What are the most common legal bases for personal data processing in the context of local public authorities' activities? Legal obligation vs Public Interest

Denitsa Kozhuharova[1]
Dilyana Kutsarova[2]

The current paper offers an overview on several provisions enshrined in Article 6 of the General Data Protection Regulation from the perspective of local public authorities. It advocates that administrative law notions might facilitate municipalities to make a better distinction when they process personal information either on the basis of legal obligation or for the performance of a task carried out in the public interest, or for the exercise of official authority vested in the controller. The paper reviews data subject rights implications in this relation. It also touches upon legitimate interests and consents applicability in day-to-day operations of personal data processing executed by local public authorities.

Introduction

The protection of personal data has become one of the central human rights over the last 20 years, given the increased importance and share of the data driven economy and the challenges that this imposes to an individual's privacy. The recent pan-European Data Protection Reform once more demonstrates the significant role of personal data protection by introducing considerable legislative measures to be applied throughout the entire European Union. The General Data Protection Regulation (GDPR) plays a major role in this respect. The Regulation entered into force on the 24th of May 2016, and is applied across member states since the 25th of May 2018.

Despite creating major buzz in the business ecosystem, the Regulation is equally applicable to the public sector as well. The Regulation envisages numerous measures aimed at enhancing the legal compliance of the public authorities' daily activities related to the processing of personal data in order to ensure the utmost respect to the right to data protection of natural persons.

However, a common feature of most of the public authorities in the EU is their insufficient readiness to face the challenges posed by the digital era, including the new data protection regime. And one of the most vulnerable public authorities are local public authorities which are exposed to continuous cyber-attacks which lead to data breaches and unlawful disclosure of personal data. In recent years there were many reported incidents in this regard – Dettlebach (Germany), Ooststellingwerf, Weststellingwerf and Opsterland (Netherlands), NotPetya (Ukraine). These cases illustrate general technical and administrative unpreparedness of local public authorities. Legal advisors employed by these institutions do not tend to be experts in the field of data protection. Meanwhile, there are more than 30 000 local public authorities in the EU. Daily activities of local public authorities as data controllers presuppose wide interaction and processing of personal data. Therefore, they need to be aware and ready to provide adequate protection of personal data to ensure citizens that their fundamental right to personal data protection is respected. All these issues require immediate actions aimed at enhancing the understanding of local public authorities regarding their new obligations and needed steps to address them. Moreover, it requires an increase of knowledge of the administrative staff that is directly engaged with the processing of personal data.

This issue has inspired partners behind the Preparing local public authorities for the new data Protection Legislation (ProLegis) plan to design a project to answer to the training needs of local public authorities' employees that are to be engaged in personal data processing activities, regardless whether they have been appointed as Data Protection Officers or not. To this end, the ProLegis project is set to develop training materials and methodology that are tailored to the needs and expectation of local public authorities. The training materials are in the basis of all planned face-to-face and online training opportunities provided by the projects.

[1] Author is one of the key researchers with Law and Internet Foundation, responsible for the ProLegis project coordination. As a lawyer she was also involved in large-scale data protection implementation projects in the public sector, most notably the GDPR implementation by the Ministry of Education and Sciences. Beyond personal data protection & privacy, the other research fields she is engaged with are procedural rights, child rights and digital rights in general.

[2] Author graduated as LL.M. with honours from the University of Sofia, Faculty of Law in 2015. She has experience in delivering legal and ethical research products related to the implementation of ICT in the public and private sector. Her main field of expertise is data protection and cybersecurity law. Most of her work is related to the implementation and coordination of tasks within diverse EU funded projects targeting the enforcement of human rights through ICT tools.

In the course of the said training materials preparation, and later on – during the planned training events, many unclear points in the data protection regime have been identified. One of the recognised challenges that local public authorities meet is the precise definition of the legal basis for personal data processing. Although this question has been clarified in the materials prepared under the project, the authors of the current publication deemed that the issue requires further examination. To this end, the paper will discuss legal obligation and public interest as bases for lawful personal data processing. It will break down their essence and then contrast the major difference of their application by providing examples from day-to-day activities of the local public authorities. In order to provide robust examination, the paper will also touch upon the nature of legitimate interest, as well as upon the possibilities for municipalities to process personal data on the basis of citizens' consent.

