**Data protection and free access to information in Montenegro**

FINAL REPORT

16/01/2020

***Authors of the report:***

***Disclaimer***

*The views articulated and expressed in this report are purely those of the author and may not in any circumstances be regarded as stating an official position of the European Commission.*

# INTRODUCTION

The objective of this peer-review mission (22- 26 July 2019, held in Podgorica), was to provide the European Commission and Montenegro with an assessment of the country's institutional framework and capacities concerning protection of personal data and free access to information. This assessment was carried out in cooperation with the Montenegrin authorities, responsible for data protection and free access to information in Montenegro.

In the course of this mission several meetings were held with relevant stakeholders (the Administrative court, the Agency for data protection and free access to information, the Ombudsman, Ministry for public administration, Ministry of interior, Ministry for defence, Directorate for classified data and the Agency for the prevention of corruption). From the stakeholders that were prepared to meet us, we received good and cooperative partners in dialogue, who fostered us with meaningful and resourceful information needed to establish a general evaluation of the state of play on the areas of free access to information and data protection in Montenegro.

## Contents

# THE SYSTEM ON FREE ACCESS TO INFORMATION AND DATA PROTECTION IN MNE

## AGENCY FOR DATA PROTECTION AND FREE ACCESS TO INFORMATION

### The competence, capacities and activities of the Agency

The Agency for Data Protection and Free Access to Information (hereinafter the Agency) is the national data protection authority and has a number of competencies related to free access of information (second instance body, authority responsible for the supervision of proactive publication of information, etc.). The Agency acts as an autonomous and independent state body. Its council consists of three members (president and two members), appointed by the national parliament. They are appointed for a period of five years and cannot be appointed to these functions more than twice. The Council's decisions are made by the majority of votes with the possibility of a separate opinion. The Council appoints the Director of the Agency who represents, organises and runs the Agency and executes its decisions. Operational funds are provided from the state budget or other sources in accordance with the law. The Agency negotiates on the amount of funds from the state budget with the Ministry of Finance. If no agreement is reached, the parliament determines the amount of funds. The amount of funds has been constant over the last few years.

The Agency's organisational structure consists of management, internal auditor and 5 departments, one of them being responsible for supervision in the field of data protection, one for matters and appeals in the field of data protection and one for free access to information. At present, the Agency's staff consists of 30 employees out of total of 47, provided for by the Act on Systemization. Only 2 out of 30 employees are IT experts.

In the field of data protection, the two abovementioned departments consist of total of 7 employees. The Agency performs supervision in the field of data protection through employees who are competent for performing supervisory activities (supervisors). They have, in performing tasks within their competences, access to personal data in the records and to files and other documentation regarding personal data processing and to the means of electronic data processing. The supervisors can issue a decision and impose a number of corrective measures, such as elimination of deficiencies, temporary prohibition of processing, ordering erasure of unlawfully collected personal data, prohibiting the transfer of personal data out of Montenegro and restriction of processing. An administrative dispute may be initiated against the decision of the Agency.

The supervision can be regular, extraordinary (following an initiative) and control. Most of them are extraordinary, following an initiative submitted by a data subject who considers that any of their rights have been violated, by any other person or based on an order from the Director of the Agency in accordance with his competences. In the first half of 2019, 4 regular (the number of regular requests has been decreasing annually), 44 extraordinary and 14 control supervisions in the field of data protection have been conducted. If the supervision is initiated ex officio or a person submits an initiative for the supervisory procedure, the record on the performed supervision has to be made within 15 days from the performed supervision and then submitted to the data controller. There is no obligation to inform the person who submitted the initiative. He/she is, though, informed of the final decision, but cannot file an appeal, which can only be filed by the data controller. If the supervision

procedure is performed upon request for the protection of rights in the field of data protection, the record has to be made within 8 days of submitting the request. The record is then submitted to the data controller and to the person who submitted the request. They both can file an appeal against the record within 8 days of the receipt of the record.

The Agency's department for matters and appeals in the field of data protection has in the first half of 2019 issued 3 opinions, 8 decisions to refuse the appeal, 14 consents to introduce video surveillance system, 1 consent to transfer personal data out of Montenegro, 1 response to a law suit, performed 2 data protection educations and prepared 45 other documents in line with its competencies. Especially matters regarding video surveillance represent a great and disproportionate burden for the Agency. In 2018, 40 consents were issued. **Most of these types of cases take a lot of time and resources to handle. We recommend finding a solution to this problem. One of possible solution would be to amend the law and abolish the obligatory consent of the agency in all cases where video surveillance is not prescribed by law.**

In the area of free access to information the Agency is, according to Law on Free Access to Information (Official journal MNE, no. 44/2012 and 30/2017; hereinafter LFAI) competent: to perform supervision over the legality of administrative decisions deciding upon requests for access to information and take the measures set forth by the law; to manage an information system of access to information; to monitor the state of play in the area of access to information and submit reports thereon; to perform inspection supervision over the implementation of this Law in relation to the creation and update of the access to the information guide, the proactive publishing of information and the delivery of legal acts and data for the purpose of managing information system for free access and re-use of information; submit initiatives for opening of misdemeanour proceedings for violations of the Law in relation to the creation and update of the access to the information guide, the proactive publishing of information and the delivery of legal documentation and data for the purpose of managing information system for free access and re-use of information; to manage and regularly update the evidence about the approved exclusive rights with regards to re-use of public information; verify the grounds for approval of exclusive rights with regards to re-use of public information. In addition, the Agency itself also works as a first instance body to provide free access to public information under their domain.

The Agency conducts complaint procedures in the area of free access to information with the capacity of 8 advisors and 3 members of the Council who deliver the final decision. Workflow: The Agency receives a written complaint which is first administratively processed in a paper form (assigned with a reference number and referred to the advisor who reviews the background of the complaint). Advisor then presents the merits and procedural circumstances of the case to the Council when his case is listed on the agenda of Council's regular meetings. All documentation of every case is also printed out for each member of the Council. When the council reaches a decision, it is delivered to the advisor, who formulates it. Inspections with regards to proactive publication of documentation are conducted independently of the Council, by any of the 4 advisors-inspectors who also work on individual complaints as explained above.

The Agency has also been engaged in awareness raising activities in the field of data protection and in the field of free access to information. They detect the vulnerable areas, also on basis of the initiatives submitted by the individuals. The Agency has first conducted internal trainings, then it began cooperating with the Chamber of Commerce and jointly organised trainings throughout the state. In

average 80 people have attended the seminars and workshops where many materials, also from other states, have been used. These trainings have been conducted by 4 employees of the Agency. They have received a lot of initiatives from the health sector. The Agency has detected a low level of awareness in many sectors, while the Agency estimates a relatively high level of awareness in the field of data protection in the banking sector and in the field of mobile service providers. The Agency considers ex officio supervision on data protection issues also as an integral part of awareness raising activities. The requests to conduct trainings on data protection issues have recently increased in the private sector. The Agency has also been involved in several awareness raising projects targeted at certain groups, for instance Roma population.

The Agency has been active in the field of international cooperation. The representative of the Agency has regularly attended European Data Protection Board plenary meetings. It has also participated at several international conferences, meetings of the TP-D at the Council of Europe and meetings of the several international working groups. They maintain good cooperation with the countries of ex-Yugoslavia within the regional in initiative and bilateral cooperation with many countries.

We consider that the powers of the Agency are appropriate to fulfil the tasks entrusted to it by the legislation. However, we recommend that the number of employees adapts to the number, provided for by the Act on Systemization, as much as possible and in a reasonable period of time to enable the Agency to fulfil its tasks in the best possible manner. We also recommend increasing the number of employees who possess IT expertise and knowledge. Currently the Agency occasionally has to outsource such experts when fulfilling its tasks and exercising its powers which is inevitable, considering that they only employ two IT experts. The increase of employees could also enable to perform some preventive actions and supervision in the most exposed areas or specific sectors. In this aspect we welcome the fact that the Agency has conducted supervision of all mobile service providers and we encourage further similar activities.

### Identified issues regarding the procedure with free access to public information

The findings of the peer review mission regarding the complaint procedure itself deriving from statements of the officials of the Agency and a research conducted on the statistical data provided, brings up the following emphasis:

#### *Alleged abuse of the of the law on free access to information*

A trend of raising the number the complaints received by the Agency can be acknowledged.

*According to the annual reports of the Agency:*

| | **2014** | **2015** | **2016** | **2017** | **2018** |
|---|---|---|---|---|---|
| no. of requests to first instance bodies | 4058 | 4434 | 6426 | 5877 | 6089 |
| no. of complaints | 1753 | 1513 | 3554 | 4862 | 3909 |

The Agency has explained that the significant increase to the number of complaints raised against the first instance bodies roots in the abuse of the free access to information system. According to their statements certain applicants abuse the right to access to public information for gaining profit on costs for legal representation before the administrative court. This is achieved by burdening the administration of a single liable body with numerous requests (over 100 per day), requesting a large amount of documentation which cannot be administratively processed in the prescribed deadline of 15 days. We received similar reports on this matter also from other first instance bodies that we have met during this peer review mission. The Agency further reports on the practice of these applicants that immediately when the deadline expires (on the 16th day) the applicant would file complaints to the Agency for the reason of administrative silence of the first instance bodies. When the Agency could not administratively process the large number of complaints before the deadline (15 days from receiving of complaints), the applicant would file a large number of lawsuits to the Administrative court, requesting a public hearing which significantly increases the costs for legal representation before the Administrative court. From the result of the administrative court decision high amount of costs are afforded to the applicant (over 400€ per lawsuit), that have to be paid by the Agency from the state budget.

