DATA PROTECTION, DATA PROCESSING BASED ON LEGITIMATE INTERESTS

IT Law Lab Research Paper
## Table of Contents

Abbreviations .................................................................................................................. 3

Introduction ..................................................................................................................... 4

1. The Legitimate Interests as a Personal Data Processing Legal Ground Under the GDPR 8
   1.1. Elements and Limitations of Legitimate Interests ............................................... 8
   1.2. Related Obligations of the Controller Upon Applying the Legitimate Interests Legal Ground .................................................................................................................. 9

2. Interplay of Legitimate Interest as Legal Basis for Data Processing with Other Legal Bases for Data Processing ................................................................. 12
   2.1. Consent .................................................................................................................. 12
   2.2. Contractual Basis ................................................................................................. 13
   2.3. Legal Obligations ................................................................................................. 15
   2.4. Vital Interests ....................................................................................................... 17
   2.5. Public Task .......................................................................................................... 17

3. Third Party’s Legitimate Interests ............................................................................... 19
   3.1. The Possibility to Apply Third Party’s Interests .................................................... 19
   3.2. Third Party Interests as Mainly a Basis for Data Disclosure or Data Transfer to the Third Party ................................................................................................................. 20
   3.3. Third Party’s Limitations Upon Receiving the Data ............................................. 22

4. Elements of Legitimate Interest Assessment ............................................................... 24
   4.1. Purpose Test ....................................................................................................... 24
   4.2. Necessity Test .................................................................................................... 27
   4.3. Balancing Test ................................................................................................... 28

Summary ......................................................................................................................... 30

Bibliography .................................................................................................................... 33
Abbreviations

WP29 – Article 29 Working Party

Art – article

CJEU – the Court of Justice of the European Union

DPD – Data Protection Directive

ECHR – European Convention of Human Rights

EDPB – European Data Protection Board

EDPI – Data Protection Inspectorate of the Republic of Estonia

EU – European Union

GDPR – General Data Protection Regulation

ICO – Information Commissioner’s Office of the United Kingdom
Introduction

In the past few years, personal data protection has been in the focus of most EU companies and public authorities. As of 25 May 2018, processing of personal data of natural persons must be conducted in accordance with the Regulation (EU) 2016/679 (the General Data Protection Regulation (‘GDPR’)). Under GDPR, the possible sanctions which can be (and must be) imposed on companies or public authorities in breach of the requirements under GDPR are more severe than what was possible under the national laws implementing the Data Protection 95/46/EC (‘DPD’), therefore having a potentially material impact on entities processing personal data. Compliance with GDPR has been taken more seriously than the compliance with obligations deriving from DPD and the respective national laws ever was. At the time of writing this research paper, there were already more than 140 fines issued under GDPR which had been made public by the data protection authorities of EU member states, several of which had already exceeded hundreds of millions of dollars, many of which issued due to processing of personal data without the legal ground or under a false legal ground. This already shows a new attitude from the supervisory authorities and demands from companies processing personal data to take compliance with GDPR seriously.

One of the most essential tasks, when processing personal data, is determining the legal grounds for doing so. Although the Estonian Personal Data Protection Act under the DPD did not reflect legitimate interest as a legal basis for personal data processing, it was already present in the DPD and GDPR did not introduce any new legal grounds for personal data processing compared to the six legal grounds set out under DPD. The GDPR did, however, set out some additional requirements and limitations to the application of such legal grounds, e.g. with the introduction of a new provision as Art 7 of GDPR additional requirements to consents were

---

2 Consolidated information about fines issued by data protection authorities of EU member states can be found in an ‘enforcement tracker’ administrated by CMS, one of the largest law firms in the world. Available at: https://www.enforcementtracker.com/ (16.12.2019).
3 Under Art 6 (1) of GDPR, processing of personal data is deemed lawful only if at least one of the following legal grounds applies: (a) data subject has provided their consent; (b) processing personal data is necessary for the performance of a contract concluded with the data subject or in order to take steps at the request of the data subject prior to entering into the contract; (c) there is a legal obligation for personal data processing; (d) processing is necessary for the protection of vital interests of the data subject or another natural person; (e) processing is necessary for the performance of tasks carried out in the public interests or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests purposed by the controller or by a third party.
added. Although the requirement to determine the legal basis for each and every data processing activity was overlooked prior to the adoption of GDPR, it is under the GDPR that companies are required to disclose to the data subject information about their data processing activities, additionally, data subject have become more aware of their rights in relation to their personal data, thus there is a higher risk of being penalised for wrongful acts.

What has been established during the past few years is that distinguishing different data processing activities and thus, determining rightful legal grounds for data processing is complicated, as in practice the activities of companies are intertwined. As application of consent as a legal basis for personal data processing is inevitably burdensome, other legal grounds for personal data processing must be considered.

Assessing whether certain data processing activities fall under any certain legal basis requires thorough assessment of the necessity of data processing for the given purpose. Where legal bases set out in Art 6 (1) (a) to (e) of GDPR already entail the possible purpose for their application, application of legitimate interest as a legal basis also brings about the requirement to explain and justify both the purpose as well as the necessity of the use of such legal basis. Therefore, it requires much more effort when making preparations for commencing personal data processing activities under legitimate interest. Although WP29 has issued guidelines on the applicability of legitimate interests as legal grounds for personal data processing, these

---


6 For example, the date of employees cannot always be processed based on the legal ground allowing processing under the employment contract (i.e. Art 6 (1) (b) of GDPR). Source: The GDPR Covers Employee / HR Data and It’s Tricky, Tricky (Tricky) Tricky: What HR Needs to Know. Available at: https://www.dickinsonwright.com/news-alerts/the-gdpr-covers-employee-hr-data-and-tricky (13.12.2019).

7 Consent as a legal basis requires a positive opt-in from the data subject, whereas it cannot be obtained with standard clauses of a contract and in general, it has to be obtained separately for each data processing activity. Data subject must be able to withdraw from a consent. Source: Consent. | ICO. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ (16.12.2019).

8 This also applies when data is processed under a consent of a data subject. WP29 has stressed that obtaining a consent from a data subject does not waive the application of other data processing principles set out in Art 5 of GDPR. Source: Opinion 15/2011 on the definition of consent (WP187), adopted on 13 July 2011, p 7. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (16.12.2019). Although Opinion 15/2011 of the WP29 was adopted to provide guidelines to interpret the provision of DPD, the principles have remained largely the same. The explanations provided for herein have also been incorporated by reference to the WP29 document WP259 (please see footnote 26 below).

guidelines date back to 2014\textsuperscript{10} and do not include any of the problems which have been detected thereafter nor focus on any specific GDPR-requirements.