The current paper was funded by the European Union's Rights, Equality and Citizenship Programme (2014–2020). The content of this publication represents views of the authors only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

The current paper introduces the vision of the authors on how the legal bases provided for in Article 6 pt. (c) and (e) of GDPR interrelate with the concepts of circumscribed powers and discretion deriving from administrative law. It should be noted that the reflections of the authors are mainly based upon the Bulgarian legal system and main terminological concepts.

Legal Obligation as a legal basis for personal data processing

1. What is to be understood as legal obligation?

According to art. 6, par. 1, pt. c GDPR, whenever personal data processing occurs pursuant to a legal obligation applicable to the controller it represents lawful processing. For example, this legal base would be applicable in cases where the controller processes personal information in relation to the applicable tax and social securities' regime, but also in scenarios where personal data is processed in the context of anti-money laundering procedures. Ultimately, what qualifies personal information processing under this particular legal ground is the fact that the controller does not make the decision whether to process personal data or not, they are obliged to do so by law. Here, the purposes of the processing are determined by the legislator, not by the controller. In fact, the controller is defined as such by the applicable law itself. Thus, the assessment of whether such processing should take place at all is made by the legislator *a priori*, and the controller is the entity/person who is responsible to carry it out. It is to be noted here that only EU and Member State legislations could be the source of the legal obligation. The latter can never derive from a third country legal order, i.e. when the controller is subject to an obligation under the legislation of a third country, this processing cannot be justified in accordance to Art. 6, par. 1, pt. c.

With regards to the essence of the respective provision itself, Recital 45 of the GDPR clearly states that it is not necessary that the legal provision details the categories of personal data to be processed or concrete operations, but the provision of the general conditions themselves is considered sufficient. Moreover, it is presumed that the legislator has carried out a balancing test how the sought purpose of the processing relates to the rights and legitimate interest of the individuals, and whether the latter prevails, as long as all data protection principles as outlined by Art. 5 GDPR are observed[3], including here also the proportionally and necessity test. In other words, it is presumed that the legislator, when adopting the respective provision, which envisages personal data processing, has already made an assessment on the necessity and proportionality of the processing. For local authorities this notion is particularly important, considering the legislative powers they may possess. However, it should be noted that depending on the particular data processing operation, the controller could be the one defining the appropriate means to achieve the purposes set by the law.

2. Why does this legal ground present a challenge to local public authorities as data controllers?

The nature of a legal obligation as a legal basis for personal data processing is quite clear to private sector controllers. The only case where they will process an individual's information as prescribed by the law would be precisely when they have to comply with a legal obligation applicable to them. They are not entities entrusted to enforce policies or realise public strategies. However, for the public sector controllers the situation is a bit more complex. Since public bodies, and local public authorities in particular, are bound to implement national, regional and local public policies, strategies, and action plans, it might pose an additional challenge to differentiate when personal data is processed in line with a legal obligation, and when this is done to fulfil a task of public interest or an

[3] For more information, please visit: Working Party 29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (access from 30.10.2019).

exercise of official authority. The fact that both legal bases are often commonly addressed in the GDPR (i.e. Recital (45), Recital (51), Recital (65)) produces further confusion to the local public authorities. The clear definition of the legal base in such a scenario is of utmost importance since this impacts data subject rights and their possible exercise and limitations.

An easy way to figure out whether the processing is carried out in order to comply with a legal obligation is for the controller to pose the question whether the respective legal provision is imperative or dispositive. If the law requires the controller to complete a certain activity and leaves no room for independent decision on their side, then the processing would take place under Art. 6, par. 1, pt. c GDPR – the processing is necessary for compliance with a legal obligation to which the controller is subject. Otherwise, if the law empowers the controller to decide how to act, then pt. e should be considered as the applicable legal basis.

Additionally, it could also be useful to examine if the controller acts with a level of discretion in relation to the particular processing operation or acts within circumscribed powers. Although this concept derives from administrative law theory, it is a quick method for local public authorities to assess which is the legal ground for a particular processing operation. In this context, one could rightfully pose the question whether each personal data processing operation occurring within circumscribed powers is falling into the scope of the provision of Art. 6, par. 1, pt. c GDPR. A public body might act within circumscribed powers pursuant to a provision deriving from primary or secondary legislation, but also whenever acting upon an order issued by a higher authority[4], according to the Bulgarian administrative law's understanding. Thus, how could following an order be considered as compliance with a legal obligation? Firstly, it should be noted that in line with the administrative legal theory, only an individual on an executive position with an administration is to be considered as administrative authority, and the administration itself is given a supporting role implementing the authority's decisions. Moreover, GDPR itself clearly provides in Art. 29 that the persons acting under the authority of the controller process personal data solely under the instructions given by the controller.

