions of the supervisory authorities or, as the case may be, to cancel and replace those decisions.[21] The CJEU did not support the position of the Federal Republic of Germany as „complete independence" requires the supervisory authorities to have functional independence in the sense that those authorities must be independent of the bodies outside the public sector which are under their supervision and that they must not be exposed to external influences, and that the State scrutiny exercised in the German *Länder* does not constitute such an external

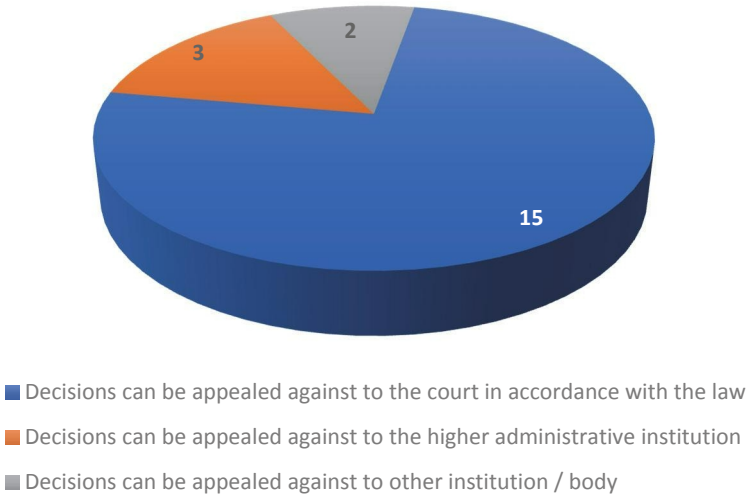
21 CJEU decision of 9 March 2010 in *European Commission v. Federal Republic of Germany* C-518/07, ECLI:EU:C:2010:125, para. 32.

influence but rather the administration's internal monitoring mechanism, implemented by the authorities attached to the same administrative machinery as the supervisory authorities and required, like the latter, to fulfil the aims of Directive 95/46.[22] Despite the arguments provided by the Federal Republic of Germany that the State only seeks to guarantee that acts of the supervisory authorities comply with the applicable national and European Community provisions, and that it therefore does not aim to oblige those authorities to potentially pursue political objectives inconsistent with the protection of individuals with regard to the processing of personal data and with fundamental rights, the CJEU held that the State scrutiny exercised over the German supervisory authorities responsible for supervising the processing of personal data outside the public sector is not consistent with the requirement of independence as defined in paragraph 30 of the judgment in question.[23]

However, independence of the supervisory authority does not mean that its decisions cannot be appealed. Where an administrative decision produces legal effects, every affected person has the right to have an effective judicial remedy in accordance with the applicable national law. Data subjects, data controllers, data processors, as well as third parties can be among those affected persons. Art. 15 (9) of the Convention 108+ establishes that decisions of the supervisory authorities may be subject to appeal in the courts. According to Art. 78 of the GDPR, without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. The data subject shall have the right to an effective judicial remedy where the supervisory authority does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint.

Following results of the survey, the majority of participants indicated that decisions of the data protection supervisory authority can be appealed to the court in accordance with the law of the Member State (see Figure 9):

Figure 9: Appealing against the Decisions of Supervisory Authority



The Croatian authority specified that no appeal shall be allowed against a ruling of the supervisory authority, but an administrative dispute may be instituted by lodging a complaint before a competent administrative court. The Greek authority indicated that decision can be appealed at the Council of State[24].

22 Ibid., para. 16.
23 Ibid., para. 33, 37.
24 According to publicly available information, the Council of State is the Supreme Administrative Court of Greece (http://www.adjustice.gr/webcenter/portal/SteEn/Home?_afrLoop=4467481217124692#!%40%40%3F_afrLoop%3D4467481217124692%26centerWidth%3D100%2525%26showHeader%3Dtrue%26_adf.ctrl-state%3Dtc3p6uucc_4, accessed 5 July 2021).

Three respondents indicated that decisions can be appealed to the higher administrative institution or body.

In conclusion, the supervisory authority should be given autonomy regarding the usage of its resources and planning of its activities and should not be subject to external control, whether direct or indirect. However, financial control exercised in accordance with the law and not affecting independence of the authority is possible. Appealing the decisions of supervisory authority should comply with the rule of law. Every affected person must be able to appeal against the decisions of the supervisory authority in the courts.

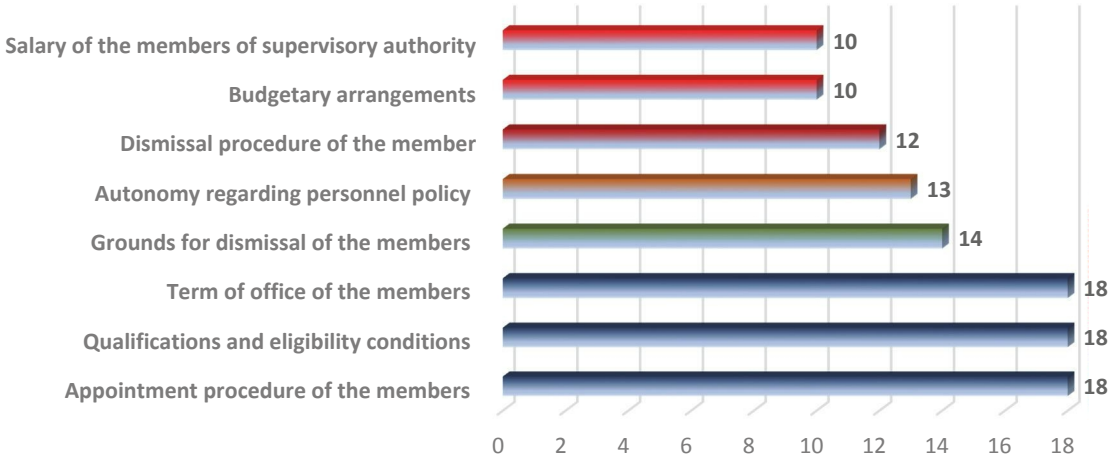
3.4.2 Legal acts adopted by the parliament as a safeguard against external influence

To ensure stable functioning of a supervisory authority, it is crucial to identify its structure and status as well as regulate the aspects relating to its independence by law or another legal act adopted by the parliament. The team of experts has tried to explore the European practices and find out which of the following aspects are regulated by the legal acts adopted by the parliament:

- Appointment of the supervisory authority head / members;
- Qualifications and eligibility requirements for appointment of the supervisory authority head / members;
- Term of office of the supervisory authority head / members;
- Grounds for dismissal of the supervisory authority head / members;
- Dismissal procedures for the supervisory authority head / members;
- Budgetary (financial) arrangements;
- Personnel policy (e.g., right to hire its own staff, etc.);
- Salary of the supervisory authority head / members.

Six participants of the survey have indicated that all the above is regulated by the acts adopted by the parliament. Almost all participants said that the acts adopted by the parliament prescribed appointment procedures for the supervisory authority head / members, qualifications and eligibility conditions required to be appointed as the supervisory authority head / members, as well as term of office of the supervisory authority head / members. The distribution of responses is shown in Figure 10:

Figure 10: Aspects Regulated by Legal Act Adopted by Parliament



In conclusion, a legal act adopted by the parliament serves as a strong guarantee for ensuring independence of the supervisory authority. Such legal act should regulate the main aspects concerning independence, such as procedures for appointment of the members, qualifications and eligibility conditions required to be appointed as a supervisory authority member, term of office of the supervisory authority members, grounds for terminating the duties and dismissal, budgetary arrangements, salary of the supervisory authority members, autonomy regarding personnel policy and activity planning.

3.4.3. Safeguards against political influence

It should be noted that the functional independence of supervisory authorities (i.e., ability not to be bound by instructions of any kind in the performance of their duties) is an essential but not sufficient condition in itself to protect supervisory authorities from external influence. This was clearly stated by the CJEU in its decision of 16 October 2012 in *European Commission v. Republic of Austria* C-614/10: "The fact that the DSK has functional independence in so far as, in accordance with paragraph 37(1) of the DSG 2000, its members are 'independent and [are not] bound by instructions of any kind in the performance of their duties' is, admittedly, an essential condition in order for that authority to satisfy the criterion of independence within the meaning of the second subparagraph of Article 28(1) of Directive 95/46. However, contrary to what the Republic of Austria maintains, such functional independence is not by itself sufficient to protect that supervisory authority from all external influence."[25]

Political influence may take various forms. The CJEU in its decision of 8 April 2014 in *European Commission v. Hungary* C-288/12 held that: "<…> the mere risk that the State scrutinizing authorities could exercise political influence over the decisions of the supervisory authorities is enough to hinder the latter in the independent performance of their tasks. First, there could be 'prior compliance' on the part of those authorities in the light of the scrutinizing authority's decision-making practice. Secondly, in view of the role adopted by those authorities as guardians of the right to private life, the second subparagraph of Article 28(1) of Directive 95/46 requires that their decisions – and, therefore, the authorities themselves – remain above all suspicion of partiality".[26] Moreover, following the CJEU practice, the restructuring or changing of the institutional model must be arranged in such a way as to meet the requirement of independence laid down in the applicable legislation (i.e., without the premature termination of the term of office of the already appointed members of the supervisory authority).

Art. 53 (4) of the GDPR stipulates that each member shall have the qualifications, experience and skills, in particular in the area of personal data protection, required to perform their duties and exercise their powers, i.e., the possibility to be appointed a supervisory authority member should depend on one's professional qualifications and experience. Obviously, political or other beliefs, membership in one or another political party and similar conditions cannot be the grounds for appointment or dismissal of a supervisory authority member. For this reason, the beginning and the end of the term of office of the supervisory authority members should not be linked to that of the appointing entity (except where it is a coincidence in time).

To sum it up, the regulation of the supervisory authority status should generally ensure that it is free from political influence. To avoid political influence, the beginning and the end of the term of office of the supervisory authority members should not be linked to that of the appointing entity (i.e., government, parliament, head of the State). Political or other beliefs shall not play any role in the process of appointment or dismissal of a member. The term of office of the supervisory authority member should not be terminated early except as provided by the law.

25 CJEU decision of 16 October 2012 in European Commission v. Republic of Austria, C-614/10, ECLI:EU:C:2012:631, para. 42.
26 CJEU decision of 8 April 2014 in European Commission v. Hungary, C-288/12, ECLI:EU:C:2014:237, para.53. See also *Commission* v *Germany* EU:C:2010:125, para. 36, and *Commission* v *Austria* EU:C:2012:631, para. 52.

4

POWERS OF INVESTIGATION, INTERVENTION, COMPLAINTS HANDLING, AND REGULATORY POWERS

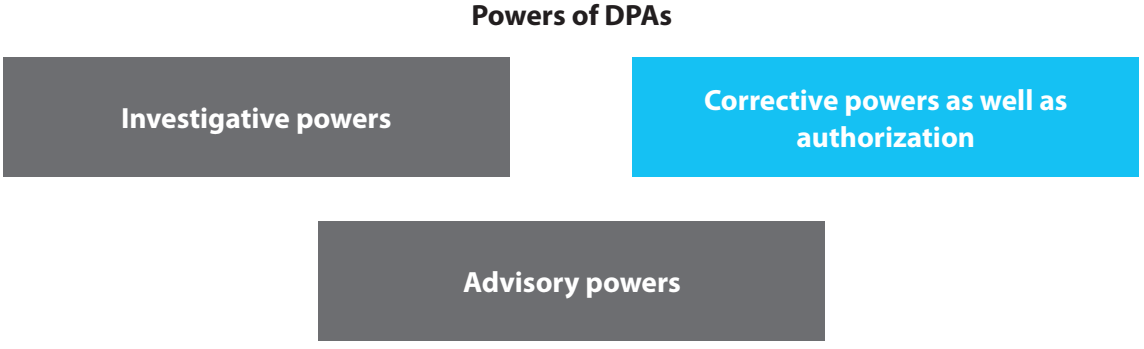
4.1. Powers of the authorities according to Convention 108+

Article 15 of Convention 108+ establishes that the authorities

- shall have powers of investigation and intervention;
- shall perform the functions relating to transfers of data provided for under Article 14, notably the approval of standardized safeguards;
- shall have powers to issue decisions with respect to violations of the provisions of this Convention and may, in particular, impose administrative sanctions;
- shall have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of Convention 108+;
- shall be consulted on proposals for any legislative or administrative measures which provide for the processing of personal data;
- shall deal with requests and complaints lodged by data subjects concerning their data protection rights and shall keep data subjects informed of progress;
- shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions.

4.2. Powers of the authorities in the GDPR

According to Recital 129 of the Regulation 2016/679, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers, as well as authorization, and advisory powers.



Article 58 of the GDPR defines what powers should be assigned to the national supervisory authority, namely:

Investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

Corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organization.

Authorization and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c) to authorize processing referred to in Article 36(5), if the law of the Member State requires such prior authorization;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorize contractual clauses referred to in point (a) of Article 46(3);

(i) to authorize administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

4.3. Scope of competence of supervisory authorities

The scope of the authority may be wider than established in the GDPR.

Application of the Estonian Personal Data Protection Act and the GDPR are established in Article 2 of this Act.

The Latvian Inspectorate is only partly responsible for data processing for journalistic purposes.

The Croatian DPA, according to Article 36 of the Law on Implementation of the General Data Protection Regulation, authorizes the Agency employees to carry out planned or ad hoc audits independently, and is specific cases also with participation of a supervisory authority representative (hereinafter authorized persons). The audited person and the controller or the processor are notified about the unannounced audit at the site and at the time when the audit takes place.

The Information Commissioner is the supervisory authority of the Republic of Cyprus that can supervise public access to official documents. The tasks and powers assigned to the Information Commissioner are exercised by the respective Commissioner for Personal Data Protection.

The Italian law identifies some additional areas in the section «Provisions applying to processing that is necessary for compliance with a legal obligation or for the performance of a task carried out in the public interests or in the exercise of official authority and processing referred to in chapter IX of the Regulation»: legal information services, processing operations by the police and the national defence and security agencies, processing operations in the public sector (public registers and professional registers), processing of personal data in the health care sector, education (processing of data concerning students), processing for archiving purposes in the public interests or for historical research purposes, processing for statistical purposes or scientific research purposes, processing activities in

employer / employee relations, remote surveillance, telework, assistance boards and welfare bodies, electronic communications services.

In addition to the provisions of Article 57 the GDPR, the Estonian Data Protection Inspectorate is authorized to

1) increase the awareness and understanding of the public, controllers and processors about the risks in the processing of personal data, the standards and safeguards and the rights related to personal data processing; the Estonian Data Protection Inspectorate may give recommendations for the performance of this function;

2) provide information to data subjects upon request about implementation of the rights arising from this Law and, where appropriate, co-operate for this purpose with the supervisory authorities of other Member States of the European Union;

3) if necessary, initiate administrative offense proceedings and impose sanctions, unless other administrative measures allow to achieve compliance with the requirements provided by law or Regulation (EU) 2016/679 of the European Parliament and the Council;

4) co-operate with international data protection supervision organizations and other data protection supervision authorities as well as other competent foreign authorities and persons;

5) monitor relevant developments insofar as they affect personal data protection, in particular the development of information and communications technologies;

6) consult on personal data processing operations referred to in § 39 of this Law;

7) participate in the European Data Protection Board;

8) apply administrative pressure on the grounds, to the extent and along the procedures prescribed by law;

9) present opinions on its own initiative or upon request on personal data protection to the parliament, the government, the Chancellor of Justice and other agencies and the public;

10) perform other duties arising from law.