The purpose of this research paper is to analyse the applicability of legitimate interest as one of the legal grounds for personal data processing. The main problems examined herein concern specifics related to who, when and under which conditions may or should apply legitimate interests as the legal basis for personal data processing. Although it may seem that legitimate interest as a legal basis for personal data processing, due to the seemingly wide possibilities for interpretation, fills the gap where no other legal basis set out in Art 6 (1) of GDPR can be applied, it is not the correct interpretation of the scope of this legal basis.\textsuperscript{11}

This research paper consists of 4 chapters. The first chapter of this research paper consists of two sub-chapters and examines a chosen selection of elements, limitations and related obligations for applying legitimate interest. The second chapter of this research paper consists of 5 sub-chapters, each of which examines the interplay of legitimate interest with each of the other legal grounds for personal data processing under Art 6 (1) of GDPR. The third chapter of this research paper has been divided into three sub-chapters which altogether examines the personal data processing in case of reliance of third-party legitimate interests by the data controller, as possible under Art 6 (1) (f) of GDPR. The fourth chapter of this research paper has been divided into three sub-chapters, analysing, respectively, the purpose test, necessity test and balance test which are required to be conducted prior to the reliance on legitimate interests as legal ground for personal data processing.

Due to the limitation to the length of this research paper, the research paper has been written with an assumption that any exemptions and limitations regarding personal data of children, special categories of personal data or transferring of personal data to third countries does not occur. What is more, for the sake of clarity, data processing specific terms e.g. as ‘personal data’, ‘processing’, ‘data subject’, ‘third party’, ‘controller’, ‘processor’ shall be used in this research paper with the meanings given to them in Art 4 of GDPR.


\textsuperscript{11} Supra nota 10, p 9. As explained above in this research paper, legitimate interest as a legal basis for personal data processing has not been subject to considerable changes if compared to the relevant provisions in Article 7 of DPD. Therefore, the guidelines of WP29, although based on DPD, are still relevant under the current applicable legal framework for personal data protection.
The structuring of research paper has been a result of a joint effort of all three authors. Each of the authors had separate responsibilities regarding the drafting of this research paper, with A. Tsuiman being the main author or chapters 1 and 3, E. Varendi being the main author of chapter 2 and M. A. Valberg being the main author of chapter 4. The introduction of this research paper was mainly prepared by E. Varendi and A. Tsuiman and the summary of this research paper by M. A. Valberg. All of the authors have equally contributed to the formatting of this research paper.
1. The Legitimate Interests as a Personal Data Processing Legal Ground Under the GDPR

1.1. Elements and Limitations of Legitimate Interests

As outlined in the introduction of this paper, the legal grounds from the DPD have been largely kept intact when having been transposed into the GDPR. Therefore, the wording of the legitimate interests as a legal basis is also based on the wording of the DPD,\(^\text{12}\) retaining its key elements. GDPR Art. 6 (1) (f) states the legal ground as follows (emphasis by underlining added by the authors): “processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

Deriving from the abovementioned and for the personal data processing based on the legitimate interests’ legal ground to be lawful, the application requirements of the legitimate interests can be broken down into three separate parts, out of which each constitutes a separate test or a criterion to be conducted and satisfied:

- **Purpose test**, meaning, an interest to be pursued must constitute legitimate. Such interests can be the interests of a data controller or of third parties. In principle, such interests may be commercial interests but also interests which carry social benefits for a larger group of persons;

- **Necessity test**, meaning, that the processing itself must be a proportional way of achieving the processing purposes. Additionally, satisfying the necessity criterion presumes that the processing does not have another reasonable and less intrusive alternative for achieving the same result;

- **Balancing test**, meaning, that it is obligatory to balance the interests of the controller or the third party against the affected data subject’s interests. The balancing test also contains the expectation evaluation, which requires the processing to be viewed in the context of the reasonable expectations of the data subject, meaning, that in case the data subjects are not expecting their data being processed in the concerned manner, the

interests of the data subject are more likely to override the interests of the data controller or the third party.\textsuperscript{13}

Despite having no case law for the interpretation of the aforesaid criterions in the context of the GDPR the relevant case law under the DPD of the CJEU is still valuable due to the small changes of the legitimate interests legal ground from its transition from the DPD to the GDPR.\textsuperscript{14} The three-tier test elaborated in the previous paragraph has been enforced by the CJEU in the \textit{Rīgas satiksme} case adjudicated in May 2017.\textsuperscript{15} The content of the aforementioned tests is elaborated in more detail in the fourth chapter of this paper.

Despite the recitals (recitals 47 – 50) of the GDPR giving the data controller exemplary indications where legitimate interests may be relied upon, such examples have to be considered as “might-be” applicable as even in those circumstances the data controller must conduct the necessary assessment.\textsuperscript{16}

The last paragraph of Art 6 (1) sets in place a limitation for the application of the legitimate interests as a legal ground, namely, the legislator has excluded for the public sector the possibility to apply the ground in the performance of their tasks. The foregoing, however, does not limit the public sector’s right to apply the legal ground as a basis for activities other than their official tasks.\textsuperscript{17}

\textbf{1.2. Related Obligations of the Controller Upon Applying the Legitimate Interests Legal Ground}

In addition to the requirement of conducting the tests, as outlined in the previous chapter, the data controller is also subject to other obligations deriving from the GDPR. This chapter does not intend to cover and elaborate on all the data controller’s (possible) obligations under the


\textsuperscript{14} Supra nota 12, I, p 26.

\textsuperscript{15} “/--/ lays down three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence.” Case C-13/16. Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA ‘Rīgas satiksme’. 4 May 2017, para 28.


\textsuperscript{17} Ibid.
GDPR but is designed to cover the key elements of which the controller should account for when the legitimate interests ground as a legal basis is used.

First and foremost, the data controller has to consider that all its personal data processing activities have to be conducted in accordance with the seven principles of the GDPR as presented in Art 5 of the GDPR.\textsuperscript{18} However, the principles of lawfulness, fairness, data minimisation, integrity, together with transparency and purpose limitation principles are particularly important due to the role they play in the assessment tests to be conducted by the data controller prior to the application of the said legal ground.\textsuperscript{19}

It should be noted that under the accountability principle from Art 5 (2) of the GDPR, according to which the data controller is responsible for ensuring compliance with the GDPR, including adherence to the lawfulness principles obligating the application of a valid legal basis for data processing, the assessment tests for applying the legitimate interests as a legal ground have to be documented\textsuperscript{20} in order for the data controller to show that the interests have indeed been balanced and weighted.

Due the somewhat hidden nature of the balancing test and ambiguity of the legitimate interests as a legal ground, the controller should, according to WP29, turn extra attention to the transparency obligations deriving from Art 13 (1) (d) and Art 14 (2) (b) of the GDPR. The controller should always state the specific legitimate interests in question to which it intends to base the processing. Information could be presented in a layered manner in order to avoid information fatigue. As a best practice example, the controller should provide information on the balancing test, indicating that the data subject is entitled to acquire more information on the balancing test by submitting a request to the data controller. Thereby, in case the data subject has doubts whether the balancing of interests has been carried out fairly the data subject could inquire the reasoning behind the assessment test.\textsuperscript{21}

The data controller should also take into account that Art 21 (1) of the GDPR gives the data subject, whose data is processed under the legitimate interests ground, a specific right to object to such processing relating to his/her particular situation. In case the data subject issues his/her

\textsuperscript{18} These principles, as stated in Art 5 (1) and (2) read as follows: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability.