Public Interest & Exercise of official authority as a legal basis for personal data processing

1. What is the essence of this legal ground for the processing of personal information?

Another commonly applied legal ground for personal data processing by the local public authorities is the one outlined by art. 6, par. 1, pt. e GDPR, which actually contains two separate basis – the personal data processing is related to the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In order to determine whether a controller is able to use this legal base to ground their personal information processing activities, one should examine if the public task/the official authority are outlined, again, in the relevant legislation. It should be noted here that only EU or Member State legislation could serve as a ground for the public task/official authority exercise. In contrast with the legal obligation, the nature of the legal provision establishing the public task/vesting the official authority should be discretionary, enabling the controllers to take a motivated decision on a certain action. The public task/official authority might be also defined in policy documents, i.e. they might be incorporated in strategy, road maps, action plans, adopted in accordance to the national law, etc., outlining authorities' and other relevant actors' prerogatives in relation to a certain societal issue. These strategic documents might be issued on a national or regional, and even local level, targeting issues from a different severity or importance. What is important here is that there should be a legal provision entrusting a particular controller (in our case a local public authority) to carry out the respective policy/task. When the implementation of these policies does also include personal data processing its legal foundation will be the performance of a public task/the exercise of an official authority. Similarly, to what has been stated in the previous section, third-country legislation is never to be considered as a legal basis for personal data processing pursuant to Art. 6, par. 1, pt. e GDPR.

Examples of processing related to the performance of a task carried out in the public interest are different information and communication campaigns carried out by municipalities in order to raise awareness on environmental issues, or an assessment of the percentage of the population using different lines of public transport. What would fall under the scope of the exercise of official authority vested in the controller are, for instance, the decrees of a mayor issuing a fine or another administrative measure towards a citizen or a company which violates the municipal orders.

At the same time, it is possible that this legal ground is used not only by public authorities, but by private entities as well, as long as they are entrusted to implement partially or completely state policies. These are the cases where private organisations are procured to deliver social services, or support a municipality in the maintenance of public infrastructure as libraries, sport centres, etc.

[4] I.e. Decision 258/26.3.2008, Blagoevgrad Administrative Court; Decision 70/26.7.2017, Shumen Administrative Court; Decision 150/10.7.2018, Yambol Administrative Court.

2. Why does this legal base present a challenge to local public authorities?

At a first glance, it might seem that the scope of application of this legal basis for personal data protection could be interpreted more broadly, ultimately establishing a more liberal regime to controllers. Nonetheless, this provision is to be interpreted and applied in a limitative manner. Although this legal basis could provide for a better flexibility of the controllers, a careful assessment is to be made on case-by-case basis to examine whether the public interest actually does prevail over the individual's one. This assessment might be made on the stage of legislation/strategic documents drafting, as again the legal provision can determine the purposes of processing.

However, this does not preclude the responsibility borne by the controller – a balancing test is still to be executed. Why is that? Going back to the presented relation between personal data processing pursuant to a legal obligation and circumscribed powers, it is clear that a comparable correlation is to be sought here as well. Furthermore, turning to administrative law theory, the notion of discretion seems appropriate to illustrate the nature of the responsibility that controllers are entrusted to bear. In accordance with the wider flexibility presented in the current section to which the local public authorities are entitled, and the necessity for local public authorities still to carry out an assessment, it is right to say that whenever they act upon discretion and this includes personal data processing, the latter is regulated by the provision of Art. 6, par. 1, pt. e GDPR.

From a practical point of view, this represents a challenge to local public authorities, as on the one hand – legal obligation and task carried out in the public interest/exercise of official authority, are regarded *en bloc* by the GDPR in numerous instances. On the other hand, the delimitation line between an imperative provision establishing a legal obligation and a dispositive provision outlining the margin of an official authority could be difficult to draw. To facilitate this process, whenever a local public authority is processing an individual's information, as a first step, it should be established whether this activity falls under the scope of discretion or circumscribed powers. From there on, municipalities would be able to easily identify the applicable legal bases for personal data processing as outlined by the GDPR, and address data subject rights exercise requests accordingly.