4.4. Authorities that can conduct investigations

In general, all the authorities have a broad range of powers established by the GPPR as well as additional powers, as referred to in Article 58 (6)[27].

At the same time, DPA officers should have access to the premises in accordance with the procedures established by criminal procedure legislation, involving law enforcement agencies where necessary.

Control activities of the Romanian supervisory authority are regulated in Chapter IV, Section 1 of Law no. 102/2005, amended. Article 14 (2) of Law no. 102/2005 states that the officers who have controlling functions have the right to carry out investigations, including unannounced ones, to request and obtain any information and documents, regardless of the storage medium, from data controllers and processors, as well as, where necessary, from their representatives, on the spot and/or within the established deadline, to make copies, to have access to any of the controller's and processor's premises,

27 https://www.dataprotection.ro/servlet/ViewDocument?id=172

as well as to have access and to audit any equipment, data storage medium or data necessary for the performance of the investigation, according to the law. Paragraph (3) of the same Article provides that, where the control officers are prevented in any way in the exercise of the tasks stipulated in paragraph (2), the National Supervisory Authority may request a judicial permission to be issued by the President of the Bucharest Court of Appeal or an authorized judge. Furthermore, the identification and preservation of the objects, as well as sealing should comply with the provisions of Law no. 135/2010 on the Criminal Procedure Code, with subsequent amendments and supplements. At the same time, the Romanian supervisory authority may decide to carry out expert assessments and hear the persons whose statements are considered relevant and necessary for the investigation.

The Italian DPA has provided a reference to the law that establishes its powers: «To correctly reply to the question, we prefer not to offer separate answers (as they can only partially reflect the Italian DPA powers), but to refer to Article 158 of the Italian Data Protection Code».[28]

It should be noted that the law refers to Article 58 of the Regulation as the one that defines the powers and further expands them by establishing procedural measures for exercise of the powers. Therefore, we can conclude that the powers of the authority generally coincide with those specified in the GDPR. It is also interesting to further identify the tasks of the body in relation to the tasks established by other European regulations, including the powers and tasks provided in the Convention 108+.

Section 154

1. In addition to the provisions found in specific legal acts as well as in Section II, Chapter VI of the Regulation, and pursuant to Article 57(1v), of the said Regulation, the Garante shall, on one's own initiative and with support of the Bureau, in accordance with the applicable legislation in respect of one or more than one controller

   a) check whether data processing operations are carried out in compliance with applicable laws and regulations;

   b) handle the complaints lodged with it in pursuance of the Regulation and the provisions of this Code, by laying down specific arrangements in its rules of procedure and prioritizing the issues resulting annually from such complaints, which issues may then become the subject of investigations in the course of the relevant year;

   c) encourage the adoption of rules of conduct in the cases envisaged under Section 2-c;

   d) report facts and/or circumstances amounting to offences to be prosecuted ex officio, which it has come to know either in carrying out or on account of its functions;

   e) transmit the annual report as drawn up pursuant to Article 59 of the Regulation to Parliament and Government by the 31st of May of the year following that to which the report refers;

   f) ensure the protection of the fundamental rights and freedoms of the individuals by implementing the Regulation and this Code as appropriate;

   g) discharge such tasks as are allocated to it by Union or State law and carry out such additional functions as are laid down in domestic law.

2. Pursuant to paragraph 1, the Garante shall also discharge supervisory or assistance tasks concerning personal data processing as provided for by laws ratifying international agreements and conventions or else by Community or EU regulations, with particular regard to the following:

28 https://www.garanteprivacy.it/data-protection-code

a) Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II);

b) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA;

c) Regulation (EU) 2015/1525 of the European Parliament and of the Council of 9 September 2015 amending Council Regulation (EC) No 515/97 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure correct application of the law on customs and agricultural matters as amended by section 4(1) of legislative decree No 109/2008 (Implementing Directive 2006/24/EC). 63 and Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes;

d) Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for identification of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining a Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice;

e) Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) and Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences;

f) Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation');

g) Chapter IV of Convention No 108 on the protection of individuals with regard to the automated processing of personal data, as adopted in Strasbourg on 28 January 1981 and implemented by Law No 98 of 21 February 1989, being the authority designated for the purpose of inter-State co-operation pursuant to Article 13 of said Convention.

3. Regarding any matters that are not addressed in the Regulation or this Code, the Garante shall regulate, by way of its own rules of procedure in pursuance of Section 156(3) hereof, the specific arrangements for any proceedings related to discharge of the tasks or exercise of the powers conferred on it by the Regulation or this Code.

4. The Garante shall co-operate with other national independent administrative authorities in discharging the respective tasks. 5. Subject to such shorter terms as may be provided for by law, the Garante's opinion shall be rendered within forty-five days of receiving the relevant request, including the requests referred to in Article 36(4) of the Regulation. Upon expiry of that term,

the requesting administrative agency may proceed irrespective of the acquisition of the Garante's opinion. If the term set out in this paragraph may not be complied with because of constraints related to preparation of the case, running of time may be suspended once only and the opinion shall have to be rendered in its final form within twenty days of receiving the information requested from the administrative agencies concerned for preparation of the case.

6. A copy of any measure taken by judicial authorities in connection with either this Code or computer crimes shall be transmitted to the Garante by the court clerk's office.

7. The Garante shall not be competent for supervision over processing that is carried out by judicial authorities acting in their judicial capacity.»

Therefore, the DPA may have other powers that complement the powers defined by the GDPR but do not contradict it.

The DPA of the Republic of Cyprus has also stated that it has additional powers as the data protection supervisory authority, established, inter alia, by Article 25(d) of Law 125(I)/2018. «In exercising investigative powers, the commissioner can seize documents or electronic devices through a search warrant in accordance with the provisions of the Criminal Procedure Law».[29]

The Greek DPA conducts, ex officio or following a complaint, investigations and audits, during which the technological infrastructure and other automated or non-automated means supporting the processing of personal data are subject to controls. In carrying out such investigations and inspections, the Authority has the power to obtain, from the controller and the processor, access to all personal data processed and to all information necessary for the purposes of such audits and the performance of its tasks, and no type of confidentiality may be relied upon against it. The Authority does not have access to data identifying associates or staff employed in entities contained in records held for national security purposes or for the purpose of investigating particularly serious crimes.

2) The Authority also:

(a) issues warnings to a controller or processor;

(b) orders the controller or processor to comply with the provisions of data protection legislation in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data;

(c) orders and imposes a temporary or definitive limitation, or even a ban on the processing of personal data;

(d) orders and imposes that documents, filing systems, equipment or means for processing personal data be delivered to it, as well as their content;

(e) seizes documents, information, filing systems for each piece of equipment and means of personal data breach, and their content which becomes known to the Authority in the exercise of its supervisory powers.

The Authority may seize the above material until a decision has been made by competent judicial and prosecutorial authorities. As far as access to residential premises is concerned, according to Article 9 of the Greek Constitution: "no home search shall be made, except when and as specified by law and always in the presence of representatives of the judiciary".

The Estonian Data Protection Inspectorate can make request electronic communications companies to provide the data required for the end-user identification through the identification tokens used in

29 http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf

public electronic communications networks, except for the data relating to the fact of transmission of messages, if the end-user identification through the identification tokens is impossible in any other manner. For the implementation of government supervision provided by national Law, the Estonian Data Protection Inspectorate may apply specific government supervision measures provided for in §§ 30-32, 44, 49-53 of the Law Enforcement Act[30], on the basis of and in accordance with the procedure provided by the Law Enforcement Act.

Polish Data Protection Authority stated that, in accordance with the law establishing its powers, it has the following investigative functions:

- to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of the data protection supervisory authority;
- to order any natural and / or legal person (other than the controller and processor) to provide any information required for the performance of the tasks of the data protection supervisory authority;
- to carry out searches and seizures in the premises of the data processor / controller without judicial warrant;
- to obtain access without a prior notice to the premises / territory of the controller / processor.

It should be noted that no authorities have the right to enter the premises owned by a natural person without a court warrant.

4.5. Authorities that corrective powers

All 19 DPAs, without exception, have corrective powers in accordance with Article 58 of the GDPR. Additionally, the Estonian and Greek DPA powers have some specific features.

The Estonian DPA does not impose administrative fines stipulated in the GDPR. The Estonian DPA has the right to impose fines for offenses, while administrative fines are not foreseen by the Estonian legal system.

The Greek supervisory authority has the power "to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 the GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met". Moreover, the authority a) has the corrective power to order the controller or processor, or a recipient, or a third party, to discontinue the processing of personal data or to return or block access to the relevant data or to destroy the filing system or the relevant data and to impose the administrative penalties provided for in Articles 82.8 and 83 of the GDPR, b) where the protection of the individual against the processing of personal data concerning him or her requires immediate decision-making, the President may, at the request of the person concerned or ex officio, issue a temporary order for immediate temporary limitation, in whole or in part, of the processing or the operation of the file. The order shall apply until the authority reaches its final decision, c) in order to ensure compliance with the provisions of the GDPR, and other regulations relating to the protection of the data subject with regard to the processing of personal data, the authority has the power to adopt administrative regulatory acts to regulate specific, technical and detailed matters referred to in those acts. The regulatory acts of the authority, which are not published in the Government Gazette, are published on the authority's website.

30 https://www.riigiteataja.ee/akt/104012019011.

4.6. Authorities with authorization and advisory powers

The supervisory authorities stated that they had all the powers set out in Article 58 of the GDPR.

Authority of the Republic of Cyprus pointed to the powers provided by national law, namely Article 25(g) of the Law 125(I)/2018: "In addition to the authorization and advisory powers provided for in Article 58, paragraph 3 of the Regulation, the Commissioner shall have the power to: - i) authorize the combination of filing systems provided for in section 10 of this Law and impose terms and conditions for the materialization of the combination, ii) impose terms and conditions in relation to the application of the measures for the restriction of the rights referred to in section 11 of this Law, iii) impose terms and conditions for the exemption to the obligation to communicate the data breach referred to in section 12 of this Law, iv) impose explicit limits for the transfer of special categories of personal data referred to in sections 17 and 18 of this Law, v. recommend to the Minister the conclusion of agreements with other countries and conclude, establish and sign the Memoranda of Understanding provided for in section 35 of this Law."[31]

The Latvian Authority carries out accreditation of certification agencies together with the Latvian National Accreditation Bureau.

Pursuant to Art 57 of the GDPR, each supervisory authority shall, on its territory, advise, in accordance with Member State laws, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to data processing.

The modernised Convention 108 prescribes that competent supervisory authorities shall be consulted on proposals for any legislative or administrative measures related to processing of personal data.

Participants of the survey were asked to indicate their competences regarding recommendations they can provide for the parliament, government, other state institutions and agencies for the adoption of legislative and administrative measures. The waste majority said that their competences included the right to present opinions on draft legal acts that had already been developed, and opinions about the bills as they were drafted.

According to Art. 14 of the Act on the Implementation of the General Data Protection Regulation, central public administration agencies and other public authorities shall submit to the Croatian Personal Data Protection Agency draft laws and other regulations related to personal data processing for its expert opinions on personal data protection.

The Estonian Data Protection Inspectorate and Austrian Data Protection Authority provide opinions to draft legal acts within their competences while the legal acts are drafted.

The Office for Personal Data Protection of the Czech Republic provide opinions within their competence upon adoption of the legal act.

4.7. Authorities that have regulatory powers

The authorities of Norway, Italy, Estonia, Croatia, the Republic of Cyprus, Lithuania, Iceland, the Duchy of Luxembourg, Latvia, the Republic of Slovenia and Bulgaria have stated that they have additional powers.

31 http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf

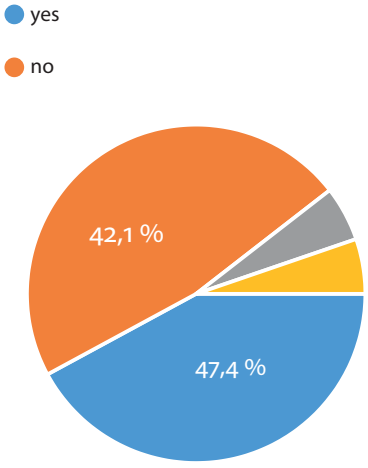
The Croatian supervisory authority noted that according to Article 6. of the Act on the Implementation of the General Data Protection Regulation, in addition to its powers laid down by the General Data Protection Regulation, the Agency performs the following tasks:

- where it is provided by a special law, it may initiate and has the right to participate in criminal proceedings, administrative offense proceedings, administrative and other court and out-of-court proceedings for breaches of the General Data Protection Regulation and this Act;
- it adopts the criteria to identify the amount of compensation for administrative costs referred to in Article 43 (2) of this Act and the criteria for to identify the amount of compensation referred to in Article 43 (3) of this Act;
- it publishes individual decisions on the Agency's website in accordance with Articles 18 and 48 of this Act;
- it initiates and takes appropriate steps against the persons responsible for breaches of the General Data Protection Regulation and this Act;
- it carries out its duties of the independent supervisory authority to monitor the implementation of Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, unless otherwise laid down by special regulations;
- it carries out other duties established by law.

The tasks assigned to the Information Commissioner are exercised by the respective Commissioner for Personal Data Protection of the Republic of Cyprus. The Commissioner is the competent supervisory authority among other European authorities.

The results of survey are shown below (see Figure12):

Figure 12: Data protection supervisory authority is endowed with the regulatory powers other than those provided in GDPR (e.g. Art. 35 (4), etc.):

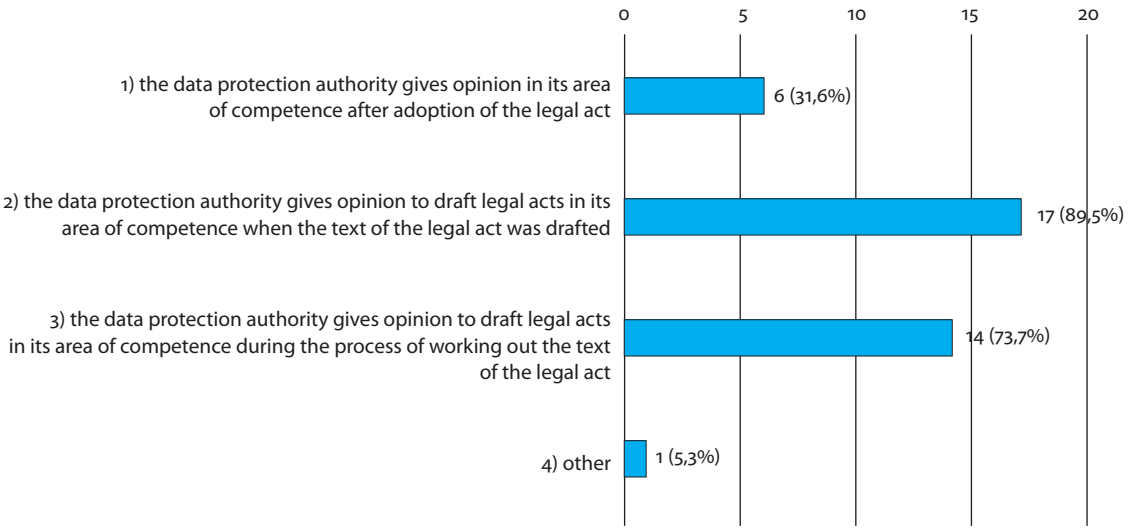


According to Article 6. of the Act on the Implementation of the General Data Protection Regulation in addition to its powers laid down by the General Data Protection Regulation, the Agency shall perform the following duties: – when laid down by a special law, it may initiate and has the right to participate in criminal, misdemeanour, administrative and other court and out-of-court proceedings for breaches of the General Data Protection Regulation and this Act – adopts the Criteria for determination of the amount of the compensation of administrative costs referred to in Article 43, paragraph 2 of this Act and the Criteria for determination of the amount of the compensation referred to In Article 43, paragraph 3 of this Act – publishes individual decisions on the Agency's website in accordance with Articles 18 and 48 of this Act – initiates and conducts appropriate procedures against responsible persons for breaches of the General Data Protection Regulation and this Act – carries out its duties of the independent supervisory authority for monitoring the implementation of Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council framework Decision 2008/977/JHA, unless otherwise laid down by special regulations and – carries out other duties laid down by law.