\textsuperscript{19} Supra nota 16, p 606 - 607.


objection to the processing carried out under the legitimate interests, the data controller has to cease the data processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or show that the processing is necessary for the establishment, exercise or defence of legal claims. It must be noted that the GDPR itself does not give much guidance on the notion of “compelling” legitimate grounds and whether (and how) those grounds (should) differ from the initial “legitimate interests” under which the assessment of the legal ground was decided prior to the processing. However, according to WP29’s opinion, which was issued under the DPD in which the objection right of the data subject was worded slightly differently, the data controller should take into account the content of the objections of the data subject and this should lead to a new assessment of the legitimate interests, as the data subject could have stated in his objection details that the controller might not have taken into account under the initial assessment. According to Art 21 (1) of the GDPR, in case the controller cannot demonstrate the compelling legitimate interests, the controller has to cease the processing of the affected data of that data subject for that specific processing purpose for which the legitimate interests’ legal ground was applied.

Provided that the controller cannot show compelling legitimate interests, as required under Art 21 (1), for the processing to which the data subject objected, the data subject is entitled, under Art 17 (1) (c) of the GDPR, to request the deletion of the personal data processed under the legitimate interests legal ground, provided that the data is not necessary for other processing purposes. However, provided as with the successful objection to the processing, the controller has lost its legal ground for the processing of the said personal data, and such data is not necessary for any other processing purposes, it is presumed that the controller is actually, on its own initiative, required to delete the said affected data, as otherwise the controller would be in breach of the lawfulness principle under Art 5 (1) (a) and with Art 6 (1).

---

22 Art 14 (a) of the DPD provided that the data subject should show the compelling legitimate grounds for objecting not the controller show the compelling legitimate grounds for continuing the processing (as worded under Art 21 (1)).

23 Supra nota 10, p 45.
2. Interplay of Legitimate Interest as Legal Basis for Data Processing with Other Legal Bases for Data Processing

2.1. Consent

It is difficult to apply consent as there are many additional requirements (especially regarding the form of obtaining consent) and the right of data subject to withdraw from a consent at any time do not allow smooth service provision for companies.\(^\text{24}\) Also, not always is it possible for companies to stop data processing upon a request of the data subject and in any such it is not even possible to rely on consent.\(^\text{25}\) As there are multiple requirements for a consent under GDPR to be valid, it is not the most preferred legal basis for personal data processing. WP29 has explained in its guidelines on consent under GDPR that a valid consent has to be freely given, specific, informed and unambiguous indication of the data subject’s decision to allow their personal data to be processed for the purposes clearly indicated to them.\(^\text{26}\) It is important to stress that the data subject must have the possibility to withdraw the consent at any time (Art 7 (3) of GDPR), generally without any material impacts to any other legal relationships between the data subject and the controller. Consent should not be “bundled” together with any other requirements, based on Art 7 (4) and recital 43 of GDPR, the situations where the provision of services to the data subject depends on whether the data subject has provided its consent and the consent can still be considered as valid, are highly exceptional.\(^\text{27}\)

Consent as a legal basis provides for least flexibility. Should the data subject withdraw from its consent, the controller must stop processing data collected and processed under a consent and would not be able to continue with the processing activity under any other legal basis. WP29 has also stressed that should it become evident that there might be problems with the validity of consent as the applicable legal basis, the controller cannot retrospectively change its views and apply legitimate interest as the legal basis instead.\(^\text{28}\) Taking into consideration the above, it is relevant that already prior to commencing planned processing activities, the controller determines whether there might be suitable alternatives to consent as legal basis, the most probable alternative being legitimate interest due to the fact that consent as a legal basis


\(^{25}\) Supra nota 4.


\(^{27}\) Ibid, p 8-9.

\(^{28}\) Ibid, p 23.
is usually not considered unless Art 6 (1) (b) to (e) apply. Therefore, when in doubt whether personal data processing activity should be executed under an explicit consent of the data subject or under legitimate interest of the controller or a third party, it would be recommended to assess whether or not it is practical to allow the data subject to withdraw its consent at any time the data processing activities. Thus, an assessment of the possibility to apply legitimate interest is recommended to be conducted.

2.2. Contractual Basis

Under Art 6 (1) (b) of GDPR, personal data may be processed where it is necessary for the performance of the contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. It is evident that the application of this legal basis for personal data processing requires a contractual relationship between the data subject and the controller or at least an initial wish to enter into, especially data processing principles such as purpose limitation and data minimisation set out in Art 5 (1) (b) and (c) of GDPR must be considered, meaning that the legal basis for personal data processing should not be interpreted too widely. The purpose for the data processing activity must be detailed enough so that it would be clear which activities are included under the given purpose. Depending on the scope of the contract itself, regarding all activities which clearly fall under the contractual basis, this legal basis can be considered as valid. Regarding all other activities, other solutions are to be found.29

To distinguish the contractual basis from other legal bases in the context of pre-contractual relationships, it has to be assessed whether the data processing activities prior to concluding a contract are necessary to make preparations for entering into contract. What also has to be considered is whether such data processing activities are conducted at the request of the data subject. WP29 as explained that should a data subject submit to the controller any request for an offer of a quote, use of the contact details of such data subject for sending a response and retention, for a limited time, of the personal data provided by the data subject in the request would fall under this legal basis, whereas any background check conducted to the data subject would not. WP 29 has indicated that such background checks are most probably conducted

under Art 6 (1) (f). Again, the actual applicability of the legitimate interest as a legal basis for personal data processing must be determined on the basis of an assessment further explained in chapter 4.

Data processing activities necessary for the performance of a contract concluded by and between a controller and a data subject should solely cover situations and data processing activities where the processing is genuinely connected to purpose of the contract itself. This is to serve the principle of purpose limitation. This legal basis should not cover any and all activities which are “unilaterally imposed on the data subject by the controller” as this does not always mean that the processing is actually necessary for the performance of the contract. It has been established by the EDPB that the interpretation of contractual basis must be narrowed down to what is explicitly necessary for the performance of the obligations of the controller deriving from the relevant contract. The EDPB has proposed that prior to application of Art 6 (1) (b) of GDPR, an assessment of the nature of the service provided to the data subject must be carried out to identify the data processing activities where the application of contractual basis as the legal basis for personal data processing is justified. Contractual basis might therefore not be a suitable legal basis for personal data processing where certain processing activities have a rather indirect connection with the initial purpose of personal data processing indicated to the data subject.