Data subject rights implications

The new data protection regime, and the GDPR in particular, continue the philosophy enshrined by the previous of EU act regulating this field – Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, by putting the individual in the centre, enabling him/her to exercise control over the way their personal data is being handled. This is particularly valid in situations where private sector organisations and information service providers might be tempted to go a step beyond the promised data processing and use personal information in a non-transparent manner to curate products and services, or even manipulate citizens. Therefore, the new, enhanced set of rights available to citizens' disposal plays a significant role in holding these controllers accountable.

At the same time, public sector controllers, and local public authorities in particular, are bound to function in a transparent manner. They are the ones who forge the relationship of trust between the citizens and the government institutions. However, the legal regime applicable to them is quite different to the one that regulates the function of the private sector. Since local public authorities are a subject to imperative legal order and are required to implement state policies, they are obliged to keep a detailed track showcasing the consecutive execution of their activities. There is a limited number of situations where local public authorities would process data outside their capacity of governmental institutions.

On a practical level, however, the difference between legal obligation and task carried out in the public interest/exercise of official authority is to be made namely in relation to data subject rights. Personal data processing pursuant to both legal bases is providing for more limited application of data subject right. Still, whenever personal information is treated in accordance with Art. 6, par. 1, pt. e GDPR, the individual has a wider range of possibilities at his/her disposal.

But which data subject rights could be limited? Firstly, the right to information might be narrowed down. In cases where the personal data is not collected directly from the data subject, but *ex officio*[5], local public authorities are not obliged to inform citizens pursuant to Art. 14 GDPR. This means that they are not required to disclose to citizen details such as the purposes of personal data processing, the categories of personal information which are being handled and for how long, where the data originated and to whom it is disclosed, including also transfers to third countries or international organisations. If a local public authority is implementing automated decision-making technologies, and if the personal information is collected *ex officio*, it is not mandatory that this information is made available to data subjects. Through this approach the responsibility to assess how the individual interest relates to the public one is borne by the legislator – as Art. 14, par. 5, pt. c of GDPR states that the non-disclosure of information to data subjects is only possible when the law

[5] Article 14, par. 5, pt. c GDPR.

provides appropriate measures to protect the data subject's legitimate interests.

Furthermore, the right to erasure is also of limited application in cases where personal data is being processed pursuant to the compliance with legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The functioning of local public authorities may be compromised in an event of personal data deletion. As it was aforementioned, the nature of governmental institutions activities requires them to keep detailed track on the on-going and already executed procedures. Therefore, the EU legislator has very rightfully recognised this risk and inserted the provision of Art. 17, par. 3, pt. b GDPR, to prevent the impediment of public bodies' work.

The most drastic difference between the legal regime of the legal bases analysed in the current paper comes from the provision of Art. 21 GDPR. The right to object is a powerful tool available to natural persons to hold controllers accountable. It enables them to challenge any processing operation as long as it is based on the controller's legitimate interest or is done for the performance of a task in the public interest or for the exercise of official authority vested in the controller. When this right is exercised, the controller (or the local public authority in this case) has to demonstrate how the public interest overrides the individual's, otherwise the processing should cease. This is why it is of primordial importance for local public authorities to make a clear distinction between the processing operations executed in accordance with Art. 6, par. 1, pt. c, and those pursuant to Art. 6, par. 1, pt. e. This way, when a municipality is met with such a request, they would easily make an assessment to satisfy or refuse it, providing appropriate argumentation.

The Notion of legitimate interest

Although the idea of the current paper is to compare the scopes of two of the legal grounds established by Art. 6 of the GDPR in the context of local public authorities' activities, the essence of Art. 6, par. 1, pt. f is to be briefly examined to provide a comprehensive picture. While legitimate interest as a ground for personal data processing is never to be applied in relation to the provision of public services[6], there are cases where it could serve as a basis to handle personal information. Local public authorities do not function solely as governmental institutions. They are also employers and contractors, and in this position their behaviour is regulated by private, and not public law. When acting in such capacity, it is possible that the personal data processed is linked to their legitimate interest. For example, in the case of on-going employment relationship, a local public authority might implement access control and video surveillance among other security measures. This operation of personal data processing would fall under the scope of its legitimate interest. Another example for the applicability of the said legal ground would be a court dispute with a contractor. In this scenario the information is once again processed pursuant to the legitimate interest of the local public authority. It is important to make the distinction in which capacity the local public authority acts, so data subject rights are appropriately managed, and citizens trust the governmental sector.