The tasks assigned to the information Commissioner are exercised by the respective Commissioner for Personal Data Protection. The Commissioner is the competent supervisory authority for other European bodies.

The supervisory authorities have also reported that they can provide recommendations to national authorities. The results of survey are depicted below (see Figure13):

Figure 13: Data protection supervisory authority competence regarding recommendation to parliament, government, other state institutions and bodies as regards adoption of legislative and administrative measures



4.8. Powers to engage in legal proceedings

Regulation 2016/679 stipulates that each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union.

According to Art. 15 of the Modernised Convention 108, supervisory authorities shall have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention.

Participants of the survey were asked to indicate the rights of data protection supervisory authorities regarding their engagement in legal proceedings. The vast majority said that they have a right to take part in legal proceedings regarding decisions adopted by the authority.

Engagement in legal proceedings

appeal against normative legal acts adopted by public administration institutions

address matter to the Constitutional court

take part in legal proceedings regarding decisions adopted by your authority

For example, the Data Protection Authority of Portugal has a right to appeal normative legal acts adopted by public authorities, to submit constitutional motions to the Constitutional Court, and to take part in legal proceedings regarding decisions adopted by the authority.

The Croatian Personal Data Protection Agency can initiate and has the right to participate in criminal proceedings, administrative offense proceedings, administrative and other court and out-of-court proceedings for breaches of the General Data Protection Regulation and the Act on the Implementation of the General Data Protection Regulation. The Croatian Personal Data Protection Agency may initiate and conduct appropriate procedures against the persons responsible for breaches of the General Data Protection Regulation and this Act.

The Cyprus Commissioner for Personal Data Protection, in accordance with the law, has a right to appeal normative legal acts adopted by public authorities, and to take part in legal proceedings regarding decisions adopted by the authority. The Commissioner notifies the Attorney General of the Republic and/ or the police of any violation of the provisions of the Regulation or of the law that may constitute an offense.

The Information Commissioner of the Republic of Slovenia has a right to submit constitutional motions to the Constitutional Court, and to take part in legal proceedings regarding decisions adopted by the authority.

The Office for Personal Data Protection of the Czech Republic has a right to appeal normative legal acts adopted by public administration institutions.

5

RAISING PUBLIC AWARENESS ON PERSONAL DATA PROTECTION

Data Protection Authorities of the EU member states conduct educational activities through their participation in data protection awareness-raising campaigns aimed at controllers, processors and the general public.

According to Art 57.1 of the GDPR, awareness-raising responsibilities of the DPAs can be divided into two groups. The first one includes DPA obligations to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to data processing. The second one requires DPAs to promote "awareness of controllers and processors".

Art. 57
Regulation 2016/679

- Promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing
- Promote the awareness of controllers and processors of their obligations under this Regulation

The Modernised Convention 108 suggests that supervisory authorities shall promote

- public awareness of their functions and powers as well as their activities;
- public awareness of the rights of data subjects and the exercise of such rights;
- awareness of controllers and processors of their responsibilities under this Convention.

Recital 132 of the GDPR notes that awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as data subjects.

The GDPR does not list the activities and events whose implementation contains awareness-raising duties. According to general communication practices, examples of various activities may include, but are not limited to, "issuing press releases, briefings, and comments; reports, research, and publications; cooperating with the media; holding public meetings and activities; holding meetings and seminars; and creating and contributing educational materials".

DPAs regularly provide expert advice on data protection independently, in cooperation with other DPAs, or within the framework of the European Data Protection Board (EDPB). This expert advice on consistent application of the GDPR can be presented as guidelines, recommendations, and best practices.

In this report, we present some of the key findings. Participants of the survey were asked to indicate the activities regarding promotion of public awareness, as well as awareness of controllers and processors about their responsibilities. The vast majority said that their activities included seminars/webinars and consulting controllers and processors on the provisions of Regulation 2016/679, launching information campaigns on data protection for controllers and processors to enhance qualifications of the civil servants responsible for personal data protection.

According to the information provided by the European Commission[32], since 2017 the European Union has allocated a total of 5 million euros to 19 projects to support the implementation of the General Data Protection Regulation.

By May 2020, a total of 5 million euros of financial support has been obtained through three rounds of funding, and the last two rounds are dedicated to supporting national data protection authorities in their efforts to reach out to individuals and small and medium-sized businesses.

For example, the Croatian Personal Data Protection Agency conducts regular weekly trainings on the tasks and roles of data protection officers that arise from the GDPR. The trainings are separate for public and private sector in order to focus on the issues of a particular sector and on certain activities, such as the security sector. Following the trainings, documents and brochures are published on the website of the Croatian Personal Data Protection Agency.

Within the EU ARC project (awareness raising campaigns for SMEs), the Croatian Personal Data Protection Agency and the Data Protection Commission of Ireland have noticed during their everyday work that there was still a lot of ambiguities in the application of the GDPR by the SMEs. These findings were also supported by a large number of written queries and even a greater number of phone calls that these two authorities received on a daily basis. Thanks to this project the Croatian Personal Data Protection Agency and the Data Protection Commission of Ireland have an additional opportunity to help these subjects with workshops, presentations and educational materials so they can implement the GDPR and understand the importance of personal data protection.

The Lithuanian State Data Protection Inspectorate raises awareness by developing public information tools and methodological documents, attending meetings with the public and private sectors, and making presentations at the events.

The Austrian Data Protection Authority places a great deal of information on its website and publishes newsletters with the authority's important decisions.

The Estonian Data Protection Inspectorate has a helpline for data controllers/processors, data subjects, other public authorities etc.

The Cyprus Commissioner for Personal Data Protection provides data protection information campaigns for controllers and processors to enhance the qualifications of civil servants responsible for personal data protection, and information campaigns for students.

The Greek Data Protection Authority makes public presentations, organizes information days and scientific conferences.

The Data Protection Authority of Poland publishes a monthly newsletter addressed to data protection officers.

32 https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en

CNIL (France) leads data protection awareness campaigns aimed at the general public through the media, its website, social media and targeted seminars. CNIL also participates in conferences, seminars and workshops to provide important information and knowledge.

The Office of the Information Commissioner (ICO) has launched a campaign to raise awareness about data protection among UK consumers. The campaign follows the ICO's recommendations for surveys using data analysis for political purposes. The campaign provided consumers with many resources, including downloadable privacy and advertising setup fact sheets, and information about people's rights under the GDPR.

Information Commissioner Elizabeth Denham said[33], "Our goal is to promote change and ensure confidence in our democratic system. And that can only happen if people are fully aware of how organizations are using their data, particularly if it happens behind the scenes". The Information Commissioner also noted, "New technologies and data analytics provide persuasive tools that allow campaigners to connect with voters and target them directly with messages based on their likes, swipes and posts. But this cannot be at the expense of transparency, fairness and compliance with the law".

Activities organized by the Data Protection Authorities

- Belgium: Privacy and GDPR awareness campaign for citizens
- Bulgaria: innovative tools for SMEs and citizens
- Hungary: training material targeting SMEs
- Latvia: awareness-raising for Latvian SMEs and minors
- Iceland: awareness-raising for Icelandic general public
- Slovenia: raise awareness on data protection in general public
- Netherlands: raising awareness about data protection in the Netherlands

Ukraine is also taking its first steps to promote public awareness in the field of personal data protection.

The Office of the Ukrainian Parliament Commissioner for Human Rights and the Council of Europe Office in Ukraine have launched an initiative online course to raise awareness of Ukrainians in the field of data protection. The course consists of two parts: the first part (general) is for a broad audience, and the second part (professional) is for data protection professionals and people who want to delve into the subject.[34]

The Ministry of Digital Transformation of Ukraine has launched a series of educational videos called "Personal Data". These videos are designed to teach people to be careful about placing their personal information online, to understand their rights as to personal data protection, and what to do if these rights are violated. This video is to reduce the number of violations in the field of personal data.[35]

33 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/05/helping-people-be-data-aware/
34 https://www.coe.int/en/web/kyiv/-/ak-zahistiti-personal-ni-dani-ofis-ombudsmana-ta-ofis-radi-evropi-v-ukraini-zapuskaut-navcal-nu-iniciativu
35 https://www.ua.undp.org/content/ukraine/en/home/presscenter/pressreleases/2020/digital-transformation-ministry--with-undp-support--launches-ser.html

Activities organized by the Data Protection Authorities	The Stichting European Lawyers Foundation organised training of lawyers on the EU data protection reform The Vrije Universiteit of Brussel supported the Hungarian DPA in organising training activities on the data protection Reform The Center for European Constitutional Law organised training on Legal professional and DPOs in Greece and Cyprus The Fondazione Lelio e Basso-ISSOCO organised, with the Italian DPA, training of Polish, Spanish, Bulgarian and Hungarian DPAs and DPO trainings.

The Ministry of Digital Transformation of Ukraine has also launched a toolkit to help companies protect personal data.[36] The initiative aims to reduce the number of violations in the field of personal data. The toolkit contains a specially designed test to assess whether the company complies with the legal requirements for the protection of personal data.

36 https://www.ua.undp.org/content/ukraine/en/home/presscenter/pressreleases/2021/undp-and-ministry-of-digital-transformation-launch-personal-data.html

6
CONCLUSIONS AND RECOMMENDATIONS

Regarding the status and place of the institution within the system of public authorities:

1. The members of the data protection supervisory can be appointed by the government, the parliament, the head of the State, or with participation of several of them. The status of the supervisory authority should be enshrined in the law or another legal act adopted by the parliament.

2. Legal personality is an indispensable precondition for independence of the supervisory authority, therefore the authority should not be embedded within the structure of any other public institution. Subordination of the supervisory authority to the ministry or another public institution should also be avoided as it could lead to restriction of other guarantees aimed at ensuring independent status of the supervisory authority.

Regarding the scope of supervision:

3. One authority can be responsible for supervising lawfulness of data processing in different sectors and for various purposes (law enforcement, electronic communications, journalistic purposes, etc.). Establishment of one data protection supervisory authority could be considered more effective and efficient in terms of unified application of data protection principles in different sectors, as well as in terms of legal regulation (i.e., no need to have several legal acts) and resources (i.e., no need for several secretariats, etc.).

4. If several authorities are responsible for supervision of application of data protection legislation, all of them should have the same independent status as provided in the Convention 108+ and the GDPR.

5. A data protection supervisory authority shall not be competent to supervise data processing operations performed by courts acting in their judicial capacity, but its competence should cover other data processing operations carried out by courts.

6. Restrictions regarding the tasks and powers of supervisory authorities referred to in Article 15 (2 a, b, c, and d) of the Convention 108+ with regard to data processing for national security and defense shall be established by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim.

Regarding guarantees for independence (appointment and termination of the duties of the supervisory authority members, term of office, budget, human resources):

7. The duration of the term of office of the supervisory authority members shall not be less than four years. The members of the supervisory authority can be eligible for reappointment, although the possibility of reappointment is not necessary for ensuring independence.

8. The duration of the term of office, possibility of reappointment, the exhaustive list of the grounds for termination of the duties and dismissal of the supervisory authority members should be prescribed by law. The procedure of dismissal should ensure due participation of the institutions in charge of the member's appointment.

9. The grounds for dismissal are closely related to the fulfillment of the conditions relating to the qualification and eligibility required for the performance of the duties, therefore the latter should also be clearly provided by law. The law should also stipulate prohibitions on actions, occupations and benefits that are incompatible with the status of members and staff of the supervisory authority during and after their term of office, as well as their obligations (e.g., the duty of professional secrecy, etc.).

10. The supervisory authority shall have a separate, public annual budget, which may be a part of the overall public or national budget. The procedure of budget allocation should ensure protection from any external influence on the supervisory authority (i.e., no institutions of executive power of the state should have decisive influence). The risk of such external influence could be significantly minimized through participation of the supervisory authority in the consultations and decision-making process on the allocation of funds.

11. The supervisory authority could have other sources of funding, however, the obligation to provide sufficient resources lies upon the state. Therefore, the public budget should remain the main source of funding.

12. The budget directly affects other resources (human, technical, etc.). As to the factors to be considered when deciding what amount of funds is required, it should be noted that the financial resources must enable the supervisory authority to have qualified personnel with the pay level at least on a par with the public sector, as well as to have proper premises, technical equipment and infrastructure. Staff training and other needs should also be taken into account.

13. The supervisory authority should be able to hire its own staff who will only report to the supervisory authority's members. The data protection supervisory authority staff should not be subordinated or accountable to any other authority in terms of hierarchy and remuneration, as well as disciplinary controls.

14. Any organizational overlap between the data protection supervisory authority and any other state institution prevents it from being above all suspicion of partiality and is therefore incompatible with the requirement of independence.

15. Whatever the status of the supervisory authority staff (whether civil servants or employees under an employment contract), guarantees against any external influence should be ensured.

16. The supervisory authority should have autonomy regarding the use of its resources and planning of the activities. It is advised to establish legal guarantees regarding autonomous use of its budget and other resources without prior authorization / approval / advice from other governmental institutions, autonomous decision-making about its internal structure, number and qualifications of the staff, and adoption of decisions about its activity planning. Activity plans should not be subject to review, coordination or approval by other institutions.

17. The supervisory authority should not be subject to external control over its internal activities and use of resources, However, financial control exercised in accordance with the law and not affecting independence of the authority is acceptable.

Regarding other safeguards against external influence:

18. A legal act adopted by the parliament serves as a strong guarantee for ensuring independence of the supervisory authority. Therefore it should prescribe at least the aspects relating to the appointment procedure of the members (who nominates the candidates, who is in charge for appointment etc.), qualifications and eligibility conditions required to be appointed as a supervisory authority member, term of office of the supervisory authority members (duration,

possibility of reappointment), grounds for termination of duties and dismissal as well as its procedures, budgetary arrangements (a separate public annual budget), autonomy regarding HR policy and activity planning, remuneration of the supervisory authority members.