Where a contract is covering services provided by the controller to the data subject, the contractual basis should mainly cover the actions the controller must take to fulfil its obligations under the contract. In the context of online services, the EDPB has found that when assessing the necessity of a personal data processing activity for the performance of a contract, the concept of necessity is not simply an assessment of what has been prescribed in the contract but also an assessment of what is actually relevant and foreseeable for the provision of such service. If as a result of such assessment it has been established that the processing activities

---

30 Supra nota 10, p 18.
31 Supra nota 10, pp 16-17. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (16.12.2019). In its opinion, WP29 refers to Art 7(b) of DPD which corresponds to Art 6 (1) (b) of GDPR.
32 Supra nota 10, p 10. The EDPB explains that attention should be given to the distinguishable characteristics of the service, rationale of the contract, essential elements of the contract, mutual perspectives and expectations of the parties to the contract.
33 Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subject, p 9-10. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf (16.12.2019). The EDPB has explained that “merely referencing or
are not necessary for the performance of the contract but necessary for the business of the controller, then other legal basis should be applied.\textsuperscript{34} WP29 for example has explained that the personal data of a data subject purchasing goods from a website should not be used based on Art 6 (1) (b) of GDPR also for profiling the data subject. Where the controller and data subject are parties to an employment agreement, the same goes for monitoring of employees of the controller which should not fall under the performance of the employment contract but must rather be conducted in accordance with other legal bases.\textsuperscript{35} Alternatives to the contractual basis would most likely be processing under consent, legal obligation or legitimate interest. In case there is no legal obligation regarding the processing activity (for further explanations, please see chapter 2.3 of this research paper) and consent would not be the appropriate legal basis (please see chapter 2.1. of this research paper), an assessment as per chapter 4 must be conducted to determine whether it would be possible to conduct planned personal data processing activities under legitimate interest as a legal basis.

2.3. Legal Obligations

Art 6 (1) (c) allows processing of personal data for the purpose of fulfilment of a legal obligation of a controller. For this legal basis to apply, the obligation of the controller must be imposed by law and not by any other arrangement. Based on recital 41 of GDPR, the legal obligations does not necessarily have to derive from a legal act adopted by a legislative body but in any case, the application of such legal measure must be clear, precise and its application should be foreseeable to the persons subject to it.\textsuperscript{36} Based on the above, for example in Estonia, all regulations of the governmental bodies are within the scope of this legal basis provided that such regulations are adopted under a mandate prescribed in a legal act of the parliament.

It is questionable whether any requirements of a controller operating its business inside the EU could rely on its legal obligations deriving from the laws of third countries outside of EU, when processing personal data of data subject. WP29 has found under the DPD that in such cases,

\textsuperscript{34} Ibid, p 11.

\textsuperscript{35} Supra nota 10, pp 17. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (16.12.2019). In its opinion, WP29 refers to Art 7(b) of DPD which corresponds to Art 6 (1) (b) of GDPR.

\textsuperscript{36} For common law countries, the provision includes clear common law obligations and also regulatory requirements where there is a statutory basis underpinning such regulatory regime. Source: Legal Obligation. | ICO. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/ (16.12.2019).
the processing activities would not be conducted under the legal obligation of the controller but rather under the legitimate interest of the controller, provided that the necessary measures for the application of legitimate interest as a legal basis have been taken. The authors of this research paper are of the opinion that the same principle shall continue to apply under GDPR, mainly due to the fact that this legal basis for personal data processing has not been subject to material changes, when comparing DPD and GDPR.

It must be stressed that a legal obligation can only be basis for data processing if the provision itself complies with the requirements of GDPR. The assessment about whether or not the obligation basis for data processing complies with data processing laws must be conducted prior to the adopting of the relevant legal provision. The collision of legal obligation and legitimate interest as legal bases for personal data processing may occur especially when it is not clear from the wording of a legal provision whether it intends to permit or oblige a controller to take an action for which the controller would need to process personal data. Should there be no obligation but solely a right to take a certain action in a legal provision, the controller must not apply legal obligation as the legal basis for personal data processing but rely on other legal basis, such as legitimate interest of the controller itself or a third person.

If the purpose of the legal provision is not clear neither from its wording nor from any accompanying documentation of the draft bill introducing such legal provision, in the opinion of the authors of this research paper, the controller should document its decision to process personal data on the basis of its legal obligation or consider applying legitimate interest as the legal basis. WP29 has in its legitimate interest opinion indicated that if a legal provision only sets out obligations which are general by nature, any processing activities conducted for the fulfilment of such purpose shall be deemed as conducted under legitimate interest and should be subject to the balancing test. In any such case it is probable that the legislator has not conducted any balance test determining when such legal provision could be relied on. The controller must therefore consider applying legitimate interest as the valid legal basis always in case of a legal obligations which can be widely interpreted or when it is evident that the legal

37 Supra nota 10, p 19.
38 For example, in explanatory notes of the relevant legal act or in any initial documents indicating legislative intent.
39 Supra nota 10, p 19.
40 The CJEU has analysed this matter in its decision for the case C-13/16. Although the judgement has been made under DPD and the circumstances of the case revolve around the right of a public authority to apply legitimate interest which is not permitted under Art 6 (1) of GDPR, in the context of GDPR the judgement is still relevant for private sector data controllers.
41 Supra nota 10, p 20.
provision only intends to provide a certain right to the controller.

2.4. Vital Interests

Vital interests as a legal basis set out in Art 6 (1) (d) only applies in situations where processing is necessary for the protection of the vital interests of a data subject or another natural person. What differentiates this legal basis from the legitimate interest under Art 6 (1) (f) is the fact that legitimate interest refers to the interests of the controller or a third party whereas this legal basis refers to the vital interests of natural persons. Vital interests refer to the application of this legal basis only if otherwise there would be a risk of death, injury or other damage to the health of the relevant natural person. WP29 has indicated that probably the legal bases set out in Art 6 (1) (c) and (e) of GDPR would be more appropriate in most circumstances. Therefore, this legal basis applies under very limited circumstances and requires a case-by-case analysis. Taking into consideration the above, it is evident that it would not be appropriate to rely on the vital interests of a data subject if in reality data processing is more of an interest of the controller and could be indirectly for the support of a natural person.

2.5. Public Task

Art 6 (1) (e) allows personal data processing for the performance of a task carried out in the public interests or in the exercise of official authority vested in the controller. The provision is thus most relevant to public authorities, but also to private entities carrying out activities under a mandate given by public authorities, if such tasks are carried out in public interests. The basis for data processing for public interests must be laid down in either EU legislation or the member state law to which the controller is subject. Under DPD, public authorities were also allowed to apply legitimate interests as a legal basis for personal data processing, under GDPR, it has been clearly stipulated that Art 6 (1) (f) “shall not apply to processing carried out by public authorities in the performance of their tasks”. Nevertheless, there are certain cases where these legal bases collide as public authorities may also carry out tasks which are not for the sake of public interests.