The claims by the Agency are supported by the following **statistics**:

| | ***2016*** | ***2017*** | ***2018*** | ***First half 2019*** |
|---|---|---|---|---|
| **No. of lawsuits at the administrative court against the Agency** | 656 | 1709 | 2970 | 1041 |

*The statistics were obtained from the Administrative court.*

According to the statement of the Agency this is currently the most damaging cause for the dis-functioning of the Agency and the system on free access to information in Montenegro. In the Agency's view, since it is occupied with the task to administratively process a large number of complaints to protect the state budget, it then lacks the capacity to adequately deal with other complaints and perform its other tasks and duties.

In our opinion and deriving from different reports the situation regarding a large amount of complaint procedures for the reason of gaining profit on legal representation costs in judicial procedures is serious and real and therefore has to be dealt with promptly and accordingly.

### Withholding of information by first instance bodies

Deriving from the annual reports of the Agency (from 2014-2018), in the section *Analysis of the state of play of free access to information* the reports indicate that **first instance bodies have been obstructing the free access to information by denying access on the account of not having the information in its possession when in further proceedings it was found that it was not true**.

The current legislative solution does not provide for an efficient remedy in cases where first instance bodies deny access for the reason of not being in possession of the requested information. The problem is that the current law does not provide the Agency with the capacity to enter the first instance body's office and perform an examination whether the first instance body indeed does not have the requested information in its possession. For such an inspection the Agency has to turn to an

outside inspection working within another state body that should perform an inspection to establish whether the first instance body is in fact not in the possession of the requested document. According to LFAI (Art 40, Para 2), the inspection should be performed and conclusions delivered to the Agency within 5 days after the request by the Agency. According to the annual report in 2014, 79 of such requests were filed but none of them were performed. According to the annual report for the year 2015 a better communication was established between the Agency and the competent ministry so that inspections were eventually performed yet still with such delays that caused the Agency to delay its decision on the merits so that the applicants filed initiatives for a misdemeanour procedure against the Agency for the denial of service. Although when inspections actually were performed, the annual report states that "…*the result was a more responsible decision making and often findings of documents for which they* (the first instance bodies) *claimed that they do not have in their possession."* [1] In 2016 the practice of non-performing the inspections continued (according to the annual report 243 requests for inspection were filed, none were performed). In 2017, 89 requests were filed and there is no information on the actual performance of those requests. **The described legislative solution is not functioning in practice therefore it must be amended.**

In addition to the abovementioned and deriving from the annual reports of the Agency, there seems to be a reoccurring practice that first instance **bodies do not deliver the requested information to the Agency for the purpose of second instance decision in merits, which also indicates the tendency of obstructing the right of free access to information by the first instance bodies.** The LFIA requires first instance bodies to deliver the requested documents upon request of the Agency (Art 40, Para 1, Point 1). If they do not do so (and it seems to be a reoccurring practice) the Agency can file an initiative for the misdemeanour procedure. From the annual reports derives that the initiatives for the misdemeanour procedures for these reasons were filed in numerous occasions:

| 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|
| 53 | 18 | 148 | No information |

Even though that the competent inspection reacts and issues fines for the public officials who have been obstructing the process, this does not seem to solve the reoccurring problem.

### Complaints due to administrative silence

It can be noticed that the number of decisions issued by the Agency instructing the first instance bodies to deliver a decision within 15 days (*administrative silence*) has diminished over the years of the application of the law. A noticeable trend of lowering the administrative silences can be acknowledged in years from 2014 (1044) to 2015(897). An increase can be again noticed in 2016 (997), although then a decreasing trend can be noticed in 2017 (941) and especially in 2018 (416). The reason for the fast lowering of the administrative silence decisions in 2018 could be because of a more efficient or productive legal practice of the Agency that is channelled towards the needs of an applicant and not towards the legal process itself (in 750 cases of administrative silence complaints in 2018, the

[1] *"za rezultat ima odgovorniji odnos prilikom odlučivanja i često pronalaženje dokumenata za koje su tvrdili da nijesu u njihovom posjedu.",* IZVJEŠTAJ O STANJU ZAŠTITE LIČNIH PODATAKA I STANJU U OBLASTI PRISTUPA INFORMACIJAMA ZA 2015. GODINU, *p. 76;* http://www.azlp.me/docs/zajednicka/izvjestaj_o_stanju/IZVJESTAJ%202015%20final.doc

procedure was stopped because the applicant pulled its complaint, since he was satisfied with the result). It needs to be noted that the Agency received a capacity building Twinning light project in 2018.

### *Material costs of free access*

Regarding the material costs, some stakeholders had described them as high and an obstacle to retrieve information, especially the 30 cent per page charged for "scanning". The Agency stated that in their belief the costs as set by the government regulation are high and that they are prone to the concept of removing all costs, including material costs for photocopying and scanning of documentation.

### *Proactive publication*

**Regarding proactive publication of information**, the annual reports issued by the Agency (2014-2018) repeatedly emphasize the importance of proactive publication of information as a prominent way to diminish the number of individual requests that occupies public administration thus rendering the right to free access and unburdening the public administration. The same conclusion also came from the analysis conducted in the Twinning project (*TWL Project Capacity Development for Agency for Personal Data Protection and Free Access to Information*) project held in 2018[2] where, one of the main goals was also to help the Agency to "*increase the level of proactive publication of information on the websites of public bodies*."[3] The cited analysis has shown the actual **necessity for the improvement of proactive publication** (pilot assessment has been conducted on 10 public bodies regarding their level of proactive publication) and provided **concrete recommendations** on:

> (1) LEGISLATION THAT NEEDS TO BE CHANGED (concrete proposals for individual articles);
>
> (2) HELPING MATERIALS THAT NEED TO BE IMPLEMENTED (*guidelines*, *self-evaluation test*, *education programme for proactive publication*, *methodological periodic review of the websites*, *expending the Agency's annual report in the section regarding proactive publication)*.
>
> (3) HOW THE FIRST INSTANCE BODIES NEED TO FOLLOW THE LEGISLATION, USE GUIDELINES AND TO BE MORE PRONE TO TRANSPARENCY.

The twinning project provided the Agency with the materials intended for helping the first instance bodies to proactively publish the information (*guidelines for the first instance bodies to proactively publish information; the self-evaluation test, etc.*). **However, in the course of the peer review mission there was no indication of those materials ever being published, promoted or otherwise disseminated.**

The analysis also strongly recommends building up the capacity of the Agency, so that it would have the human and financial resources to see through the implementation of the suggested measures. According to the analysis (Recommendation 4: Improve the capacities of the supervisory authority), *regarding the current capacities of the Agency it is unreasonable to expect a thorough supervision and therefore increase of proactive publication.*[4] Deriving also from the findings in the course of this peer

---

[2] Analysis and recommendations for increasing proactive publication of information by public bodies, final version 13 October 2018.

[3] "*Povećan nivo proaktivnog objavljivanja informacija na internetskim stranicama organa vlasti;"* IZVJEŠTAJ O STANJU ZAŠTITE LIČNIH PODATAKA I STANJU U OBLASTI PRISTUPA INFORMACIJAMA ZA 2018. GODINU, p. 104.

[4] "*U odnosu na postojeće kapacitete Agencija, nerealno je očekivati temeljit nadzor i time jačanje proaktivne objave informacija."* Analysis and recommendations for increasing proactive publication of information by public bodies, final version 13 October 2018, p. 31.

review mission, the Agency is currently dealing with a large number of individual complaint procedures (also for the reason of the aforementioned circumstances of alleged abuse of the law). In these circumstances, given that resources are limited, the Agency should carefully and mindfully prioritise its activities in order to ensure that it implements the recommendations that would address the root cause of the issue of free access to information in MNE.

## EXAMPLES OF PRACTICE OF 1ST INSTANCE BODIES

### Ministry of defence, directorate for classified data

The Ministry of defence as the first instance organ for the access to public information, has been receiving around 30 – 45 requests per year (2015 - 2018). Lately the number has significantly increased, until 31.7.2019 was 120 – from this there were 110 received in one day. The Ministry designated an employee responsible for dealing with requests for free access to information.

The Ministry explained that in cases when classified data were requested, they had been performing the harm test in every request procedure. In 2017 came the ruling of the administrative court, stating that the harm test is in essence conducted already with the decision declaring the document as secret – and that there is no need for another test when the document is requested in the procedure of access to public documents. In practice there has not been any occasion when the harm test would result in removal of the level of secrecy.

The Ministry/Armed Forces of Montenegro is one of the institutions in the country with the highest number of classified data. The vast majority of such data is classified as RESTRICTED. In 2012, the Ministry/Armed forces of Montenegro removed the secrecy label from approximately 20.000 documents. All these documents were very old, originating from 1945 on. There is no case of removing the secrecy label before the expiration of a deadline, i.e. none of the periodical assessments of classified information performed by a commission established within the individual state authority have resulted in a removal of a secrecy label.

The Directorate for classified data is an independent state body, its supervision is conducted by the Ministry of Defence. Ministry conducts its supervision over the implementation of the legislation and administrative acts and activities. It issues personal and facility security clearances for the classified information and it decides on restriction or termination of such clearances even before the expiration if it establishes that person holding security clearance does not handle or safeguard classified information in accordance with this law and other regulations or that he/she does not anymore fulfil conditions necessary for the issuing of security clearance. The Directorate has so far issued a large number of security clearances and only a few facility security clearances. Before issuing a security clearance a vetting procedure shall be carried out. The aim of this procedure is to establish the facts significant for the issuing of security clearance. The request for the vetting procedure is submitted by the Directorate, the procedure is then carried out by the National Security Agency according to the written consent of the person cleared. After completing the vetting procedure, the National Security Agency submits the report to the Directorate with the recommendation for issuing or refusing of the security clearance. The Directorate then decides to issue or refuse the clearance. A person subject to vetting procedure is entitled to inspect the collected information, except the information regarding sources and the manner of their collecting.

The Directorate also enables the access to classified information to a foreign legal entity under the jurisdiction of the other state and to a person with the nationality of the other state, or by the international organization he is a member, in accordance with the international agreement. It also informs the holders of a security clearance that they are entitled to submit the request for prolongation of validity of security clearance (this obligation of the Directorate might be abolished by a forthcoming amending of the Law on classified information). It is responsible for providing the implementation of standards and regulations pertaining to the protection of classified information and coordinates activities that ensure their protection. It keeps and manages records on issued security clearances and establishes and maintain the Central Registry and sub-registries of classified information. The Directorate also has many responsibilities related to the classified information of EU and NATO.

One of the Directorate's core and important tasks is to undertake measures in order to train users of classified information and bodies for handling of classified information in accordance with standards and regulations. It performs e-learning activities and seminars. The applicants for the security clearance have to participate in the process, they take a test consisting of several questions that they have to pass in order to get the clearance. They also perform periodical annual classes for the holders of the security clearances. We hereby recommend that the Directorate properly trains and educates certain employees of the individual authorities so these employees could then perform internal trainings within their authority (the so called "train the trainers" principle). Such a solution would in our opinion relieve and take some burden of the Directorate and contribute to effective and regular training within individual authorities. It would also raise awareness regarding the importance of handling of classified data and its purpose. In that way it could also contribute to more precise and thoughtful designation of classified data and determining its classification level by the competent authorities.

The Directorate is responsible for the inspection supervision over the enforcement of the Law on classified information and implementation of the international agreements. It has to be taken into account that the Directorate only performs administrative supervision and checks the formal procedure of determining the information as classified and the measures for its protection, but does not check the content of the information and thus not contribute to more precise and thoughtful designation of classified data. The supervision is conducted through the competent inspectors. The internal control in larger authorities is carried out by the inspectorates and in the rest of the authorities by individual employees. They notify the Directorate of their findings and the Directorate also conducts inspections on the basis of these findings.

The supervision of the legality of work of the Directorate is conducted by the Ministry.

The Law on classified information is currently in the process of being amended. A working group has been formed to prepare the amendments. The public consultation in the duration of 30 days has been taking place for the second time. The inspection supervision is supposed to be a bit more precise, also the penal provisions will be amended in order to make it clearer and more precise. It was confirmed that the suggested amendments of Art 3 and 12, that had raised most concern among the public, especially non-governmental organisations, will be taken out of the draft law. The individual authorities that produce the most classified information will be obliged to prepare internal regulations that will set up the criteria for uniform classification of certain categories of information.

### Ministry of interior

The Ministry of interior is the first instance body for free access to information that receives the largest number of requests. In 2018 they received 460 requests, 445 were resolved within the 15 days deadline, 212 were rejected. There were 115 complaints over their decisions, 65 applicants have pulled their complaint and 13 were rejected by the second instance decision.

The Ministry of interior has reported on an individual case in which the Administrative court issued a decision regarding a classified document. According to the Ministry, the Law on classified data prevents the person responsible for free access to information to obtain, review and consider possible declassification of a classified document in order to deliver the information to the applicant. According to the Ministry, only the person within the ministry that set a classification level can consider declassifying the document.

### The Police - Analytics and Development department

The Analytics and Development department, established within the Police, also deals with the requests for free access to information. The department received 56 such requests in the first half of 2019, 29 of them were granted, 5 were transferred to other authority, 1 was referred to the web page where the information was published, others were denied or rejected. The majority of the requests were filed by media and non-governmental organisations.

### Ombudsman

Over the past three years, the Ombudsman has received 53 (2017), 51 (2018) and 2 (2019) requests for free access to information. All requests have been dealt with and answered. The majority of requests have been filed by non-governmental organisations, especially in relation to spending financial resources and realisation of action plans.

In the last couple of years, the Ombudsman has actually received no complaints regarding free access to information (none in 2018-2019, 4 in 2017). In these 4 cases the matters were referred to the Agency and the Ombudsman followed the further procedure. The agency adopted decisions and served them to the applicants.

Until 2016 the number of complaints was much higher (31 in total in 2016, mostly filed by non-governmental organisations, addressed to state and local self-government authorities), the majority of them was filed due to administrative silence and disrespect for the administrative court decisions. In the same year the recommendations were issued in that field. These recommendations have been followed and complied with. The violations that were identified on ground of complaints were corrected. In cases of administrative silence, the ombudsman does not adopt meritorious decisions, however it instructs the authority in question to issue a decision. The Ombudsman shares the opinion that the extension of a deadline to provide answer to the applicant is a possible solution in order to combat the increasing and large amount of administrative silence. The Ombudsman is of the opinion that the current solution in the Law on free access to information that a decision on denying a request for access to information that contains data that indicated as classified information cannot be appealed, is not appropriate and that the possibility of a complaint to the Agency against the decision of the public authority on the request for access to information should also be possible in these cases. The Ombudsman is also of the opinion that the provisions of the Law on free access to information should be adapted to the provisions of the Law on administrative procedure, of course having in mind

the specifics of the individual procedures. The ombudsman also recommends a complete assessment of a current situation in the field of classified data.

The ombudsman itself issues opinions, including recommendations on the measures that have to be taken to eliminate the violations and the appropriate deadline to do so. They often refer to the jurisprudence of the European Court of Human rights. They are also very engaged in a proactive activity.

The Ombudsman received one complaint regarding personal data protection in 2019. They have contacted the Agency who conducted an inspection and identified some irregularities and deficiencies. In the previous years no such complaints have been filed.

## JUDICIAL REVIEW

The Administrative court is *inter alia* responsible for the judicial review over the legality of the procedures and decisions regarding free access to information. At the meeting with the Administrative court, the court expressed its concern and awareness of the fact that a large number of lawsuits are being raised against the procedures of the Agency responsible for free access to information. The law on administrative dispute enables clients to request for a public hearing in any given case. In cases regarding free access to information this possibility is seldom used for earning profit on the account of administrative silence disputes.

In order to cope this issue, we discussed the possibility of using the current general provisions of abuse of the law. The institute of abuse of the law is currently introduced within the Law on general administrative procedure and the Law on administrative dispute. The mentioned institutes have so far not been applied in any individual case concerning free access to public information (not even in the current circumstances). We would like to emphasize that the application of such a provision is always delicate, especially in cases concerning free access to information where the applicant does not need to show any legal interest or other justifiable cause for gathering information.

The procedure of the court to deliver a decision in merits is long regarding the need for promptness in cases dealing with free access to information. The court explained that they are working according to their priorities and capacities. The Administrative court is covering over 200 legal areas with 15 judges, each of them handling approximately 1500 cases. There has been a significant increase of new cases in 2016. An independent analysis, conducted by SIGMA, showed that the most drastic increase of lawsuits was against the Agency for the protection of personal data and free access to information for the reason of silence of administration.

The current legislative solution does not provide the Agency with the capacity to review the decision denying access to a classified document. Against such a decision of the first instance body an applicant can only raise administrative dispute. Taking into account the nature and length of the procedure before the administrative court, this legislative solution prolongs the length to deliver a decision in cases regarding free access to information, where delivering a prompt decision is of essential importance.

The court further explained their practice regarding the review of legality of a decision denying access to a classified document. In this procedure, the court does not obtain the document itself – it only decides on the base of a decision that has assigned the document with a certain level of secrecy. In our

opinion this solution raises questions – does this solution provide an effective remedy to the applicants whose access was denied?

A general impression reflected from the NGO reports and the judicial practice of the Administrative court indicates a finding that many administrative decisions are insufficiently reasoned and that they do not render the possibility to review the merits of the case. The reasons for this are *inter alia* vaguely regulated exceptions to free access to information. The term *business secret,* for example, lacks a more detailed definition of what entails a *business secret.* Many reports also indicate that the first instance body's decisions are vaguely or insufficiently reasoned.

### PROCESS OF AMENDING THE LAW ON FREE ACCESS TO INFORMATION

The Ministry of public administration is leading the working group for the amendment of Law on free access to information (LFAI). The working group consists of representatives from the Agency for the protection of personal data and access to public information, Directorate for classified data, Ministry of justice, representative from the NGO sector (MANS), Administrative inspection and the representative from the Administrative court (who has declined cooperation due to the division of power) and an outside expert (Dr. Anamarija Musa). The Ministry has explained that the working group is functioning well and in a good working atmosphere. Up to the meeting of this peer review mission on 24/7/2019 there have been 7 working group meetings, recorded with minutes for each meeting.

As preparatory activities for the drafting of legislation changes, an analysis on this subject has been conducted. The Ministry has analysed the requirements of the NGO sector and the government sector in an analysis from April 2019[5]. A thorough research on this subject was also conducted

From these reports derive the necessity to amend the LFAI so that it will serve its purpose. The Ministry has outlined several issues that need to be tackled with the legislative amendments to improve the current status of right on free access to public information:

- the level of proactively published information, which is not satisfactory to the point that it would serve the need for the majority of information seekers,
- the second instance body procedure - the review if the first instance body is in the possession of the information (current solution where the second instance body has to wait for another investigative body to perform an investigation so that second instance body could decide in merits is not functioning in practice).
- short deadlines which cannot be prolonged even for justifiable reasons (large number of requests/ large amount of documentation, etc.)
- the damaging practice of abuse of the law,
- the exception of *classified data.*

## IDENTIFIED PROBLEMS AND RECOMMENDATIONS

### FREE ACCESS TO INFORMATION

The free access to information system in MNE is currently undergoing necessary changes that will enable its future development. **The awareness among first instance bodies about the importance of**

[5] *Analiza normativnog okvira u oblasti slobodnog pristupa informacijama.*

**transparency necessarily needs to be augmented.** The occasions of hiding documents by not delivering them to the Agency upon request for their decision on the merits (about this problem speaks a concerning high number of initiatives to impose misdemeanours for the violation of Art 40 Para 1 Point 1, as described above); prolonging the decision-making process by hiding information or not delivering a decision in a timely manner; deciding NOT in accordance with court' instruction in case of classified data concerned, etc. – all these occasions are a cause for concern and call out for raising the level of awareness among first instance bodies on how to deal with individual request procedures.

A concerning cause for the dis-functioning of the system of access to public information is also a large number of complaint procedures that burdens public administration (the percentage of complaint procedures in relation to the number of requests received by the first instance bodies – the percentage is relatively high in comparison to Slovenia (MNE: 2014 (43%), 2015 (34%), 2016 (55%); SLO 2014 (8%), 2015 (8%), 2016 (6%)).

**The causes for this are numerous and have to do with:**

(1) insufficient proactive publication practice;
(2) abuse of the system of access to public information for making profit;
(3) inefficient procedure that allows obstructions and delays;
(4) insufficient and poor reasoning of the decisions, that are also a consequence of vague and unclear exceptions prescribed by law;
(5) low level of awareness about the importance of transparency and a distrust between public sector bodies and the civil society, especially NGO-s and journalists.

All of the stated problems are addressed below.

### Proactive publication

**The proactive publication needs to be set up as a standard and transparency "on demand" an exception to this standard.** This will lower the number of requests and consequently the complaint procedures that administratively burden the second instance body. On proactive publication of information there are many good recommendations from the 2018 Twinning capacity building light project, which are supported by a thorough analysis of the situation. Guidelines for the first instance bodies were prepared, and also the methodology for the implementation of recommendations. All the prepared materials should be made use of. They would first need to be published and their usage promoted among first instance bodies. For this purpose, one has to prioritise the allocation of resources carefully in order to see the recommendations through. It is our view and that of previous expert assessments that the Agency for the protection of personal data and access to public information does currently not have the capacity to implement the recommended changes. **Either the Agency is strengthened financially and/or in human resources or the authority regarding proactive publication is assigned to another public authority (for example the Ministry for public administration as it is the case in Slovenia).**

It is important to emphasise that with proactive publication the mere fact that the information is published does not necessarily make a document *transparent*. **Websites containing many documents have to be structured in a meaningful and user-friendly way, taking into account a typical information seeker.** This will enable the positive effects of proactive publication of the documentation, thus lowering the number of documents requested on demand.

**It would also be recommendable to establish collaboration with the NGO sector that has the knowledge and tools to implement the solutions on proactive publication.**

### The procedure to review if the first instance body is in the possession of the requested document

As described in the section 2.1.2.2. of this report, the current legislative solution does not provide for an efficient remedy in cases where first instance bodies deny access for the reason of not having the requested information. The current law does not provide the Agency with the capacity to enter the first instance body's office and perform an examination whether the first instance body indeed does not have the requested information in its possession. In such instances the Agency has to turn to an outside inspection working within another state body that performs an inspection to establish whether the first instance body is in fact not in the possession of the requested document. According to LFAI (Art 40, Para 2), the inspection should be performed and conclusions delivered to the Agency within 5 days after the request by the Agency. Deriving from the annual reports 2014-2016 the law is not applied accordingly and the solution is not functioning in practice. As a result, free access to information is *de facto* denied or at least significantly delayed.

According to Slovenian legislation the Information commissioner has the inspection authority to inspect the premises and documentation of the first instance body when the first instance body has rejected the request with the argumentation that he is not in a possession of the sought document (so called "*in camera examination"* without the presence of the client). **Our recommendation is to introduce a similar solution to the LFAI as is our *in-camera examinations* in Slovenian legislation.**

### Abuse of the law on free access to information

It is clear from the reports and statistics of every stakeholder that current circumstances allow the abuse of access to public information system for obtaining financial profit. The current situation is damaging the system of free access to public information. It is a concerning issue that needs to be addressed urgently.

In order to cope with the mentioned problem, we have identified three possible solutions that were considered by different stakeholders that we have been communicating in the course of this peer review mission. The most important is that the solution is accepted in consolidation with government and NGO sector in order for the solutions work in practice. Every solution has its strengths and weaknesses and we are trying to present them in the most transparent way as possible. We have ranked the solutions from the one that in our opinion enjoys the highest-level consensus between the stakeholders to the one with the least.

i. **Removing all costs (court fees, administration fees and advocacy fees) from free access to information procedures at all stages.**

The Analysis of the law on free access to information and recommendations for improvement from June 2019 refers, inter alia, to the solution regarding cost (pages 41-44 of the analysis) in an adequate way, and we agree with the suggested recommendations therein. The root cause of the problem is that the Law on administrative dispute entitles a client of administrative dispute to request for a public hearing, even if lawsuit is being raised on an issue of administrative silence, which is generally a simple case that does not require a profound legal reasoning and discussion. In the case of a public hearing before the administrative court, the lawyer representing the case is entitled to a higher remuneration. When a client requests for a public hearing, the court does not have the discretion to discard the

request. Furthermore, when the court holds a public hearing, all expenses (including legal representation costs) carries the defeated client. The solution from the named analysis recommends:

a. Removal of administrative and judicial fees (recommendation 9.1).
b. To amend LFAI so that each party carries its own costs in administrative and in a court procedure (recommendation 9.2).
c. To amend the Law on administrative dispute so that the court would have the discretion to refuse or discard the client' request for a public hearing in cases of administrative silence – when the court would estimate that the public hearing could contribute to the case, than it could uphold the public hearing (recommendation 9.6).

| Strengths | Weaknesses |
|---|---|
| By removing all costs from access to public information procedure, any intent to follow the request only for the reason of receiving profit would be in vain, thus the solution would solve the problem. | The danger that an applicant with little resources and a justifiable request will not be entitled to have his legal representation costs returned, which can raise questions regarding access to court and "equality of arms" that is part of the concept of *fair trial,* which is a fundamental right. |
| Free access to information right is more accessible. | The danger that by easing the accessibility to the court may cause overburdening the court with "unfounded lawsuits." These lawsuits would be than "stealing" the time from court to deal with those cases that are better reasoned and founded in merits or have a more justifiable cause. |

We are in favour of this solution and in observation to the input we received from different stakeholders we believe that this solution enjoys the highest level of consensus. We believe that the mentioned analysis adequately addresses the problem and that it includes all necessary observations.

**ii. Extending the deadlines**

| Strengths | Weaknesses |
|---|---|
| May solve the problem of the abuse of the system (earnings on the account of administrative silence disputes). | The danger is that first instance bodies that are not prone to transparency would "use the opportunity" to deal all requests in accordance with the longest deadline (also simple requests that could be resolved quickly). |
| Will help first instance bodies who objectively cannot resolve the request in the short deadline, to resolve within the deadline. | |

With extending the deadlines it is important that first instance bodies are aware that *justice delayed means justice denied*. This is especially true in cases with free access to public information. Therefore, if the possibility of the prolongation of the deadlines is adopted than all democratic institutions established to protect the right to access to public information as a human right (especially the Agency, the Ombudsman, the Ministry for public administration, etc.) should note to be very much attentive of the application of the provisions. They will have to find ways to raise awareness and call to responsibility those liable public bodies that do not respect the essence of delivering a decision in a timely manner.

If the solution on the prolongation of deadlines is accepted than it would be our recommendation to introduce the prolongation of the deadline as **a possibility**, in justifiable cases (large amount of documentation requested, etc.). The prolongation needs to require a procedural conclusion issued by the time that the fifteen days deadline expires. The conclusion must contain an explanation of reasons for the prolongation of the deadline. The applicant needs to have a legal remedy regarding this conclusion.

**iii. introducing an institute of abuse**

| Strengths | Weaknesses |
|---|---|
| May help to reject the requests for which the aim is not acquiring information but abuse of the system. | The danger is that first instance bodies would "abuse the institute of abuse" by rejecting every request that does not come from a favourable applicant or that the requested information is not in favour of the liable body or official. |
| | Low level of consensus – especially among the NGO sector. |

The application of this institute can be challenging in practice from the perspective of argumentation of such a decision and because of the danger of abuse of the institute by the first instance bodies. In essence the application of this institute has to be limited to a very few examples. It has to be interpreted extremely strictly since it has to be the last resort (*ultima ratio*) – therefore all other steps have to be taken before rejecting a request due to the abuse.

We need to emphasize the fact is that the institute of abuse raises the most resistance from the civil society – especially the NGOs. As already mentioned, it is recommended that the legislative solution to work in practice should be accepted in consolidation with government and NGO sector. One of the key purposes of free access to information system is to bring closer the civil society and the governmental sector. The fear from the NGO sector is a possibility of misuse of the institute of abuse by first instance bodies. If hypothetically, the institute of abuse was introduced and, then the first instance body rejected the request on the account of abuse – where this would objectively not be justified - the applicant would be denied access without consideration of the merits of the case. Upon appeal, the considerations of the second instance body would deal with questions that are irrelevant to the transparency of a requested document, such as: is the applicant excessively using his right, how many times has he been turning to the same body, how will resolving his request influence the rights

of other or the public benefit, etc. This could result in denial of access or unjustified delays. If these examples were numerous, the system of free access to information would not work for the applicants.

The purpose of introducing an institute of abuse would be to prevent the massive complaint procedures from certain applicants aimed for making profit from free access to information procedures. The abovementioned analysis from June 2019, elaborates on the legislative framework and international standards regarding the institute of abuse. It needs to be stressed that it emphasises that the institute of abuse would not be necessary to tackle the existing problem if other measures, such as the solution of costs, would be adopted. In addition, there already exists an institute of abuse (for the abuse of procedural provisions) as a general provision in the Law on administrative procedure and also in the Law on Contentious Civil Procedure (that is used in cases when the Law on administrative dispute does not state otherwise). These institutes were not used for the purpose of preventing the existing practice of abuse, or challenged before the court so that they would result in a case law. Since the occurring problem with excessive number of lawsuits is of procedural nature, it is questionable how an additional institute of abuse in the Law on free access to information would in fact add to the solution of the problem.

It also needs to be emphasized that the analysis from June 2019 has expressed a concern regarding possible abuse of the institute by the first instance bodies. It has also listed several protective measures to be taken for a proper implementation of the institute, such as education activities for the first instance bodies, obligatory preparation of guidelines on how and when an institute of abuse could be appropriate etc. The adoption of the institute is recommended as an alternative to the amendment regarding costs (recommendation 4.1).

**We are aware that the institute of abuse is part of legislation on free access to information from many European countries (including Slovenia), and of international conventions (including conventions from the Council of Europe). However, deriving from the purpose of the free access to information system (that should increase the transparency of and confidence towards public bodies from the civil society), it is in our observation counter-constructive towards this purpose if the institute of abuse was adopted within the current circumstances in MNE. We also share the opinion from the analysis that that the introduction of this institute is not necessary to solve the current situation, under the condition that the solution of costs is adopted.**

### The exceptions: law and practice

The legal frame to apply individual exceptions is too wide and offers the liable public bodies too much space to apply the exceptions in an arbitrary way. Such legal provisions and practice is not in conformity with the constitutional aspect of narrow interpretation, when it comes to exceptions that limit or intervene with human rights. The legal awareness on these topics has shown to be rather low. Many reports indicate poor or insufficient reasoning of the administrative decisions. An awareness needs to be raised regarding the application and the purpose of each exceptions according to law.

#### *Business (trade) secret*

According to Art 14 of the Law on free access to information (Official Gazette of the Republic of Montenegro, No. 044/12, 030/17) the public authority may restrict access to information or a part thereof if it is in the interest of following: protection of privacy from disclosure of personal data prescribed by Law; security, defence, foreign, monetary and economic policy of Montenegro, and particularly information containing data marked as classified, in accordance with the laws regulating

the field of data secrecy; prevention of investigation and criminal prosecution; performing the official duty in regard to protect disclosure of the certain data; protection of trade and other economic interests of the publication of data which relate to the protection of the competition and business secret in connection with business property rights; if the information is a business secret or tax secret in accordance with law.

In Montenegro, the institute of business (trade) secret is one of the most widely used exceptions used to restrict free access to information. As such, it is of the utmost importance that the institute is clearly defined in the legislation. Currently that is not the case. The Criminal Code (Official Gazette of the Republic of Montenegro, No. 070/03, 013/04, 047/06, 040/08, 025/10, 073/10, 032/11, 064/11, 040/13, 056/13, 014/15, 042/15, 058/15, 044/17, 049/18) states in the Art. 280 that revealing a business secret is a criminal offence. Business secrets are generally considered to be data and documents which by law, other regulations and decisions of competent authorities passed on the basis of law, are proclaimed a business secret, revealing of which would or could cause harmful consequences for a company or other business entity. However, in Montenegro only a few provisions of the individual laws refer to business secret, leaving it without a uniform, clear and precise definition.

As an example, the Banking Law (Official Gazette of the Republic of Montenegro, No. 017/08, 044/10, 040/11, 073/17) defines the institute of bank secrecy, and also states that banking secrets shall represent a business secret. The following shall be considered a banking secret: information about the account holders and their account numbers opened in a bank; information on individual deposit accounts and transactions in individual accounts of legal persons and natural persons opened in a bank; other information on a client in the bank's knowledge obtained on the basis of providing services to the bank client..

It is of utmost importance to establish a uniform, clear and precise definition of the term "business secret". It should follow the criteria established by the Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

It is also important to identify the circumstances in which legal protection of business secrets is justified. For this reason, it is necessary to establish the conduct and practices which are to be regarded as unlawful acquisition, use or disclosure of a business secret. The unlawful acquisition, use or disclosure of a business secret by a third party could have devastating effects on the legitimate business secret holder, as once publicly disclosed, it would be impossible for that holder to revert to the situation prior to the loss of the business secret. **Its protection should not, however, extend to cases in which disclosure of a business secret serves the public interest, insofar as directly relevant misconduct, wrongdoing or illegal activity is revealed.**

Another thing that has to be noted is that, unlike other reasons for restriction of access to information (ex. protection of privacy, classified information, prevention of investigation and criminal prosecution, performing an official duty, protection of trade or other economic interest) the restriction of access on the ground that the information requested is business (or tax) secret, is not time-limited. When adding the fact that no business or tax secret has so far been removed on the state level, it is obvious that this is an extremely strong exception to the free access to information and it therefore has to be regulated in a clear and precise way in line with relevant European and international standards.

We recommend that the definition of business secret follows certain criteria, especially that such information would be defined as: containing unrevealed expertise, experience and professional knowledge that is secret in the sense that it is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question, has commercial value and it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. Information that is public by law or information about breach of law or good business practices cannot be classified as business secret.

**It is also important to notice that the institute of a business secret by nature belongs to the private, not the public sector, especially to small and medium-sized enterprises and non-commercial research institutions, while in Montenegro this institute is widely used as an exception to free access to information held by state authorities, public institutions and other public authorities. Such practice opposes the sole essence of the institute of business secret, explained above. Documents that refer to state funding of certain subjects and enterprises or any other documentation referring to allocation of budgetary funds should also not be proclaimed as business secret. The same stands for the salaries of the public employees and for various statistical reports (ex. concerning possible state aid).**

*Classified information*

The other widely used exception to restrict free access to information is the interest of security, defence, foreign, monetary and economic policy of Montenegro, and particularly information containing data marked as classified, in accordance with the laws regulating the field of data secrecy. These interests currently mean an automatic rejection of the request to free access to information according to Art 1, paragraph 2, point 2 of the Law on free access to information. It should and may not mean an automatic rejection. **A mandatory harm test should be implemented and conducted in each individual case where public access to data is restricted on the basis that the information requested is classified in accordance with the laws regulating the field of data secrecy.** We recommend that a uniform, clear and precise methodology on how to perform such tests is drafted. Its basic elements and the way how to implement the harm test by the public authorities should be specified. The Agency for personal data protection and free access to information could probably be the authority competent to provide detailed instructions on the methodology of conducting the harm test in order to protect the overriding interest.

Currently the institution that determines the information as classified, has total control over the information and no mechanisms are practically in place to remove or change the classification level. According to Law on classified information (Art 19b) such level could be changed by performing a periodical assessment of classified information based on which level of secrecy can be changed or declassification can be done. The mentioned periodical assessment is performed by a commission established within the state authority. This procedure practically never results in removal or change of classification level. Also, no regulations that would determine the methodology of such assessment are in place.

There is no independent body that could perform a check whether the ground to determine the information as classified were/are at place, whether classification was necessary in a democratic society and whether the interest that disclosure of such information to an unauthorized person has or might have harmful consequences onto security and defence, foreign affairs, monetary and economic

policy of Montenegro prevails over the interest for free access to information. In case the latter interest prevails, the access to information should be granted, except for the top or top two levels of classification (top secret, secret – the vast majority of classified information are given lower classification level) or classified information of foreign countries and international organisations.

We strongly recommend that such a procedure, and an independent body competent for its performance, are provided for by law. The independent body should have access to the decision that designated the information as classified and to the classified document itself. Authorised personnel of the independent body should of course be able to access the classified document in accordance with the provisions of the Law on classified information, i.e. persons performing access should hold a security clearance and solely access to classified information within their area of responsibility. It could also be useful to provide the independent body with the possibility to contact all recipients of such information and obtain their opinion on the matter. Given the current state, it would probably be most appropriate if the Agency is designated as such an independent body (in the complaint procedure regarding free access to information). The independent body should adopt mandatory decisions and mechanisms should be in place to enforce it. The Directorate for classified data only performs administrative supervision and checks the formal procedure of determining the information as classified and the measures for its protection, but does not check the content of the information.

The other matter in question is the role of the Administrative court. It is important to emphasize the procedural differences when free access to information is restricted on the ground that the data is classified. In such a case an appeal could be lodged straight to the Administrative court and not to the Agency which is the case when other restrictions are used. We recommend the solution that in cases when the requested document is assigned with the two lower level of secrecy, the appeal could be lodged to the Agency and not straight to the Administrative court. In this way the procedures regarding free access to information would be faster for the applicant (the court proceedings everywhere are usually lengthier than the second instance administrative proceedings). According to the current solution if the Administrative court determines that the formal procedure of determining the information as classified was not performed in line with the provisions of the law, it returns the matter to the state authority in question to perform it again. The Administrative court does not rule on the merits and consequently no classification labels are removed.

In our opinion it would be recommendable that in cases of rejected requests for free access for the reason that a document is assigned with any of the two lower levels of secrecy (‘*restricted’ or ‘confidential’)* the Agency as the second instance body should have the jurisdiction to review the document itself and to establish if the document meets the criteria from Law on classified data. In such a case the Agency should also have the power to instruct declassification of the document.

Also, some internal regulations and rules on how to determine the information as classified, issued by certain public institutions, are labelled as classified which additionally reduces the transparency of the procedure. The same goes for some decisions that designate the information as classified and determine its classification level. These decisions should contain a detailed explanation/argumentation (harm test) in order to justify why the disclosure of such information to an unauthorized person would have or could have harmful consequences onto security and defence, foreign affairs, monetary and economic policy of Montenegro. These decisions should not be labelled as classified, therefore they should be adopted in a way that the classified information as such could not be disclosed or possible

to comprehend. Potential harmful consequences for the security of the state and its protected interests that would derive from the disclosure of information to an unauthorized person should be precisely determined. These harm tests should also always take place during the periodical assessment of classified information which is currently not the case.

We also notice the practice that some information or documents are in advance determined as classified, for instance all documents referring to certain project, working group or matter. Such practice should be abolished, the content of every single information and its importance for the protected interests of the state has to be evaluated and designated as classified only if it fulfils these conditions. **The practice of designating classified information in advance opposes the essence of the institute and is as such not acceptable.**

Finally, it is important to emphasize that court decisions have to be strictly followed and enforced. We were notified of a case where the Administrative court has annulled the first instance decision and ordered the first instance body to review the merits and consider removing the level of secrecy since the explanation from the decision assigning the classification level does not meet the required criteria from the Law on classified data. The first instance body has not followed the court decision and has once again issued the same decision with the explanation that the person in charge for dealing with free access to information requests is not authorised to remove the level of secrecy – only the person that assigned the level of secrecy has that authority. The applicant took the second decision of the first instance body once again to the Administrative court who repeated its first ruling. The case has been juggling between the first instance and the court for years with no promise of an effective closure. At the time of the meeting (24/7/2019) the case was pending before the first instance body to make its third decision on the same matter.

### *Protection of personal data as an exception to free access*

The public authority may also restrict access to information if it is in the interest of protection of privacy from disclosure of personal data prescribed by Law. This exception to free access to information does not include public officials in connection to the exercise of public function, as well as incomes, assets and conflicts of interest of those persons and their certain family members. It does also not include resources allocated from public funds, except for the social benefits, healthcare and protection against unemployment. **Nevertheless, this exception is often used in a broad and very extensive way in order to protect information on public officials. In that way it is often more difficult to access information on public officials (especially high ranked) than information of the "regular" citizens: the lead principle should be opposite, public officials should be more exposed to public control,** because they have greater power and responsibility. Sometimes also information on enterprises are protected as personal data which is not in line with data protection principles. Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The information on enterprises do not comply with these criteria and cannot be protected as personal data.

### Awareness raising and building mutual trust between the public authority and civil society

Raising awareness of the importance of transparency needs to become a common goal of national importance since it is an important pillar of democracy. For this reason, a common strategy is lacking where all of the stakeholders (the Agency as the second instance body, the Ombudsman, the Ministry of Administration, the Parliament and the Government) **need to become the promotors of transparency. A good approach can also be an overall national strategy anticipating concrete awareness raising missions that will help to implement the missing factor towards a transparency-oriented society.**

Reports that informal mechanisms to access information are used over formal ones is a concern. This can show that in Montenegro the first instance bodies are not by default against sharing information, but they are rather uncomfortable if they have to formally disclose the information. In our experience this can be the consequence of an imaginary fear from the responsibility. The informal way on the other hand is always less documented and there exists a sense of lower responsibility. **This approach is wrong and needs to be turned. A general sense that also the governmental bodies, will benefit from transparency has to be promoted and incepted into every formal decision-making process.** When this change-of-mind will be incepted, the cases of hiding the documentation by obstructing the process will be lowered or even minimised.

The former mentioned can in our opinion only be achieved with an awareness raising activities that will involve both public bodies and NGOs, the journalists, individuals and all other relevant stakeholders who are (or are supposed to be) the overall concerned with the free access to information right.

Awareness raising activities can be in numerous forms from wide-ranging (ex. *overall strategy on a national level to promote transparency*) to very narrow and miniature (ex. individual workshops on *how to write a request*, online campaigns, etc.). **We strongly recommend that these activities are used as a method for building a bridge between the public bodies and the civil society.**

## PERSONAL DATA PROTECTION

### Law on personal data protection

A working group consisting of 5 members (3 members from the Ministry of Interior, including the chair of the group, and 2 members from the Agency) has been formed to prepare the new law on personal data protection. They have so far not held any official meetings. The Agency was previously not much involved in the process of drafting but the situation has recently improved and the Agency has since been engaged in the drafting in a sufficient way. The majority of group members are constantly in touch via phone and e-mail and all correspondence has been shared within the group by its chair. They have received some help and support from the independent EU experts during the drafting process. The public consultation on the first draft of the law was held, approximately 40 comments were received. All of them were considered and examined and most of them were included in the draft law, according to the Ministry. The report on the public consultation consists of 230 pages.

**It is important to underline that the law in question is of extreme importance and deals with a very complex and sensitive topic. Data protection laws in EU have been thoroughly prepared by leading state and other experts. In some cases, this process took several years. Therefore, we strongly recommend not to rush with the preparation and adoption of the law. Taken into consideration the**

**complexity and importance of the law, we suggest to deal with it systematically and with caution, to involve all relevant institutions and other entities, governmental and non-governmental, in order to come up with the best possible draft of the law.**

The intention of the draft law is to align the area of data protection with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter: GDPR) on one side and with the 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 (also known as the "Police Directive" or "Law Enforcement Directive"; hereinafter: LED).

Since the provisions of the draft law, as mentioned above, are intended to harmonise the area of data protection with both, GDPR and LED, we suggest to consider the solution would to create a separate chapter of the draft law that would deal with specifics of the LED. In that way, the exceptions to the general provisions of the draft law that are specific to LED could be regulated in this separate chapter. Exceptions should apply in particular to the purposes of processing, right of access of the data subject, informing of the data subject, data quality, automated decision-making, logging, transfer of personal data to third countries and other issues that need to be regulated differently following the provisions of the LED. Those provisions should be clear and precise and in the best possible way bring added value and contribute to legal clarity. They should also offer useful information that would facilitate the harmonisation with the LED and applicability of its provisions.

When listing the tasks and powers of the Agency regarding processing by competent authorities for special purposes, it should be kept in mind that this important issue should be regulated as far as possible in a similar way to the GDPR. Powers of the Agency should be effective and enforceable. In that way both, LED and GDPR, would be homogenously interpreted and would in that way contribute to consistent and coherent practice in the field of data protection.

This kind of methodology would make the draft law more structured and most of all, easier to read and comprehend.

The draft law should also be clear and precise in determining that processing by competent authorities which is performed for purposes other than for special purposes determined by LED, falls under the scope of this law and is governed by its (general) provisions. Such solution would, in our opinion, significantly contribute to the legal clarity and certainty of the Law and the legal security of data subjects.

We emphasize that the draft law should precisely determine the right of access of the data subject, since the current data protection legislation does not address this right in an adequate way. The legislator has to ensure that the data controller provides and communicates information to the data subject in a concise, transparent, understandable and easily accessible form, using clear and plain language. At present, data subjects in the vast majority of cases (over 90%) exercise their right of access indirectly, through the Agency which means additional work for the Agency. It has to be noted that the right of indirect access is not foreseen in the GDPR. It is though foreseen in the LED, but only as a

possibility to exercise the right to information, access or information about refusal of rectification or erasure by the data controller through the competent supervisory authority (the Agency) when these rights have been restricted by the controller on the basis of legislative measures allowing for restrictions, and not where these rights could be exercised directly with the data controller. We recommend to follow this example when determining the possibility of indirect access in the draft law.

### Police data protection

According to the Law on Internal Affairs (Official Gazette of the Republic of Montenegro, No. 44/12, 36/13, 1/15, 87/18) collection and processing of personal and other data is a police power (the police has a total of 14 powers). As a rule (Art 38), data shall be collected directly from the person they refer to. If it is not possible to collect data directly from the person they refer to, or if such collection would jeopardise use of police powers, data may also be collected from other state authorities, state administration bodies, local self-government bodies, organisations, institutions or other legal or natural persons. The abovementioned authorities and legal and natural persons, which under the law, within their jurisdictions keep data records, shall upon the police request provide the information necessary to carry out statutory duties and powers under its scope of work or jurisdiction.

The Police shall keep proper records on collected, processed and used data. Currently 17 such records are managed and kept by the Police. According to the Law on Internal Affairs the Police shall obtain approval issued by the Agency prior to establishing these records. This provision is not in line with the data protection standards, has not been applied in practice and should therefore be deleted.

The data retention periods for all records are also determined by law. When these periods expire, re-consideration of further keeping of data for police purposes shall be done. Data which keeping is not justified shall be deleted from records upon expiry the period prescribed for their keeping. The mentioned reconsideration is not in any way further regulated, nor in the law nor in the by-law. Therefore, many questions regarding it remain unclear, especially who performs such reconsideration and on what criteria it is based on, where and for how long is it kept, the further retention periods if their further retention is justified and who and under what conditions can access the data. Usually such reconsideration is done by the employee that works on a specific case and he also sets the further retention periods. The procedure should be regulated in an appropriate and transparent manner.

The form, content and manner of keeping records (except for the DNA analysis record that is regulated in a specific law on DNA register) shall be laid down by the Ministry of Interior. The Ministry adopted Rules on the form, content and manner of keeping records on collected, processed and used data and international data exchange (Official Gazette of the Republic of Montenegro, No. 51/13, 45/15; hereinafter: Rules). These Rules contain 21 provisions and a vast majority of them deals with the content of the individual records. It contains only one short and superficial provision on the form which states that records shall be kept in a written or electronic form. There are no provisions on the access to data, awareness raising training of the police officers, logical and technical safety measures and procedures, protection of facilities and premises, IT equipment protection, internal controls and supervision and other important aspects of data protection.

The content of each individual record is prescribed in detail in the Rules. The content of some records is quite extensive, especially records on operational information, wanted persons and criminal intelligence on terrorism and international organized crime. We recommend to review the content of each individual record, having in mind the principle of data minimisation as one of the basic data

protection principles. Records should therefore only contain data that are not excessive, i.e. that are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. We also suggest considering the possibility that the law and not the rules would prescribe the content of records. In that way all relevant acts of processing (collection, providing, exchange, storage, blocking, deletion) would be determined by law.

Records are mostly kept in a written form, some also in electronic form. The form is uniform and the data is synchronized on a state level within a month. We recommend setting up a central automated electronic system that would enable keeping electronic records. Such system should be established as soon as possible, of course having in mind that subsequent financial and technological resources would have to be provided in order to achieve this goal. The setting of such a system would significantly contribute to legal safety of the citizens and transparency of the police work.

It should be noted that the Law on Internal Affairs (Art 45) provides the data subjects with the right to access the data. It states that a person to whom the information in the police records relates, shall have the right to access the data. This right can be exercised pending certain events (for instance, final and enforceable ruling on confirmation of the indictment, the information archiving or final and enforceable ruling to terminate the investigation). There are no written forms that would facilitate the exercise of this right and no central point that would reply to such request. The reply is therefore provided by the police unit that receives the request to access data. The time point after which the data subject can access his data in some records is described very generally and vague; i.e. once the reasons due to which they were kept ceased to exist. The provision could be amended in a way that establishes more precise criteria to determine this time point. In order to provide more clarity, it would also be recommended to clearly define the obligation to inform the data subject whose personal data were collected without his consent and were not deleted. Such subject shall be informed thereof if it is permitted by the nature of police work. This provision is very wide, vague and open to many different interpretations therefore it should be more amended and set precise and clear criteria under which the data subject shall not be informed about the collection of his data. Such criteria could be obstructing official or legal inquiries, investigations or procedures, protection of national or public security, protection the rights and freedoms of other persons and similar.

So far, this right has barely been exercised by the citizens. Their awareness level is very low and efforts have to be made to raise it. Taken into account that citizens will eventually be more aware of their rights in the field of data protection the setting up of an automated electronic system of record keeping would facilitate the police work when dealing with such request from the citizens and enable to provide an accurate and swift reply to their justified request.

The police employees access the written data records after receiving an authorisation of their superior. Certain divisions are appointed on central and regional level that physically possess records. Access to records should be monitored and manually logged and also limited to the employees that need to access the data for the implementation of their work tasks. They should have access to the minimum scope of data needed to fulfil his work duties and tasks. There are also employees that are responsible for individual records and ensure that the processing of data in the records is conducted in accordance with the rules. We recommend that such persons are officially named as such and that their tasks and responsibilities are clearly determined. We welcome the fact that the Police has within its structure established the Analytics and Development department. It is important to provide the department

with enough resources to perform many tasks in the field of data protection that have to be fulfilled in order to reach an adequate and satisfactory level and comply with data protection standards and practices. The Analytics and Development department has been aware of the need to establish the central automated electronic system of records and has taken some effort and promised full support in achieving this goal.

The authorised police users access the electronic data records with a smart card pending entering their user name and password. The level of the access varies. The level of an individual employee is suggested by his superior and then granted and technically enabled by the Ministry of Interior. The whole data access regime of the police employees should be prescribed, based on a "need to know principle". This principle and not the principle of seniority has to be strictly followed when accessing the data records.

At the moment the internal control over the police is carried out by a special organisational unit of the Ministry of Interior. Internal control includes control of lawfulness of performance of police activities, in particular in regard to compliance and protection of human rights when performing police tasks and exercising police powers. It also includes implementation of counter-intelligence procedures and other control relevant for efficient and legal work. The internal control over police work is conducted by a police officer authorised to conduct internal control over the police. For the purpose of internal control, the authorised officer has several powers, including a power to review the records, documents and databases which in accordance with its jurisdiction are collected, compiled or issued by the police.

**Despite the appropriate legal basis, the internal control system has not been functioning.** It is therefore necessary to establish a complete and effective system of internal control regarding access to data in the police records. Every act of access and any other processing of data should be logged. These logs should not be kept indefinitely, but for a definite period of time. The content of the logs and access to them should also be precisely determined. The logs should be available to a minimum number of authorised users. Log checks should take place, not only reactive (following actions, complaints or based on certain indications) but also preventive (random periodical checks). Sanctions should be provided and imposed for any identified irregularities. The system of checks and controls has not been established within the police and so far, no employee has ever been fined or in any way sanctioned for the unlawful or excessive processing of the data subjects' personal data.

Establishing a system of internal control would mean a significant step towards awareness raising of the personnel regarding access and processing of data in the police records and other relevant data. The other step that has to be taken in the awareness raising efforts is the adoption of a complete data protection policy, including a general, "umbrella" document and specific documents dealing with certain aspects of data protection and information security (password policy, access management, IT environment and equipment protection, mobile device management, e-mail, internet access, external providers, …). On top of that it is vital to establish data protection education and training of employees. Such training should be periodical and could include various internal and external courses and other forms of training. All suggested methods are an important and urgent step in awareness raising process. Currently the Ministry of the Interior (HR division) performs some training. The police experts do not participate in this training and evaluate this training as insufficient and inadequate.

Important question that has to be considered is the relation between the Ministry of the Interior and the Police. Their relation has changed several times over the last decade (Police has during that period

been both, a body within the Ministry and an autonomous body). According to Art 22a of the Law on Internal Affairs the Ministry performs certain tasks regarding the Police. One of them is performing training and professional development of the police employees which means that the ministry is responsible for the realisation of methods and practices suggested above. Another important aspect of the relation between the mentioned institutions is the IT support. According to art 22a the Ministry projects, sets up, manages, develops and maintains information and communication technologies to provide appropriate work conditions for the work of both, the Ministry and the Police. Therefore, the police data records are kept in the system run by the Ministry and on their infrastructure. There are no contracts or other legal acts that would specify their mutual relation, rights and obligations. During the discussions with the employees we were not able to create a clear picture of the nature of that relation. In our opinion the relation is vague and unclear and due to frequent changes creates a confusion and a condition where many questions stay open, unprecise and subject to different interpretations. The Ministry also manages human resources for the police. The relation between the mentioned subjects, their organisation and structure, including the issue of funding (budget) has to be clearly regulated and not leave any room for confusion or ambiguities. The complete system of internal control and data protection training also has to be established.

As already mentioned, the Ministry also prescribes the content of each individual police record which is another important reason for thorough examination of their relation, organisation, structure and powers. We were informed that the police as such cannot adopt by-laws which is another aspect that should be reviewed. If the Police is an autonomous state authority then it should be able to adopt its own by-laws, including the content of its own data records. Currently the Ministry adopts all police specific by-laws, including the one that regulates the exercise of the police powers.

Civil control over the police is performed by the Council for civil control over the work of the police (hereinafter: the council). The council was established in 2005 and is a civil body that assesses exercise of police powers to protect human rights and freedoms. It consists of five members and may be addressed by citizens and police officers. The council has to act within 6 months from the date of the alleged violation. The police shall, upon request, provide necessary information and notifications to the council. This is exercised in different forms, either the police provide or send the required information or it makes it available to the council at their premises. The council can also inspect and review official notes. However, the council has no power or legal remedy to enforce a proper reply from the police. The police contact point is the Analytics and Development department. The department has shared the opinion that their mutual cooperation has so far been very positive, smooth and effective.

If the violation has occurred, the council issues recommendations that are submitted to the Minister of Interior who has to inform the council on the undertaken measures. Sometimes the recommendations are also submitted to the committees of the Parliament.

The authorised police officer with powers to conduct internal control over the police also acts, among others, upon analysis of assessment and recommendations of the council.

## ORGANISATIONAL IMPROVEMENTS

The Agency for the protection of personal data and access to public information is handling its documentation and archives manually, therefore a huge amount of paper is being used and piled

around the offices. Much can be done to improve these processes, notably in terms of digitalisation, which will in our belief contribute to the efficiency of the organisation.

# CONCLUSIONS

## ACCESS TO PUBLIC INFORMATION

The essence of free access to information is to build trust between the public authority and the civil society. The method is transparency. If the public authority is transparent than the civil society will trust the authority that it has nothing to hide and that it is doing in the civil society's best interest. Trust in good governance is essential for good democracy, because only under those terms, the coexistence of government and civil society will be fruitful, longstanding and channelled towards a common perspective that can bring prosperity. If this might seem utopic, it is only because of the current circumstances that prevent the transparency to work its way towards this common goal.

**Upon our visit we noticed a great gap between the civil society/media and the government.** We sense that civil society stakeholders generally do not trust the first instance bodies to be willing to disclose any information. Some applicants claim they would rather use informal methods that give them no legal security for a remedy, but that they are more successful in this way than if they used formal path. A general impression received from voices of the civil society is that applicants are generally considered *persona non-grata* for public bodies if they file a formal request for information and then the first instance bodies would use every "*procedural excuse*" they have, to prolong the delivery of the information. Some NGOs wait for several months, or even years to get closure on their requests. On the other hand, first instance bodies report of receiving over a hundred requests on a certain day which they cannot process. The administrative silence court disputes that are initiated as a result lead to high legal representation costs that are paid from the state budget. Public bodies also complain about repeated/systematic requests from the same applicant and often wonder of the purpose for these requests, etc. It occurs that the first instance bodies do not follow the Administrative court decisions on the assessment of law and facts and are reissuing a decision with the same reasoning that was annulled by the court the first time. All of the abovementioned builds up a feeling of distrust between the civil society and the government. **It is a great task to breach this gap and it is important at this stage for every stakeholder in Montenegro to be aware of it.**

Since the problem is rather deep, current legislative amendments (which are urgent) can only help to remove some problems of acute nature (to prevent abuse, to improve the efficiency of the Agency's procedures, etc). The process of building the desired trust is long. Much effort needs to be put in order to create the awareness among first instance bodies to be prone to transparency and to be keen to disclose public information. The first instance bodies should generally not fear the disclosing or publishing of information. **Therefore, it can be advised that EU should closely follow every legislative provision being adopted, and to make every step possible to recommend and encourage the necessary amendments of the legislation. The amendment provisions must be as concise and detailed as possible**; so that the liable bodies will be more assured that by working towards transparency cannot push them in an unfavourable position.

**The proactive publication needs to be set up as a standard and "transparency on demand" an exception to this standard.** This will lower the number of requests and consequently the complaint

procedures that administratively burden the second instance body. There are many good recommendations, guidelines and other outputs from previous expert assessments, supported by a thorough analysis of the situation. For example, guidelines for the first instance bodies on how to address the issue of proactive publication have been prepared, and should be made use of. Previous recommendations, as well as those from this peer review, need to be properly followed-up and implemented, although mind has to be put to the **allocation of resources in order to see the recommendations through**. It is our assessment, as well as that of previous expert reviews, that the Agency for the protection of personal data and access to public information is currently not in a capacity to implement the necessary changes. **Either the Agency is strengthened financially and/or in human resources or the authority regarding proactive publication is assigned to another public authority (for example the Ministry for public administration as it is the case in Slovenia).** It would also be recommendable to establish a collaboration with the NGOs who have the knowledge and tools to implement the solutions on proactive publication.

**Furthermore, a good coherent legal practice needs to be established from the practice of Administrative court and the Agency and it needs to be assured that this practice is followed by the first instance bodies.** This also requires a strong independent institution that has the capacity to lead the practice based on international and European transparency standards.

**An awareness raising campaigns can be introduced**, joining different "promotors of transparency", for instance – the Agency, the Ombudsman and NGO-s. Such actions can not only help to promote transparency but also to bridge the gap between the public authority and the civil society.

**The working group working on the amendments of LFAI brings confidence that it is functioning well and that it will deliver good legislative solutions that will improve the current state of play on access to public information in Montenegro.**

### Summary of recommendations

**Deriving from the identified problems in our opinion the following questions need to be addressed within the open legislative process**:

- The current system allows for the abuse for gaining profit on the account of administrative silence disputes. This matter needs to be dealt promptly, yet with caution. In order to cope this problem, we recommend adopting amendments to the Law on free access to information regarding costs (section 3.1.3, (i.)) and the to the Law on administrative dispute regarding the request for a public hearing – as has been recommended also in previous expert assessments. We are not against the extension of the deadline for justifiable reasons. We are not in favour of the institute of *abuse* for we believe that in the occurring circumstances, as the abovementioned solutions are more proportional and carry less risk. Moreover, it would be counter-productive towards building trust between governmental bodies and civil society, to accept a solution to which the civil society is so strongly against.
- Proactive publication of documents must be improved and we are in favour of the suggested amendments suggested in the Twinning light capacity building project from 2018.
- The procedure for reviewing if the requested document is in the possession of the first instance institution needs to be made more efficient, for example by transposing the jurisdiction for its performance to the Agency.

- To harmonise the legislation on classified data and access to public information to prevent the occasions of uncontrolled classification of documents with no effective remedy that can overturn the decisions on classification.
- For cases when requests are rejected for the reason that a document is assigned with any of the two lower levels of secrecy (*'restricted' or 'confidential')* the Agency as the second instance body should have the jurisdiction to review the requested classified document itself (provided that the conditions form Law on classified data are met, such as clearance, technical requirements etc.) and that the Agency has the jurisdiction to establish if the classified document meets the criteria from Law on classified data. In such instances, the Agency should also have the power to instruct declassification of the document.
- To precisely specify a uniform, clear and precise definition of the *business secret*, that follows the essence of this institute and enables protection of information and expertise that have commercial value and give a competitive edge over the competition,
- To more precisely define all exceptions from the principle of free access to information provided for in the law, so that their scope and purpose will be clear and determined.

**There are also some measures of organisational character that can be implemented:**

- The implementation of measures regarding proactive publication as outlined in the Twinning light project, namely: the dissemination and promotion of the prepared guidelines for proactive publication; introducing the produced self-evaluation test regarding proactive publication, etc.
- Strict internal control mechanisms may be placed to control if the court decisions are adequately followed and sanctions can be provided in cases of violation.
- Enlarging the number of employees in public institutions according to the approved acts on the systematisation.
- Awareness raising campaigns that include public bodies, NGO-s and other stakeholders in joint activities.
- An overall strategy or to improve the level of transparency on a national level.

## PERSONAL DATA PROTECTION

The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data.

The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally.

Those developments require a strong and more coherent data protection framework on one side and strong and effective enforcement mechanism on the other side. Therefore, it is of vital importance for

Montenegro to prepare and adopt the best possible Law on personal data protection that will be a mutual product of all institutions and other entities interested.

At present, people are not much aware of their right to the protection of personal data. Especially personal data processing performed by law enforcement and military authorities is among people considered as necessary and justified and very rarely raises any doubts. An awareness raising campaigns could be introduced to educate the population of their rights in field of data protection. Different institutions could jointly perform awareness raising activities (for instance the Agency, the Ombudsman and NGO-s). Such actions can not only help to educate the population but also to bridge the gap between the public authorities and the civil society.

### Summary of recommendations

- The setting up of a central automatic electronic record keeping system. Such a system would significantly contribute to legal safety of the citizens and transparency of the police work and would also be very valuable for providing replies to eventual requests by data subjects.
- The establishment of a system of internal control regarding data processing, especially within the authorities that process large amount of personal data.
- The adoption of data protection policies.
- The establishment and implementation of data protection education and trainings.
- The clarification of relation between Ministry of the Interior and the Police.
- Awareness raising campaigns that include public bodies, NGO-s and other stakeholders in joint activities.
- The adaption of institutional capacities of the individual authorities to the number provided for in the Acts on Systemization and to the tasks of individual authorities and providing authorities with sufficient resources.