19. The overall regulation of the supervisory authority status should make it free from political influence. The beginning and the end of the term of office of the supervisory authority members should not be linked to that of appointing entity (i.e., government, parliament, or head of the State). Members of the supervisory authority shall be appointed and dismissed from theit duties only in accordance with the law.

20. The term of office of the supervisory authority members should not end otherwise than on the grounds provided by the law. The active members shall be safeguarded from early termination of their term of office in case of restructuring or changing of the institutional model by appropriate provisions of the law.

21. Appealing the decisions of the supervisory authority should follow the rule of law. Every affected person (data subject, data controller, etc.) should be able to appeal the decisions of the supervisory authority to the courts.

Regarding powers of investigation, intervention, complaints handling, and regulatory powers

22. In order to ensure the fulfillment of the tasks provided for in Article 57 of the GDPR, the supervisory authority must be competent under Article 15 of Convention 108+ and Article 58 of the GDPR to investigate, intervene, have the necessary regulatory powers while respecting the fundamental constitutional human rights.

23. The DPA must be endowed with sufficient law enforcement functions modelled on the Estonian Data Protection Inspectorate.

24. After the entry into force of the GDPR, most European countries revised the powers of their DPAs to ensure the protection of personal data and supplement their respective tasks and powers.

25. No DPA shall have the right to obtain access to residential premises (including premises leased or used on any other basis) of a natural person without a court order authorizing entry into the residential premises. It is recommended to resolve the issue of admission to the premises of natural persons-entrepreneurs where they carry out activities through the use of court decisions in accordance with the procedures provided by law.

26. Consultation procedures should be established by law, but with safeguards against abuse and exploitation of the DPA as a permanent free consultant.

27. Certification issues have so far been taken up only by the Grand Duchy of Luxembourg DPA. Other European institutions are still in the process of developing criteria or are waiting to get them from the European Data Protection Board. It is recommended to consider certification after the introduction of all other powers of the DPA.

28. The supervisory authority should have the power to bring infringements of the GDPR to the attention of the judicial authorities and where appropriate, to commence or otherwise engage in legal proceedings in order to enforce the GDPR.

29. The DPA should have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of law and Convention 108+ or to ensure consistency of the protection of personal data.

30. The DPA may have other powers that do not conflict with the GDPR, but directly or indirectly affect the protection of personal data. For example, the powers provided by international agreements, such as interaction with other international institutions (Eurojust[37], Europol[38]). It is advisable to delegate oversight to one designated authority.

31. Regarding the engagement in legal proceedings, the following fundamental DPA rights should be established in the national data protection legislation: to appeal against normative legal acts adopted by public authorities, and to take part in legal proceedings regarding decisions adopted by the supervisory authority.

32. DPAs provide opinions to draft legal acts in its s of competence in three cases: after adoption of the legal act, when the text of the legal act has been drafted, and while the legal act is being drafted.

Regarding raising public awareness:

33. Data protection awareness campaigns are an instrument by which DPAs can not only promote public awareness in the area of data protection through seminars, trainings, lectures, guidelines and other materials but also promote effective incorporation of the GDPR in the national data protection legislation.

34. Data protection awareness campaigns shall be developed with the overall goal to raise awareness of data subjects, data controllers and/or data processors about personal data protection.

35. Regular seminars, trainings and lectures, workshops for civil servants on theoretical and practical aspects of personal data protection will enhance qualifications of the civil servants responsible for personal data protection.

36. European Union DPAs conduct data protection awareness campaigns in different ways:
    - with seminars/webinars;
    - consultations for controllers and processors on the provisions of Regulation 2016/679;
    - educational videos;
    - media campaigns, website and social media campaigns, and targeted seminars;
    - monthly newsletters on data protection;
    - data protection information days and scientific conferences;
    - helplines for data controllers/processors, data subjects, and other authorities;
    - privacy and advertising setup fact sheets.

37. Training and development of civil servants in the area of personal data protection should be funded and centralized by the government.

Kyiv, Vilnius, 6 July, 2021

Dijana Šinkūnienė

Lilia Oleksiuk

Oleksandr Shevchuk

37 https://zakon.rada.gov.ua/laws/show/984_024-16#Text
38 https://zakon.rada.gov.ua/laws/show/984_001-16#Text

7

ANNEXES

Annex 1. Questionnaire for the data protection supervisory authorities

Country	The title	E-mail address
Norway	Datatilsynet - Norwegian Data Protection Authority	postkasse@datatilsynet.no
The Slovak Republic	The Office for Personal Data Protection of the Slovak Republic	statny.dozor@pdp.gov.sk
Romania	Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (Romanian Supervisory Authority)	anspdcp@dataprotection.ro
Italia	Il Garante per la protezione dei dati personali	a.pierucci@gpdp.it
Estonia	Estonian Data Protection Inspectorate	info@aki.ee
Croatia	Croatian Personal Data Protection Agency	azop@azop.hr
Republic of Cyprus	Commissioner for Personal Data Protection	commissioner@dataprotection.gov.cy
Lithuania	State Data Protection Inspectorate (hereinafter referred to as SDPI)	ada@ada.lt
Iceland	Persónuvernd (Icelandic Data Protection Authority)	postur@personuvernd.is
Greece	Hellenic Data Protection	contact@dpa.gr
Principality of Liechtenstein	Datenschutzstelle	marie-louise.gaechter@llv.li
Portugal	Comissão Nacional de Proteção de Dados	geral@cnpd.pt
Grand Duchy of Luxembourg	CNPD	tine.larsen@cnpd.lu
Latvia	Data State Inspectorate of Latvia	pasts@dvi.gov.lv
The Czech Republic	Office for Personal Data Protection of the Czech Republic	posta@uoou.cz
Austria	Austrian Data Protection Authority	dsb@dsb.gv.at
The Republic of Slovenia	Informacijski pooblaščenec (Information Commissioner of the Republic of Slovenia) gp.ip@ip-rs.si	gp.ip@ip-rs.si
Bulgaria	Commission for Personal Data Protection	kzld@cpdp.bg

1. Is your data protection supervisory authority:

Norway	lead by a single Commissioner (director, etc.)
The Slovak Republic	lead by a single Commissioner (director, etc.)
Romania	lead by a single Commissioner (director, etc.)
Italia	a collegiate body (Commission etc.)
Estonia	lead by a single Commissioner (director, etc.)
Croatia	lead by a single Commissioner (director, etc.)
Republic of Cyprus	lead by a single Commissioner (director, etc.)
Lithuania	lead by a single Commissioner (director, etc.)
Iceland	Both, the daily work is lead by a Commissioner but the DPA also has a Board of Directors that issues decisions in major cases and issues fines etc.
Greece	a collegiate body (Commission etc.)
Principality of Liechtenstein	lead by a single Commissioner (director, etc.)
Portugal	a collegiate body (Commission etc.)
Grand Duchy of Luxembourg	a collegiate body (Commission etc.)
Latvia	lead by a single Commissioner (director, etc.)
The Czech Republic	lead by a single Commissioner (director, etc.)

Austria	lead by a single Commissioner (director, etc.)
The Republic of Slovenia	lead by a single Commissioner (director, etc.)
Bulgaria	a collegiate body (Commission etc.)

2. Your data protection supervisory authority:

Norway	has legal personality
The Slovak Republic	has legal personality
Romania	has legal personality
Italia	has legal personality
Estonia	is subordinated to the ministry or other state institution, independent authority under Ministry of Justice
Croatia	has legal personality
Republic of Cyprus	has legal personality
Lithuania	has legal personality, The SDPI is an institution of the Government of the Republic of Lithuania.
Iceland	has legal personality
Greece	has legal personality
Principality of Liechtenstein	has legal personality
Portugal	has legal personality
Grand Duchy of Luxembourg	has legal personality
Latvia	has legal personality
The Czech Republic	has legal personality
Austria	has legal personality
The Republic of Slovenia	has legal personality
Bulgaria	has legal personality

3. Please indicate the status of your data protection supervisory authority:

Norway	government agency with special status enshrined in the Law
The Slovak Republic	government agency with special status enshrined in the Law
Romania	Public authority with legal personality, autonomous and independent in relation to other authority of the public administration, as well as to any natural or legal person from the private sector
Italia	independent supervisory authority
Estonia	government agency with special status enshrined in the Law
Croatia	According to Article 4 paragraph 2 of the Act on the Implementation of the General Data Protection Regulation the Agency is an independent public authority.
Republic of Cyprus	independent supervisory authority enshrined in the Law
Lithuania	The SDPI is government institution. It is an independent authority. The Director of the Inspectorate is accountable to the Government of the Republic of Lithuania and Minister of Justice.
Iceland	government agency with special status enshrined in the Law
Greece	constitutionally established independent public authority.
Principality of Liechtenstein	government agency with special status enshrined in the Law
Portugal	government agency enshrined in the Constitution
Grand Duchy of Luxembourg	government agency with special status enshrined in the Law
Latvia	government agency with special status enshrined in the Law
The Czech Republic	government agency with special status enshrined in the Law
Austria	government agency with special status enshrined in the Law
The Republic of Slovenia	Independet state body (separate from the government, similar to Ombudsperson)
Bulgaria	government agency with special status enshrined in the Law

4. Your data protection supervisory authority receives resources (several answers are possible):

Norway	directly from the state budget (e.g. has separate budget which is part of the overall state or national budget)
The Slovak Republic	from the budget allocated to the ministry or other state institution
Romania	directly from the state budget (e.g. has separate budget which is part of the overall state or national budget)
Italia	directly from the state budget (e.g. has separate budget which is part of the overall state or national budget)
Estonia	from the budget allocated to the ministry or other state institution, separate line in the state budget (under Ministry of Justice's jurisdiction)
Croatia	directly from the state budget (e.g. has separate budget which is part of the overall state or national budget)
Republic of Cyprus	directly from the state budget (e.g. has separate budget which is part of the overall state or national budget)
Lithuania	directly from the state budget (e.g. has separate budget which is part of the overall state or national budget), The SDPI is a budgetary institution maintained from the state budget of the Republic of Lithuania. Other legally received funds may be used to finance the SDPI. The legal basis for the financing of the SDPI is Point 6 of the Regulation of the State Data Protection Inspectorate, approved by the Government of the Republic of Lithuania 25 September 2001 resolution No. 1156
Iceland	from the budget allocated to the ministry or other state institution
Greece	The Hellenic Data Protection Authority's resources are coming from the State Budget. They are part of the Ministry of Justice's budget and they appear on a separate budget line.
Principality of Liechtenstein	directly from the state budget (e.g. has separate budget which is part of the overall state or national budget)
Portugal	directly from the state budget (e.g. has separate budget which is part of the overall state or national budget), through the revenues obtained when exercising tasks with regard to data controllers / processors, through the administrative fines / other monetary sanctions imposed as a penalty for the infringement
Grand Duchy of Luxembourg	from the budget allocated to the ministry or other state institution
Latvia	directly from the state budget (e.g. has separate budget which is part of the overall state or national budget), from the budget allocated to the ministry or other state institution
The Czech Republic	directly from the state budget (e.g. has separate budget which is part of the overall state or national budget)
Austria	from the budget allocated to the ministry or other state institution
The Republic of Slovenia	directly from the state budget (e.g. has separate budget which is part of the overall state or national budget)
Bulgaria	directly from the state budget (e.g. has separate budget which is part of the overall state or national budget)

5. Your data protection supervisory authority (several answers are possible):

Norway	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides autonomously about internal structure of the authority, decides autonomously about number and qualification of the staff, decides autonomously about activity planning (e.g. strategic plans and other)
The Slovak Republic	decides autonomously about internal structure of the authority, decides autonomously about activity planning (e.g. strategic plans and other)
Romania	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides autonomously about internal structure of the authority, decides about the number of staff within the limits set up by legal act, decides autonomously about activity planning (e.g. strategic plans and other)

Italia	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides autonomously about internal structure of the authority, decides about the number of staff within the limits set up by legal act, decides autonomously about activity planning (e.g. strategic plans and other)
Estonia	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides autonomously about internal structure of the authority, decides autonomously about number and qualification of the staff, decides about the number of staff within the limits set up by legal act, decides autonomously about activity planning (e.g. strategic plans and other)
Croatia	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides autonomously about internal structure of the authority, decides autonomously about number and qualification of the staff, decides about the number of staff within the limits set up by legal act, decides autonomously about activity planning (e.g. strategic plans and other)
Republic of Cyprus	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides autonomously about internal structure of the authority, decides autonomously about activity planning (e.g. strategic plans and other)
Lithuania	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides autonomously about internal structure of the authority, decides about the number of staff within the limits set up by legal act, decides autonomously about activity planning (e.g. strategic plans and other)
Iceland	decides autonomously about internal structure of the authority, decides autonomously about number and qualification of the staff, decides autonomously about activity planning (e.g. strategic plans and other)
Greece	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides about the number of staff within the limits set up by legal act, decides autonomously about activity planning (e.g. strategic plans and other)
Principality of Liechtenstein	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides autonomously about internal structure of the authority, decides about the number of staff within the limits set up by legal act, decides autonomously about activity planning (e.g. strategic plans and other)
Portugal	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides about the number of staff within the limits set up by legal act, decides autonomously about activity planning (e.g. strategic plans and other)
Grand Duchy of Luxembourg	decides autonomously about internal structure of the authority, decides autonomously about activity planning (e.g. strategic plans and other)
Latvia	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides autonomously about internal structure of the authority, decides autonomously about number and qualification of the staff, decides autonomously about activity planning (e.g. strategic plans and other)
The Czech Republic	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution)
Austria	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides autonomously about internal structure of the authority, decides autonomously about activity planning (e.g. strategic plans and other)
The Republic of Slovenia	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides autonomously about internal structure of the authority, decides autonomously about number and qualification of the staff, decides autonomously about activity planning (e.g. strategic plans and other)
Bulgaria	has complete control over how it uses its budget (e.g. without prior authorisation / approval / advice from other governmental institution), decides autonomously about internal structure of the authority, decides autonomously about number and qualification of the staff, decides about the number of staff within the limits set up by legal act, decides autonomously about activity planning (e.g. strategic plans and other)

6. The head / members of your data protection supervisory authority is / are appointed by:

Norway	the Government
The Slovak Republic	the Parliament
Romania	The President of the Romanian SA is appointed by the Senate

Italia	the Parliament, Please note that the Panel of Commissioners includes four members, of whom two elected by the Chamber of Deputies and two by the Senate through a specific voting procedure.
Estonia	the Government
Croatia	the Parliament
Republic of Cyprus	Article 19(1) of the Law 125(I)/2018. "The Commissioner for Personal Data Protection shall be appointed by the Council of Ministers, upon the recommendation of the Minister."
Lithuania	the Government
Iceland	the Government
Greece	the Parliament
Principality of Liechtenstein	the Parliament
Portugal	the Parliament, the Government
Grand Duchy of Luxembourg	the head of the State (e.g. the President)
Latvia	the Government
The Czech Republic	the head of the State (e.g. the President)
Austria	the head of the State (e.g. the President)
The Republic of Slovenia	the Parliament
Bulgaria	the Parliament