As per Art 6 (3) of GDPR, the application of Art 6 (1) (e) of GDPR requires that the relevant tasks are laid down by the law and thus member states of the EU are permitted to introduce authorisation for personal data processing for the performance of certain public tasks. It may be that the exercise of official authority does not allow for such processing, but other legislative

---

42 Supra nota 10, p 20.
43 Supra nota 13.
bases such as “health and safety” for the protection of employees, visitors and employees may provide limited scope of processing, while still having regard for GDPR obligations and data subject rights.\textsuperscript{44} This does not enable the legislator to deviate from the data processing principles set out in Art 5 of GDPR.

Art 6 (1) does not allow public authorities to rely on Art 6 (1) (f) of GDPR for the performance of their tasks but only if they are processing for a legitimate reason other than performing their tasks as a public authority.\textsuperscript{45} This leaves little to none room for the public authorities to apply this legal basis, so that the legitimate interests under Art 6 (1) (f) of GDPR is not to be taken as a considerable alternative for Art 6 (1) (e) of GDPR. Where the collision of these two legal bases might take place is where there is no certainty to whether or not a certain data processing activity conducted by a public authority falls under the performance of a public task. In any of these cases, it must be assessed initially whether there is a possibility to apply legitimate interests as a legal basis and thereafter it must be assessed, as further explained in chapter 4, whether the legitimate interests of such public authority when conducting data processing activities not connected to the fulfilment of its public tasks, are overridden by the interests or fundamental rights and freedoms of the data subjects.


3. Third Party’s Legitimate Interests

3.1. The Possibility to Apply Third Party’s Interests

This and the following sub-chapters focus on the possibilities of the data controller to rely on the legitimate interests of a third party, instead of the data controller’s interests.

The wording of the Art. 6 (1) (f) allows the processing to be lawful when legitimate interests are being pursued by the controller or by a third party. Both the terms “controller” and “third party” have been defined in Art. 4 of the GDPR – in Art. 4 (7) and Art. 4 (10), respectively.\(^46\)

The definition of a third party is provided via an exclusion method, meaning, that in the context of the concerned personal data processing operation, a third party can be a natural or a legal person (including a public authority, agency or a body) who is not the data subject, the controller, a processor nor a person who processes the data under the direct authority (or control) of the latter two.

Confusion may exist in allocating a processing role, i.e. a data controller or a data processor, to a third party, particularly, as the term’s definition provided in Art. 4 (10) does exclude it from being a data controller or a processor. However, the foregoing concept should be viewed similarly as used in civil law, meaning, someone who is not a party to an agreement, meaning, currently, someone who is not part of the data subject – data controller (or data subject – data processor for that matter) relationship in the context of which the personal data for a certain purpose is processed.\(^47\)

This does not, however, exclude the third party, for whose legitimate interests the controller processes the said data, for having, and setting, separate data processing purposes and means. In case the third party has its own set of interests, and providing that the other conditions for controllership as defined in Art. 4 (7) are satisfied, it is most likely that the third party (for example after granted access to the data as a result of a data transfer or disclosure) qualifies as a (separate) data controller (or a data processor who is processing the concerned data on behalf of a separate data controller).\(^48\)

\(^{46}\) Art. 4 (7) defines the “controller” as a “—/— natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data /—/; Art. 4 (10) defines a third party as a “—/— natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data”

\(^{47}\) Supra nota 12, p 13

under Art. 4 (8) of the GDPR, is processing personal data on behalf of the data controller then from the perspective of lawfulness, meaning, the legal basis for processing, the data processor’s data processing activity is determined by the data controller. Therefore, as the activities’ mandate of the data processor is provided and covered by the data controller, then the data controller, by definition of Art. 4 (7) of the GDPR and pursuant to the interpretation of the WP29, decides also the purposes and means of the data processor for the specific data processing operations which in turn would indicate that the data processor in itself would not have any interests (legitimate or otherwise) of its own in the processing. Namely, this would indicate that in case the interests of the third party are assessed for the purposes of the application of the legitimate interests' ground, the interests of the data controller are assessed instead of the data processor. Pursuant to the aforementioned interpretation this would not be affected by the mere technicalities of the data processing operation for which the contemplated legitimate interests as a legal ground would be used, for example in case of a data transfer, the fact that a data processor would be the one receiving the personal data would mean that the controller transferring the data would need to assess the legitimate interests of the data processor.

Therefore, generally, the legitimate interests of the third party concern the interests of the third party as a, at least potential, separate controller – however, there are possible exceptions as discussed in the following chapter.

3.2. Third Party Interests as Mainly a Basis for Data Disclosure or Data Transfer to the Third Party

The text of the GDPR does not limit any third party interests as such, however, as explained in the following paragraphs, available literature and guidance papers mainly focus on the usability of the third party interests in situations whereby the data controller intends to process the personal data for making it available, including transferring or disclosing, the data to the third parties whose interests are concerned.

For example, the ICO explains the third party’s interests in the context of disclosure of data to the third party, stating, among others, that the disclosing data controller should be mainly concerned with justifying its own interests for the disclosure (meaning, whether the disclosure

---

itself is justified) as the receiving third party is responsible for ensuring the lawfulness and fairness of its own (further) processing\(^{50}\), indicating that the receiving third party is a (separate) data controller.

In its April 2014 opinion on the notion of legitimate interests of the data controller, the WP29 illustrates the possibility to apply third party’s interests in the context of a possible publication of the data for the purposes of transparency and accountability, disclosing the data for the purposes of research and for taking measures which serve the interests of a general public. Thereby, the possible examples do include again making the concerned data available, e.g. through disclosure, to the third parties based on whose interests the disclosure takes place. WP29, however, does accept the possibility to evaluate the interests of the “third party” as a group, section or subsection of the society.\(^{51}\) Therefore, it can be deducted that the evaluation of the legitimate interests does not have to be limited only in the context of a third party as an single entity but it is also possible for the disclosing controller to consider and evaluate a third party as a group of (potential) data controllers which carry, at least in relation to the disclosure, a homogenic set of interests. Nevertheless, it should be noted that the aforementioned conclusion of the authors of this research paper is contradictory as it is not in line with the understandings of the EDPI - according to the latter, no permanent data processing operations can rely on the legitimate interests legal basis, as its application presumes assessing the possible effects on the individual’s private life each and every time\(^{52}\), making it impossible to apply any interests on a general basis without conducting a separate balancing test each time.

The only instance whereby the CJEU has dealt with the issue of third-party legitimate interests in the context of a data disclosure to third parties and the possibility to rely on the legitimate interests of the third party by the disclosing data controller was in the Rīgas satiksme case. In the aforementioned case, a third party’s (legitimate) interest of receiving/obtaining personal data about a person who had damaged their property was confirmed, as the third party’s interests were of asserting its legal claims against the inflictor of the damage.\(^{53}\)

Deriving from the aforementioned, the legitimate interests of the third party can, as a general

\(^{50}\) Supra nota 9.

\(^{51}\) WP29 does discuss the interests of the general public and scientific researchers for the purposes of accessing databases. Supra nota 10, pp 27 – 29.

\(^{52}\) For example, please see the Estonian Data Protection Authority’s response in an inquiry 2.1.-5/18/1619, 05.07.2018. Available at: https://adr.rik.ee/aki/dokument/5861602 (12.12.2019)

\(^{53}\) Case C-13/16, Valsts policijas Rīgas regiona pārvaldes Kārtības policijas pārvalde vs Rīgas pašvaldības SIA ‘Rīgas satiksme’
rule, be used as the underlying interests or the purpose(s) for the processing in cases where it concerns the third party’s intention or need to obtain the personal data, or the disclosing controller’s intention to disclose the personal data to the third party. However, the receiving third party should still keep in mind the obligation deriving from the GDPR, as explained in the chapter below.

3.3. Third Party’s Limitations Upon Receiving the Data

According to Art. 3 (1) and Art. 5 (2) of the GDPR\textsuperscript{54}, the GDPR applies to the personal data controllers and personal data processors while the controllers are under the obligation, pursuant to the accountability principle, to ensure that the personal data is processed in accordance with the principles of the GDPR.

As demonstrated in chapter 3.1. above, assessing a third party’s legitimate interests for the purposes of applying the legitimate interests ground as a basis for personal data processing would most likely taken place prior to a disclosure or transfer situation of the concerned data to the third party whose interests are applied in the assessment. As in principle, the third party receiving the personal data would be considered a (separate) data controller\textsuperscript{55} upon receipt of the personal data\textsuperscript{56} then the receiving controller is responsible for ensuring its own lawful basis for such data processing\textsuperscript{57}, including fulfilling other obligations to which the controller is subject pursuant to the GDPR.

It must be noted that in case a third party, i.e. a receiving data controller, received a set of data from a separate data controller, the receiving data controller, whose legitimate interests also formed a basis for the data transfer, must take into account that it is further affected, and likely limited, in its data processing operations by the same legitimate interests and by the set of

\textsuperscript{54} Art. 3 (1) states that the GDPR, meaning, rights and obligations deriving from it ”/–/ applies to the processing of personal data in the context of the activities /–/ of a controller or a processor in the Union.”; Art. 5 (2) sets in place the accountability principle of the GDPR, meaning, that it is the controller who is responsible for the protection of personal data: ”(The) controller shall be responsible for, and be able to demonstrate compliance with paragraph 1.” "Paragraph 1” indicates to the principles of the GDPR, including to the principle of lawfulness, fairness and transparency under which the controllers are obligated to ensure that their processing is based on a legal ground pursuant to Article 6 of the GDPR.

\textsuperscript{55} As explained in the beginning of chapter 3 of this research paper, the interests of the processor should be interpreted, due to the definition of a data processor, to be aligned with the controller’s, meaning, provided that the data processor does not set its own data processing purposes and means, the disclosure of personal data to the processor should be viewed as a disclosure of data to the controller. Please see footnote 49.

\textsuperscript{56} Supra nota 12, p 14

information made available by the transferring controller to the affected data subject, as required under its transparency obligations pursuant to Article 13 of the GDPR. It is recommended that the receiving controller takes steps to make sure that the information initially made available to the data subject by the transferring controller regarding the purposes of the transfer covers the intended processing operations to be taken by the receiving controller. Deriving from the aforementioned, in case the data processing operation, meaning, the transfer, took place under the legitimate interests of the receiving controller, then upon receipt using the data for another purpose by the receiving controller instead of the one forming part of the interests on which the transfer took place (and which were communicated to the data controller), may render the transfer of the said data unlawful, causing the transferring controller to breach its obligations under Article 5 (1) (a) and Article 6 (1) due to the actions of the receiving controller. In case the receiving controller intends to process the received personal data also under the legitimate interests legal ground, then in case the communicated interests by the transferring data controller differ from the interests for which the processing by the receiving controller should take place, then a mismatch may incur in the data subject’s reasonable expectations making it difficult for the receiving controller to rely on its own legitimate interests for the processing.

58 The transferring controller is required to disclose the interests in question to the data subject before processing his/her data under the legitimate interests legal basis under Art. 6 (1) (f). As a matter of best practice, the controller can also provide information on the balancing test itself. Supra nota 21, p 36.


60 According to recital 47 of the GDPR, the reasonable expectations of the data subject have to be viewed at the time and in the context of the collection of the personal data, meaning that the data subject should have expected that the specific processing for that processing may take place. In case the data subject does not expect such (further) processing, the interests and fundamental rights of the data subject could easily override the legitimate interests of the controller in a balancing test. However, critique has been launched against the “reasonable expectation of the data subject”, as what is reasonable is most likely influenced by previous and dominant market practices of large players on the field. Supra nota 12, p 17
4. Elements of Legitimate Interest Assessment

4.1. Purpose Test

As it is outlined in the chapter 1.1 of this research paper, the required elements for the GDPR Art 6 (1) (f) assessment are necessity, purposefulness and balance between the controller’s rights and data subject’s fundamental rights and obligations. Applicability of the GDPR Art 6 (1) (f) as a legal basis for personal data processing requires thus a legitimate interests assessment.

The GDPR does not set out as a precise legal obligation to conduct a legitimate interest assessment nor its specific requirements. However, the necessity to conduct such legitimate interest assessment derives from Art 5 (2) of the GDPR in relation to the data controller’s accountability purposes. Furthermore, the obligation to conduct a legitimate interest assessment is in line with the CJEU case law. The CJEU set out three cumulative conditions that must be fulfilled for personal data processing to be lawful on the “legitimate interest basis”, specifying that personal data processing must firstly pursue a legitimate interest (have a specific purpose), secondly, that the processing of personal data must be necessary for the purposes of the legitimate interests pursued and thirdly, the fundamental rights and freedoms of the data subject must not take precedence over the controller’s or third parties’ legitimate interest. The balance of interest must be done on a case-by case basis, taking into account elements such as the severity of the infringement of the data subject’s rights or even the age of data subject in certain circumstances. Some guidelines for conducting legitimate interest assessment are also stipulated in the recitals of the GDPR.

Pursuant to the recital 47 of the GDPR, the legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Prior to the processing, a legitimate interest of the controller would need careful assessment, including whether a data subject can reasonably expect, at the time and in the collection of the personal data, that processing for that

---

61 As opposed, for example deriving from Art 35 of the GDPR, the explicit obligation to conduct a data protection impact assessment if a type of processing in particular using new technologies and taking into account the nature and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

62 Supra nota 53.
purpose may take place. The recital 47 of the GDPR further provides couple of examples what kind of data processing activities could be regarded as carried out for a controller’s legitimate interest. Such examples are processing of personal data the purposes of preventing fraud and for direct marketing purposes. However, even though the GDPR explicitly sets forth that controller’s may rely on their legitimate interest when processing personal data for the purposes suggested in the recital 47 controllers, willing to rely on legitimate interest as a legal basis, are still not excluded of conduction of the legitimate interest assessment.

The ICO has outlined comprehensive set of questions for the controllers to be able to assess, whether the data is collected for the legitimate purpose. According to the guidelines of the ICO the controller should ask itself, prior to personal data processing activities under the GDPR Art 6 (1) (f) the precise purpose of the personal data processing; what kind of benefits controller is expecting to get from the processing; do any third parties benefit from the processing; are there any wider public benefits to the processing and what is the importance of aforementioned benefits. Furthermore, the controller should ask itself, what could be the impact if the processing activities are not commenced; what is the outcome for individuals; is the controller complying with other relevant laws; is the controller complying with industry guidelines or codes of practice; and are there any ethical issues with the processing. It can be thus derived from above, that sole determination of the necessity to commence personal data processing activities is not sufficient for the processing procedures under the Art 6 (1) (f) of the GDPR. The ICO guidance indicates, that there are multiple different aspects the controllers must weigh in order to justify their legitimate interest for the personal data processing.

Some interests are likely to be “legitimate” because they are necessary for an administrative function or compliance issue. This is often the case, when the processing is not required by law, but the processing is essential to ensure the controller’s external or internal governance obligations, for example the provision of physical or internet security. As mentioned above,
the recital 47 of the GDPR itself provides these cases where legitimate interest can be relied upon. The controller thus has a legitimate interest for personal data processing when the processing takes place within a client relationship, when it processes personal data for direct marketing purposes, to prevent fraud or to ensure the network and information security of the company’s IT-systems. However, pursuant to the guidelines of the ICO even if personal data is used for one of the purposes which are specifically outlined in the GDPR that these should fall under the legitimate interests then the necessary assessment should still be carried out. However, depending on the circumstances, in some cases the legitimate interest assessment could be quite brief but still containing all its elements.\(^{65}\) It thus must be concluded that even though the GDPR itself provides guidelines for in which cases the personal data are likely to be processed under the controller’s legitimate interests, the legitimate interest assessment must be concluded in full, to determine, whether the circumstances of personal data processing activities allow the shorter legitimate interest assessment.

As an example, legitimate interest might be a legal ground for conducting video surveillance. In practice, the purpose to protect property against burglary, theft or vandalism can constitute a legitimate interest for video surveillance. However, a real-life situation of distress needs to be at hand – such as damages or serious incidents in the past – before starting the surveillance. In light of the principle of accountability, controllers would be well advised to document relevant incidents (date, manner, financial loss) and related criminal charges. Those documented incidents can be a strong evidence for the existence of a legitimate interest. Imminent danger situations may constitute a legitimate interest, such as shops selling precious goods (e.g.) jewellers, or areas that are known to be typical crime scene for property offences (e.g. petrol stations).\(^{66}\) Furthermore, even if there is an existence of a necessary purpose (protection of assets), the controller must assess, whether it is possible to use any less invasive measures (for example hiring a security officer). However, the mere fact that the controller has such a legitimate interest (purpose) does not mean that the personal data processing can necessarily rely on such legitimate interest,\(^{67}\) but continuing with the assessment is still necessary.

---

65 Ibid.
66 Supra nota 44, p 8.
67 Supra nota 10, p 24.
4.2. Necessity Test

The second element of the legitimate interest assessment is a test for determining the necessity for the purpose of the personal data processing. The necessity must be evaluated carefully from the perspective of the controller, or in case the processing concerns a third party, then from the perspective of the respective party.68 In practice, legitimate interest can only be relied upon as a lawful basis of processing to the extent where it is necessary. The necessity of personal data processing has to be interpreted together with the Art 5 (1) (c) of the GDPR, according to which personal data collected, should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation principle). It thus must be concluded, that the “necessity” requirement applies to all legal grounds under the GDPR but is particularly relevant in the case of relying on Art 6 (1) (f) of the GDPR to ensure that processing of data based on legitimate interest will not lead to unduly broad interpretation of the necessity. Nevertheless, the necessity criteria mean that it should be considered whether other less invasive means are available to serve the same end.69

Legitimate interest gives the controller the obligation to explain their processing purpose and to justify why this is the personal data processing necessary and the controller must ensure and demonstrate that its interests are balanced with the individual’s.70 The ICO has set forth multiple guiding elements which need to be analysed when assessing the necessity of the personal data processing. According to the ICO, the controller should evaluate: whether the processing actually helps the controller to achieve its purpose; is the processing proportionate to that purpose; is it possible to achieve the controller’s purpose without processing the data or by processing less data and if it is possible to achieve the purpose by processing the data in another more obvious or less intrusive way.71 The necessity has to be determined per the specific purpose chosen by the controller for the processing since the legitimate interest as a legal basis for personal data processing is not purpose-specific. However, it also promotes a risk-based approach to compliance as controllers need to think about the impact of personal data processing on individuals, which aims to help controllers to identify possible risks and take appropriate safeguards.72

---

68 Supra nota 10, p 29.
69 Supra nota 10, p 11.
70 Supra nota 9.
71 Supra nota 64.
72 Supra nota 9.
Referring to the video-surveillance system example introduced already in the previous chapter, when installing such system, the controller should always on a case-by-case basis critically examine, if this measure is firstly suitable to attain the desired goal (generally the goal is the protection of the one’s property), and secondly adequate, meaning necessary for its purposes. Video surveillance measures should only be chosen if the purpose of the processing could not reasonably be fulfilled by other means which are less intrusive to the fundamental rights and freedoms of the data subject.

4.3. Balancing Test

The necessity of conducting a balance test prior to the processing activities was introduced already under the DPD. This approach requires balancing not only of the controllers’ legitimate interest and the data subjects’ right to privacy but assessing the impact to other relevant fundamental rights of data subjects. Again, there is no exhaustive list of what the controller should take account when conducting the balancing test. However, the ICO has set out three minimum aspects that need to be considered. Firstly, the nature of the personal data the controller wants to process. Hereby, the controller should think about the sensitivity of the personal data it intends to process and assess, whether the personal data being processed falls in the special category data, criminal offence data or children’s data or data relating to other vulnerable individuals. The reasonable expectations of the individual and the likely impact of the processing on the individual and whether any safeguards can be put in place to mitigate negative impacts.

According to the opinion of WP29 there are only a few human rights that cannot be balanced against the rights of others, or the interests of the wider community. These are absolute rights that can never be limited or restricted. Such rights are for example right not be tortured or treated in an inhuman or degrading way. Examples of non-absolute human rights include the right to respect for private and family life, the right to freedom of expression and the right to freedom of thought, conscience and religion. Among the fundamental rights and freedoms enshrined in the European Charter of the Fundamental Rights and interpreted by the ECHR, several may come into conflict with the right to privacy and the right to the protection of personal data, such as freedom of expression and information, freedom of the arts and sciences,

73 Supra nota 10, p 11.
74 Supra nota 64.
75 Supra nota 64.
76 Supra nota 10, p 11.
right of access to documents, as well as for instance the right to liberty and security, the freedom of thought etc. For the controller’s legitimate interest to prevail, the data processing must be necessary (as explained above) and proportionate in order to exercise the fundamental right concerned.\footnote{Supra nota 10, p 34.}

Interests and rights should be given a broad interpretation. From one hand, the broader interpretation ensures stronger protection of data subjects. However, in practice, determining the relevant fundamental rights would be rather difficult. This test may lead to the conclusion in certain cases that the balance weighs in favour of the interests and fundamental rights of the data subjects, and that consequently the processing activity cannot take place. On the other hand, an appropriate balance, often with an opportunity to opt-out of the processing may in other cases be a valid alternative to inappropriate use of, for instance, the ground of consent or the performance of a contract (Article 6 (1) (a) and (c) of the GDPR).

Looking at the other side of the balance, the impact of the processing on the interests or fundamental rights and freedoms of the data subject is a crucial criterion. Working Party has determined several elements, that can be useful when weighing the balance between the controllers’ legitimate interest and data subject rights. In assessing the impact of the processing, both positive and negative consequences should be taken into account. These may include potential future decisions or actions by third parties, and situations where the processing may lead to the exclusion of, or discrimination against, individuals, defamation, or more broadly, situation where there is a risk of damaging the reputation, negotiating power, or autonomy of the data subject. Furthermore, broader emotional impacts also need to be taken into account, such as the irritation, fear and distress that may result from a data subject losing control over personal information or realising that it has been or may be misused or compromised.
Summary

The GDPR has brought data protection and its requirements to the centrepiece of many companies and public authorities in the EU due to enhanced obligations compared to the DPD, and national legislation based on the DPD, and due to the possibility to be subject to high sanctions for breaches.

One of the most essential tasks for the controller when processing personal data is determining the legal grounds for doing so. The GDPR provides six legal grounds for data processing, each with different prerequisites and limitations. Although some legal grounds may be clearer and less burdensome to apply, others create challenges to the data controllers due to the multiple requirements and limitations attached to it. In this research paper the authors analysed one of the most challenging legal grounds, namely the legitimate interests ground under Art 6 (1) (f) of the GDPR. For any data controllers located in Estonia, the aforementioned legal ground did not exist before the application of the GDPR, although, it did exist in the DPD as well.

In the limits of the legitimate interests legal ground, the authors focused on highlighting the limitations of the legal ground, controller-related obligations and on the interplay of the legal ground with other legal grounds present in the GDPR. Additionally, attention was given to the third party’s legitimate interests to which the controllers can rely on when processing data subject’s personal data under the legitimate interests ground and to the elements forming the legitimate interests assessment test.

There are a number of obligations which relate more specifically to the application of the legitimate interests legal ground by the controller. The prerequisite of applying the legitimate interests legal ground is the legitimate interests assessment test, which consists of the purpose test, necessity test and balancing test. Each test has to be completed in a positive manner for the controller to be able to rely on it. Public authorities are limited in their application of the legitimate interests ground, as for them it is only possible for tasks outside their official tasks. The research paper further highlights key obligations of the controller, namely, the requirement to have more detailed attention on some of the principles of the GDPR, as they are more related and affected by the assessment test, i.e. the principles of lawfulness, fairness, data minimisation, integrity, transparency and purpose limitation. The accountability principle brings along documentation obligation of the assessment test. Moreover, the data controller should focus on the data subjects right to object to the use of the legitimate interests legal
ground, as this may bring along to adjust its assessment test to the circumstances of the specific data subject.

Regarding the interplay with the other legal grounds under the GDPR, the data controller should consider the pros and cons of each legal ground. This research paper brings out the strengths and weaknesses of each possible ground. The data controller should be careful when choosing to base its data processing activities on the consent of the data subject, as consent provides very little flexibility and is withdrawable at any given moment leaving the data controller without a legal ground of further processing. For applying the contractual basis for data processing, the controller is firstly challenged with the need to have the contract in place directly with the data subject as a party to it and limiting its data processing operations only to what are truly necessary for such purposes – the controller should not unilaterally impose purposes onto the data subject in case they fall outside the contract’s scope. Therefore, in case the data controller would like to broaden its scope of processing activities to purposes side-lining with the agreement, the data controller could consider the legitimate interests ground. In certain cases, the data controller is also entitled to rely on its legal obligations for the data processing. The legal obligation has to be an obligation and not a right. Legitimate interests could come into play when the controller would like to rely on third country laws for certain processing, e.g. in case the controller belongs to a group of companies, or for enforcing its rights (and not obligations) granted to it under relevant laws. The vital interests and public task grounds were also analysed, however, in those cases the possible collision of the legitimate interests ground is less likely, however, in times, public authorities could find it difficult to interpret when are they acting outside their official capacity and are entitled to apply the legitimate interests ground.

According to the analysis conducted in the scope of this paper, the authors concluded that the legitimate interests of a third party might be applied by the data controller usually in the cases where the concerned data is to be transferred or disclosed to the same third party based on whose interests the data controller processes the data. The third party receiving the data is, as a general rule, to be interpreted as a separate data controller with all the relevant obligations of a data controller under the GDPR. However, the receiving data controller should exercise care for determining which interests the transferring controller has communicated to the affected data subjects, as the receiving controller is usually limited in its data processing operation by the same interests, especially, in case it also relies on the legitimate interests legal ground.
The legitimate interests assessment test is a key element for successfully applying the legal ground. No part of the test should be preferred to the other. The authors have heavily relied on the ICO’s guidance in this matter, as the ICO has thorough information available online. Firstly, the data controller should understand whether its interests are legitimate in terms of. Usually processing which serves an administrative or compliance function, including possible security functions, can be considered legitimate. Secondly, the necessity test does centre the purpose of the processing - the necessity has to be determined per the specific purpose chosen by the controller for the processing since the legitimate interest as a legal basis for personal data processing is not purpose-specific. Finally, the balancing test has to consider the rights and interests of the data subject in a wide and broad scale, while the controller does need to weigh conflicting rights.

Therefore, the legitimate interests as a legal ground does offer a great degree of flexibility to the data controller, however, its application is connected with many considerations, which are not to be taken likely. Due to its many elements and requirements, relying on the legal is connected to a considerable risk of breach of the GDPR, however, when applied with care offers much opportunities to the data controllers and third parties for achieving their legitimate processing purposes by offering necessary protection for the data subjects.
Bibliography

List of literature:


Case law:


Internet resources:

- When can we rely on legitimate interests? | Information Commissioner’s Office of the


Legal acts:

- Directive 95/46/EC of the European Parliament and of the Council dated 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive)

- Regulation (EU) 2016/679 of the European Parliament and of the Council dated 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)