And what about the consent?

Around the 25th of May 2018, a lot of the public debates on data protection revolved around consent. In addition to that, users of variety of platforms were bombarded with emails to re-affirm their consent. And then suddenly, consent forms were pushed everywhere – in electronic environment, but also on the spot, in relation to the provision of services, regardless whether they are public or not. A person would go to their dentist, and even a hair dresser, and they would ask for their consent in order to perform services. The misunderstanding was so great that the Bulgaria Commission for Personal Data Protection issued a list with activities where personal data processing is never based on consent[7]. Although the mission of the present paper is to shed further light into the complex issue of the delimitation between personal data processing pursuant to a legal obligation and the one done in the public interest, the authors think it is quite necessary to highlight why consent cannot be the legal basis for personal data processing in the context of the local public authorities' activities.

Even though the data subject consent is listed first in the enumeration provided by art. 6, par. 1 of GDPR, this should not be understood in the sense that this is the main legal base for personal data processing that controllers have at their disposal. On the contrary – controllers and processors should resort to obtain natural persons' consent in the limited situations where there is no other legal basis present and where their legitimate interest would not override the individual's one. As it is outlined above, local public authorities would mainly process personal data either on the basis of a legal obligation, to which they are subject, or in accordance with the public interest. Practices where, for example, municipalities seek citizens' consent to enter personal data in a public registry, or for the purposes of participation in elections, should be abandoned.

[6] Art. 6 par. 2 GPDR.

[7] For more information, please visit: List of processing operations requiring data protection impact assessment (DPIA) pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/679, https://www.cpdp.bg/en/index.php?p=element&aid=1186 (access from 30.10.2018).

In a very limited amount of cases a municipality might employ consent as a legal basis to process citizens' personal information. For instance, if a local public authority administration maintains an electronic newsletter, then the consent of the subscribers would be the legal base for its regular distribution.

Conclusion

At first glance, it might seem easy to differentiate which legal basis enshrined in Art 6, par. 1 of GDPR is applicable. However, on a practical level public sector controllers, and local public authorities in particular meet obstacles determining whether their activities are to be regulated under Art 6, par. 1 pt. c or pt. e. The situation is further tangled by the popular understanding of consent as the legal ground for personal data processing, and wide applicability of legitimate interest in the private sector. The current paper tries to solve this complex situation by offering a simple assessment based upon administrative law theory – whether the authority acts within circumscribed powers or discretion. This assessment would facilitate local government bodies to identify whether a certain processing operation is based on the compliance with legal obligation or falls under the performance of a task carried out in the public interest or the exercise of official authority vested in the controller.

To this end, whenever personal data is processed upon a legal obligation, it should be noted that the controller has no legal possibility to decide, nor discretion whether or not to carry out the processing. The law imposing such an obligation could be of primary or secondary nature detailing what kind of personal information is the object of the processing, and what is the specific purpose pursued. On the other hand, whenever a local government organisation has a room to decide whether and how to carry out an activity within its capacity as public body entrusted to implement laws and policies, any personal data processing in this relation would fall under the scope of Art. 6, par. 1, pt. e GDPR. In cases when they are able to act upon a discretion, a local public authority will process the personal data for the performance of a task in the public interest or for the exercise of an official authority.

Last but not least, the paper provides for an examination of the applicability of other legal bases for personal data processing by the local public authorities. The analysis also deduces that scenarios where local governments' actions are regulated by private law are not to be ignored. Thus, it is reasonable to consider their legitimate interest as a basis to handle personal information. Still, a clear distinction between these activities should be in place to enhance citizens' trust and provide for better data subject rights management. Consent is also reviewed from this point of view, stating its narrow applicability in the context of local government – only in case when a municipality carries out an atypical activity which is neither funded in law nor pursuant to its legitimate interest.

Key words: data protection, privacy, GDPR, legal bases, public interest, legal obligation.