7. Please indicate who nominates a candidate in a position of the head / members of data protection supervisory authority:

Norway	public competition, candidate is nominated by the nomination committee of higher civil servants
The Slovak Republic	candidate is nominated by the Government
Romania	The candidate is nominated by the Standing Bureau of the Senate
Italia	The members of the Authority must be elected among those who submit their candidacy as part of a selection procedure whose notice must be published on the websites of the Senate of the Republic, the Chamber of Deputies and the Data Protection Authority at least sixty days before the appointment.
Estonia	public competition, candidate is nominated by the Ministry of Justice
Croatia	candidate is nominated by the Government
Republic of Cyprus	Article 19(1) of the Law 125(I)/2018. "The Commissioner for Personal Data Protection shall be appointed by the Council of Ministers, upon the recommendation of the Minister."
Lithuania	Public competition (except for certain exceptions to the Republic of Lithuania Law on the Civil Service). Candidate is appointed by the Government.
Iceland	candidate is nominated by the Government
Greece	candidate is nominated by the Parliament
Principality of Liechtenstein	candidate is nominated by the Government
Portugal	candidate is nominated by the Parliament
Grand Duchy of Luxembourg	candidate is nominated by the Government
Latvia	public competition, candidate is nominated by the nomination committee of higher civil servants
The Czech Republic	candidate is nominated by the Parliament
Austria	candidate is nominated by the Government
The Republic of Slovenia	candidate is nominated by the President
Bulgaria	public competition, candidate is nominated by the nomination committee of higher civil servants, candidate is nominated by the Government

8. Please specify the grounds for ending of the duties / dismissal of the head / members of your data protection supervisory authority:

Norway	expiry of the term of office, resignation, in case of serious misconduct
The Slovak Republic	expiry of the term of office, resignation, compulsory retirement, in case of serious misconduct

Romania	expiry of the term of office, resignation, compulsory retirement, in case of serious misconduct, the head / member no longer fulfils the conditions required for the performance of the duties
Italia	expiry of the term of office, resignation, in case of serious misconduct, the head / member no longer fulfils the conditions required for the performance of the duties
Estonia	expiry of the term of office, resignation, compulsory retirement, in case of serious misconduct, the head / member no longer fulfils the conditions required for the performance of the duties
Croatia	According to Article 9. of the Act on the Implementation of the General Data Protection Regulation The Croatian Parliament shall relieve from duty the Director and the Deputy Director before the expiry of the term of office for which they were appointed: – at his or her own request – if circumstances arise due to which he or she no longer fulfils the conditions for appointment – if he or she committed a serious misconduct. It shall be considered that the Director or the Deputy Director committed a serious misconduct if he or she does not carry out his or her duty in accordance with the law. The procedure for relieving from duty of the Director and the Deputy Director shall be initiated at the proposal of the Government of the Republic of Croatia.
Republic of Cyprus	expiry of the term of office, resignation, compulsory retirement, in case of serious misconduct, the head / member no longer fulfils the conditions required for the performance of the duties, Article 20 of the Law 125(I)/2018. "The Commissioner shall be dismissed, if during his or her term of office:- (a) takes any action incompatible with his or her duties or engages in any incompatible occupation, whether gainful or not; or (b) is convicted for the offence provided for in subsection (3) of section 21 of this Law. "
Lithuania	expiry of the term of office, resignation, compulsory retirement, in case of serious misconduct, the head / member no longer fulfils the conditions required for the performance of the duties
Iceland	expiry of the term of office, resignation, compulsory retirement, in case of serious misconduct
Greece	expiry of the term of office, resignation, in case of serious misconduct, According to article 12 of law 4624/2019 (available at www.dpa.gr (EN) > Information > Legal Framework) "any person who, following his or her appointment: (a) Acquires one of the functions constituting a barrier to appointment referred to paragraph 1. (b) Engages in actions or undertakes any work or project, or acquires another capacity which, in the Authority's view, is incompatible with his or her duties as a member of the Authority, shall be automatically disqualified as President, Deputy President or member of the Authority"
Principality of Liechtenstein	expiry of the term of office, resignation, in case of serious misconduct
Portugal	expiry of the term of office, resignation, compulsory retirement, in case of serious misconduct
Grand Duchy of Luxembourg	expiry of the term of office, resignation, in case of serious misconduct, the head / member no longer fulfils the conditions required for the performance of the duties
Latvia	expiry of the term of office, resignation, in case of serious misconduct, the head / member no longer fulfils the conditions required for the performance of the duties
The Czech Republic	expiry of the term of office
Austria	Only stipulates that the dismissal of the head is to be carried out by the Federal President on the proposal of the Federal Government.
The Republic of Slovenia	expiry of the term of office, resignation, in case of serious misconduct, the head / member no longer fulfils the conditions required for the performance of the duties
Bulgaria	expiry of the term of office, resignation, compulsory retirement, in case of serious misconduct, the head / member no longer fulfils the conditions required for the performance of the duties

9. What of the following is regulated by the legal act adopted by Parliament (e.d. the Law on Personal Data Protection or other):

Norway	appointment procedure of the head / members of supervisory authority
The Slovak Republic	qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, grounds for dismissal of the head / members of supervisory authority, salary of the head / members of supervisory authority
Romania	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, grounds for dismissal of the head / members of supervisory authority, dismissal procedure of the head / members of supervisory authority, personnel policy (e.g. right to employ its own staff, etc.)

Italia	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, personnel policy (e.g. right to employ its own staff, etc.), salary of the head / members of supervisory authority
Estonia	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, dismissal procedure of the head / members of supervisory authority
Croatia	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, grounds for dismissal of the head / members of supervisory authority, dismissal procedure of the head / members of supervisory authority, budgetary (financial) arrangements, personnel policy (e.g. right to employ its own staff, etc.), salary of the head / members of supervisory authority
Republic of Cyprus	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, grounds for dismissal of the head / members of supervisory authority, dismissal procedure of the head / members of supervisory authority, personnel policy (e.g. right to employ its own staff, etc.)
Lithuania	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, grounds for dismissal of the head / members of supervisory authority, dismissal procedure of the head / members of supervisory authority, budgetary (financial) arrangements, personnel policy (e.g. right to employ its own staff, etc.), salary of the head / members of supervisory authority
Iceland	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, grounds for dismissal of the head / members of supervisory authority, personnel policy (e.g. right to employ its own staff, etc.)
Greece	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, grounds for dismissal of the head / members of supervisory authority, dismissal procedure of the head / members of supervisory authority, budgetary (financial) arrangements, personnel policy (e.g. right to employ its own staff, etc.), salary of the head / members of supervisory authority
Principality of Liechtenstein	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, grounds for dismissal of the head / members of supervisory authority, dismissal procedure of the head / members of supervisory authority, budgetary (financial) arrangements, personnel policy (e.g. right to employ its own staff, etc.)
Portugal	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, grounds for dismissal of the head / members of supervisory authority, dismissal procedure of the head / members of supervisory authority, budgetary (financial) arrangements, personnel policy (e.g. right to employ its own staff, etc.), salary of the head / members of supervisory authority
Grand Duchy of Luxembourg	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, grounds for dismissal of the head / members of supervisory authority, dismissal procedure of the head / members of supervisory authority, budgetary (financial) arrangements, personnel policy (e.g. right to employ its own staff, etc.), salary of the head / members of supervisory authority
Latvia	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, grounds for dismissal of the head / members of supervisory authority, dismissal procedure of the head / members of supervisory authority, personnel policy (e.g. right to employ its own staff, etc.), salary of the head / members of supervisory authority
The Czech Republic	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, budgetary (financial) arrangements
Austria	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority

The Republic of Slovenia	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, grounds for dismissal of the head / members of supervisory authority, dismissal procedure of the head / members of supervisory authority, budgetary (financial) arrangements, personnel policy (e.g. right to employ its own staff, etc.), salary of the head / members of supervisory authority
Bulgaria	appointment procedure of the head / members of supervisory authority, qualifications and eligibility conditions required to be appointed as head / member of supervisory authority, term of office of the head / members of supervisory authority, grounds for dismissal of the head / members of supervisory authority, budgetary (financial) arrangements, salary of the head / members of supervisory authority

10. What is the duration of the term of the head / member of the data protection supervisory authority:

Norway	6 years
The Slovak Republic	5 years
Romania	5 years
Italia	7 years (not renewable). Please note that this term was introduced by section 47-c of Law No 31/2008, which brought about amendments to the term of office of the commissioners appointed to certain independent authorities (seven years) including the members making up the data protection authority. The previous term of office was four years and was renewable once.
Estonia	5 years
Croatia	4 years
Republic of Cyprus	6 years
Lithuania	5 years
Iceland	5 years, The Board of directors are appointed members for a 5 year term, which can be prolonged twice (total of 15 years). The Commissioner is appointed for a 5 year term but no limit on reappointment
Greece	6 years
Principality of Liechtenstein	6 years
Portugal	5 years
Grand Duchy of Luxembourg	6 years
Latvia	5 years
The Czech Republic	5 years
Austria	5 years
The Republic of Slovenia	5 years
Bulgaria	5 years

11. The head / members of the data protection supervisory authority:

Norway	Currently eligible for reappointment once, but this is under revision as the possibility of reappointment may jeopardise their independence.
The Slovak Republic	is / are eligible for reappointment for two terms
Romania	The mandate of the president can be renewed only once
Italia	is not / are not eligible for reappointment
Estonia	not regulated
Croatia	is / are eligible for reappointment for two terms
Republic of Cyprus	is / are eligible for reappointment for two terms
Lithuania	is / are eligible for reappointment for two terms
Iceland	is / are eligible for reappointment for two terms, To avoid confusion - they are eligible for reappointment for the total of three terms.
Greece	is not / are not eligible for reappointment
Principality of Liechtenstein	eligible without restrictions

Portugal	is / are eligible for reappointment for two terms
Grand Duchy of Luxembourg	is / are eligible for reappointment for two terms
Latvia	is / are eligible for reappointment for two terms
The Czech Republic	is / are eligible for reappointment for two terms
Austria	No limit on reappointment is specified.
The Republic of Slovenia	is / are eligible for reappointment for two terms
Bulgaria	is / are eligible for reappointment for two terms

12. Please indicate the status of the employees of the office of data protection supervisory authority (several answers are possible):

Norway	officials are civil servants; legally guaranteed independence in procedural matters, officials are employees under an employment contract
The Slovak Republic	officials are civil servants; legally guaranteed independence in procedural matters
Romania	officials are employees under an employment contract
Italia	officials are employees under an employment contract
Estonia	officials are civil servants; legally guaranteed independence in procedural matters
Croatia	officials are civil servants; legally guaranteed independence in procedural matters
Republic of Cyprus	Article 22 of the Law 125(I)/2018. "The Commissioner shall have an office, that may be staffed by permanent, temporary and open ended contract public servants."
Lithuania	officials are civil servants; legally guaranteed independence in procedural matters, officials are employees under an employment contract
Iceland	officials are employees under an employment contract
Greece	officials are civil servants; legally guaranteed independence in procedural matters, The staff is appointed under a public or private law employment relationship of unlimited duration to positions set out in the Organisational Chart of the Authority.
Principality of Liechtenstein	officials are civil servants; legally guaranteed independence in procedural matters
Portugal	officials are civil servants; legally guaranteed independence in procedural matters
Grand Duchy of Luxembourg	officials are civil servants; legally guaranteed independence in procedural matters
Latvia	officials are civil servants; legally guaranteed independence in procedural matters, officials are employees under an employment contract
The Czech Republic	officials are civil servants; legally guaranteed independence in procedural matters, officials are employees under an employment contract
Austria	officials are employees under an employment contract
The Republic of Slovenia	officials are civil servants; legally guaranteed independence in procedural matters
Bulgaria	officials are civil servants; legally guaranteed independence in procedural matters, officials are employees under an employment contract

13. Please indicate the level of salary of the employees of the office of data protection supervisory authority:

Norway	The level may be slightly higher than the average of civil servants in the state sector
The Slovak Republic	level of salary is average of civil servants in the state sector
Romania	N/A
Italia	level of salary is a percentage of other supervisory authorities
Estonia	level of salary is average of civil servants in the state sector
Croatia	level of salary is average of civil servants in the state sector, level of salary is average of employees in the state sector
Republic of Cyprus	level of salary is average of civil servants in the state sector

Lithuania	level of salary is average of civil servants in the state sector
Iceland	level of salary is average of employees in the state sector
Greece	level of salary is average of civil servants in the state sector
Principality of Liechtenstein	level of salary is average of civil servants in the state sector
Portugal	level of salary is average of civil servants in the state sector
Grand Duchy of Luxembourg	level of salary is average of civil servants in the state sector, level of salary is average of employees in the state sector
Latvia	level of salary is average of civil servants in the state sector
The Czech Republic	
Austria	level of salary is average of employees in the state sector
The Republic of Slovenia	level of salary is average of civil servants in the state sector
Bulgaria	level of salary is average of civil servants in the state sector

14. Please indicate to whom reports the head of your data protection supervisory authority:

Norway	Parliament, Government
The Slovak Republic	Parliament
Romania	he National Supervisory Authority's President presents on annual basis the activity reports in the plenary session of the Senate.
Italia	The Italian DPA transmits its annual report to the government and the Parliament as said below. In respect of its interplay with Parliament/Government, the DPA is consulted by Parliament and Government prior to the enactment of legislation impacting data protection; -It can draw the attention of Government and Parliament, wherever appropriate, to the need for passing specific laws or regulations in various walks of life; - It participates in the debates on law-making activities through hearings before Parliament;
Estonia	Parliament
Croatia	Parliament
Republic of Cyprus	the Commissioner for Personal Data Protection is independent supervisory authority
Lithuania	Government, Minister of Justice
Iceland	Since the DPA is an independent authority the Commissioner doesn't report to anybody, unless its a budgetary matter. However, the DPA is under the obligation to send its annual report to the government and parliament.
Greece	Parliament
Principality of Liechtenstein	Parliament
Portugal	Parliament
Grand Duchy of Luxembourg	Parliament
Latvia	Parliament, Government
The Czech Republic	Parliament
Austria	Government
The Republic of Slovenia	Parliament
Bulgaria	Parliament

15. Annual report on the activities of your data protection supervisory authority (several answers are possible):

Norway	shall be transmitted to the government, shall be transmitted to the parliament, shall be approved by the parliament, shall be made available to the public
The Slovak Republic	shall be transmitted to the government, shall be transmitted to the parliament, shall be made available to the public

Romania	shall be transmitted to the government, shall be transmitted to the parliament, The annual report shall be transmitted to the Romanian Senate, the Chamber of Deputires, the Romanian Governement, the European Commission and the European Data Protection Board.
Italia	shall be transmitted to the government, shall be transmitted to the parliament, The Annual report is published on the DPA's website www.garanteprivacy.it
Estonia	shall be transmitted to the parliament, shall be transmitted to other authority, transmitted to the Chancellor of Justice, and Constitutional Committee of the Parliament
Croatia	shall be transmitted to the parliament
Republic of Cyprus	Article 26 of the Law 125(I)/2018. "The Commissioner shall submit an annual activity report to the President of the Republic and to the President of the House of Representatives which shall published on the Office's website."
Lithuania	shall be transmitted to the government, shall be transmitted to the parliament, shall be made available to the public
Iceland	shall be transmitted to the government, shall be transmitted to the parliament, shall be made available to the public
Greece	shall be transmitted to the parliament, shall be made available to the public, shall be transmitted to the Prime Minister too.
Principality of Liechtenstein	shall be transmitted to the government, shall be transmitted to the parliament, shall be approved by the parliament, shall be made available to the public
Portugal	shall be made available to the public
Grand Duchy of Luxembourg	shall be transmitted to the government, shall be transmitted to the parliament, shall be made available to the public
Latvia	shall be transmitted to the government, shall be transmitted to the parliament, shall be made available to the public
The Czech Republic	shall be transmitted to the parliament, shall be made available to the public
Austria	shall be transmitted to the government, shall be made available to the public
The Republic of Slovenia	shall be transmitted to the parliament, Shall be transmitted also to the European data protection Board (GDPR)
Bulgaria	shall be transmitted to the parliament, shall be approved by the parliament, shall be made available to the public, shall be transmitted to the European Data Protection Board

16. Please indicate at what intervals the head of your data protection supervisory authority reports:

Norway	once a year
The Slovak Republic	once a year
Romania	once a year
Italia	once a year
Estonia	once a year
Croatia	once a year
Republic of Cyprus	once a year
Lithuania	once a year
Iceland	once a year
Greece	once a year
Principality of Liechtenstein	once a year
Portugal	once a year
Grand Duchy of Luxembourg	once a year
Latvia	once a year
The Czech Republic	once a year
Austria	once a year
The Republic of Slovenia	once a year
Bulgaria	once a year

17. Is your data protection supervisory authority competent for supervision of:

Norway	data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties
The Slovak Republic	public access to official documents, data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties
Romania	data processing for journalistic purposes and the purposes of academic, artistic or literary expression, data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, privacy protection in electronic communications sector, With reference to the data processing of journalistic purposes and the purposes of academic, artistic or literary expression, we take into account Article 85 of the GDPR and Article 7 of Law no. 190/2018
Italia	data processing for journalistic purposes and the purposes of academic, artistic or literary expression, data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, data processing for national security and defence purposes, privacy protection in electronic communications sector
Estonia	data processing for journalistic purposes and the purposes of academic, artistic or literary expression, public access to official documents, data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, data processing for national security and defence purposes, privacy protection in electronic communications sector, Specifications for application of Estonian Personal Data Protection Act and the GDPR are forseen in the Article 2 of this Act: https://www.riigiteataja.ee/en/eli/523012019001/consolide
Croatia	According to Article 36. of the Act on the Implementation of the General Data Protection Regulation authorised employees of the Agency may independently, and is specific cases also with participation of a representative of the seconding supervisory authority (hereinafter: authorised persons), carry out announced or unannounced supervisions. The supervised person and the controller or the processor shall be notified about the carrying out of the unannounced supervision at the site and at the time of carrying out of the supervision.
Republic of Cyprus	data processing for journalistic purposes and the purposes of academic, artistic or literary expression, data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, data processing for national security and defence purposes, The supervisory authority competent for supervision of public access to official documents is the Information Commissioner. The tasks and powers assigned to the Information Commissioner are exercised by the respective Commissioner for Personal Data Protection.
Lithuania	data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, privacy protection in electronic communications sector
Iceland	data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties
Greece	data processing for journalistic purposes and the purposes of academic, artistic or literary expression, data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, data processing for national security and defence purposes, privacy protection in electronic communications sector
Principality of Liechtenstein	data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, privacy protection in electronic communications sector
Portugal	data processing for journalistic purposes and the purposes of academic, artistic or literary expression, public access to official documents, data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, data processing for national security and defence purposes, privacy protection in electronic communications sector
Grand Duchy of Luxembourg	data processing for journalistic purposes and the purposes of academic, artistic or literary expression, data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, data processing for national security and defence purposes, privacy protection in electronic communications sector
Latvia	data processing for journalistic purposes and the purposes of academic, artistic or literary expression, data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, privacy protection in electronic communications sector, Inspectorate only partly is competent for the data processing for the journalistic purposes
The Czech Republic	data processing for journalistic purposes and the purposes of academic, artistic or literary expression, public access to official documents, data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, privacy protection in electronic communications sector

Austria	data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, data processing for national security and defence purposes, privacy protection in electronic communications sector, + data processing for the purposes of academic, artistic or literary expression
The Republic of Slovenia	data processing for journalistic purposes and the purposes of academic, artistic or literary expression, public access to official documents, data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, data processing for national security and defence purposes
Bulgaria	data processing for journalistic purposes and the purposes of academic, artistic or literary expression, data processing by competent authorities for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, privacy protection in electronic communications sector

18. Please indicate which of investigative powers does your data protection supervisory authority has:

Norway	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to obtain access, subject to a prior notice in writing, to the premises / territory of the controller / processor, to obtain access without a prior notice to the premises / territory of the controller / processor, to access the premises / territory of a legal person at any time
The Slovak Republic	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to order any natural and / or legal person (other than the controller and processor) to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to carry out searches and seizures in the premises of the data processor / controller without judicial warrant, to carry out searches and seizures in the premises of the data processor / controller after obtaining a judicial warrant, to obtain access, subject to a prior notice in writing, to the premises / territory of the controller / processor, to access the premises / territory of a legal person at any time
Romania	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to obtain access without a prior notice to the premises / territory of the controller / processor, to access the premises / territory of a legal person only during office hours of that legal person, The control activity of the Romanian SA is regulated in Chapter IV Section 1 of Law no. 102/2005, republished. Article 14 (2) of Law no. 102/2005 states that the control personnel has the right to carry out investigations, including unannounced ones, to request and to obtain from the data controller and processor, as well as, if necessary, from their representative, on the spot and/or within the established deadline, any information and documents, regardless of the storage medium, to pick up copies of them, to have access to any of the controller's and processor's premises, as well as to have access and to verify any equipment, media or data storage medium necessary for the performance of the investigation, according to the law. Paragraph (3) of the same Article provides that, where the control personnel is prevented in any way in the exercise of the tasks provided in paragraph (2), the National Supervisory Authority may request the judicial authorisation given by the president of the Bucharest Court of Appeal or by a judge delegated by it. Furthermore, the identification and preservation of the objects, as well as the applying seals are done according to the provisions of Law no. 135/2010 on the Criminal Procedure Code, with subsequent amendments and completions. At the same time, the Romanian SA may order the carrying out of expertise and the hearing of persons whose statements are considered relevant and necessary for conducting the investigation
Italia	To correctly reply to the question we prefer not to mark the single answers (as they could only partially mirrors the IT DPA powers)but to refer to Article 158 of the Italian Data Protection Code available at: https://www.garanteprivacy.it/documents/10160/0/Data+Protection+Code.pdf/7f4dc718-98e4-1af5-fb44-16a313f4e70f?version=1.3
Estonia	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to order any natural and / or legal person (other than the controller and processor) to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to carry out searches and seizures in the premises of the data processor / controller after obtaining a judicial warrant, to obtain access, subject to a prior notice in writing, to the premises / territory of the controller / processor, to obtain access without a prior notice to the premises / territory of the controller / processor, to access the premises / territory of a legal person at any time, to obtain access to residential premises (including premises leased or used on any other basis) of a natural person only upon producing a court order authorising entry into the residential premises, to use the police if necessary, for the performance of powers of data protection supervisory authority

Croatia	"According to Article 58 of GDPR the Agency has the following investigative powers: (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks; (b) to carry out investigations in the form of data protection audits; (c) to carry out a review on certifications issued pursuant to Article 42(7); (d) to notify the controller or the processor of an alleged infringement of this Regulation; (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law."
Republic of Cyprus	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to order any natural and / or legal person (other than the controller and processor) to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to obtain access without a prior notice to the premises / territory of the controller / processor, to access the premises / territory of a legal person at any time, to use the police if necessary, for the performance of powers of data protection supervisory authority, Article 25(d) of the Law 125(I)/2018. "In the exercise of his or her investigative powers, the Commissioner may seize documents or electronic equipment by virtue of a search warrant in accordance with the Criminal Procedure Law."
Lithuania	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to order any natural and / or legal person (other than the controller and processor) to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to carry out searches and seizures in the premises of the data processor / controller without judicial warrant, to obtain access without a prior notice to the premises / territory of the controller / processor, to access the premises / territory of a legal person only during office hours of that legal person, to access the premises / territory of a legal person at any time, to obtain access to residential premises (including premises leased or used on any other basis) of a natural person only upon producing a court order authorising entry into the residential premises, to use the police if necessary, for the performance of powers of data protection supervisory authority
Iceland	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to obtain access, subject to a prior notice in writing, to the premises / territory of the controller / processor, to obtain access without a prior notice to the premises / territory of the controller / processor, to access the premises / territory of a legal person at any time, to use the police if necessary, for the performance of powers of data protection supervisory authority
Greece	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to order any natural and / or legal person (other than the controller and processor) to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to carry out searches and seizures in the premises of the data processor / controller without judicial warrant, to carry out searches and seizures in the premises of the data processor / controller after obtaining a judicial warrant, to obtain access, subject to a prior notice in writing, to the premises / territory of the controller / processor, to obtain access without a prior notice to the premises / territory of the controller / processor, to access the premises / territory of a legal person only during office hours of that legal person, to access the premises / territory of a legal person at any time, to use the police if necessary, for the performance of powers of data protection supervisory authority, The Authority conducts, ex officio or following a complaint, investigations and audits, during which the technological infrastructure and other automated or non-automated means supporting the processing of personal data are subject to controls. In carrying out such investigations and inspections, the Authority has the power to obtain, from the controller and the processor, access to all personal data processed and to all information necessary for the purposes of such audits and the performance of its tasks, and no type of confidentiality may be relied upon against it. The Authority does not have access to data identifying associates or staff employed in entities contained in records held for national security purposes or for the purpose of investigating particularly serious crimes. 2) The Authority also: (a) issues warnings to a controller or processor b) orders the controller or processor to comply with the provisions of data protection legislation in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data; (c) orders and imposes a temporary or definitive limitation, or even a ban on the processing of personal data;(d) orders and imposes that documents, filing systems, equipment or means for processing personal data be delivered to it, as well as their content (e) seizes documents, information, filing systems for each piece of equipment and means of personal data breach, and their content which becomes known to the Authority in the exercise of its supervisory powers. The Authority is the sequestrator of the above material until a decision has been reached by the competent judicial and prosecutorial authorities It is also noted that as far as access to residential premises is concerned, according to article 9 of the Greek Constitution "no home search shall be made, except when and as specified by law and always in the presence of representatives of the judicial power".

Principality of Liechtenstein	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to order any natural and / or legal person (other than the controller and processor) to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to obtain access, subject to a prior notice in writing, to the premises / territory of the controller / processor, to access the premises / territory of a legal person only during office hours of that legal person
Portugal	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to order any natural and / or legal person (other than the controller and processor) to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to carry out searches and seizures in the premises of the data processor / controller without judicial warrant, to obtain access without a prior notice to the premises / territory of the controller / processor, to access the premises / territory of a legal person at any time, to obtain access to residential premises (including premises leased or used on any other basis) of a natural person only upon producing a court order authorising entry into the residential premises, to use the police if necessary, for the performance of powers of data protection supervisory authority
Grand Duchy of Luxembourg	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to obtain access without a prior notice to the premises / territory of the controller / processor, to access the premises / territory of a legal person only during office hours of that legal person
Latvia	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to order any natural and / or legal person (other than the controller and processor) to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to obtain access, subject to a prior notice in writing, to the premises / territory of the controller / processor, to access the premises / territory of a legal person only during office hours of that legal person, to use the police if necessary, for the performance of powers of data protection supervisory authority
The Czech Republic	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to order any natural and / or legal person (other than the controller and processor) to provide any information required for the performance of the tasks of data protection supervisory authority, to carry out searches and seizures in the premises of the data processor / controller after obtaining a judicial warrant, to obtain access, subject to a prior notice in writing, to the premises / territory of the controller / processor
Austria	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to order any natural and / or legal person (other than the controller and processor) to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to carry out searches and seizures in the premises of the data processor / controller without judicial warrant, to obtain access, subject to a prior notice in writing, to the premises / territory of the controller / processor, For the purpose of inspection, the data protection authority shall be entitled, after notifying the owner of the premises and the controller or processor, to enter premises where data processing is carried out.
The Republic of Slovenia	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to order any natural and / or legal person (other than the controller and processor) to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to carry out searches and seizures in the premises of the data processor / controller without judicial warrant, to carry out searches and seizures in the premises of the data processor / controller after obtaining a judicial warrant, to obtain access without a prior notice to the premises / territory of the controller / processor, to access the premises / territory of a legal person at any time, to obtain access to residential premises (including premises leased or used on any other basis) of a natural person only upon producing a court order authorising entry into the residential premises, to use the police if necessary, for the performance of powers of data protection supervisory authority

Bulgaria	to order the controller and the processor, and, where applicable, their representative to provide any information required for the performance of the tasks of data protection supervisory authority, to order any natural and / or legal person (other than the controller and processor) to provide any information required for the performance of the tasks of data protection supervisory authority, to obtain access to data banks and filing systems, data processing equipment and means from the controller / processor, to use the police if necessary, for the performance of powers of data protection supervisory authority

19. Please note which of these corrective powers does your data protection supervisory authority has:

Norway	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation, We can also issue coercive fines.
The Slovak Republic	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation
Romania	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation, The Romanian SA has the powers provided in Article 58 of the GDPR.
Italia	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been

	disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation
Estonia	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to order the suspension of data flows to a recipient in a third country or to an international organisation, Estonia has an exemption of adminsitrative fines foreseen in the GDPR. We have right to enact misdemeanour fines, Estonian judicial system does not foresee administrative fines
Croatia	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation
Republic of Cyprus	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation, Article 25(f) of the Law 125(I)/2018. "The Commissioner shall denounce the Cyprus Organization for the Promotion of Quality to the European Commission , in the case where the Cyprus Organization for the Promotion of Quality does not revoke an accreditation of a certification body in accordance with subsections (3) and (4) of section 16 of this Law."
Lithuania	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to

	order the suspension of data flows to a recipient in a third country or to an international organisation, The SDPI has investigative powers enshrined in the Article 58 of GDPR and has the right to apply measures enshrined in the Article 41 of Law of the Republic of Lithuania on Legal Protection of Personal Data, Processed for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences, or the Execution of Criminal Penalties, or National Security, or Defence which transposes Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. The Office of the Inspector of Journalistic Ethics (hereinafter referred to as Office) (https://www.zeit.lt/en) monitors the application of GDPR and Republic of Lithuania Law on Legal Protection of Personal Data (hereinafter referred to as Law) and ensures that this legislation applies to the processing of personal data for journalistic purposes and academic, artistic or literary purposes. Office has powers enshrined in the Article 58 of GDPR (except the powers enshrined in the Article 58 (1) (b) and (c), (2) (e), (g), (h) (j), and (3) (a), (c) and (e) – (j) of GDPR).
Iceland	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation
Greece	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation, The Authority has the power "to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met". Moreover, the Authority a) has the corrective power to order the controller or processor, or a recipient, or a third party, to discontinue the processing of personal data or to return or lock (block) the relevant data or to destroy the filing system or the relevant data and to impose the administrative penalties provided for in Articles 82.8 and 83 of the GDPR, b) where the protection of the individual against the processing of personal data concerning him or her requires immediate decision-making, the President may, at the request of the person concerned or ex officio, issue a temporary order for immediate temporary limitation, in whole or in part, of the processing or the operation of the file. The order shall apply until the Authority reaches its final decision, c) in order to ensure compliance with the provisions of the GDPR, and other regulations relating to the protection of the data subject with regard to the processing of personal data, the Authority has the power to adopt administrative regulatory acts to regulate specific, technical and detailed matters referred to in those acts. The regulatory acts of the Authority, which are not published in the Government Gazette, are published on the Authority's website.
Principality of Liechtenstein	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been

	disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation
Portugal	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation
Grand Duchy of Luxembourg	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation
Latvia	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation
The Czech Republic	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation

Austria	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation
The Republic of Slovenia	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to order the suspension of data flows to a recipient in a third country or to an international organisation
Bulgaria	to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR, to issue reprimands to a controller or a processor where processing operations have infringed provisions of GDPR, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR, to order the controller or processor to bring processing operations into compliance with the provisions of GDPR, where appropriate, in a specified manner and within a specified period, to order the controller to communicate a personal data breach to the data subject, to impose a temporary or definitive limitation including a ban on processing, to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR, to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met, to impose an administrative fine pursuant to Article 83 GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case, to order the suspension of data flows to a recipient in a third country or to an international organisation

20. Please note which of these authorization and advisory powers does your data protection supervisory authority has:

Norway	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to accredit certification bodies pursuant to Article 43 GDPR, to issue certifications and approve criteria of certification in accordance with Article 42(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR
The Slovak Republic	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to accredit certification bodies pursuant to Article 43 GDPR, to issue certifications and approve criteria of certification in accordance with Article 42(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR

Romania	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to accredit certification bodies pursuant to Article 43 GDPR, to issue certifications and approve criteria of certification in accordance with Article 42(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR
Italia	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to accredit certification bodies pursuant to Article 43 GDPR, to issue certifications and approve criteria of certification in accordance with Article 42(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR
Estonia	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to accredit certification bodies pursuant to Article 43 GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR
Croatia	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to accredit certification bodies pursuant to Article 43 GDPR, to issue certifications and approve criteria of certification in accordance with Article 42(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR
Republic of Cyprus	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to accredit certification bodies pursuant to Article 43 GDPR, to issue certifications and approve criteria of certification in accordance with Article 42(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR, Article 25(g) of the Law 125(I)/2018. "In addition to the authorisation and advisory powers provided for in Article 58, paragraph 3 of the Regulation, the Commissioner shall have the power to: - i. authorise the combination of filing systems provided for in section 10 of this Law and impose terms and conditions for the materialisation of the combination, ii. impose terms and conditions in relation to the application of the measures for the restriction of the rights referred to in section 11 of this Law, iii. impose terms and conditions for the exemption to the obligation to communicate the data breach referred to in section 12 of this Law, iv. impose explicit limits for the transfer of special categories of personal data referred to in sections 17 and 18 of this Law, v. recommend to the Minister the conclusion of agreements with other countries and conclude, establish and sign the Memoranda of Understanding provided for in section 35 of this Law."

Lithuania	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to accredit certification bodies pursuant to Article 43 GDPR, to issue certifications and approve criteria of certification in accordance with Article 42(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR
Iceland	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to issue certifications and approve criteria of certification in accordance with Article 42(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR
Greece	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR, to "approve criteria of certification in accordance with Article 42(5) GDPR"
Principality of Liechtenstein	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to accredit certification bodies pursuant to Article 43 GDPR, to issue certifications and approve criteria of certification in accordance with Article 42(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR
Portugal	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to accredit certification bodies pursuant to Article 43 GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR
Grand Duchy of Luxembourg	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to accredit certification bodies pursuant to Article 43 GDPR, to issue certifications and approve criteria of certification in accordance with Article 42(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR

Latvia	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to issue certifications and approve criteria of certification in accordance with Article 42(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR, accrediation of certification bodies is done together with Latvian National Accreditation Bureau (https://www.latak.gov.lv/index.php?lang=en)
The Czech Republic	to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR
Austria	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to accredit certification bodies pursuant to Article 43 GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR
The Republic of Slovenia	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR
Bulgaria	to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) GDPR, to accredit certification bodies pursuant to Article 43 GDPR, to issue certifications and approve criteria of certification in accordance with Article 42(5) GDPR, to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) GDPR, to authorise contractual clauses referred to in point (a) of Article 46(3) GDPR, to authorise administrative arrangements referred to in point (b) of Article 46(3) GDPR, to approve binding corporate rules pursuant to Article 47 GDPR

21. Is your data protection supervisory authority endowed with the regulatory powers other than those provided in GDPR (e.g. Art. 35 (4), etc.):

Norway	yes
The Slovak Republic	no
Romania	no
Italia	yes
Estonia	yes
Croatia	According to Article 6. of the Act on the Implementation of the General Data Protection Regulation in addition to its powers laid down by the General Data Protection Regulation, the Agency shall perform the following duties: – when laid down by a special law, it may initiate and has the right to participate in criminal, misdemeanour, administrative and other court and out-of-court proceedings for breaches of the General Data Protection Regulation and this Act – adopts the Criteria for determination of the amount of the compensation of administrative costs referred to in Article 43, paragraph 2 of this Act and the Criteria for determination of the amount of the compensation referred to in Article 43, paragraph 3 of this Act – publishes individual decisions on the Agency's website in accordance with Articles 18 and 48 of this Act – initiates and conducts appropriate procedures against responsible persons for breaches

	of the General Data Protection Regulation and this Act – carries out its duties of the independent supervisory authority for monitoring the implementation of Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, unless otherwise laid down by special regulations and – carries out other duties laid down by law.
Republic of Cyprus	The tasks assigned to the Information Commissioner are exercised by the respective Commissioner for Personal Data Protection. The Commissioner is the competent supervisory authority for other European bodies.
Lithuania	yes
Iceland	yes
Greece	no
Principality of Liechtenstein	no
Portugal	no
Grand Duchy of Luxembourg	yes
Latvia	yes
The Czech Republic	no
Austria	no
The Republic of Slovenia	yes
Bulgaria	yes

22. Please indicate your data protection supervisory authority competence regarding recommendation to parliament, government, other state institutions and bodies as regards adoption of legislative and administrative measures

Norway	the data protection authority gives opinion in its area of competence after adoption of the legal act, the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted, the data protection authority gives opinion to draft legal acts in its area of competence during the process of working out the text of the legal act
The Slovak Republic	the data protection authority gives opinion in its area of competence after adoption of the legal act, the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted, the data protection authority gives opinion to draft legal acts in its area of competence during the process of working out the text of the legal act
Romania	the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted, the data protection authority gives opinion to draft legal acts in its area of competence during the process of working out the text of the legal act
Italia	the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted, the data protection authority gives opinion to draft legal acts in its area of competence during the process of working out the text of the legal act
Estonia	the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted
Croatia	According to Article 14. of the Act on the Implementation of the General Data Protection Regulation Central state administration bodies and other public authorities shall submit to the Agency the drafts of proposals of laws and proposals of other regulations governing issues related to personal data processing in order to enable giving expert opinions regarding the area of personal data protection.
Republic of Cyprus	the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted, the data protection authority gives opinion to draft legal acts in its area of competence during the process of working out the text of the legal act
Lithuania	the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted, the data protection authority gives opinion to draft legal acts in its area of competence during the process of working out the text of the legal act

Iceland	the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted, the data protection authority gives opinion to draft legal acts in its area of competence during the process of working out the text of the legal act
Greece	the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted
Principality of Liechtenstein	the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted, the data protection authority gives opinion to draft legal acts in its area of competence during the process of working out the text of the legal act
Portugal	the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted, the data protection authority gives opinion to draft legal acts in its area of competence during the process of working out the text of the legal act
Grand Duchy of Luxembourg	the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted, the data protection authority gives opinion to draft legal acts in its area of competence during the process of working out the text of the legal act
Latvia	the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted, the data protection authority gives opinion to draft legal acts in its area of competence during the process of working out the text of the legal act
The Czech Republic	the data protection authority gives opinion in its area of competence after adoption of the legal act
Austria	the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted
The Republic of Slovenia	the data protection authority gives opinion in its area of competence after adoption of the legal act, the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted, the data protection authority gives opinion to draft legal acts in its area of competence during the process of working out the text of the legal act
Bulgaria	the data protection authority gives opinion in its area of competence after adoption of the legal act, the data protection authority gives opinion to draft legal acts in its area of competence when the text of the legal act was drafted, the data protection authority gives opinion to draft legal acts in its area of competence during the process of working out the text of the legal act

23. Is the performance of the tasks of your data protection supervisory authority free of charge:

Norway	Yes, for all of the above
The Slovak Republic	for the data subject
Romania	Yes to all of the above
Italia	The perfomance of the tasks of the Italian DPA is free of charge
Estonia	all answers apply
Croatia	According to Article 43. of the Act on the Implementation of the General Data Protection Regulation the Agency shall perform its tasks without compensation with respect to data subjects, personal data protection officers, journalists and public authorities. The Agency shall collect a reasonable compensation based on administrative expenses or shall refuse to act upon a request if requests of data subjects are clearly unfounded or excessive, and especially because of their frequency. The Agency shall charge the compensation for providing opinions to business entities (law firms, consultants etc.) requested by business entities for the purpose of carrying out their regular activities or provision of services.
Republic of Cyprus	all the above
Lithuania	free of charge
Iceland	The performance is in general free for all but under certain circumstances the DPA can charge a controller/processor for auditing tasks in accordance with the DPAs tariffs
Greece	It is free of charge for all the aforementioned stakeholders.
Principality of Liechtenstein	It is free for data subjects, DPOs and controllers and processors
Portugal	for the data subject
Grand Duchy of Luxembourg	fees can be charged in the area of certification accreditation

Latvia	fee is prescribed for data protection officers examination, seminars organised by Inspectorate, accreditation of code of conducts, accreditation of credit bureau, other tasks are free of charge
The Czech Republic	for the controllers and processors
Austria	for the data subject
The Republic of Slovenia	For all of the above
Bulgaria	All of the above

24. Decisions of your data protection supervisory authority:

Norway	can be appealed against to the court in accordance with the law of the Member State, can be appealed against to other institution / body
The Slovak Republic	can be appealed against to the higher administrative institution / body, can be appealed against to the court in accordance with the law of the Member State
Romania	can be appealed against to the court in accordance with the law of the Member State
Italia	can be appealed against to the court in accordance with the law of the Member State, can be appealed against to other institution / body
Estonia	can be appealed against to the court in accordance with the law of the Member State
Croatia	According to Article 34. of the Act on the Implementation of the General Data Protection Regulation anyone who considers that any of his or her rights guaranteed by this Act and the General Data Protection Regulation have been violated, may submit to the Agency a request for determination of a violation of a right. The Agency shall decide on the violation of rights by a ruling. The ruling of the Agency shall be an administrative act. No appeal shall be allowed against the ruling of the Agency, but an administrative dispute may be instituted by lodging a complaint before a competent administrative court.
Republic of Cyprus	can be appealed against to the court in accordance with the law of the Member State
Lithuania	can be appealed against to the court in accordance with the law of the Member State
Iceland	can be appealed against to the court in accordance with the law of the Member State
Greece	can be appealed against at the Council of State.
Principality of Liechtenstein	can be appealed against to the higher administrative institution / body
Portugal	can be appealed against to the court in accordance with the law of the Member State
Grand Duchy of Luxembourg	can be appealed against to the court in accordance with the law of the Member State, adeministrative court
Latvia	can be appealed against to the court in accordance with the law of the Member State
The Czech Republic	can be appealed against to the higher administrative institution / body
Austria	can be appealed against to the court in accordance with the law of the Member State
The Republic of Slovenia	can be appealed against to the court in accordance with the law of the Member State
Bulgaria	can be appealed against to the court in accordance with the law of the Member State

25. Regarding engagement in legal proceedings your data protection supervisory authority, in accordance with the law, has a right (several answers are possible):

Norway	to take part in legal proceedings regarding decisions adopted by your authority
The Slovak Republic	to take part in legal proceedings regarding decisions adopted by your authority
Romania	to take part in legal proceedings regarding decisions adopted by your authority
Italia	to take part in legal proceedings regarding decisions adopted by your authority
Estonia	do not understand the question and possible answers
Croatia	According to Article 6. of the Act on the Implementation of the General Data Protection Regulation the Agency, when laid down by a special law, may initiate and has the right to participate in criminal, misdemeanour, administrative and other court and out-of-court proceedings for breaches of the General Data Protection Regulation and this Act and initiates and conducts appropriate procedures against responsible persons for breaches of the General Data Protection Regulation and this Act.

Republic of Cyprus	to appeal against normative legal acts adopted by public administration institutions, to take part in legal proceedings regarding decisions adopted by your authority, Article 25(h) of the Law 125(I)/2018. "Subject to the provisions of Article 58, paragraph 5 of the Regulation, the Commissioner shall notify to the Attorney General of the Republic and/ or to the police any contravention of the provisions of the Regulation or of this law, that may constitute an offense in accordance with provisions of section 33 of this Law"
Lithuania	to take part in legal proceedings regarding decisions adopted by your authority
Iceland	to take part in legal proceedings regarding decisions adopted by your authority
Greece	to take part in legal proceedings regarding decisions adopted by your authority
Principality of Liechtenstein	to take part in legal proceedings regarding decisions adopted by your authority
Portugal	to appeal against normative legal acts adopted by public administration institutions, to address matter to the Constitutional court, to take part in legal proceedings regarding decisions adopted by your authority
Grand Duchy of Luxembourg	to take part in legal proceedings regarding decisions adopted by your authority
Latvia	to take part in legal proceedings regarding decisions adopted by your authority
The Czech Republic	to appeal against normative legal acts adopted by public administration institutions, to take part in legal proceedings regarding decisions adopted by your authority
Austria	to take part in legal proceedings regarding decisions adopted by your authority
The Republic of Slovenia	to address matter to the Constitutional court, to take part in legal proceedings regarding decisions adopted by your authority
Bulgaria	to appeal against normative legal acts adopted by public administration institutions, to take part in legal proceedings regarding decisions adopted by your authority

26. Does your data protection supervisory authority interact with other regulators and authorities in the event of incidents related to personal data leaks?

		If you answer "yes" to 26 questionnaire, at what level are the mechanisms of interaction defined:
Norway	Yes	Cooperation on a voluntary basis
The Slovak Republic	No	
Romania	Yes	authority law
Italia	No	
Estonia	Yes	co-operation between European DPAs are foreseen in the GDPR, co-operation with other auhtorities on the national level is regulated by the agreements
Croatia	Yes	Where necessary, we communicate with other supervisory authorities through voluntary mutual assistance.
Republic of Cyprus	Yes	all the above
Lithuania	Yes	- authority law; - regulations of the body; - cybersecurity law; - law on electronic communications
Iceland	Yes	cybersecurity law
Greece	Yes	law on electronic communications
Principality of Liechtenstein	No	
Portugal	Yes	regulations of the body
Grand Duchy of Luxembourg	Yes	law on electronic communications
Latvia	Yes	authority law
The Czech Republic	No	
Austria	No	
The Republic of Slovenia	Yes	Independent decision of the SA depending on the case
Bulgaria	Yes	All of the above

27. As regards administrative fines in your country for public authorities:

Norway	Administrative fines are as indicated in the Art. 83 of GDPR
The Slovak Republic	Administrative fines are as indicated in the Art. 83 of GDPR
Romania	Minimum - 10000 lei and maximum 200000 lei
Italia	Administrative fines are set up in the national legislation (please indicate minimum and maximum limits of administrative fine)
Estonia	Estonia has misdemenaour fines (recital 151 in the GDPR), misdemenaour fines cannot be imposed for public authorities, amount of fines are imposed in the Perosnal Data Portection Act Chapter 6: https://www.riigiteataja.ee/en/eli/523012019001/consolide
Croatia	Administrative fines cannot be imposed for public authorities
Republic of Cyprus	Article 32(3) of the Law 125(I)/2018. "An administrative fine imposed to a public authority or body, which relates to non-profitable activities shall not exceed two hundred thousand (200,000) euro."
Lithuania	Administrative fines are set up in the national legislation (please indicate minimum and maximum limits of administrative fine)
Iceland	Administrative fines are as indicated in the Art. 83 of GDPR
Greece	According to Article 39 par. 1 of law 4624/2019 the Authority may, in a specific reasoned decision and following a previous notice summoning the interested parties to provide explanations, impose to bodies of the public sector, an administrative fine of up to ten million euros (EUR 10,000,000)
Principality of Liechtenstein	Administrative fines cannot be imposed for public authorities
Portugal	Administrative fines are set up in the law. But Public authorities may request exemption of application.
Grand Duchy of Luxembourg	Administrative fines cannot be imposed for public authorities
Latvia	till 1000 eur for the natural person (civil servant).
The Czech Republic	Administrative fines are as indicated in the Art. 83 of GDPR
Austria	Administrative fines cannot be imposed for public authorities
The Republic of Slovenia	Administrative fines are set up in the national legislation (please indicate minimum and maximum limits of administrative fine)
Bulgaria	Administrative fines are as indicated in the Art. 83 of GDPR

28. As regards prior consultation procedure referred to in Article 36 of GDPR:

Norway	consultation with the data protection supervisory authority is mandatory during the preparation of a proposal for a legislative measure to be adopted by a national parliament
The Slovak Republic	the procedure of prior consultation by the controller in accordance with Art. 36 (1) of GDPR is regulated by national legislation
Romania	consultation with the data protection supervisory authority is mandatory during the preparation of a proposal for a legislative measure to be adopted by a national parliament
Italia	The prior consultation procedure is provided for by Article 36.4 GDPR to which we refer: our supervisory authority must be therefore consulted during the preparation of a proposal for a legislative measure, or of a regulatory measure based on such a legislative measure, which relates to processing of personal data. Please note that Secction 110 of the DPCode (Medical, Biomedical and Epidemiological Research) also refers to the need for prior consultation under Article 36 GDPR.With regard to Article 36.5 GDPR we refer to Section 2-p (Processing entailing a high risk for the performance of a task carried out in the public interest) of the DP Code (see the link above)
Estonia	consultation with the data protection supervisory authority is mandatory during the preparation of a proposal for a legislative measure to be adopted by a national parliament
Croatia	According to Article 36 of GDPR the controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.
Republic of Cyprus	consultation with the data protection supervisory authority is mandatory during the preparation of a proposal for a legislative measure to be adopted by a national parliament, consultation with the data protection supervisory authority is mandatory during the preparation of a regulatory measure based on the legislative measure adopted by a national parliament, Articles 10(2), 11(2), 12(2) and 18(1) of the Law 125(I)/2018.

Lithuania	the procedure of prior consultation by the controller in accordance with Art. 36 (1) of GDPR is regulated by national legislation, The alignment (with the data protection supervisory authority) of the draft legislation is carried out in accordance with the Republic of Lithuania Law on Legislative Framework and the Rules of Procedure of the Government of the Republic of Lithuania approved by Resolution No 728 of the Government of the Republic of Lithuania of 11 August 1994.
Iceland	consultation with the data protection supervisory authority is voluntary during the preparation of a proposal for a legislative measure to be adopted by a national parliament, consultation with the data protection supervisory authority is voluntary during the preparation of a regulatory measure based on the legislative measure adopted by a national parliament
Greece	consultation with the data protection supervisory authority is mandatory during the preparation of a proposal for a legislative measure to be adopted by a national parliament, consultation with the data protection supervisory authority is mandatory during the preparation of a regulatory measure based on the legislative measure adopted by a national parliament
Principality of Liechtenstein	the procedure of prior consultation by the controller in accordance with Art. 36 (1) of GDPR is regulated by national legislation, consultation with the data protection supervisory authority is voluntary during the preparation of a proposal for a legislative measure to be adopted by a national parliament, consultation with the data protection supervisory authority is voluntary during the preparation of a regulatory measure based on the legislative measure adopted by a national parliament
Portugal	the procedure of prior consultation by the controller in accordance with Art. 36 (1) of GDPR is regulated by national legislation
Grand Duchy of Luxembourg	There are no specific national law provisions specifying article 36 of the GDPR.
Latvia	consultation with the data protection supervisory authority is voluntary during the preparation of a proposal for a legislative measure to be adopted by a national parliament, consultation with the data protection supervisory authority is voluntary during the preparation of a regulatory measure based on the legislative measure adopted by a national parliament
The Czech Republic	consultation with the data protection supervisory authority is voluntary during the preparation of a regulatory measure based on the legislative measure adopted by a national parliament
Austria	the procedure of prior consultation by the controller in accordance with Art. 36 (1) of GDPR is regulated by national legislation
The Republic of Slovenia	consultation with the data protection supervisory authority is voluntary during the preparation of a proposal for a legislative measure to be adopted by a national parliament, consultation with the data protection supervisory authority is voluntary during the preparation of a regulatory measure based on the legislative measure adopted by a national parliament
Bulgaria	the procedure of prior consultation by the controller in accordance with Art. 36 (1) of GDPR is regulated by national legislation, consultation with the data protection supervisory authority is mandatory during the preparation of a proposal for a legislative measure to be adopted by a national parliament, consultation with the data protection supervisory authority is mandatory during the preparation of a regulatory measure based on the legislative measure adopted by a national parliament, consultation with the data protection supervisory authority is voluntary during the preparation of a regulatory measure based on the legislative measure adopted by a national parliament, national legislation require controllers to consult with and to obtain prior authorization from the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health (Art. 36 para. 5 of GDPR), Answer 4 is in case of rectification

29. Please indicate your activities regarding promotion of public awareness, as well as awareness of controllers and processors about their responsibilities:

Norway	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679
The Slovak Republic	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679
Romania	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679

Italia	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679, launching data protection informational campaign for controllers and processors to enhance qualifications of civil servants required to hold the position of a person responsible for personal data protection, awareness raising campaigns on the obligations/rights under the GDPR
Estonia	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679, launching data protection informational campaign for controllers and processors to enhance qualifications of civil servants required to hold the position of a person responsible for personal data protection, we also have a helpline for data controllers/processors, data subjects, other authorities etc.
Croatia	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679, The Agency holds regular weekly trainings that follow a number of tasks and roles of data protection officers that arise from the General Regulation on Data Protection. The mentioned trainings are separated for public and private sector in order to focus on the issues of a particular sector and there are additional distinctions for certain activities, such as the security sector. Mentioned trainings are followed with complianed documents and brochures available on our website. Within the EU ARC project (AWARENESS RAISING CAMPAIGN FOR SMEs) Croatian Personal Data Protection Agency and Data Protection Commission Ireland during their every day work noticed that there is still a lot of ambiguities in the application of the GDPR by the SMEs. These findings are also supported by a large number of written queries and even greater number of phone calls which these two authorities receive on a daily basis. Through this project AZOP and DPC have an additional opportunity to help these subjects in full GDPR implementation and in understanding the importance of personal data protection through workshops and presentations and educational materials.
Republic of Cyprus	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679, launching data protection informational campaign for controllers and processors to enhance qualifications of civil servants required to hold the position of a person responsible for personal data protection, conducting public information campaigns and campaigns for students
Lithuania	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679, launching data protection informational campaign for controllers and processors to enhance qualifications of civil servants required to hold the position of a person responsible for personal data protection, - SDPI also raises awareness through the following activities: prepares public information tools, drawns up methodological documents, attends meetings with public and private sectors, makes presentations at the events.
Iceland	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679
Greece	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679, Giving speeches, organizing information days and scientific conferences.
Principality of Liechtenstein	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679, launching data protection informational campaign for controllers and processors to enhance qualifications of civil servants required to hold the position of a person responsible for personal data protection
Portugal	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679
Grand Duchy of Luxembourg	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679, launching data protection informational campaign for controllers and processors to enhance qualifications of civil servants required to hold the position of a person responsible for personal data protection
Latvia	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679, launching data protection informational campaign for controllers and processors to enhance qualifications of civil servants required to hold the position of a person responsible for personal data protection
The Czech Republic	launching data protection informational campaign for controllers and processors to enhance qualifications of civil servants required to hold the position of a person responsible for personal data protection
Austria	The Austrian DPA publishes a great deal of information on its website and publishes newsletters with important decisions of the authority.
The Republic of Slovenia	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679
Bulgaria	conducting seminars/webinars and consultations of controller and processor on the provisions of Regulation 2016/679, launching data protection informational campaign for controllers and processors to enhance qualifications of civil servants required to hold the position of a person responsible for personal data protection, international conferences, information leaflets, Mobile App, Self-assessment and awareness tool

30. Please inform, whether the authority has the right to transfer materials of inspections with signs of a crime to the law enforcement authority?

Norway	It depends on whether the information is covered by our statutory duty of confidentiality, and if so, whether any exceptions to that duty apply.
The Slovak Republic	No
Romania	No
Italia	Yes
Estonia	Yes
Croatia	According to Article 38. of the Act on the Implementation of the General Data Protection Regulation if, during the supervision, knowledge is gained or objects found that indicate a criminal offence prosecuted ex officio has been committed, the authorised persons shall, within the shortest term possible, inform the competent police station or a state attorney.
Republic of Cyprus	Yes
Lithuania	Yes
Iceland	Yes
Greece	Yes
Principality of Liechtenstein	Yes
Portugal	Yes
Grand Duchy of Luxembourg	Yes
Latvia	Yes
The Czech Republic	Yes
Austria	Yes
The Republic of Slovenia	Yes
Bulgaria	Yes

Dijana ŠINKŪNIENĖ graduated from the Department of Law, Vilnius University, Lithuania, in 2000. In 2001-2018, she was the Deputy Director of the State Data Protection Inspectorate of the Republic of Lithuania, where, among other activities, she was responsible for legal analysis of the draft legal acts as well as the existing legislation of the Republic of Lithuania, including submitting proposals regarding their drafting, amending and repealing as far as personal data protection and privacy issues were concerned. In 2017-2018, she was engaged in preparatory work at the national level regarding the European Data Protection Reform: she led a working group responsible for amending the Law on the Legal Protection of Personal Data with regard to the General Data Protection Regulation (EU) 2016/679, and participated in stakeholders' meetings, and awareness raising activities. Dijana Šinkūnienė also took part in various activities aimed at strengthening institutional capacities of data protection supervisory authorities, including as the Key Expert in the EU Twinning Project UA/47b "Implementation of the best European practices with the aim of strengthening the institutional capacity of the Apparatus of the Ukrainian Parliament Commissioner for Human Rights to protect human rights and freedoms (Apparatus)". In 2018 Dijana Šinkūnienė left the civil service. Currently she is a personal data and privacy consultant, co-founder of a firm working in this field, as well as a Privacy, security and technologies (Privacytech) lecturer at Mykolas Romeris University (Vilnius, Lithuania).

Lilia OLEKSIUK graduated from the Department of Law, Kyiv University of Tourism, Economics and Law in 2003. For many years (1998 - 2011) she worked at a state enterprise supporting the functioning of public state automated systems, where she was responsible for enterprise development, interaction with government agencies and the development of regulatory support for state registers and the land cadastre. From 2011 to 2014 she worked as the First Deputy Head of the State Service of Ukraine for Personal Data Protection organizing oversight in the field of personal data protection, registration of personal data bases and legal drafting. She has a master's degree in social development management and PhD in public administration in the field of electronic access to public information and open data. She is a member of one of the Association Agreement between Ukraine and the EU bodies, the Ukrainian side of the Civil Society Platform. Ms. Oleksiuk chairs the All-Ukrainian Association «Information Security and Information Technology». She lectures at Kyiv National University of Trade and Economics to future civil servants on strategic and regional management, digital economy and organization of access to public information with the protection of personal data. She has her own practice and is a consultant, since 2018, in the field of personal data protection, development of national automated systems, electronic trust services, digital economy development and integration into the EU Digital Single Market. Since 2019, she has been a freelance advisor to the Verkhovna Rada Committee on Digital Transformation, and is one of the authors of the draft law "On Personal Data Protection" (reg.# 5628 of June 7, 2021).

Oleksandr SHEVCHUK graduated from the Department of International Law, Institute of International Relations, Taras Shevchenko National University in 2015. In 2016-2019, he was the legal approximation expert in the EU Project «Support to the implementation of the EU-Ukraine Association Agreement». He worked at the Government Office for Coordination on European and Euro-Atlantic Integration, where, among other activities, he was responsible for comparative analysis of EU and Ukrainian laws. In 2019, he got a PhD in Law with «Legal Regulation of Personal Data Protection in the European Union». In 2019-2020, he was the national expert on e-justice in the area of personal data protection in the EU Project "Pravo-Justice". He worked on assessment of the concepts and practical steps for the development and adoption of the new data protection legislation. Currently he is a national consultant on personal data protection in the Joint EU/Council of Europe project to strengthen the Ombudsperson's capacity to protect human rights. He has worked on the development of the online training course «Personal Data Protection», and on preparatory work for the Data Protection Reform in Ukraine (2019-2021). He is a member of the working group on reforming the national legislation in the area of processing and protection of personal data. Oleksandr Shevchuk is one of the authors of the draft law "On Personal Data Protection" (reg.# 5628 of June 7, 2021).

ENG

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

www.coe.int

The member states of the European Union have decided to link together their know-how, resources and destinies. Together, they have built a zone of stability, democracy and sustainable development whilst maintaining cultural diversity, tolerance and individual freedoms. The European Union is committed to sharing its achievements and its values with countries and peoples beyond its borders.

www.europa.eu

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE