ARTICLE 29 DATA PROTECTION WORKING PARTY

844/14/EN
WP 217

Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC

Adopted on 9 April 2014

Table of contents

Executive Summary 3
I. Introduction 4
II. General observations and policy issues 6
II.1. Brief history 6
II.2. Role of concept 9
II.3. Related concepts 10
II.4. Context and strategic consequences 12
III. Analysis of provisions 13
III.1. Overview of Article 7 13
III.1.1. Consent or 'necessary for...' 13
III.1.2. Relationship with Article 8 14
III.2. Article 7(a)-(e) 16
III.2.1. Consent 16
III.2.2. Contract 16
III.2.3. Legal obligation 19
III.2.4. Vital interest 20
III.2.5. Public task 21
III.3. Article 7(f): legitimate interests 23
III.3.1. Legitimate interests of the controller (or third parties) 24
III.3.2. Interests or rights of the data subject 29
III.3.3. Introduction to applying the balancing test 30
III.3.4. Key factors to be considered when applying the balancing test 33
III.3.5. Accountability and transparency 43
III.3.6. The right to object and beyond 44
IV. Final observations 48
IV.1. Conclusions 48
IV. 2. Recommendations 51
Annex 1. Quick guide on how to carry out the Article 7(f) balancing test 55
Annex 2. Practical examples to illustrate the application of the Article 7(f) balancing test 57

Executive Summary

This Opinion analyses the criteria set down in Article 7 of Directive 95/46/EC for making data processing legitimate. Focusing on the legitimate interests of the controller, it provides guidance on how to apply Article 7(f) under the current legal framework and makes recommendations for future improvements.

Article 7(f) is the last of six grounds for the lawful processing of personal data. In effect it requires a balancing of the legitimate interests of the controller, or any third parties to whom the data are disclosed, against the interests or fundamental rights of the data subject. The outcome of this balancing test will determine whether Article 7(f) may be relied upon as a legal ground for processing.

The WP29 recognises the significance and usefulness of the Article 7(f) criterion, which in the right circumstances and subject to adequate safeguards may help prevent over-reliance on other legal grounds. Article 7(f) should not be treated as 'a last resort' for rare or unexpected situations where other grounds for legitimate processing are deemed not to apply. However, it should not be automatically chosen, or its use unduly extended on the basis of a perception that it is less constraining than the other grounds.

A proper Article 7(f) assessment is not a straightforward balancing test consisting merely of weighing two easily quantifiable and comparable 'weights' against each other. Rather, the test requires full consideration of a number of factors, so as to ensure that the interests and fundamental rights of data subjects are duly taken into account. At the same time it is scalable which can vary from simple to complex and need not be unduly burdensome. Factors to consider when carrying out the balancing test include:

- the nature and source of the legitimate interest and whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest, or benefits from recognition in the community concerned;

- the impact on the data subject and their reasonable expectations about what will happen to their data, as well as the nature of the data and how they are processed;

- additional safeguards which could limit undue impact on the data subject, such as data minimisation, privacy-enhancing technologies; increased transparency, general and unconditional right to opt-out, and data portability.

For the future, the WP29 recommends implementing a recital to the proposed Regulation on the key factors to consider when applying the balancing test. The WP29 also recommends that a recital be added requiring the controller, when appropriate, to document its assessment in the interests of greater accountability. Finally, the WP29 would also support a substantive provision for controllers to explain to data subjects why they believe their interests would not be overridden by the data subject's interests, fundamental rights and freedoms.

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT OPINION:

I. Introduction

This Opinion analyses the criteria set forth in Article 7 of Directive 95/46/EC[1] (the 'Directive') for making data processing legitimate. It focuses, in particular, on the legitimate interests of the controller, under Article 7(f).

The criteria listed in Article 7 are related to the broader principle of 'lawfulness' set forth in Article 6(1)(a), which requires that personal data must be processed 'fairly and lawfully'.

Article 7 requires that personal data shall only be processed if at least one of six legal grounds listed in that Article apply. In particular, personal data shall only be processed (a) based on the data subject's unambiguous consent[2]; or if - briefly put[3] - processing is necessary for:

(b) performance of a contract with the data subject;
(c) compliance with a legal obligation imposed on the controller;
(d) protection of the vital interests of the data subject;
(e) performance of a task carried out in the public interest; or
(f) legitimate interests pursued by the controller, subject to an additional balancing test against the data subject's rights and interests.

This last ground allows processing 'necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests (f)or[4] fundamental rights and freedoms of the data subject which require protection under Article 1(1)'. In other words, Article 7(f) allows processing subject to a balancing test, which weighs the legitimate interests of the controller - or the third party or parties to whom the data are disclosed – against the interests or fundamental rights of the data subjects.[5]

---

[1] Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281,23.11.1995, p. 31).

[2] See Opinion 15/2011 of the Article 29 Data Protection Working Party on the definition of consent, adopted on 13.07.2011 (WP187).

[3] These provisions are discussed in greater detail at a later stage.

[4] As explained in Section III.3.2, the English version of the Directive appears to contain a typo: the text should read 'interests or fundamental rights' rather than 'interests for fundamental rights'.

[5] The reference to Article 1(1) should not be interpreted to limit the scope of the interests and fundamental rights and freedoms of the data subject. Rather, the role of this reference is to emphasise the overall objective of data

Need for a more consistent and harmonized approach across Europe

Studies conducted by the Commission in the framework of the review of the Directive[6] as well as cooperation and exchange of views between national data protection authorities ('DPAs') have shown a lack of harmonised interpretation of Article 7(f) of the Directive, which has led to divergent applications in the Member States. In particular, although a true balancing test is required to be performed in several Member States, Article 7(f) is sometimes incorrectly seen as an 'open door' to legitimise any data processing which does not fit in one of the other legal grounds.

The lack of a consistent approach may result in lack of legal certainty and predictability, may weaken the position of data subjects and may also impose unnecessary regulatory burdens on businesses and other organisations operating across borders. Such inconsistencies have already led to litigation before the Court of Justice of the European Union ('ECJ')[7].

It is therefore particularly timely, as work towards a new general Data Protection Regulation continues, that the sixth ground for processing (referring to 'legitimate interests') and its relationship with the other grounds for processing, be more clearly understood. In particular, the fact that fundamental rights of data subjects are at stake, entails that the application of all six grounds should - duly and equally - take into account the respect of these rights. Article 7(f) should not become an easy way out from compliance with data protection law.

This is why the Article 29 Data Protection Working Party ('Working Party'), as part of its Work Programme for 2012-2013, has decided to take a careful look at this subject and - to execute this Work Programme[8] - committed to draft this Opinion.

Implementing the current legal framework and preparing for the future

The Work Programme itself clearly stated two objectives: 'ensuring the correct implementation of the current legal framework' and also 'preparing for the future'.

Accordingly, the first objective of this Opinion is to ensure a common understanding of the existing legal framework. This objective follows earlier Opinions on other key provisions of

---

protection laws and the Directive itself. Indeed, Article 1(1) does not only refer to the protection of privacy but also to the protection of all other 'rights and freedoms of natural persons', of which privacy is only one.

[6] On 25 January 2012, the European Commission adopted a package for reforming the European data protection framework. The package includes (i) a 'Communication' (COM(2012)9 final), (ii) a proposal for a general 'Data Protection Regulation' ('proposed Regulation') (COM(2012)11 final), and (iii) a proposal for a 'Directive' on data protection in the area of criminal law enforcement (COM(2012)10 final). The accompanying 'Impact Assessment', which contains 10 annexes, is set forth in a Commission Working Paper (SEC(2012)72 final). See, in particular, the study entitled 'Evaluation of the implementation of the Data Protection Directive', which forms Annex 2 to the Impact Assessment accompanying the European Commission's data protection reform package.

[7] See page 7, under the heading 'II.1 Brief History', *'Implementation of the Directive; the ASNEF and FECEMD judgment'*.

[8] See Work programme 2012-2013 of the Article 29 Data Protection Working Party adopted on 1 February 2012 (WP190).

the Directive[9]. Secondly, building on the analysis, the Opinion will also formulate policy recommendations to be considered during the review of the data protection legal framework.

Structure of the Opinion

After a brief overview of the history and role of legitimate interests and other grounds for processing in Chapter II, Chapter III will examine and interpret the relevant provisions of the Directive, taking into account common ground in their national implementation. This analysis is illustrated with practical examples based on national experience. The analysis supports the recommendations in Chapter IV both on the application of the current regulatory framework and in the context of the review of the Directive.

II. General observations and policy issues

II.1. Brief history

This overview focuses on how the concepts of lawfulness and legal grounds for processing, including legitimate interests, have developed. It explains in particular how the need for a legal basis was first used as a requirement in the context of derogations to privacy rights, and subsequently developed into a separate requirement in the data protection context.

European Convention on Human Rights ('ECHR')

Article 8 of the European Convention on Human Rights, adopted in 1950, incorporates the right to privacy - i.e. respect for everyone's private and family life, home and correspondence. It prohibits any interference with the right to privacy except if 'in accordance with the law' and 'necessary in a democratic society' in order to satisfy certain types of specifically listed, compelling public interests.

Article 8 ECHR focuses on the protection of private life, and requires justification for any interference with privacy. This approach is based on a general prohibition of interference with the right of privacy and allows exceptions only under strictly defined conditions. In cases where there is 'interference with privacy' a legal basis is required, as well as the specification of a legitimate purpose as a precondition to assess the necessity of the interference. This approach explains that the ECHR does not provide for a list of possible legal grounds but concentrates on the necessity of a legal basis, and on the conditions this legal basis should meet.

Convention 108

The Council of Europe's Convention 108[10], opened for signature in 1981, introduces the protection of personal data as a separate concept. The underlying idea at the time was not that processing of personal data should always be seen as *'interference* with privacy', but rather that to *protect* everyone's fundamental rights and freedoms, and notably their right to privacy,

[9] Such as Opinion 3/2013 on purpose limitation, adopted on 03.04.2013 (WP203), Opinion 15/2011 on the definition of consent (cited in footnote 2), Opinion 8/2010 on applicable law, adopted on 16.12.2010 (WP179) and Opinion 1/2010 on the concepts of 'controller' and 'processor', adopted on 16.02.2010 (WP169).

[10] Convention 108 for the Protection of Individuals with regard to automatic processing of personal data.

processing of personal data should always fulfil certain conditions. Article 5 thus establishes the fundamental principles of data protection law, including the requirement that 'personal data undergoing automatic processing shall be: (a) obtained and processed fairly and lawfully'. However, the Convention did not provide detailed grounds for processing.[11]

OECD Guidelines[12]

The OECD Guidelines, prepared in parallel with Convention 108 and adopted in 1980, share similar ideas of 'lawfulness', although the concept is expressed in a different way. The guidelines were updated in 2013, without substantive changes to the principle of lawfulness. Article 7 of the OECD Guidelines in particular provides that 'there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.' Here the legal ground of consent is explicitly mentioned as an option, to be used 'where appropriate'. This will require an appreciation of the interests and rights at stake, as well as assessing how intrusive the processing is. In this sense the OECD approach shows some similarities with the – much more developed – criteria provided in Directive 95/46/EC.

Directive 95/46/EC

When adopted in 1995, the Directive was built on early data protection instruments, including Convention 108 and the OECD Guidelines. Early experience with data protection in some Member States was also considered.

In addition to a broader requirement set forth in its Article 6(1)(a) that personal data must be processed 'fairly and lawfully', the Directive added a specific set of additional requirements, not yet present as such in either Convention 108 or the OECD Guidelines: the processing of personal data must be based on one of the six legal grounds specified in Article 7.

Implementation of the Directive; the ASNEF and FECEMD judgment[13]

The report of the Commission entitled 'Evaluation of the implementation of the Data Protection Directive'[14] underlines that the implementation of the provisions of the Directive in national law has sometimes been unsatisfactory. In the technical analysis of the transposition of the Directive in the Member States[15], the Commission gives further details on the implementation of Article 7. The analysis explains that while laws in most Member States set out the six legal grounds in relatively similar terms to the ones used in the Directive, the flexibility of these principles, in fact, has led to divergent applications.

It is particularly relevant given this context that in its judgment of 24 November 2011 in *ASNEF and FECEMD*, the ECJ held that Spain had not transposed correctly Article 7(f) of

[11] The draft text of the modernised Convention adopted by the T-PD plenary of November 2012 states that data processing can be carried out on the basis of consent of the data subject or on the basis 'of some legitimate basis laid down by law', similarly to the European Union Charter of Fundamental Rights mentioned below on page 8.
[12] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 11 July 2013.
[13] ECJ judgment of 24.11.2011 in cases C-468/10 and C-469/10 (*ASNEF and FECEMD*).
[14] See Annex 2 of the Impact Assessment to the Commission's data protection reform package, cited in footnote 6 above.
[15] Analysis and impact study on the implementation of Directive EC 95/46 in Member States. See http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf.

the Directive, by requiring that - in the absence of the data subject's consent - any relevant data used should appear in public sources. The judgment also held that Article 7(f) has direct effect. The judgment limits the margin of discretion that Member States have in implementing Article 7(f). In particular, they must not overstep the fine line between clarification on the one hand, and setting additional requirements, which would amend the scope of Article 7(f) on the other hand.

The judgment, making it clear that Member States are not allowed to impose additional unilateral restrictions and requirements regarding the legal grounds for lawful data processing in their national laws, has significant consequences. National courts and other relevant bodies must interpret national provisions in light of this judgment and, if necessary, set aside any conflicting national rules and practices.

In light of the judgment, it is all the more important that a clear and common understanding be found by national data protection authorities ('DPA's) and/or European legislators on the applicability of Article 7(f). This should be done in a balanced way, without either unduly restricting or unduly broadening the scope of this provision.

The Charter of Fundamental Rights

Since the Lisbon Treaty entered into force on 1 December 2009, the European Union Charter of Fundamental Rights ('the Charter') enjoys 'the same legal value as the Treaties'.[16] The Charter enshrines the protection of personal data as a fundamental right under Article 8, which is distinct from the respect for private and family life under Article 7. Article 8 lays down the requirement for a legitimate basis for the processing. In particular, it provides that personal data must be processed 'on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[17] These provisions reinforce both the importance of the principle of lawfulness and the need for an adequate legal basis for the processing of personal data.

The proposed Data Protection Regulation

In the context of the data protection review process, the scope of the grounds for lawfulness under Article 7, and in particular, the scope of Article 7(f) is now subject to discussion.

Article 6 of the proposed Regulation lists the grounds for lawful processing of personal data. With some exceptions (as will be described further), the six available grounds remain largely unchanged from those currently provided in Article 7 of the Directive. The Commission has however proposed to provide further guidance in the form of delegated acts.

It is interesting to note that, in the context of the work in the relevant European Parliamentary Committee,[18] attempts were made to clarify the concept of legitimate interests in the proposed

[16] See Article 6(1) TEU.
[17] See Article 8(2) of the Charter.
[18] Draft Report of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) on the Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), dated 16.1.2013 ('Draft LIBE Committee Report').

Regulation itself. A list of cases was drafted in which the legitimate interests of the data controller as a rule would override the legitimate interests and fundamental rights and freedoms of the data subject, and a second list of cases in which this would be the other way around. These lists - laid down either in provisions or in recitals - provide relevant input to the assessment of the balance between the rights and interests of the controller and the data subject, and are taken into account in this Opinion.[19]

II.2. Role of concept

Legitimate interests of the controller: balancing test as a final option?

Article 7(f) is listed as the last option among six grounds allowing for the lawful processing of personal data. It calls for a balancing test: what is necessary for the legitimate interests of the controller (or third parties) must be balanced against the interests or fundamental rights and freedoms of the data subject. The outcome of the balancing test determines whether Article 7(f) may be relied upon as a legal ground for processing.

The open-ended nature of this provision raises many important questions regarding its exact scope and application, which will be analysed in turn in this Opinion. However, as will be explained below, it does not necessarily mean that this option should be seen as one that can only be used sparingly to fill in gaps for rare and unforeseen situations as 'a last resort', or as a last chance if no other grounds apply. Nor should it be seen as a preferred option and its use unduly extended because it would be considered as less constraining than the other grounds.

Instead, it may well be that Article 7(f) has its own natural field of relevance and that it can play a very useful role as a ground for lawful processing, provided that a number of key conditions are fulfilled.

Appropriate use of Article 7(f), in the right circumstances and subject to adequate safeguards, may also help prevent misuse of, and over-reliance on, other legal grounds.

The first five grounds of Article 7 rely on the data subject's consent, contractual arrangement, legal obligation or other specifically identified rationale as ground for legitimacy. When processing is based on one of these five grounds, it is considered as *a priori* legitimate and therefore only subject to compliance with other applicable provisions of the law. There is in other words a presumption that the balance between the different rights and interests at stake – including those of the controller and the data subject - is satisfied - assuming, of course, that all other provisions of data protection law are complied with. Article 7(f) on the other hand requires a *specific* test, for cases that do not fit in the scenarios pre-defined under grounds (a) to (e). It ensures that, outside these scenarios, any processing has to meet the requirement of a balancing test, taking duly into account the interests and fundamental rights of the data subject.

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

---

See, in particular, amendments 101 and 102. See also the amendments adopted by the Committee on 21.10.2013 in their final report ('Final LIBE Committee Report').

[19] See Section III.3.1, in particular, the bullet-points on pages 24-25 containing a non-exhaustive list of some of the most common contexts in which the issue of legitimate interest under Article 7(f) may arise.

activity cannot take place. On the other hand, an appropriate assessment of the balance under Article 7(f), 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 'necessity for the performance of a contract'. Considered in this way, Article 7(f) presents complementary safeguards - which require appropriate measures - compared to the other pre-determined grounds. It should thus not be considered as 'the weakest link' or an open door to legitimise all data processing activities which do not fall under any of the other legal grounds.

The Working Party reiterates that when interpreting the scope of Article 7(f), it aims at a balanced approach, which ensures the necessary flexibility for data controllers for situations where there is no undue impact on data subjects, while at the same time providing sufficient legal certainty and guarantees to data subjects that this open-ended provision will not be misused.

II.3. Related concepts

Relationship of Article 7(f) with other grounds for lawfulness

Article 7 starts with consent, and goes on to list the other grounds for lawfulness, including contracts and legal obligations, moving gradually to the legitimate interest test, which is listed as the last among the six available grounds. The order in which the legal grounds are listed under Article 7 has sometimes been interpreted as an indication of the respective importance of the different grounds. However, as already emphasised in the Working Party's Opinion on the notion of consent[20], the text of the Directive does not make a legal distinction between the six grounds and does not suggest that there is a hierarchy among them. There is not any indication that Article 7(f) should only be applied in exceptional cases and the text also does not otherwise suggest that the specific order of the six legal grounds would have any legally relevant effect. At the same time, the precise meaning of Article 7(f) and its relation with other grounds for lawfulness have long been rather unclear.

Against this background and considering the historical and cultural diversities and the open-ended language of the Directive, different approaches have developed: some Member States have tended to see Article 7(f) as a least preferred ground, which is meant to fill the gaps only in a few exceptional cases when none of the five other grounds could or would apply.[21] Other Member States, in contrast, see it only as one of six options, and one which is no more or no less important than the other options, and which may apply in a large number and large variety of situations, provided the necessary conditions are met.

Considering these diversities, and also in light of the ASNEF and FECEMD judgment, it is important to clarify the relationship of the 'legitimate interests' ground with the other grounds of lawfulness - e.g. in relation to consent, contracts, tasks of public interest - and also in relation to the right of the data subject to object. This may help better define the role and function of the legitimate interests ground and thus may contribute to legal certainty.

[20] See footnote 2 above.

[21] It should also be noted that the Draft LIBE Committee Report, in its Amendment 100 proposed to separate Article 7(f) from the rest of the legal grounds and also proposed additional requirements for the case when this legal ground is relied on, including more transparency and stronger accountability, as will be shown later.

It should also be noted that the legitimate interests ground, along with the other grounds apart from consent, requires a 'necessity' test. This strictly limits the context in which they each can apply. The European Court of Justice considered that 'necessity' is a concept which has its own independent meaning in Community law.[22] The European Court of Human Rights also provided helpful guidance.[23]

Moreover, having an appropriate legal ground does not relieve the data controller of its obligations under Article 6 with regard to fairness, lawfulness, necessity and proportionality, as well as data quality. For instance, even if the processing of personal data is based on the legitimate interests ground, or on the performance of a contract, this would not allow for the collection of data which is excessive in relation to the purpose specified.

Legitimate interests and other grounds of Article 7 are alternative grounds and thus, it is sufficient if only one of them applies. However, they come as cumulative not only with the requirements of Article 6, but also with all other data protection principles and requirements that may be applicable.

Other balancing tests

Article 7(f) is not the only balancing test foreseen in the Directive. For example, Article 9 calls for balancing the right to the protection of personal data and freedom of expression. This Article allows Member States to provide the necessary exemptions and derogations for the processing of personal data 'carried out solely for journalistic purposes or the purpose of artistic or literary expression' if these are 'necessary to reconcile the right to privacy with the rules governing freedom of expression'.

In addition, many other provisions of the Directive also require case-by-case analysis, balancing of interests and rights at stake, and a flexible multi-factor assessment. These include the provisions on necessity, proportionality, and purpose limitation, Article 13 exceptions, and scientific research, just to name a few.

Indeed, it appears that the Directive was designed to leave room for interpretation and balancing of interests. This was, of course, at least in part meant to leave further room for Member States for implementation into national law. However, in addition to this, the need for some flexibility also comes from the very nature of the right to the protection of personal data and the right to privacy. Indeed, these two rights, along with most (but not all) other fundamental rights, are considered relative, or qualified, human rights.[24] These types of rights

[22] Judgment of the European Court of Justice of 16 December 2008 in case C-524/06 (Heinz Huber v Bundesrepublik Deutschland), para 52: 'Consequently, having regard to the objective of ensuring an equivalent level of protection in all Member States, the concept of necessity laid down by Article 7(e) of Directive 95/46, the purpose of which is to delimit precisely one of the situations in which the processing of personal data is lawful, cannot have a meaning which varies between the Member States. It therefore follows that what is at issue is a concept which has its own independent meaning in Community law and which must be interpreted in a manner which fully reflects the objective of that directive, as laid down in Article 1(1) thereof.'

[23] Judgment of the European Court of Human Rights in case Silver & Others v United Kingdom of 25 March 1983, para 97 discussing the term 'necessary in a democratic society': 'the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" ….'

[24] 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 known as absolute rights. These rights can never be limited or restricted, whatever

must always be interpreted in context. Subject to appropriate safeguards, they can be balanced against the rights of others. In some situations - and also subject to appropriate safeguards - they can also be restricted on public interest grounds.

II.4. Context and strategic consequences

Ensuring legitimacy but also flexibility: means for specification of Article 7(f)

The current text of Article 7(f) of the Directive is open-ended. This means that it can be relied upon in a wide range of situations, as long as its requirements, including the balancing test, are satisfied. However, such flexibility may also have negative implications. To prevent it from leading to inconsistent national application or lack of legal certainty, further guidance would play an important role.

The Commission foresees such guidance in the proposed Regulation in the form of delegated acts. Other options include providing clarifications and detailed provisions in the text of the proposed Regulation itself[25], and/or entrusting the European Data Protection Board ('EDPB') with the task of providing further guidance in this area.

Each of these options in turn, has benefits and drawbacks. If the assessment were to be made case by case without any further guidance, this would risk inconsistent application and lack of predictability, as it has been the case in the past.

On the other hand, providing, in the text of the proposed Regulation itself, for detailed and exhaustive lists of situations in which the legitimate interests of the controller as a rule prevail over the fundamental rights of the data subject or vice versa, could risk being misleading, unnecessarily prescriptive, or both.

These approaches could nevertheless inspire a balanced solution, providing for some more detail in the proposed Regulation itself, and further guidance in delegated acts or in EDPB guidance.[26]

The analysis in Chapter III aims to lay the groundwork for finding such an approach, neither too general so as to be meaningless, nor too specific so as to be overly rigid.

---

the circumstances – even in a state of war or emergency. One example is the right not to be tortured or treated in an inhuman or degrading way. It is never permissible to torture or treat someone in an inhuman or degrading way, regardless of the circumstances. 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.

[25] See Section II.1 Brief History, under *'The proposed Data Protection Regulation'* on pages 8-9.

[26] As to delegated acts and EDPB guidance, the Working Party's Opinion 08/2012 providing further input on the data protection reform discussions, adopted on 05.10.201 (WP199) expressed a strong preference for the latter (see p. 13-14).

III. Analysis of provisions

III.1. Overview of Article 7

Article 7 requires that personal data shall only be processed if at least one of the six legal grounds listed in that Article apply. Before analysing each of these grounds, this Section III.1 gives an overview of Article 7 and its relationship with Article 8 on special categories of data.

III.1.1. Consent or 'necessary for...'

A distinction can be made between the case when personal data are processed based on the data subject's unambiguous consent (Article 7(a)) and the remaining five cases (Article 7(b)-(f)). These five cases - briefly put – describe scenarios where processing may be necessary in a specific context, such as the performance of a contract with the data subject, compliance with a legal obligation imposed on the controller, etc.

In the first case, under Article 7(a), it is the data subjects themselves who authorise the processing of their personal data. It is up to them to decide whether to allow their data to be processed. At the same time, consent does not eliminate the need to respect the principles provided in Article 6[27]. In addition, consent still has to fulfil certain essential conditions to be legitimate, as explained in Opinion 15/2011 of the Working Party[28]. As the processing of the user's data is ultimately at his/her discretion, the emphasis is on the validity and the scope of the data subject's consent.

In other words, the first ground, Article 7(a), focuses on the self-determination of the data subject as a ground for legitimacy. All other grounds, in contrast, allow processing – subject to safeguards and measures – in situations where, irrespective of consent, it is appropriate and necessary to process the data within a certain context in pursuit of a specific legitimate interest.

Paragraphs (b), (c), (d) and (e) each specify a criterion making the processing legitimate:

(b) performance of a contract with the data subject;
(c) compliance with a legal obligation imposed on the controller;
(d) protection of the vital interests of the data subject;
(e) performance of a task carried out in the public interest.

Paragraph (f) is less specific and refers, more generally, to (any kind of) legitimate interest pursued by the controller (in any context). This general provision, however, is specifically made subject to an additional balancing test, which aims to protect the interests and rights of the data subjects, as will be shown below in Section III.2.

[27] Judgment of the Dutch Supreme Court of 9 September 2011 in case ECLI:NL:HR:2011:BQ8097, §3.3(e) as to the principle of proportionality. See also page 7 of the Working Party Opinion 15/2011 cited in footnote 2 above: '... obtaining consent does not negate the controller's obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality. For instance, even if the processing of personal data is based on the consent of the user, this would not legitimise the collection of data which is excessive in relation to a particular purpose.'

[28] See pages 11-25 of Opinion 15/2011, cited in footnote 2 above.

The assessment of whether the criteria set out in Article 7 (a) - (f) have been fulfilled, is in all cases, initially made by the data controller, subject to applicable law and guidance on how the law should be applied. In the second instance, the legitimacy of the processing may be subject to further evaluation, and may possibly be challenged, by data subjects, other stakeholders, the data protection authorities, and ultimately decided on by the courts.

To complete this brief overview, it should be mentioned that, as will be discussed in Section III.3.6, at least in the cases referred to in paragraphs (e) and (f), the data subject can exercise the right to object as provided for in Article 14[29]. This will trigger a new evaluation of the interests at stake, or, in the case of direct marketing (Article 14(b)), will require the controller to stop the processing of personal data without any further evaluation.

III.1.2. Relationship with Article 8

Article 8 of the Directive regulates further the processing of certain special categories of personal data. It applies specifically to data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life' (Article 8(1)), and to data 'relating to offences or criminal convictions' (Article 8(5)).

The processing of such data is in principle prohibited, subject to some exceptions. Article 8(2) provides for a number of exceptions from such prohibition, under paragraphs (a) through (e). Article 8(3) and (4) provides for further exceptions. Some of these provisions are similar - but not identical – to the provisions set forth in Article 7(a) through (f).

The specific conditions of Article 8, as well as the fact that some of the grounds listed in Article 7 resemble the conditions set forth in Article 8, raise the question of the relationship between the two provisions.

If Article 8 is designed as a *lex specialis*, it should be considered whether it excludes the applicability of Article 7 altogether. If so, it would mean that special categories of personal data can be processed without satisfying Article 7, provided one of the exceptions in Article 8 applies. It is, however, also possible that the relationship is more complex and Articles 7 and 8 should be applied cumulatively.[30]

Either way, it is clear that the policy objective is to provide additional protection for special categories of data. Therefore, the final outcome of the analysis should be equally clear: the application of Article 8, whether in itself or in a cumulative way with Article 7, aims at providing for a higher level of protection to special categories of data.

In practice, while in some cases Article 8 brings stricter requirements - such as 'explicit' consent in Article 8(2)(a), compared to 'unambiguous consent' in Article 7 - this is not true

[29] Further to Article 14(a), this right applies 'save where otherwise provided by national legislation'. For instance, in Sweden national law does not allow the possibility to object to a processing which is based on Article 7(e).

[30] Since Article 8 is set up as a *prohibition with exceptions*, these exceptions may be seen as requirements, which only limit the scope of the prohibition but do not, in and of themselves, provide a sufficient legal ground for the processing. In this reading, the applicability of Article 8 exceptions does not exclude the applicability of the requirements in Article 7, and the two, when appropriate, must be applied cumulatively.

for all provisions. Some exceptions foreseen by Article 8 do not appear equivalent or stricter than the grounds listed in Article 7. It would be inappropriate to conclude for instance that the fact that someone has made special categories of data manifestly public under Article 8(2)(e) would be - always and in and of itself - a sufficient condition to allow any type of data processing, without an assessment of the balance of interests and rights at stake as required in Article 7(f)[31].

In some situations, the fact that the data controller is a political party would also lift the prohibition on processing special categories of data under Article 8(2)(d). This, however, does not mean that any processing within the scope of that provision is necessarily lawful. This has to be assessed separately and the controller may have to demonstrate, for instance, that the data processing is necessary for the performance of a contract (Article 7(b)), or that its legitimate interest under Article 7(f) prevails. In this latter case, the balancing test under Article 7(f) needs to be conducted, after it has been assessed that the data controller complies with Article 8 requirements.

In a similar way, the mere fact that 'the processing of data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services', and those data are processed under an obligation of secrecy - all as mentioned in Article 8(3) - implies that such processing of sensitive data is *exempted from the prohibition* of Article 8(1). This is however not necessarily sufficient to also ensure lawfulness under Article 7, and will require a legal ground such as a contract with the patient under Article 7(b), a legal obligation under Article 7(c), performance of a task carried out in the public interest under Article 7(e) or an assessment under Article 7(f).

In conclusion, the Working Party considers that an analysis has to be made on a case-by-case basis whether Article 8 in itself provides for stricter and sufficient conditions[32], or whether a cumulative application of both Article 8 and 7 is required to ensure full protection of data subjects. In no case shall the result of the examination lead to a lower protection for special categories of data[33].

This also means that a controller processing special categories of data may never invoke *solely* a legal ground under Article 7 to legitimise a data processing activity. Where applicable, Article 7 will not *prevail* but always apply in a *cumulative* way with Article 8 to ensure that all relevant safeguards and measures are complied with. This will be all the more relevant in case Member States decide to add additional exemptions to those of Article 8, as foreseen in Article 8(4).

---

[31] Moreover, Article 8(2)(e) should not be interpreted *a contrario* as meaning that, when the data made public by the data subject are not sensitive, they can be processed without any additional condition. Publicly available data are still personal data subject to data protection requirements, including compliance with Article 7, irrespective whether or not they are sensitive data.

[32] See the analysis made in the WADA Opinion of the Working Party, point 3.3, which takes into consideration both Article 7 and Article 8 of the Directive: Second opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations, adopted on 06.04.2009 (WP162).

[33] It goes without saying that also in the case of application of Article 8 the respect for the other provisions of the Directive, including Article 6, must be ensured.

III.2. Article 7(a)-(e)

This Section III.2 provides a brief overview of each of the legal grounds in Article 7(a) through (e) of the Directive, before the Opinion focuses, in Section III.3, on Article 7(f). This analysis will also highlight some of the most common interfaces between these legal grounds, for instance involving 'contract', 'legal obligation' and 'legitimate interest', depending upon the particular context and the facts of the case.

III.2.1. Consent

Consent as a legal ground has been analysed in Opinion 15/2011 of the Working Party on the definition of consent. The main findings of the Opinion are that consent is one of several legal grounds to process personal data, rather than the main ground. It has an important role, but this does not exclude the possibility, depending on the context, that other legal grounds may be more appropriate either from the controller's or from the data subject's perspective. If it is correctly used, consent is a tool giving the data subject control over the processing of his data. If incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing.

Among its recommendations, the Working Party insisted on the need to clarify what 'unambiguous consent' means: "Clarification should aim at emphasizing that unambiguous consent requires the use of mechanisms that leave no doubt of the data subject's intention to consent. At the same time it should be made clear that the use of default options which the data subject is required to modify in order to reject the processing (consent based on silence) does not in itself constitute unambiguous consent. This is especially true in the on-line environment." [34] It also required data controllers to put in place mechanisms to demonstrate consent (within a general accountability obligation) and requested the legislator to add an explicit requirement regarding the quality and accessibility of the information forming the basis for consent.

III.2.2. Contract

Article 7(b) provides a legal ground in situations where 'processing is necessary for the performance of a 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'. This covers two different scenarios.

i) First, the provision covers situations where processing is necessary for the performance of the contract to which the data subject is a party. This may include, for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to effect payment. In the employment context this ground may allow, for example, processing salary information and bank account details so that salaries could be paid.

   The provision must be interpreted strictly and does not cover situations where the processing is not genuinely *necessary* for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. Also the fact that some data

[34] See page 36 of the Working Party's Opinion 15/2011 on the definition of consent.

processing is covered by a contract does not automatically mean that the processing is necessary for its performance. For example, Article 7(b) is not a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on his click-stream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services, for example. Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them 'necessary' for the performance of the contract.

There is a clear connection here between the assessment of necessity and compliance with the purpose limitation principle. It is important to determine the exact *rationale* of the contract, i.e. its substance and fundamental objective, as it is against this that it will be tested whether the data processing is necessary for its performance.

In some borderline situations it may be arguable, or may require more specific fact-finding to determine whether processing is necessary for the performance of the contract. For example, the establishment of a company-wide internal employee contact database containing the name, business address, telephone number and email address of all employees, to enable employees reach their colleagues, may in certain situations be considered as necessary for the performance of a contract under Article 7(b) but it could also be lawful under Article 7(f) if the overriding interest of the controller is demonstrated and all appropriate measures are taken, including for instance adequate consultation of employees' representatives.

Other cases, for example, electronic monitoring of employee internet, email or telephone use, or video-surveillance of employees more clearly constitute processing that is likely to go beyond what is necessary for the performance of an employment contract, although here also this may depend on the nature of the employment. Fraud prevention - which may include, among others, monitoring and profiling customers - is another typical area, which is likely to be considered as going beyond what is necessary for the performance of a contract. Such processing could then still be legitimate under another ground of Article 7, for instance, consent where appropriate, a legal obligation or the legitimate interest of the controller (Article 7(a), (c) or (f)).[35] In the latter case, the processing should be subject to additional safeguards and measures to adequately protect the interests or rights and freedoms of data subjects.

Article 7(b) only applies to what is necessary for the *performance* of a contract. It does not apply to all further actions triggered by non-compliance or to all other incidents in the execution of a contract. As long as processing covers the normal execution of a contract, it could fall within Article 7(b). If there is an incident in the performance, which gives rise to a conflict, the processing of data may take a different course.

[35] Another example of multiple legal grounds can be found in the Working Party's Opinion 15/2011 on the definition of consent (cited in footnote 2). To buy a car, the data controller may be entitled to process personal data according to different purposes and on the basis of different grounds:
- Data necessary to buy the car: Article 7(b),
- To process the car's papers: Article 7(c),
- For client management services (e.g. to have the car serviced in different affiliate companies within the EU): Article 7(f),
- To transfer the data to third parties for their own marketing activities: Article 7(a).

Processing of basic information of the data subject, such as name, address and reference to outstanding contractual obligations, to send formal reminders should still be considered as falling within the processing of data necessary for the performance of a contract. With regard to more elaborated processing of data, which may or may not involve third parties, such as external debt collection, or taking a customer who has failed to pay for a service to court, it could be argued that such processing does not take place anymore under the 'normal' performance of the contract and would therefore not fall under Article 7(b). However, this would not make the processing illegitimate as such: the controller has a legitimate interest in seeking remedies to ensure that his contractual rights are respected. Other legal grounds, such as Article 7(f) could be relied upon, subject to adequate safeguards and measures, and meeting the balancing test.[36]

ii) Second, Article 7(b) also covers processing that takes place *prior* to entering into a contract. This covers pre-contractual relations, provided that steps are taken at the request of the data subject, rather than at the initiative of the controller or any third party. For example, if an individual requests a retailer to send her an offer for a product, processing for these purposes, such as keeping address details and information on what has been requested, for a limited period of time, will be appropriate under this legal ground. Similarly, if an individual requests a quote from an insurer for his car, the insurer may process the necessary data, for example, the make and age of the car, and other relevant and proportionate data, in order to prepare the quote.

However, detailed background checks, for example, processing the data of medical check-ups before an insurance company provides health insurance or life insurance to an applicant would not be considered as necessary steps made at the request of the data subject. Credit reference checks prior to the grant of a loan are also not made at the *request* of the data subject under Article 7(b), but rather, under Article 7(f), or under Article 7(c) in compliance with a legal obligation of banks to consult an official list of registered debtors.

Direct marketing at the initiative of the retailer/controller will also not be possible on this ground. In some cases, Article 7(f) could provide an appropriate legal ground instead of Article 7(b), subject to adequate safeguards and measures, and meeting the balancing test. In other cases including those involving extensive profiling, data-sharing, online direct marketing or behavioural advertisement, consent under Article 7(a) should be considered, as follows from the analysis below.[37]

[36] With regard to special categories of data, Article 8(1)(e) - 'necessary for the establishment, exercise or defence of legal claims' - may also need to be taken into account.

[37] See Section III.3.6 (b) under heading ' Illustration: the evolution in the approach to direct marketing' on pages 45-46.

III.2.3. Legal obligation

Article 7(c) provides a legal ground in situations where 'processing is necessary for compliance with a legal obligation to which the controller is subject'. This may be the case, for example, where employers must report salary data of their employees to social security or tax authorities or where financial institutions are obliged to report certain suspicious transactions to the competent authorities under anti-money-laundering rules. It could also be an obligation to which a public authority is subject, as nothing limits the application of Article 7(c) to the private or public sector. This would apply for instance to the collection of data by a local authority for the handling of penalties for parking at unauthorised locations.

Article 7(c) presents similarities with Article 7(e), as a public interest task is often based on, or derived from, a legal provision. The scope of Article 7(c) is however strictly delimited.

For Article 7(c) to apply, the obligation must be imposed by law (and not for instance by a contractual arrangement). The law must fulfil all relevant conditions to make the obligation valid and binding, and must also comply with data protection law, including the requirement of necessity, proportionality[38] and purpose limitation.

It is also important to emphasise that Article 7(c) refers to the laws of the European Union or of a Member State. Obligations under the laws of third countries (such as, for example, the obligation to set up whistleblowing schemes under the Sarbanes–Oxley Act of 2002 in the United States) are not covered by this ground. To be valid, a legal obligation of a third country would need to be officially recognised and integrated in the legal order of the Member State concerned, for instance under the form of an international agreement[39]. On the other hand, the need to comply with a foreign obligation may represent a legitimate interest of the controller, but only subject to the balancing test of Article 7(f), and provided that adequate safeguards are put in place such as those approved by the competent data protection authority.

The controller must not have a choice whether or not to fulfil the obligation. Voluntary unilateral engagements and public-private partnerships processing data beyond what is required by law are thus not covered under Article 7(c). For example, if - without a clear and specific legal obligation to do so – an Internet service provider decides to monitor its users in an effort to combat illegal downloading, Article 7(c) will not be an appropriate legal ground for this purpose.

Further, the legal obligation itself must be sufficiently clear as to the processing of personal data it requires. Thus, Article 7(c) applies on the basis of legal provisions referring explicitly to the nature and object of the processing. The controller should not have an undue degree of discretion on how to comply with the legal obligation.

[38] See also the Working Party's Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, adopted on 27.02.2014 (WP 211).

[39] See on this issue Section 4.2.2 of the Working Party's Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), adopted on 20.11.2006 (WP128) and Working Party's Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, adopted on 01.02.2006 (WP 117).

The legislation may in some cases set only a general objective, while more specific obligations are imposed at a different level, for instance, either in secondary legislation or by a binding decision of a public authority in a concrete case. This may also lead to legal obligations under Article 7(c) provided that the nature and object of the processing is well defined and subject to an adequate legal basis.

However, this is different if a regulatory authority would only provide general policy guidelines and conditions under which it might consider using its enforcement powers (e.g. regulatory guidance to financial institutions on certain standards of due diligence). In such cases, the processing activities should be assessed under Article 7(f) and only be considered legitimate subject to the additional balancing test.[40]

As a general remark, it should be noted that some processing activities may appear to be close to falling under Article 7(c), or to Article 7(b), without fully meeting the criteria for these grounds to apply. This does not mean that such processing is always necessarily unlawful: it may sometimes be legitimate, but rather under Article 7(f), subject to the additional balancing test.

III.2.4. Vital interest

Article 7(d) provides for a legal ground in situations where 'processing is necessary in order to protect the vital interests of the data subject'. This wording is different to the language used in Article 8(2)(c) which is more specific and refers to situations where 'processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent'.

Both provisions nevertheless appear to suggest that this legal ground should have a limited application. First, the phrase 'vital interest' appears to limit the application of this ground to questions of life and death, or at the very least, threats that pose a risk of injury or other damage to the health of the data subject (or in case of Article 8(2)(c) also of another person).

Recital 31 confirms that the objective of this legal ground is to 'protect an interest which is essential to the data subject's life'. However, the Directive does not state precisely whether the threat must be immediate. This raises issues concerning the scope of the collection of data, for instance as a preventive measure or on a wide scale, such as the collection of airline passengers' data where a risk of epidemiological disease or a security incident has been identified.

The Working Party considers that a restrictive interpretation must be given to this provision, consistent with the spirit of Article 8. Although Article 7(d) does not specifically limit the use of this ground to situations when consent cannot be used as a legal ground, for the reasons specified in Article 8(2)(c), it is reasonable to assume that in situations where there is a possibility and need to request a valid consent, consent should indeed be sought whenever practicable. This would also limit the application of this provision to a case by case analysis and cannot normally be used to legitimise any massive collection or processing of personal

[40] Guidance by a regulatory authority may still play a role in assessing the controller's legitimate interest (see Section III.3.4 under point (a) notably on page 36).

data. In case where this would be necessary, Article 7(c) or (e) would be more appropriate grounds for processing.

III.2.5. Public task

Article 7(e) provides a legal ground in situations where 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed'.

It is important to note that just like Article 7(c), Article 7(e) refers to the public interest of the European Union or of a Member State. Similarly, 'official authority' refers to an authority granted by the European Union or a Member State. In other words, tasks carried out in the public interest of a third country or in the exercise of an official authority vested by virtue of foreign law do not fall within the scope of this provision.[41]

Article 7(e) covers two situations and is relevant both to the public and the private sector. First, it covers situations where the controller itself has an official authority or a public interest task (but not necessarily also a legal obligation to process data) and the processing is necessary for exercising that authority or performing that task. For example, a tax authority may collect and process an individual's tax return in order to establish and verify the amount of tax to be paid. Or a professional association such as a bar association or a chamber of medical professionals vested with an official authority to do so may carry out disciplinary procedures against some of their members. Yet another example could be a local government body, such as a municipal authority, entrusted with the task of running a library service, a school, or a local swimming pool.

Second, Article 7(e) also covers situations where the controller does not have an official authority, but is requested by a third party having such authority to disclose data. For example, an officer of a public body competent for investigating crime may ask the controller for cooperation in an on-going investigation rather than ordering the controller to comply with a specific request to cooperate. Article 7(e) may furthermore cover situations where the controller proactively discloses data to a third party having such an official authority. This may be the case, for example, where a controller notices that a criminal offence has been committed, and provides this information to the competent law enforcement authorities at his own initiative.

Unlike in the case of Article 7(c), there is no requirement for the controller to act under a legal obligation. Using the example above, a controller accidentally noticing that theft or fraud has been committed, may not be under a legal obligation to report this to the police but may, in appropriate cases, nevertheless do so voluntarily on the basis of Article 7(e).

However, the processing must be 'necessary for the performance of a task carried out in the public interest'. Alternatively, either the controller or the third party to whom the controller discloses the data must be vested with an official authority and the data processing must be

[41] See Section 2.4 of the Working Party's working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, adopted on 25 November 2005 (WP114) for a similar interpretation of the notion of 'important public interest grounds' in Article 26(1)(d).

necessary to exercise the authority.[42] It is also important to emphasise that this official authority or public task will have been typically attributed in statutory laws or other legal regulations. If the processing implies an invasion of privacy or if this is otherwise required under national law to ensure the protection of the individuals concerned, the legal basis should be specific and precise enough in framing the kind of data processing that may be allowed.

These situations are becoming increasingly common, also outside the confines of the public sector, considering the trend to outsource governmental tasks to entities in the private sector. This can be the case, for instance, in the context of processing activities in the transport or health sector (e.g. epidemiological studies, research). This ground could also be invoked in a law enforcement context as already suggested in the examples above. However, the extent to which a private company may be allowed to cooperate with law enforcement authorities, for instance in the fight against fraud or illegal content on the Internet, requires analysis not only under Article 7, but also under Article 6, considering purpose limitation, lawfulness and fairness requirements[43].

Article 7(e) has potentially a very broad scope of application, which pleads for a strict interpretation and a clear identification, on a case by case basis, of the public interest at stake and the official authority justifying the processing. This broad scope also explains why, just like for Article 7(f), a right to object has been foreseen in Article 14 when processing is based on Article 7(e)[44]. Similar additional safeguards and measures may thus apply in both cases [45].

In that sense, Article 7(e) has similarities with Article 7(f), and in some contexts, especially for public authorities, Article 7(e) may replace Article 7(f).

When assessing the scope of these provisions to public sector bodies, especially in light of the proposed changes in the data protection legal framework, it is useful to note that the current text of Regulation 45/2001,[46] which contains the data protection rules applicable to European Union institutions and bodies, has no provision comparable to Article 7(f).

However, Recital 27 of this Regulation provides that 'processing of personal data for the performance of tasks carried out *in the public interest* by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies.' This provision thus allows data processing on a broadly interpreted 'public task' ground in a large variety of cases, which could have otherwise been covered by a provision similar to Article 7(f). Video-surveillance of premises for security

[42] In other words, in these cases the public relevance of the tasks, and the correspondent responsibility will continue to be present even if the exercise of the task has been moved to other entities, including private ones.

[43] See in that sense the Working Party's Opinion on SWIFT (cited in footnote 39 above), the Working Party's Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, adopted on 13.06.2003 (WP78) and the Working Document on data protection issues related to intellectual property rights, adopted on 18.01.2005 (WP 104).

[44] As mentioned above, this possibility to object does not exist in some Member States (e.g. Sweden) for processing of data based on Article 7(e).

[45] As will be shown below, the Draft LIBE Committee Report suggested further safeguards – in particular, enhanced transparency – for the case when Article 7(f) applies.

[46] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. (OJ L 8, 12.1.2001, p. 1).

purposes, electronic monitoring of email traffic, or staff evaluations are just a few examples of what may come under this broadly interpreted provision of 'tasks carried out in the public interest'.

Looking ahead, it is also important to consider that the proposed Regulation, in Article 6(1)(f) specifically provides that the legitimate interest ground 'shall not apply to processing carried out by public authorities in the performance of their tasks'. If this provision is enacted and will be interpreted broadly, so as to altogether exclude public authorities from using legitimate interest as a legal ground, then the 'public interest' and 'official authority' grounds of Article 7(e) would need to be interpreted in a way as to allow public authorities some degree of flexibility, at least to ensure their proper management and functioning, just the way Regulation 45/2001 is interpreted now.

Alternatively, the referred last sentence of 6(1)(f) of the proposed Regulation could be interpreted in a way, so as not to altogether exclude public authorities from using legitimate interest as a legal ground. In this case, the terms 'processing carried out by public authorities in the performance of their tasks' in the proposed Article 6(1)(f) should be interpreted narrowly. This narrow interpretation would mean that processing for proper management and functioning of these public authorities would fall outside the scope of 'processing carried out by public authorities in the performance of their tasks'. As a result, processing for proper management and functioning of these public authorities could still be possible under the legitimate interest ground.

III.3. Article 7(f): legitimate interests

Article 7(f)[47] calls for a balancing test: the legitimate interests of the controller (or third parties) must be balanced against the interests or fundamental rights and freedoms of the data subject. The outcome of the balancing test largely determines whether Article 7(f) may be relied upon as a legal ground for processing.

It is worth mentioning already at this stage that this is not a straightforward balancing test which would simply consist of weighing two easily quantifiable and easily comparable 'weights' against each other. Rather, as will be described below in more detail, carrying out the balancing test may require a complex assessment taking into account a number of factors. To help structure and simplify the assessment, we have broken down the process into several steps to help ensure that the balancing test can be carried out effectively.

Section III.3.1 first examines one side of the balance: what constitutes 'legitimate interest pursued by the controller or by a third party to whom the data are disclosed'. In Section III.3.2, we examine the other side of the balance, what constitutes 'interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)'.

In Sections III.3.3 and III.3.4, guidance is provided on how to carry out the balancing test. Section III.3.3 gives a general introduction with the help of three different scenarios. Following this introduction, Section III.3.4 outlines the most important considerations that must be taken into account when carrying out the balancing test, including the safeguards and

[47] For a full text of Article 7(f) see page 4 above.

measures provided by the data controller.

In Sections III.3.5 and III.3.6, we will finally also look into some particular mechanisms, such as accountability, transparency and the right to object, that may help ensure - and further enhance – an appropriate balance of the various interests that may be at stake.

III.3.1. Legitimate interests of the controller (or third parties)

The concept of 'interest'

The concept of 'interest' is closely related to, but distinct from, the concept of 'purpose' mentioned in Article 6 of the Directive. In data protection discourse, 'purpose' is the specific reason why the data are processed: the aim or intention of the data processing. An interest, on the other hand, is the broader stake that a controller may have in the processing, or the benefit that the controller derives - or that society might derive - from the processing.

For instance, a company may have an *interest* in ensuring the health and safety of its staff working at its nuclear power-plant. Related to this, the company may have as a *purpose* the implementation of specific access control procedures which justifies the processing of certain specified personal data in order to help ensure the health and safety of staff.

An interest must be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject. Moreover, the interest at stake must also be 'pursued by the controller'. This requires a real and present interest, something that corresponds with current activities or benefits that are expected in the very near future. In other words, interests that are too vague or speculative will not be sufficient.

The nature of the interest may vary. Some interests may be compelling and beneficial to society at large, such as the interest of the press to publish information about government corruption or the interest in carrying out scientific research (subject to appropriate safeguards). Other interests may be less pressing for society as a whole, or at any rate, the impact of their pursuit on society may be more mixed or controversial. This may, for example, apply to the economic interest of a company to learn as much as possible about its potential customers so that it can better target advertisement about its products or services.

What makes an interest 'legitimate' or 'illegitimate'?

The objective of this question is to identify the threshold for what constitutes a legitimate interest. If the data controller's interest is illegitimate, the balancing test will not come into play as the initial threshold for the use of Article 7(f) will not have been reached.

In the view of the Working Party, the notion of legitimate interest could include a broad range of interests, whether trivial or very compelling, straightforward or more controversial. It will then be in a second step, when it comes to balancing these interests against the interests and fundamental rights of the data subjects, that a more restricted approach and more substantive analysis should be taken.

The following is a non-exhaustive list of some of the most common contexts in which the issue of legitimate interest in the meaning of Article 7(f) may arise. It is presented here

without prejudice to whether the interests of the controller will ultimately prevail over the interests and rights of the data subjects when the balancing is carried out.

- exercise of the right to freedom of expression or information, including in the media and the arts
- conventional direct marketing and other forms of marketing or advertisement
- unsolicited non-commercial messages, including for political campaigns or charitable fundraising
- enforcement of legal claims including debt collection via out-of-court procedures
- prevention of fraud, misuse of services, or money laundering
- employee monitoring for safety or management purposes
- whistle-blowing schemes
- physical security, IT and network security
- processing for historical, scientific or statistical purposes
- processing for research purposes (including marketing research)

Accordingly, an interest can be considered as legitimate as long as the controller can pursue this interest in a way that is in accordance with data protection and other laws. In other words, a legitimate interest must be 'acceptable under the law'[48].

In order to be relevant under Article 7(f), a 'legitimate interest' must therefore:

- be lawful (i.e. in accordance with applicable EU and national law);
- be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently specific);
- represent a real and present interest (i.e. not be speculative).

The fact that the controller has such a legitimate interest in the processing of certain data does not mean that it can necessarily rely on Article 7(f) as a legal ground for the processing. The legitimacy of the data controller's interest is just a starting point, one of the elements that need to be analysed under Article 7(f). Whether Article 7(f) can be relied on will depend on the outcome of the balancing test that follows.

To illustrate: controllers may have a legitimate interest in getting to know their customers' preferences so as to enable them to better personalise their offers, and ultimately, offer products and services that better meet the needs and desires of the customers. In light of this, Article 7(f) may be an appropriate legal ground to be used for some types of marketing

[48] The observations about the nature of 'legitimacy' in Section III.1.3 of the Working Party's Opinion 3/2013 on purpose limitation (cited in footnote 9 above) also apply here *mutatis mutandis*. As in that Opinion on pages 19-20, 'the notion of 'law' is used here in the broadest sense. This includes other applicable laws such as employment, contract, or consumer protection law. Further, the notion of law 'includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts. Within the confines of law, other elements such as customs, codes of conduct, codes of ethics, contractual arrangements, and the general context and facts of the case, may also be considered when determining whether a particular purpose is legitimate. This will include the nature of the underlying relationship between the controller and the data subjects, whether it be commercial or otherwise.' Further, what can be considered as a legitimate interest 'can also change over time, depending on scientific and technological developments, and changes in society and cultural attitudes.'

activities, on-line and off-line, provided that appropriate safeguards are in place (including, among others, a workable mechanism to allow objecting to such a processing under Article 14(b), as will be shown in Section III.3.6 *The right to object and beyond*).

However, this does not mean that controllers would be able to rely on Article 7(f) to unduly monitor the on-line or off-line activities of their customers, combine vast amounts of data about them from different sources that were initially collected in other contexts and for different purposes, and create - and, for example, with the intermediary of data brokers, also trade in - complex profiles of the customers' personalities and preferences without their knowledge, a workable mechanism to object, let alone informed consent. Such a profiling activity is likely to present a significant intrusion into the privacy of the customer, and when this is so, the controller's interest would be overridden by the interests and rights of the data subject.[49]

As another example, in its opinion on SWIFT[50], although the Working Party acknowledged the legitimate interest of the company in complying with the subpoenas under US law, to avoid the risk of being sanctioned by US authorities, it concluded that Article 7(f) could not be relied on. The Working Party considered in particular that because of the far reaching effects on individuals of the processing of data in a 'hidden, systematic, massive and long term manner', 'the interests (f)or fundamental rights and freedoms of the numerous data subjects override SWIFT's interest not to be sanctioned by the US for eventual non-compliance with the subpoenas'.

As will be shown later, if the interest pursued by the controller is not compelling, the interests and rights of the data subject are more likely to override the legitimate - but less significant - interests of the controller. At the same time, this does not mean that less compelling interests of the controller cannot sometimes override the interests and rights of the data subjects: this typically happens when the impact of the processing on the data subjects is also less significant.

Legitimate interest in the public sector

The current text of the Directive does not specifically exclude controllers that are public authorities from processing data using Article 7(f) as a legal ground for processing[51].

However, the proposed Regulation[52] excludes this possibility for 'processing carried out by public authorities in the performance of their tasks'.

[49] The issue of tracking technologies and the role of consent under Article 5(3) of the e-Privacy Directive will be discussed separately. See Section III.3.6 (b) under heading 'Illustration: the evolution in the approach to direct marketing'.

[50] See Section 4.2.3 of the Opinion already cited in footnote 39 above. The legitimate interest of the controller in this case was also linked to the public interest of a third country, which could not be accommodated under Directive 95/46/EC.

[51] Originally the first Commission Proposal for the Directive covered separately data processing in the private sector and processing activities of the public sector. This formal distinction between the rules applying to the public sector and the private sector was dropped in the Amended Proposal. This may also have led to diversities in interpretation and implementation by the various Member States.

[52] See Article 6(1)(f) of the proposed Regulation.

The proposed legislative change highlights the importance of the general principle that public authorities, as a rule, should only process data in performance of their tasks if they have appropriate authorisation by law to do so. Adherence to this principle is particularly important - and clearly required by the case law of the European Court of Human Rights - in cases where the privacy of the data subjects is at stake and the activities of the public authority would interfere with such privacy.

Sufficiently *detailed and specific* authorisation by law is therefore required - also under the current Directive - in case the processing by public authorities interferes with the privacy of the data subjects. This may either take the form of a specific legal obligation to process data, which can satisfy Article 7(c), or a specific authorisation (but not necessarily an obligation) to process data, which can meet the requirements of Article 7(e) or (f).[53]

Legitimate interests of third parties

The current text of the Directive does not only refer to the 'legitimate interests pursued by the controller' but also allows Article 7(f) to be used when the legitimate interest is pursued by 'the third party or parties to whom the data are disclosed'[54]. The following examples illustrate some of the contexts where this provision may apply.

Publication of data for purposes of transparency and accountability. One important context where Article 7(f) may be relevant is the case of publication of data for purposes of transparency and accountability (for example, the salaries of top management in a company). In this case it can be considered that the public disclosure is done primarily not in the interest of the controller who publishes the data, but rather, in the interest of other stakeholders, such as employees or journalists, or the general public, to whom the data are disclosed.

From a data protection and privacy perspective, and to ensure legal certainty, in general, it is advisable that personal data be disclosed to the public on the basis of a law allowing and - when appropriate - clearly specifying the data to be published, the purposes of the publication and any necessary safeguards.[55] This also means that it may be preferable that Article 7(c), rather than Article 7(f) be used as a legal basis when personal data are disclosed for purposes of transparency and accountability[56].

---

[53] In this respect, see also Section III.2.5 above on public tasks (pages 21-23) as well as the discussions below under the heading *Legitimate interests of third parties* (on pages 27-28). See also reflections on the limits of 'private enforcement' of the law on page 35 under the heading 'public interests/the interests of the wider community'. In all these situations, it is particularly important to ensure that the limits of Article 7(f) and also 7(e) are fully respected.

[54] The proposed Regulation aims at limiting the use of this ground to 'legitimate interests pursued by a controller. It is not clear from the text alone whether the proposed language means a mere simplification of the text or whether its intention is to exclude situations where a controller might disclose data in the legitimate interests of others. This text is however not definitive. The interest of third parties was for instance reintroduced in the Final LIBE Committee Report on the occasion of the vote on compromised amendments by the LIBE Committee of the European Parliament on 21 October 2013. See amendment 100 on Article 6. Reintroduction of third parties into the Proposal is supported by the Working Party on grounds that its use may continue to be appropriate in some situations, including the ones described below.

[55] This best practice recommendation should not prejudice national legal rules on transparency and public access to documents.

[56] Indeed, in some Member States different rules have to be complied with in respect of processing carried out by public and private parties. For example, according to the Italian Data Protection Code the dissemination of personal data by a public body shall only be permitted if it is provided for by a law or regulation (Section 19.3).

However, in the absence of a specific legal obligation or permission to publish data, it would nevertheless be possible to disclose personal data to relevant stakeholders. In appropriate cases, it would also be possible to publish personal data for purposes of transparency and accountability.

In both cases - i.e. irrespective of whether personal data are disclosed on the basis of a law allowing so or not - disclosure directly depends on the result of the Article 7(f) balancing test and the implementation of appropriate safeguards and measures.[57]

In addition, further use for further transparency of already released personal data (for instance, re-publication of the data by the press, or further dissemination of the originally published dataset in a more innovative or user-friendly way by an NGO), may also be desirable. Whether such re-publication and re-use is possible, will also depend on the outcome of the balancing test, which should take into account, among others, the nature of the information and the effect of the re-publication or re-use on the individuals.[58]

Historical or other kinds of scientific research. Another important context where disclosure in the legitimate interests of third parties may be relevant is historical or other kinds of scientific research, particularly where access is required to certain databases. The Directive provides specific recognition of such activities, subject to appropriate safeguards and measures[59], but it should not be forgotten that the legitimate ground for these activities will often be a well-considered use of Article 7(f).[60]

General public interest or third party's interest. Finally, the legitimate interest of third parties may also be relevant in a different way. This is the case where a controller - sometimes encouraged by public authorities - is pursuing an interest that corresponds with a general public interest or a third party's interest. This may include situations where a controller goes beyond its specific legal obligations set in laws and regulations to assist law enforcement or private stakeholders in their efforts to combat illegal activities, such as money laundering,

[57] As explained in the Working Party's Opinion 06/2013 on open data (see page 9 of that Opinion, cited in footnote 88 below), 'any national practice or national legislation with regard to transparency must comply with Article 8 of the ECHR and Articles 7 and 8 of the EU Charter. This implies, as the European Court of Justice held in the *Österreichischer Rundfunk* and *Schecke* rulings, that it should be ascertained that the disclosure is necessary for and proportionate to the legitimate aim pursued by the law.' See ECJ 20 May 2003, Rundfunk, Joined Cases C-465/00, C-138/01 and C-139/01 and ECJ 9 November 2010, Volker und Markus Schecke, Joined Cases C-92/09 and C-93/09.

[58] Purpose limitation is also an important consideration here. On page 19 of the Working Party's Opinion 06/2013 on open data (cited in footnote 88 below), the WP29 recommends 'that any legislation calling for public access to data clearly specify the purposes for disclosing personal data. If this is not done, or only done in vague and broad terms, legal certainty and predictability will suffer. In particular, with regard to any request for re-use, it will be very difficult for the public sector body and potential re-users concerned to determine, what were the intended initial purposes of the publication, and subsequently, what further purposes would be compatible with these initial purposes. As it was already mentioned, even if personal data are published on the Internet, it is not to be assumed that they can be further processed for any possible purposes.'

[59] See e.g. Article 6(1)(b) and (e).

[60] As explained in Opinion 3/2013 of the Working Party on Purpose Limitation (cited in footnote 9 above), further use of data for secondary purposes should be subject to a double test. First, it should be ensured that the data will be used for compatible purposes. Second, it should be ensured that there will be an appropriate legal basis under Article 7 for the processing.

child grooming, or illegal file sharing online. In these situations, however, it is particularly important to ensure that the limits of Article 7(f) are fully respected.[61]

Processing must be necessary for the purpose(s) intended

Finally, the processing of personal data must also be 'necessary for the purpose of the legitimate interests' pursued either by the controller or - in the case of disclosure - by the third party. This condition complements the requirement of necessity under Article 6, and requires a connection between the processing and the interests pursued. This 'necessity' requirement applies in all situations mentioned in Article 7, paragraphs (b) to (f), but is particularly relevant in the case of paragraph (f) to ensure that processing of data based on legitimate interests will not lead to an unduly broad interpretation of the necessity to process data. As in other cases, this means that it should be considered whether other less invasive means are available to serve the same end.

III.3.2. Interests or rights of the data subject

Interests or rights (rather than interests for rights)

Article 7(f) of the Directive refers to 'the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)'.

The Working Party noted, however, when comparing the different language versions of the Directive that the phrase 'interests for' has been translated as 'interests or' in other key languages which were used at the time when the text was negotiated.[62]

Further analysis suggests that the English text of the Directive is simply a result of a misspelling: 'or' was mistakenly typed as 'for'.[63] Thus, the correct text should read 'interests or fundamental rights and freedoms'.

'Interests' and 'rights' should be given a broad interpretation

The reference to 'interests or fundamental rights and freedoms' has a direct impact on the scope of application of the provision. It provides more protection for the data subject, namely it requires the data subjects' 'interests' to be also taken into account, not only his or her fundamental rights and freedoms. However, there is no reason to assume that the restriction in

[61] See in this respect, for instance, the Working document on data protection issues related to intellectual property rights, adopted on 18.01.2005 (WP104).

[62] For example, 'l'intérêt ou les droits et libertés fondamentaux de la personne concernée' in French, 'l'interesse o i diritti e le libertà fondamentali della persona interessata' in Italian; 'das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person' in German.

[63] The Working Party notes that the grammatically correct English version should have read 'interests in' rather than 'interests for', if this is what had been meant. In addition, the phrase 'interests for' or 'interest in' seems to be redundant, in the first place, because reference to 'fundamental rights and freedoms' should have normally sufficed, if this is what had been meant. The interpretation that there has been a misspelling is also confirmed by the fact that the Common Position (EC) No 1/95 adopted by the Council on 20 February 1995 also refers to 'interests or fundamental rights and freedoms'. Finally, the Working Party also notes that the Commission intended to correct this misspelling in the proposed Regulation: Article 6(1)(f) refers to 'the interests or fundamental rights and freedoms of the data subject which require protection of personal data' and not 'interests for' such rights.

Article 7(f) to fundamental rights 'which require protection under Article 1(1)' - and thus the explicit reference to the object of the Directive[64] - would not also apply to the term 'interests'. The clear message is nevertheless that all relevant interests of the data subject should be taken into account.

This interpretation of the text makes sense not only grammatically, but also when taking into account the broad interpretation of the notion of the 'legitimate interests' of the controller. If the controller - or the third party in the case of disclosure - can pursue any interests, provided they are not illegitimate, then the data subject should also be entitled to have all categories of interests to be taken into account and weighed against those of the controller, as long as they are relevant within the scope of the Directive.

At a time of increasing imbalance in 'informational power', when governments and business organisations alike amass hitherto unprecedented amounts of data about individuals, and are increasingly in the position to compile detailed profiles that will predict their behaviour (reinforcing informational imbalance and reducing their autonomy), it is ever more important to ensure that the interests of the individuals to preserve their privacy and autonomy be protected.

Finally, it is important to note that unlike the case of the controller's interests, the adjective 'legitimate' is not used here to precede the 'interests' of the data subjects. This implies a wider scope to the protection of individuals' interests and rights. Even individuals engaged in illegal activities should not be subject to disproportionate interference with their rights and interests[65]. For example, an individual who may have perpetrated theft in a supermarket could still see his interests prevailing against the publication of his picture and private address on the walls of the supermarket and/or on the Internet by the owner of the shop.

III.3.3. Introduction to applying the balancing test

It is useful to imagine both the legitimate interests of the controller and the impact on the interests and rights of the data subject on a spectrum. Legitimate interests can range from insignificant through somewhat important to compelling. Similarly, the impact on the interests and rights of the data subjects may be more or may be less significant and may range from trivial to very serious.

Legitimate interests of the controller, when minor and not very compelling may, in general, only override the interests and rights of data subjects in cases where the impact on these rights and interests are even more trivial. On the other hand, important and compelling legitimate interests may in some cases and subject to safeguards and measures justify even significant intrusion into privacy or other significant impact on the interests or rights of the data subjects[66].

---

[64] See Article 1(1): 'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'.

[65] Of course, one of the consequences of criminality might be the collection and possible publication of personal data about criminals and suspects. This, however, must be subject to strict conditions and safeguards.

[66] See as an illustration the reasoning of the Working Party in several opinions and working documents:
- Opinion 4/2006 on the Notice of proposed rule-making by the US Department of Health and Human Services on the control of communicable disease and the collection of passenger information of 20 November 2005

Here it is important to highlight the special role that safeguards may play[67] in reducing the undue impact on the data subjects, and thereby changing the balance of rights and interests to the extent that the data controller's legitimate interests will not be overridden. The use of safeguards alone is of course not sufficient to justify any kind of processing in all contexts. Further, the safeguards in question must be adequate and sufficient, and must unquestionably and significantly reduce the impacts on data subjects.

Introductory scenarios

Before moving on to provide guidance on how to carry out the balancing test, the following three introductory scenarios may give a first illustration of how balancing of interests and rights may look like in real life. All three examples build on a simple and innocent scenario that starts with a special offer for Italian take-away food. The examples gradually introduce new elements that show how the balance is tipped as the impact on the data subjects increases.

Scenario 1: special offer by a pizza chain

Claudia orders a pizza via a mobile app on her smartphone, but does not opt-out of marketing on the website. Her address and credit card details are stored for the delivery. A few days later Claudia receives discount coupons for similar products from the pizza chain in her letterbox at home.

Brief analysis: the pizza chain has a legitimate, but not particularly compelling, interest in attempting to sell more of its products to its customers. On the other hand, there does not appear to be any significant intrusion into Claudia's privacy, or any other undue impact on her interests and rights. The data and the context are relatively innocent (consumption of pizza). The pizza chain established some safeguards: only relatively limited information is used (contact details) and the coupons are sent by traditional mail. In addition, an easy-to-use opportunity is provided to opt-out of marketing on the website.

On balance, and considering also the safeguards and measures in place (including an easy-to-use opt-out tool), the interests and rights of the data subject do not appear to override the legitimate interests of the pizza chain to carry out this minimal amount of data processing.

(Control of Communicable Disease Proposed 42 CFR Parts 70 and 71), adopted on 14.06.2006 (WP 121), where serious specific public health threats are at stake.
- Opinion 1/2006 on whistleblowing schemes (cited above in footnote 39), where the seriousness of an alleged offence is one of the elements of the balancing test.
- Working Document on the surveillance of electronic communications in the workplace, adopted on 29.05.2002 (WP 55), which balances the employer's right to run his business efficiently against the human dignity of the worker, as well as secrecy of correspondence.

[67] Safeguards may include, among others, strict limitations on how much data are collected, immediate deletion of data after use, technical and organisational measures to ensure functional separation, appropriate use of anonymisation techniques, aggregation of data, and privacy-enhancing technologies but also increased transparency, accountability, and the possibility to opt-out of the processing. See further in Section III.3.4(d) and beyond.

Scenario 2: targeted advertisement for the same special offer

The context is the same, but this time not only Claudia's address and credit card details but also her recent order history (for the past three years) are stored by the pizza chain. In addition, the purchase history is combined with data from the supermarket where Claudia does her shopping online, which is operated by the same company as the one running the pizza chain. Claudia is provided by the pizza chain with special offers and targeted advertisement based on her order history for the two different services. She receives the adverts and special offers both online and off-line, by regular mail, email, and placement on the website of the company as well as on the website of a number of selected partners (when she accesses these sites on her computer or via her mobile telephone). Her browsing history (click-stream) is tracked as well. Her location data is also tracked via her mobile phone. An analytics software is run through the data and predicts her preferences and the times and locations when she will be most likely to make a larger purchase, willing to pay a higher price, susceptible to being influenced by a particular rate of discount, or when she craves most strongly for her favourite desserts or ready-meals.[68] Claudia is thoroughly annoyed by persistent ads popping up on her mobile phone when she is checking the bus schedule on her way home advertising the latest take-away offers she is trying to resist. She was unable to find user-friendly information or a simple way to switch off these advertisements although the company claims there is an industry-wide opt-out scheme in place. She was also surprised to see when she moved to a less affluent neighbourhood, that she no longer received her special offers. This resulted in an approximately 10% increase on her monthly food bill. A more tech-savvy friend showed her some speculations in an online blog that the supermarket was charging more for orders from 'bad neighbourhoods', on grounds of the statistically higher risks of credit card fraud in such cases. The company did not comment and claimed that their policy on discounts and the algorithm they are using to set prices are proprietary and cannot be disclosed.

Brief analysis: the data and the context remain of relatively innocent nature. However, the scale of data collection and the techniques used to influence Claudia (including various tracking techniques, predicting times and locations of food cravings and the fact that at these times Claudia is most vulnerable to succumb to temptation), are factors to be considered when assessing the impact of the processing. Lack of transparency about the logic of the company's data processing that may have led to *de facto* price discrimination based on the location where an order is placed, and the significant potential financial impact on the customers ultimately tip the balance even in the relatively innocent context of take-away foods and grocery shopping. Instead of merely offering the possibility to opt out of this type of profiling and targeted advertisement, an informed consent would be necessary, pursuant to Article 7(a) but also under Article 5(3) of the ePrivacy Directive. As a consequence, Article 7(f) should not be relied on as a legal ground for the processing.

[68] See, for example, http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards: *'Recent research suggests that willpower is a finite resource that can be depleted or replenished over time.[10] Imagine that concerns about obesity lead a consumer to try to hold out against her favourite junk food. It turns out there are times and places when she cannot. Big data can help marketers understand exactly how and when to approach this consumer at her most vulnerable—especially in a world of constant screen time in which even our appliances are capable of a sales pitch.'*

Scenario 3: use of food orders to adapt health insurance premiums

Claudia's pizza consumption habits, including the time and nature of food orders, are sold by the chain to an insurance company, which uses them to adapt its health insurance premiums.

Brief analysis: the health insurance company may have a legitimate interest - to the extent applicable regulations allow this - in assessing the health risks of its customers and charge differentiated premiums according to the different risks. However, the way in which the data are collected and the scale of the data collection in itself are excessive. A reasonable person in the situation of Claudia would be unlikely to have expected that information about her pizza consumption would have been used to calculate her health insurance premiums.

In addition to the excessive nature of the profiling and possible inaccurate inferences (the pizza could be ordered for someone else), the inference of sensitive data (health data) from seemingly innocuous data (take-away-orders) contributes to tipping the balance in favour of the data subject's interests and rights. Finally, the processing also has a significant financial impact on her.

On balance, in this specific case the interests and rights of the data subject override the legitimate interests of the health insurance company. As a consequence, Article 7(f) should not be relied on as a legal ground for the processing. It is also questionable whether Article 7(a) could be used as a legal ground, considering the excessive scale of the data collection, and possibly, also due to further specific restrictions under national law.

The above scenarios and the possible introduction of variations with other elements underline the need for a limited number of key factors that can help focus the assessment, as well as the need for a pragmatic approach that allows the use of practical assumptions ('rules of thumb') based primarily on what a reasonable person would find acceptable under the circumstances ('reasonable expectations') and based on the consequences of the data processing activity for data subjects ('impact').

III.3.4. Key factors to be considered when applying the balancing test

Member States have developed a number of useful factors to be considered when carrying out the balancing test. These factors are discussed in this Section under the following four main headings: (a) assessing the controller's legitimate interest, (b) impact on the data subjects, (c) provisional balance and (d) additional safeguards applied by the controller to prevent any undue impact on the data subjects.[69]

To carry out the balancing test it is first important to consider the nature and source of the legitimate interests on the one hand and the impact on the data subjects on the other hand. This assessment should already take into account the measures that the controller plans to adopt to comply with the Directive (for example, to ensure purpose limitation and proportionality under Article 6, or to provide information to the data subjects under Articles 10 and 11).

[69] Due to their importance, some specific issues related to safeguards will be further discussed under separate headings in Sections III.3.5 and III.3.6.

After analysing and weighing the two sides against each other, a provisional 'balance' may be established. Where the outcome of the assessment still leaves doubts, the next step will be to assess whether additional safeguards, bringing more protection to the data subject, may tip the balance in a way that would legitimise the processing.

(a) Assessing the controller's legitimate interest

Whereas the notion of legitimate interests is fairly broad, as explained in Section III.3.1 above, its nature plays a crucial role when it comes to the balancing of interests against the rights and interests of the data subjects. While it is impossible to make value judgments with regard to all possible legitimate interests, it is possible to provide some guidance. As mentioned above, such interest can range from trivial to compelling, and be straightforward or more controversial.

i) Exercise of a fundamental right

Among the fundamental rights and freedoms enshrined in the European Charter of Fundamental Rights (the 'Charter')[70] and the European Convention on Human Rights ('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[71], freedom of the arts and sciences[72], right of access to documents[73], as well as for instance the right to liberty and security[74], the freedom of thought, conscience and religion[75], the freedom to conduct a business[76], the right to property[77], the right to an effective remedy and to a fair trial[78], or the presumption of innocence and right of defence[79].

For the controller's legitimate interest to prevail, the data processing must be 'necessary' and 'proportionate' in order to exercise the fundamental right concerned.

To illustrate, depending on the facts of the case it may well be necessary and proportionate for a newspaper to publish certain incriminating details about the spending habits of a high-level government official involved in an alleged corruption scandal. On the other hand, there should be no blanket permission for the media to publish any and all irrelevant details of the private life of public figures. These and similar cases typically raise complex issues of assessment, and to help guide the assessment, specific legislation, case law, jurisprudence,

[70] The provisions of the Charter are addressed to the institutions and bodies of the EU with due regard for the principle of subsidiarity and the national authorities only when they are implementing EU law.
[71] Article 11 of the Charter and Article 10 of the ECHR.
[72] Article 13 of the Charter and Articles 9 and 10 of the ECHR.
[73] Article 42 of the Charter. 'Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, has a right of access to European Parliament, Council and Commission documents.' Similar rights of access exist in a number of Member States with regard to documents held by public bodies in those Member States.
[74] Article 6 of the Charter and Article 5 of the ECHR.
[75] Article 10 of the Charter and Article 9 of the ECHR.
[76] Article 16 of the Charter.
[77] Article 17 of the Charter and Article 1 of Protocol n°1 to the ECHR.
[78] Article 47 of the Charter and Article 6 of the ECHR.
[79] Article 48 of the Charter and Articles 6 and 13 of the ECHR.

guidelines, as well as codes of conduct and other formal or less formal standards may all play an important role.[80]

When appropriate, in this context also, additional safeguards may play an important role and help determine which way the - sometimes fragile - balance is to be struck.

ii) Public interests/the interests of the wider community

In some cases, the controller may wish to invoke the public interest or the interest of the wider community (whether or not this is provided for in national laws or regulations). For example, a charitable organisation may process personal data for purposes of medical research, or a non-profit organisation in order to raise awareness of government corruption.

It can also be the case that a private business interest of a company coincides with a public interest to some degree. This may happen, for example, with regard to combatting financial fraud or other fraudulent use of services.[81] A service provider may have a legitimate business interest in ensuring that its customers will not misuse the service (or will not be able to obtain services without payment), while at the same time, the customers of the company, taxpayers, and the public at large also have a legitimate interest in ensuring that fraudulent activities are discouraged and detected when they occur.

In general, the fact that a controller acts not only in its own legitimate (e.g. business) interest, but also in the interests of the wider community, can give more 'weight' to that interest. The more compelling the public interest or the interest of the wider community, and the more clearly acknowledged and expected it is in the community and by data subjects that the controller can take action and process data in pursuit of these interests, the more heavily this legitimate interest weighs in the balance.

On the other hand, 'private enforcement' of the law should not be used to legitimise intrusive practices that would, were they carried out by a government organisation, be prohibited pursuant to the case law of the European Court of Human Rights on grounds that the activities of the public authority would interfere with the privacy of data subjects without meeting the stringent test under Article 8(2) of the ECHR.

iii) Other legitimate interests

In some cases, as already discussed in Section III.2, the context in which a legitimate interest arises may come close to one of the contexts in which some of the other legal grounds, in particular, the legal grounds of Article 7(b) (contract), 7(c) (legal obligation), or 7(e) (public task) may apply. For example, a data processing activity may not be strictly necessary, but

[80] With regard to the criteria to be applied in cases involving freedom of expression, the case law of the European Court of Human Rights also provides useful guidance. See, for example, the judgment of the ECHR in the Case of von Hannover v Germany (No 2) on 7 February 2012, in particular, para 95-126. It must also be considered that Article 9 of the Directive (under the title *Processing of personal data and freedom of expression*) allows Member States to 'provide for exemptions or derogations from [certain provisions of the Directive] for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression' provided these are 'necessary to reconcile the right to privacy with the rules governing freedom of expression'.

[81] See, for example, 'Example 21: Smart metering data mined to detect fraudulent energy use' on page 67 in the Working Party's Opinion 3/2013 on purpose limitation (cited above in footnote 9).

can still be relevant to the performance of a contract - or, a law may only permit, but not require that certain data be processed. As we have seen, it may not always be easy to draw a clear dividing line between the different grounds, but this makes it all the more important to bring the Article 7(f) balancing test into the analysis.

Here also, as well as in all possible other cases not mentioned thus far, the more compelling the interest of the controller, and the more clearly acknowledged and expected it is in the wider community that the controller may take action and process data in pursuit of such an interest, the more heavily this legitimate interest weighs in the balance.[82] This brings us to the following, more general point.

iv) Legal and cultural/societal recognition of the legitimacy of the interests

In all the above contexts, it is certainly also relevant whether EU law or the law of a Member State specifically allows (even if it does not require) controllers to take steps in pursuit of the public or private interest concerned. The existence of any duly adopted, non-binding guidance issued by authoritative bodies, for example, by regulatory agencies, encouraging controllers to process data in pursuit of the interest concerned is also relevant.

Compliance with any non-binding guidance provided by data protection authorities or other relevant bodies with regard to the modalities of the data processing will also be likely to contribute towards a favourable assessment of the balance. Cultural and societal expectations, even when not reflected directly in legislative or regulatory instruments, may also play a role, and may help tip the balance either way.

The more explicitly recognised it is in the law, in other regulatory instruments - be they binding or not on the controller - or even in the culture of the given community overall without any specific legal basis, that the controllers may take action and process data in pursuit of a particular interest, the more heavily this legitimate interest weighs in the balance[83].

(b) The impact on data subjects

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. The first subsection below discusses in general terms how to assess the impact on the data subject.

Several elements can be useful here and they are analysed in further subsections, including the nature of personal data, the way the information is being processed, the reasonable expectations of the data subjects and the status of the controller and data subject. We will also briefly discuss issues related to potential sources of risk that may lead to impact on the individuals concerned, the severity of any impacts on the individuals concerned and the likelihood of such impacts materialising.

[82] Of course, the assessment must also include reflection on the possible prejudice suffered by the controller, by third parties or the broader community if the data processing does not take place.

[83] This interest can however not be used to legitimise intrusive practices that would otherwise not meet the test of Article 8(2) of the ECHR.

i) Assessment of impact

In assessing the impact[84] 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, situations where there is a risk of damaging the reputation, negotiating power, or autonomy of the data subject.

In addition to adverse outcomes that can be specifically foreseen, 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, – for example through exposure on the internet. The chilling effect on protected behaviour, such as freedom of research or free speech, that may result from continuous monitoring/tracking, must also be given due consideration.

The Working Party emphasises that it is crucial to understand that relevant 'impact' is a much broader concept than harm or damage to one or more specific data subjects. 'Impact' as used in this Opinion covers any possible (potential or actual) consequences of the data processing. For the sake of clarity, we also emphasise that the concept is unrelated to the notion of data breach and is much broader than impacts that may result from a data breach. Instead, the notion of impact, as used here, encompasses the various ways in which an individual may be affected - positively or negatively - by the processing of his or her personal data. [85]

It is also important to understand that more often than not a series of related and unrelated occurrences can lead cumulatively to the ultimate negative impact on the data subject and it may be difficult to identify which processing activity by which controller played a key role in the negative impact.

Considering that establishment of a case for compensation of a suffered harm or damage is often difficult for the data subjects in this context, even where the effect itself is very real, it is all the more important to focus on prevention and ensuring that data processing activities may only be carried out, provided they carry no risk or a very low risk of undue negative impact on the data subjects' interests or fundamental rights and freedoms.

When assessing impact, the terminology and methodology of traditional risk assessment may be helpful to some degree, and therefore some elements of this methodology will be briefly

[84] This assessment of impact must be understood in the context of Article 7(f). In other words, we do not refer to a 'risk analysis' or a 'data protection impact assessment' in the sense of the proposed Regulation (Articles 33 and 34) and the various LIBE amendments to it. The question what methodology should be followed in a 'risk analysis' or a 'data protection impact assessment' goes beyond the scope of this Opinion. On the other hand, it should be kept in mind that - one way or another - the analysis of impact under Article 7(f) can be an important part of any 'risk assessment' or 'data protection impact assessment' and can also help identify situations where the data protection authority should be consulted.

[85] The risk of financial damage, for example, if a data breach releases financial information that was meant to be in a secure environment, and this eventually leads to identity theft or other forms of fraud, or the risk of personal injury, pain, suffering and loss of amenity that might ultimately result from, for example, unauthorised alteration of medical records, and a subsequent mistreatment of a patient, must always be duly taken into account, although it is by no means limited to situations under the scope of Article 7(f). At the same time, such risks are not the only ones to be considered when assessing impact under Article 7(f).

highlighted below. However, a comprehensive methodology for assessment of impact - in the context of Article 7(f) or more broadly - would go beyond the scope of this Opinion.

In this context as elsewhere, it is important to identify the sources of potential impacts on the data subjects.

The likelihood that a risk can materialise is one of the elements to take into consideration. For example, access to the Internet, exchanges of data with sites outside the EU, interconnections with other systems and a high degree of system heterogeneity or variability can represent vulnerabilities that hackers could exploit. This risk source bears a relatively high likelihood for the risk of compromising data to materialise. Conversely, a homogeneous, stable system that has no interconnections and is disconnected from the Internet bears a far lower likelihood of compromising data.

Another element of the risk assessment is the severity of the consequences of a materialized risk. This severity can range from low levels (like the annoying need to enter again personal contact details lost by the data controller) to very high levels (like the loss of life when personal location patterns of protected individuals go into the hands of criminals or when power supply is remotely cut off through smart metering devices in critical weather or personal health conditions).

These two key elements - the likelihood that the risk materializes on the one hand, and the severity of the consequences on the other hand - each contribute to the overall assessment of the potential impact.

Finally, in applying the methodology, it should be recalled that assessing impact under Article 7(f) cannot lead to a mechanical and purely quantitative exercise. In traditional risk assessment scenarios, 'severity' can take into account the number of individuals potentially impacted. Nevertheless, it should be kept in mind that processing of personal data having an impact on a minority of data subjects - or even a single individual only - still requires a very careful analysis especially if such impact on each individual concerned is potentially significant.

ii) Nature of the data

It would first be important to evaluate whether the processing involves sensitive data, either because they belong to the special categories of data under Article 8 of the Directive, or for other reasons, as in the case of biometric data, genetic information, communication data, location data, and other kinds of personal information requiring special protection. [86]

To illustrate, in the view of the Working Party, as a general rule, the use of biometrics for general security requirements of property or individuals is regarded as a legitimate interest that would be overridden by the interests or fundamental rights and freedoms of the data subject. On the other hand, biometric data such as fingerprint and/or iris scan could be used

[86] Biometric data and genetic information are considered as special categories of data in the Proposal of the Commission for a Data Protection Regulation, read together with the amendments proposed by the LIBE Committee. See amendment 103 to Article 9 in the Final LIBE Committee Report. On the relationship between Articles 7 and 8 of Directive 95/46/EC, see Section II.1.2 above on pages 14-15.

for the security of a high-risk area such as a laboratory doing research on dangerous viruses, provided that the controller has demonstrated concrete evidence of a considerable risk[87].

In general, the more sensitive the information involved, the more consequences there may be for the data subject. This, however, does not mean that data that may in and of themselves seem innocuous, can be freely processed based on Article 7(f). Indeed, even such data, depending on the way they are processed, can have significant impact on individuals, as will be shown in Subsection (iii) below.

In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. Here, first of all, it is important to highlight that personal data, even if it has been made publicly available, continues to be considered as personal data, and its processing therefore continues to require appropriate safeguards.[88] There is no blanket permission to reuse and further process publicly available personal data under Article 7(f).

That said, the fact that personal data is publicly available may be considered as a factor in the assessment, especially if the publication was carried out with a reasonable expectation of further use of the data for certain purposes (e.g. for purposes of research or for purposes related to transparency and accountability).

iii) The way data are being processed

Assessing impact in a wider sense may involve considering whether the data are publicly disclosed or otherwise made accessible to a large number of persons, or whether large amounts of personal data are processed or combined with other data (e.g. in case of profiling, for commercial, law enforcement or other purposes). Seemingly innocuous data, when processed on a large scale and combined with other data may lead to inferences about more sensitive data, as shown above in Scenario 3 illustrating the relationship between pizza consumption patterns and health insurance premiums.

In addition to potentially leading to the processing of more sensitive data, such analysis may also lead to uncanny, unexpected, and sometimes also inaccurate predictions, for example, concerning the behaviour or personality of the individuals concerned. Depending on the nature and impact of these predictions, this may be highly intrusive to the individual's privacy.[89]

The Working Party also stressed in a previous Opinion the risks inherent in certain security solutions (including for firewalls, anti-virus or anti-spam), as they may lead to large scale

[87] See Opinion 3/2012 of the Article 29 Working Party on developments in biometric technologies (WP193). As another illustration, in its Opinion 4/2009 on the World Anti-Doping Agency (cited above in footnote 32), the Working Party emphasised that Article 7(f) would not be a valid ground to process medical data and data related to offences in the context of anti-doping investigations, in view of the 'gravity of privacy intrusions'. The processing of data should be foreseen by law and meet the requirements of Article 8(4) or (5) of the Directive.

[88] See the Working Party's Opinion 3/2013 on purpose limitation (cited in footnote 9 above) and the Working Party's Opinion 06/2013 on open data and public sector information ('PSI') reuse, adopted on 05.06.2013 (WP207).

[89] See Section III.2.5 and Annex 2 (Big data and open data) of the Opinion on Purpose Limitation (cited above in footnote 9).

deployment of deep packet inspection, which may have a significant influence on the assessment of the balance of rights[90].

In general, the more negative or uncertain the impact of the processing might be, the more unlikely it is that the processing will be considered, on balance, as legitimate. The availability of alternative methods to achieve the objectives pursued by the controller, with less negative impact for the data subject, would certainly have to be a relevant consideration in this context. When appropriate, privacy and data protection impact assessments can be used to determine whether this is a possibility.

iv) Reasonable expectations of the data subject

The reasonable expectations of the data subject with regard to the use and disclosure of the data are also very relevant in this respect. As also highlighted with regard to the analysis of the purpose limitation principle[91], it is 'important to consider whether the status of the data controller[92], the nature of the relationship or the service provided[93], or the applicable legal or contractual obligations (or other promises made at the time of collection) could give rise to reasonable expectations of stricter confidentiality and stricter limitations on further use. In general, the more specific and restrictive the context of collection, the more limitations there are likely to be on use. Here again, it is necessary to take account of the factual context rather than simply rely on text in small print.

v) Status of the data controller and data subject

The status of the data subject and the data controller is also relevant when assessing the impact of the processing. Depending on whether the data controller is an individual or a small organisation, a large multi-national company, or a public sector body, and on the specific circumstances, its position may be more or less dominant in respect of the data subject. A large multinational company may, for instance, have more resources and negotiating power than the individual data subject, and therefore, may be in a better position to impose on the data subject what it believes is in its 'legitimate interest'. This may be even more so if the company has a dominant position on the market. If left unchecked, this may happen to the detriment of the individual data subjects. Just as consumer protection and competition laws help ensure that this power will not be misused, data protection law could also play an important role in ensuring that the rights and interests of the data subjects will not be unduly prejudiced.

On the other hand, the status of the data subject is also relevant. While the balancing test should in principle be made against an average individual, specific situations should lead to a more case-by-case approach: for example, it would be relevant to consider whether the data subject is a child[94] or otherwise belongs to a more vulnerable segment of the population

[90] See Section 3.1 of the Working Party's Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive) (WP159).
[91] See pages 24-25 of the Working Party's Opinion 3/2013 on purpose limitation (cited above in footnote 9).
[92] 'Such as, for example, an attorney or a physician.'
[93] 'Such as, for example, cloud computing services for personal document management, email services, diaries, e-readers equipped with note-taking features, and various life-logging applications that may contain very personal information.'
[94] See the Working Party's Opinion 2/2009 on the protection of children's personal data, (General Guidelines and the special case of schools), adopted on 11.02.2009 (WP160). This opinion insists on the specific vulnerability of

requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly. The question whether the data subject is an employee, a student, a patient, or whether there is otherwise an imbalance in the relationship between the position of the data subject and the controller must certainly be also relevant. It is important to assess the effect of actual processing on particular individuals.

Finally, it is important to emphasise that not all negative impact on the data subjects 'weighs' equally on the balance. The purpose of the Article 7(f) balancing exercise is not to prevent any negative impact on the data subject. Rather, its purpose is to prevent disproportionate impact. This is a crucial difference. For example, the publication of a well-researched and accurate newspaper article on alleged government corruption may damage the reputation of the government officials involved and may lead to significant consequences, including loss of reputation, loss of elections, or imprisonment, but it could still find a basis under Article 7(f).[95]

(c) Provisional balance

When balancing the interests and rights at stake as described above, the measures taken by the controller to comply with its general obligations under the Directive, including in terms of proportionality and transparency, will greatly contribute to ensuring that the data controller meets the requirements of Article 7(f). Full compliance should mean that the impact on individuals is reduced, that data subjects' interests or fundamental rights or freedoms are *less likely* to be interfered with and that therefore it is *more likely* that the data controller can rely on 7(f). This should encourage controllers to better comply with all horizontal provisions of the Directive[96].

This does not mean, however, that compliance with these horizontal requirements will as such always be sufficient to secure a legal basis based on Article 7(f). Indeed, if this were the case, Article 7(f) would be superfluous or become a loophole that would render meaningless the entire Article 7, which calls for an adequate specific legal basis for the processing.

For this reason, it is important to carry out a further assessment in the balancing exercise in cases where - based on the preliminary analysis - it is not clear which way the balance should be struck. The controller may consider whether it is possible to introduce additional measures, going beyond compliance with horizontal provisions of the Directive, to help reduce the undue impact of the processing on the data subjects.

Additional measures may include, for example, providing an easily workable and accessible mechanism to ensure an unconditional possibility for data subjects to opt-out of the processing. These additional measures may in some (but not all) cases help tip the balance and help ensure that the processing can be based on Article 7(f), while at the same time, also protecting the rights and interests of the data subjects.

---

the child, and in case the child is represented, on the need to take into account the child's best interest and not that of its representative.

[95] As explained above, any relevant derogations for processing for journalistic purposes under Article 9 of the Directive must also be taken into account.

[96] On the important role of 'horizontal compliance' see also page 54 of the Working Party's Opinion 3/2013 on purpose limitation, cited in footnote 9 above.

(d) Additional safeguards applied by the controller

As explained above, the way in which the controller would apply appropriate measures could, in some situations, help 'tip the balance' on the scale. Whether the result is acceptable will depend on the assessment as a whole. The more significant the impact on the data subject, the more attention should be given to relevant safeguards.

Examples of the relevant measures may include, among other things, strict limitation on how much data is collected, or immediate deletion of data after use. While some of these measures may already be compulsory under the Directive, they are often scalable and leave room for controllers to ensure better protection of data subjects. For instance, the controller may collect less data, or provide additional information compared to what is specifically listed in Articles 10 and 11 of the Directive.

In some other cases, the safeguards are not *explicitly* required under the Directive but may well be in the future under the proposed Regulation, or they are only required in specific situations, such as:

- technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation' as is often the case in a research context)
- extensive use of anonymisation techniques
- aggregation of data
- privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments
- increased transparency
- general and unconditional right to opt-out
- data portability & related measures to empower data subjects

The Working Party notes that with respect to some key issues, including functional separation and anonymisation techniques, some guidance has already been provided in the relevant parts of its Opinions on purpose limitation, on open data and on anonymisation techniques.[97]

As far as pseudonymisation and encryption are concerned, the Working Party would like to emphasise that if data are not directly identifiable, this does not as such affect the appreciation of the legitimacy of the processing: it should not be understood as turning an illegitimate processing into a legitimate one[98].

At the same time, pseudonymisation and encryption, just like any other technical and organisational measures introduced to protect personal information, will play a role with regard to the evaluation of the potential impact of the processing on the data subject, and thus, may in some cases play a role in tipping the balance in favour of the controller. The use of

[97] See Sections III.2.3, III.2.5 and Annex 2 f the Working Party's Opinion 3/2013 on purpose limitation, cited above in footnote 9, on further processing for historical, statistical and scientific purposes, and on big data and open data; see also relevant parts of the Working Party's Opinion 06/2013 on open data (cited in footnote 88 above) and Opinion 5/2014 on Anonymisation Techniques

[98] See on this point the amendments voted by the LIBE Committee in the Final LIBE Committee Report, and in particular amendment 15 on Recital 38 connecting pseudonymisation and the legitimate expectations of the data subject.

less risky forms of personal data processing (e.g. personal data that is encrypted while in storage or transit, or personal data that are less directly and less readily identifiable) should generally mean that the likelihood of data subjects' interests or fundamental rights and freedoms being interfered with is reduced.

In connection with these safeguards - and the overall assessment of the balance - the Working Party wishes to highlight three specific issues that often play a crucial role in the context of Article 7(f):

- the relationship between the balancing test, transparency, and the accountability principle;
- the right of the data subject to object to the processing, and beyond objection, the availability of an opt out without the need for any justification, and
- empowering data subjects: data portability and the availability of workable mechanisms for the data subject to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data.

Due to their importance, these subjects will be discussed under separate headings.

III.3.5. Accountability and transparency

In the first place, before a processing operation on the basis of Article 7(f) is to take place, the controller has the responsibility to evaluate whether it has a legitimate interest; whether the processing is necessary for that legitimate interest and whether the interest is overridden by the interests and rights of the data subjects in the specific case.

In that sense, Article 7(f) is based on the accountability principle. The controller must perform a careful and effective test in advance, based on the specific facts of the case rather than in an abstract manner, taking also into account the reasonable expectations of data subjects. As a matter of good practice, where appropriate, carrying out this test should be documented in a sufficiently detailed and transparent way so that the complete and correct application of the test could be verified - when necessary - by relevant stakeholders including the data subjects and data protection authorities, and ultimately, by the courts.

The controller will first define the legitimate interest and make the balancing test, but this is not necessarily the final and definitive assessment: if, in reality, the interest pursued is not the one that was specified by the controller or if the controller only defined the interest in insufficient detail, the balance has to be re-assessed, based on the actual interest, to be determined either by a data protection authority or by a Court.[99] As is the case for other key aspects of data protection, such as the identification of the data controller or the specification of purpose[100], what matters is the reality behind any assertion made by the controller.

The notion of accountability is closely linked to the notion of transparency. In order to enable data subjects to exercise their rights, and to allow public scrutiny by stakeholders more broadly, the Working Party recommends that controllers explain to data subjects in a clear and user-friendly manner, the reasons for believing that their interests are not overridden by

[99] For example, following a complaint or an Article 14 objection.
[100] See Opinions cited in footnote 9.

the interests or fundamental rights and freedoms of the data subjects, and also explain to them the safeguards they have taken to protect personal data, including, where appropriate, the right to opt out of the processing.[101]

In this respect the Working Party emphasises that consumer protection law, in particular, laws protecting consumers against unfair commercial practices, is also highly relevant here.

If a controller hides important information regarding unexpected further use of the data in legalistic terms buried in the small print of a contract, this may infringe consumer protection rules concerning unfair contractual terms (including the prohibition against 'surprising terms'), and it will also not fulfil the requirements of Article 7(a) for a valid and informed consent, or the requirements of Article 7(f) in terms of reasonable expectations of the data subject and an overall acceptable balance of interests. It would of course also raise questions of compliance with Article 6 as to the need for a fair and lawful processing of personal data.

For instance, in a number of cases, users of 'free' online services, such as search, email, social media, file storage or other online or mobile applications, are not fully aware of the extent to which their activity is logged and analysed in order to generate value for the service provider and therefore they remain unconcerned of the risks involved.

In order to empower data subjects in these situations, a first necessary - but by no means in itself sufficient - precondition[102] is to make it clear that the services are not free, and that rather, the consumers pay using their personal data. The conditions and safeguards subject to which data may be used must also be clearly spelled out in each case to ensure the validity of Article 7(a) consent, or a favourable balance under Article 7(f).

III.3.6. The right to object and beyond

(a) The right to object under Article 14 of the Directive

Article 7(e) and (f) are particular in the sense that while they mainly rely on an objective assessment of the interests and rights involved, they also allow the self-determination of the data subject to come into play with a right to object[103]: at least in the case of these two grounds, Article 14(a) of the Directive provides that ('save where otherwise provided by national legislation') the data subject 'can object at any time on compelling legitimate grounds

[101] As explained on page 46 of the Working Party's Opinion 3/2013 on purpose limitation (cited above in footnote 9), in case of profiling and automated decision-making, 'to ensure transparency, data subjects/consumers should be given access to their 'profiles', as well as to the logic of the decision-making (algorithm) that led to the development of the profile. In other words: organisations should disclose their decisional criteria. This is a crucial safeguard and all the more important in the world of big data'. Whether or not an organisation offers this transparency is a highly relevant factor to be considered also in the balancing exercise.

[102] For further possible safeguards with regard to the increasingly common situations in which consumers pay with their personal data, see Section III.3.6 in particular pages 47-48 on 'Data protection-friendly alternatives to 'free' on-line services' and on 'Data portability, 'midata' and related issues'.

[103] This right to object should not be confused with consent based on Article 7(a), where the data controller cannot process the data before he obtains such consent. In the context of Article 7(f), the controller can process the data, subject to conditions and safeguards, as long as the data subject has not objected. In this sense, the right to object can rather be considered as a specific form of opt-out. See more details in the Working Party's Opinion 15/2011 on the definition of consent (cited in footnote 2).

relating to his particular situation to the processing of data relating to him'. It adds that if the objection is justified the processing of their data must cease.

In principle, under current law, the data subject will thus have to demonstrate 'compelling legitimate interests' to stop the processing of his/her personal data (Article 14(a)), except in the context of direct marketing activities where the objection does not need to be justified (Article 14(b)).

This should not be seen as contradicting the balancing test of Article 7(f), which is made 'a priori': it rather complements the balance, in the sense that, where the processing is allowed further to a reasonable and objective assessment of the different rights and interests at stake, the data subject still has an *additional* possibility to object on grounds relating to his/her particular situation. This will then have to lead to a new assessment taking into account the particular arguments submitted by the data subject. This new assessment is in principle again subject to verification by a data protection authority or the courts.

(b) Beyond objection: the role of opt-out as an additional safeguard

The Working Party emphasises that, even if the Article 14(a) right to object is subject to justification by the data subject, nothing prevents the controller from offering an opt-out that would be broader, and that would not require any additional demonstration of legitimate interest (compelling or otherwise) from the data subject. Such an unconditional right would not need to be based on the specific situation of data subjects.

Indeed, and especially in borderline cases where the balance is difficult to strike, a well-designed and workable mechanism for opt-out, while not necessarily providing data subjects with all the elements that would satisfy a valid consent under Article 7(a), could play an important role in safeguarding the rights and interests of the data subjects.

For this a nuanced approach is required, which distinguishes between cases where an Article 7(a) opt-in consent is required, and cases where a workable opportunity to opt-out of the processing (combined with possible other additional measures) may contribute to protecting data subjects under Article 7(f).

The more widely applicable the mechanism for opt-out and the more easy it is to exercise it, the more it will contribute to tipping the balance in favour of the processing to find a legal ground in Article 7(f).

Illustration: the evolution in the approach to direct marketing

To illustrate how a distinction is made between cases where Article 7(a) consent is required and cases where an opt-out could be used as a safeguard under Article 7(f), it is helpful to use the example of direct marketing, for which traditionally there has been a specific opt-out provision included in Article 14(b) of the Directive. To address new technological developments, this provision has later been complemented by specific provisions in the ePrivacy Directive.[104]

[104] On Article 13 of the ePrivacy Directive, see also Section III.2.4 of the Working Party's Opinion 3/2013 on purpose limitation (cited above in footnote 9).

Under Article 13 of the ePrivacy Directive, for certain types of - more intrusive - direct marketing activities (such as e-mail marketing and automated calling machines) consent is the rule. As an exception, in existing client relationships where a controller advertises its own 'similar' products or services, it is sufficient to provide an (unconditional) opportunity to 'opt-out' without justification.

Technologies have evolved, which has called for similar, relatively simple solutions following a similar logic for new marketing practices.

First, the way in which marketing material is being delivered has evolved: instead of simple emails arriving to mailboxes, now targeted behavioural advertisements also pop up on smart phones and computer screens. In the near future, advertisement may also be embedded in smart objects linked within the internet of things.

Second, advertisements are becoming ever-more specifically targeted: rather than based on simple customer profiles, consumers' activities are increasingly tracked and stored online and offline and analysed with more sophisticated automated methods.[105]

As a result of these developments, the object of the balancing exercise has shifted: the issue is no longer about the right to free commercial speech, but primarily the economic interests of business organisations to get to know their customers by tracking and monitoring their activities online and offline, which should be balanced against the (fundamental) rights to privacy and the protection of personal data of these individuals and their interest not to be unduly monitored.

This shift in prevailing business models and the rise of the value of personal data as an asset to business organisations explains the recent requirement for consent in this context, pursuant to Article 5(3) and Article 13 of the ePrivacy Directive.

There are thus different specific rules, depending on the form of marketing, including:

- the unconditional right to object to direct marketing (designed for the traditional, postal mailing context, and for the marketing of similar products) under Article 14(b) of the Directive; Article 7(f) could be the legal ground in that case;
- the requirement for consent under Article 13 of the ePrivacy Directive for automated calling systems, fax, text messages and e-mail marketing (subject to exceptions)[106], and *de facto* application of Article 7(a) of the Data Protection Directive.
- the requirement for consent under Article 5(3) of the ePrivacy Directive (and Article 7(a) of the Data Protection Directive) for behavioural advertising based on tracking techniques such as cookies storing information in the terminal of the user[107].

While the legal grounds applicable are clear as far as Articles 5(3) and 13 of the ePrivacy Directive are concerned, not all forms of marketing are covered and it would be desirable to

[105] See Section III.2.5 and Annex 2 (on big data and open data) of the Working Party's Opinion 3/2013 on purpose limitation (cited above in footnote 9).

[106] See also Article 13(3) of the ePrivacy Directive, which leaves Member States the choice between opt-in and opt-out for direct marketing via other means.

[107] See for the application of this provision the Opinion 2/2010 of the Working Party on online behavioural advertising (WP171).

have guidance on which situations require Article 7(a) consent, and for which situations a balance under Article 7(f) is achieved, including an opportunity to opt-out.

In this respect, it is useful to recall the Working Party's Opinion on purpose limitation, where it is specifically stated that 'when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform 'measures or decisions' that are taken with regard to those customers .... free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible. Importantly, such consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research.'[108]

Data protection-friendly alternatives to 'free' on-line services

In the context where customers signing up for 'free' online services actually 'pay for' these services by allowing the use of their personal data, it would also contribute towards a favourable assessment of the balance - or towards the finding that the consumer had a genuine freedom of choice, and therefore valid consent was provided under Article 7(a) - if the controller also offered an alternative version of its services, in which 'personal data' were not used for marketing purposes.

As long as such alternative services are not available, it is more difficult to argue that a valid (freely given) consent has been granted under Article 7(a) by the mere use of free services or that the balance under Article 7(f) should be struck in favour of the controller.

The above considerations underline the important role that additional safeguards, including a workable mechanism to opt-out of the processing may play in modifying the provisional balance. At the same time, they also suggest that in some cases, Article 7(f) cannot be relied on as a ground for processing and controllers must ensure a valid consent under Article 7(a) – or fulfil some other conditions of the Directive – for the processing to take place.

Data portability, 'midata' and related issues

Among the additional safeguards which might help tip the balance, special attention should be given to data portability and related measures, which may be increasingly relevant in an on-line environment. The Working Party recalls its Opinion on Purpose Limitation where it has emphasised that 'in many situations, safeguards such as allowing data subjects/customers to have direct access to their data in a portable, user-friendly and machine-readable format may help empower them, and redress the economic imbalance between large corporations on the one hand and data subjects/consumers on the other. It would also let individuals 'share the wealth' created by big data and incentivise developers to offer additional features and applications to their users.[109]

[108] See Annex II (on Big Data and Open Data) of the Opinion (cited in footnote 9 above), page 45.

[109] 'See initiatives such as 'midata' in the UK, which are based on the key principle that data should be released back to consumers. Midata is a voluntary programme, which over time should give consumers increasing access to their personal data in a portable, electronic format. The key idea is that consumers should also benefit from big data by having access to their own information to enable them to make better choices. See also 'Green button'

The availability of workable mechanisms for the data subjects to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data will empower data subjects and let them benefit more from digital services. In addition, it can foster a more competitive market environment, by allowing customers more easily to switch providers (e.g. in the context of online banking or in case of energy suppliers in a smart grid environment). Finally, it can also contribute to the development of additional value-added services by third parties who may be able to access the customers' data at the request and based on the consent of the customers. In this perspective, data portability is therefore not only good for data protection, but also for competition and consumer protection.[110]

IV. Final observations

In this Opinion the Working Party analysed the criteria set forth in Article 7 of the Directive for making data processing legitimate. Beyond guidance on the practical interpretation and application of Article 7(f) under the current legal framework, it aims at formulating policy recommendations to assist policy makers as they consider changes to the current data protection legal framework. Before developing these recommendations, the main findings concerning the interpretation of Article 7 are summarised below.

IV.1. Conclusions

Overview of Article 7

Article 7 requires that personal data shall only be processed if at least one of six legal grounds listed in that Article apply.

The first ground, Article 7(a), focuses on the consent of the data subject as a ground for legitimacy. The rest of the grounds, in contrast, allow processing – subject to safeguards – in situations where, irrespective of consent, it is appropriate and necessary to process the data within a certain context in pursuit of a specific legitimate interest.

Paragraphs (b), (c), (d) and (e) each specify a particular context, within which the processing of personal data can be considered legitimate. The conditions which apply in each of these different contexts require careful attention, as they determine the scope of the various grounds for legitimacy. More specifically, the criteria 'necessary for the performance of a contract', 'necessary for compliance with a legal obligation', 'necessary in order to protect the vital interests of the data subject', and 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority' contain different requirements, which have been discussed in Section III.2.

Paragraph (f) refers, more generally, to (any kind of) legitimate interest pursued by the controller (in any context). This general provision, however, is specifically made subject to an additional balancing test, which requires the legitimate interests of the controller - or the third

initiatives that allow consumers to access their own energy usage information.' For more information on initiatives in the UK and in France see http://www.midatalab.org.uk/ and http://mesinfos.fing.org/.

[110] On the right to data portability, see Article 18 of the Proposed Regulation.

party or parties to whom the data are disclosed – to be weighed against the interests or fundamental rights of the data subjects.

Role of Article 7(f)

Article 7(f) should not be seen as a legal ground that can only be used sparingly to fill in gaps for rare and unforeseen situation as ‘a last resort’ - or as a last chance if no other grounds may apply. Nor should it be seen as a preferred option and its use unduly extended because it would be considered as less constraining than the other grounds. Rather, it is as valid a means as any of the other grounds for legitimising the processing of personal data.

Appropriate use of Article 7(f), in the right circumstances and subject to adequate safeguards, may help prevent misuse of, and over-reliance on, other legal grounds. An appropriate assessment of the balance under Article 7(f), often with an opportunity to opt-out of the processing, may in some cases be a valid alternative to inappropriate use of, for instance, the ground of 'consent' or ‘necessary for the performance of a contract'. Considered in this way, Article 7(f) presents complementary safeguards compared to the other pre-determined grounds. It should thus not be considered as 'the weakest link' or an open door to legitimise all data processing activities which do not fall under any of the other legal grounds.

Legitimate interests of the controller / interests or fundamental rights of the data subject

The concept of 'interest' is the broader stake that a controller may have in the processing, or the benefit that it derives - or that society might derive - from the processing. It may be compelling, straightforward or more controversial. Situations referred to by Article 7(f) may thus range from the exercise of fundamental rights or the protection of important personal or social interests to other less obvious or even problematic contexts.

To be considered as 'legitimate' and be relevant under Article 7(f), the interest will need to be lawful, that is, in accordance with EU and national law. It must also be sufficiently clearly articulated and specific enough to allow the balancing test to be carried out against the interests and fundamental rights of the data subject. It must also represent a real and present interest - that is, it must not be speculative.

If the controller, or the third party to whom the data are to be disclosed, has such a legitimate interest, this does not necessarily mean that it can rely on Article 7(f) as a legal ground for the processing. Whether Article 7(f) can be relied on will depend on the outcome of the balancing test that follows. The processing must also be 'necessary for the purposes of the legitimate interests' pursued by the controller or - in the case of disclosure - by the third party. Less invasive means to serve the same purpose should therefore always be preferred.

The notion of the 'interests' of the data subjects is defined even more broadly as it does not require a ‘legitimacy’ element. If the data controller or third party can pursue any interests, provided they are not illegitimate, the data subject, in turn, is entitled to have all categories of interests to be taken into account and weighed against those of the controller or third party, as long as they are relevant within the scope of the Directive.

Applying the balancing test

When interpreting the scope of Article 7(f), the Working Party aims at a balanced approach, which ensures the necessary flexibility to data controllers for situations where there is no undue impact on data subjects, while at the same time providing sufficient legal certainty and guarantees to data subjects that this open-ended provision will not be misused.

To carry out this balancing test, it is first important to consider the nature and source of the legitimate interests, and whether the processing is necessary to pursue those interests, on the one hand, and the impact on the data subjects on the other hand. This initial assessment should take into account the measures, such as transparency or limited collection of data that the controller plans to adopt to comply with the Directive.

After analysing and weighing the two sides against each other, a provisional 'balance' may be established: a preliminary conclusion may be drawn as to whether the legitimate interests of the controller prevail over the rights and interests of the data subjects. There may however be cases where the outcome of the balancing test is unclear, and there is doubt on whether the legitimate interest of the controller (or third party) prevails and whether the processing can be based on Article 7(f).

For this reason, it is important to carry out a further assessment in the balancing exercise. In this phase, the controller may consider whether it is able to introduce additional measures, going beyond compliance with other horizontal provisions of the Directive, to help protect data subjects. Additional measures may include, for example, providing an easily workable and accessible mechanism to ensure an unconditional possibility for data subjects to opt-out of the processing.

Key factors to be considered when applying the balancing test

Based on the foregoing, useful factors to be considered when carrying out the balancing test include:

- the nature and source of the legitimate interest, including:

  - whether the data processing is necessary for the exercise of a fundamental right, or
  - is otherwise in the public interest or benefits from social, cultural or legal/regulatory recognition in the community concerned;

- the impact on the data subjects, including:

  - the nature of the data, such as whether the processing involves data that may be considered sensitive or has been obtained from publicly available sources;
  - the way data are being processed, including whether the data are publicly disclosed or otherwise made accessible to a large number of persons, or whether large amounts of personal data are processed or combined with other data (e.g. in case of profiling, for commercial, law enforcement or other purposes);
  - the reasonable expectations of the data subject, especially with regard to the use and disclosure of the data in the relevant context;

- the status of the data controller and data subject, including the balance of power between the data subject and the data controller, or whether the data subject is a child or otherwise belongs to a more vulnerable segment of the population.

- additional safeguards to prevent undue impact on the data subjects, including:

  - data minimisation (e.g. strict limitations on the collection of data, or immediate deletion of data after use);
  - technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation');
  - extensive use of anonymisation techniques, aggregation of data, privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments;
  - increased transparency, general and unconditional right to opt-out, data portability & related measures to empower data subjects.

Accountability, transparency, the right to object and beyond

In connection with these safeguards - and the overall assessment of the balance - three issues often play a crucial role in the context of Article 7(f) and therefore require special attention:

- the existence of some and possible need for additional measures to increase transparency and accountability;
- the right of the data subject to object to the processing, and beyond objection, the availability of opt-out without the need for any justification;
- empowering data subjects: data portability and the availability of workable mechanisms for the data subject to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data.

IV. 2. Recommendations

The current text of Article 7(f) of the Directive is open-ended. This flexible wording leaves much room for interpretation and has sometimes - as experience has shown - led to lack of predictability and lack of legal certainty. However, if used in the right context, and with the application of the right criteria, as set out in this Opinion, Article 7(f) has an essential role to play as a legal ground for legitimate data processing.

The Working Party therefore supports the current approach in Article 6 of the proposed Regulation, which maintains the balance of interests as a separate legal ground. Further guidance would however be welcome to ensure an adequate application of the balancing test.

Scope and means for further specification

An essential requirement would be that the provision remains sufficiently flexible, and that it reflects both the perspectives of the data controller and the data subject, and the dynamic nature of the relevant contexts. For this reason, the Working Party is of the view that providing - in the text of the proposed Regulation or in delegated acts - for detailed and exhaustive lists of situations in which an interest would be qualified *de facto* as legitimate is not advisable, The Working Party would equally be against defining cases where the interest or right of one party should *as a principle* or *as a presumption* override the interest or right of

the other party, merely because of the nature of such an interest or right, or because certain protective measures have been taken, for example, the data have merely been pseudonymised. This would risk being both misleading and unnecessarily prescriptive.

Rather than taking definitive judgments on the merits of different rights and interests, the Working Party insists on the *crucial role of the balancing test* in the assessment of Article 7(f). There is a need to keep the flexibility of the test, but the way it is carried out must be made more effective in practice and must allow for more effective compliance. This should translate into an *enhanced* obligation of *accountability* for data controllers, where the controller bears the responsibility to *demonstrate* that its interest is not overridden by the interests and rights of the data subject.

Guidance and accountability

To achieve this, the Working Party recommends that guidance be provided in the proposed Regulation, in the following way.

1) It would be helpful to identify and provide in a recital a non-exhaustive list of key factors to be considered when applying the balancing test, such as the nature and source of the legitimate interest, the impact on the data subjects, and the additional safeguards that may be applied by the controller to prevent any undue impact of the processing on the data subjects. These safeguards may include, among others,
   - functional separation of data, appropriate use of anonymisation techniques, encryption and other technical and organisational measures to limit the potential risks to the data subjects;
   - but also measures to ensure increased transparency and choice to data subjects, such as, where appropriate, the possibility for an unconditional opportunity to opt out of the processing, free of charge and in a manner that can be easily and effectively invoked.

2) The Working Party would also support further clarification in the proposed Regulation on how the controller could *demonstrate*[111] enhanced accountability.

   The change in the conditions for data subjects to exercise the right to object as foreseen in Article 19 of the proposed Regulation is already an important element of accountability. If the data subject objects to the processing of his/her data under Article 7(f), under the proposed Regulation it will be up to the data controller to demonstrate that his/her interest prevail. This reversal of the burden of proof is strongly supported by the Working Party as it contributes to an enhanced accountability obligation.

   If the data controller does not succeed in demonstrating to the data subject in a specific case that its interest prevails, this may also have broader consequences on the whole processing, not just with respect to the data subject who objected. As a result, the controller may put into question or decide to reorganise the processing, when appropriate for the benefit of not only the specific data subject but also for the benefit of all other data subjects who may be in a similar situation.[112]

[111] Such demonstration must remain reasonable and focus on outcome rather than administrative process.

[112] In addition to reversing the burden of proof, the Working Party also supports that the proposed Regulation would no longer require that an objection be made on '*compelling* legitimate grounds relating to [the] particular situation' [of the data subject]. Rather, pursuant to the proposed Regulation, reference to any (not necessarily

This requirement is necessary but not sufficient. To ensure protection from the start, and to avoid that the shifting of the burden of proof is circumvented[113], it is important that steps are taken *before* the processing starts, and not only in the course of ex-post 'objection' procedures.

It is therefore proposed that, in the first stage of any processing activity, the data controller shall take several steps. The two first steps could be listed in a recital of the proposed Regulation and the third one in a specific provision:

- Conduct an assessment[114], which should include the different stages of the analysis developed in this Opinion and summarised in Annex 1. The controller would have to identify explicitly the prevailing interest(s) at stake, and why they prevail over the interests of the data subjects. Such prior assessment should not be too burdensome, and remains *scalable*: it may be limited to essential criteria if the impact of the processing on the data subjects is *prima facie* insignificant, while on the other hand it should be performed more thoroughly if the balance was difficult to achieve and would require for instance adoption of several additional safeguards. Where appropriate - i.e. when a processing operation presents specific risks to the rights and freedoms of data subjects - a more comprehensive privacy and data protection impact assessment (according to Article 33 of the proposed Regulation) should be carried out, of which the assessment under Article 7(f) could become an important part.

- Document this assessment. Just as it is *scalable* in how much detail the assessment needs to be carried out, the extent of documentation should also be scalable. With that said, some basic documentation should be available in all but the most trivial cases, independently of the appreciation of the impact of the processing on the individual. It

---

'compelling') legitimate grounds relating to the particular situation of the data subject would be sufficient. Indeed, a further option, which was proposed in the Final LIBE Committee Report is to also do away with the requirement that the objection would have to relate to the particular situation of the data subject. The Working Party supports this approach in the sense that it recommends that data subjects would be able to take advantage of either or both opportunities, as appropriate, that is, either object based on their own particular situation, or with a more general scope, and in this latter case without being required to provide any specific justification. See in that sense amendment 114 to Article 19(1) of the proposed Regulation in the Final LIBE Committee Report.

[113] Data controllers, for example, may be tempted to avoid case-by-case demonstration that their interest prevails, by using standard justification forms, or may make the exercise of the right to object otherwise cumbersome.

[114] This assessment, as stated earlier in footnote 84, should not be confused with a comprehensive privacy and data protection impact assessment. At present, there is no comprehensive guidance on impact assessments at European level, although in some areas, namely for RFID and smart metering, a number of welcome efforts have been made to define a sector-specific methodology/framework (and/or template) that could apply across the European Union. See 'Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications' and 'Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems' prepared by Expert Group 2 of the Commission's Smart Grid Task Force. The Working Party issued repeated opinions with regard to both these methodologies.
In addition, there have been some initiatives to define a generic data protection impact assessment methodology, from which 'field specific' efforts could benefit. See, for example, PIAF Project (A Privacy Impact Assessment Framework for data protection and privacy rights): http://www.piafproject.eu/.
Further, for guidance at national level, see, for example, CNIL methodology:
http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf
and the ICO's Privacy Impact Assessment Handbook at
http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

is on the basis of such documentation that the assessment of the controller may be further evaluated and possibly contested;

- Give transparency and visibility to this information to the data subjects and other stakeholders. Transparency should be ensured both towards data subjects and data protection authorities, and when appropriate, the public at large. As to data subjects, the Working Party refers to the Draft LIBE Committee Report[115], which stated that the controller should inform the data subject about the reasons for believing that its interests are not overridden by the data subject's interests or fundamental rights and freedoms. Such information should in the view of the Working Party be provided to data subjects together with the information the controller has to provide under Article 10 and 11 of the present Directive (Article 11 of the proposed Regulation). This will allow possible objection by the data subject in a second phase, and additional justification on a case-by-case basis by the controller of the prevailing interests. In addition, upon request, the documentation upon which the controller based their assessment should be made available to data protection authorities, in order to allow for possible verification and enforcement where relevant.

The Working Party would support that these three steps are explicitly included in the proposed Regulation in ways as set out above. This would recognise the specific role of legal grounds in the assessment of legitimacy, and would clarify the importance of the balancing test within the wider context of accountability measures and impact assessments in the proposed new legal framework.

The Working Party considers it also advisable to entrust the EDPB with providing further guidance where necessary on the basis of this framework. This approach would allow both sufficient clarity in the text and sufficient flexibility in its implementation.

[115] Draft Report on the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

Annex 1. Quick guide on how to carry out the Article 7(f) balancing test

Step 1: Assessing which legal ground may potentially apply under Article 7(a)-(f)

Data processing can be implemented only if one or more of the six grounds - (a) through (f) - of Article 7 applies (different grounds can be relied on at different stages of the same processing activity). If it *prima facie* appears that Article 7(f) might be appropriate as a legal ground, proceed to step 2.

Quick tips:

- Article 7(a) applies only if free, informed, specific and unambiguous consent is given; the fact that an individual has not objected to a processing under Article 14 should not be confused with Article 7(a) consent - however, an easy mechanism to object to a processing may be considered as an important safeguard under Article 7(f);
- Article 7(b) covers processing that is necessary for the implementation of the contract; just because the data processing is related to the contract, or foreseen somewhere in the terms and conditions of the contract does not necessarily mean that this ground applies; where appropriate, consider Article 7(f) as an alternative;
- Article 7(c) addresses only clear and specific legal obligations under the laws of the EU or a Member State; in case of non-binding guidelines (for instance by regulatory agencies), or a foreign legal obligation, consider Article 7(f) as an alternative.

Step 2: Qualifying an interest as 'legitimate' or 'illegitimate'

To be considered as legitimate, an interest must cumulatively fulfil the following conditions:

- be lawful (i.e. in accordance with EU and national law);
- be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently concrete);
- represent a real and present interest (i.e. not be speculative).

Step 3: Determining whether the processing is necessary to achieve the interest pursued

To meet this requirement, consider whether there are other less invasive means to reach the identified purpose of the processing and serve the legitimate interest of the data controller.

Step 4: Establishing a provisional balance by assessing whether the data controller's interest is overridden by the fundamental rights or interests of the data subjects

- Consider the nature of the interests of the controller (fundamental right, other type of interest, public interest);
- Evaluate the possible prejudice suffered by the controller, by third parties or the broader community if the data processing does not take place;
- Take into account the nature of the data (sensitive in a strict or broader sense?);
- Consider the status of the data subject (minor, employee, etc.) and of the controller (e.g. whether a business organisation is in a dominant market position);
- Take into account the way data are processed (large scale, data mining, profiling, disclosure to a large number of people or publication);
- Identify the fundamental rights and/or interests of the data subject that could be impacted;

- Consider data subjects' reasonable expectations;
- Evaluate impacts on the data subject and compare with the benefit expected from the processing by the data controller.

Quick tip: Consider the effect of actual processing on particular individuals – do not see this as an abstract or hypothetical exercise.

Step 5: Establishing a final balance by taking into account additional safeguards

Identify and implement appropriate additional safeguards resulting from the duty of care and diligence such as:
- data minimisation (e.g. strict limitations on the collection of data, or immediate deletion of data after use)
- technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation')
- wide use of anonymisation techniques, aggregation of data, privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments;
- increased transparency, general and unconditional right to object (opt-out), data portability & related measures to empower data subjects.

Quick tip: Using privacy enhancing technologies and approaches can tip the balance in favour of the data controller and protect individuals too.

Step 6: Demonstrate compliance and ensure transparency

- Draw a blueprint of steps 1 to 5 to justify the processing before its launch.
- Inform data subjects of the reasons for believing the balance tips in the controller's favour.
- Keep documentation available to data protection authorities.

Quick tip: This step is *scalable*: details of assessment and documentation should be adapted to the nature and context of the processing. These measures will be more extensive where a large amount of information about many people is being processed, in a way that could have a significant impact on them. A comprehensive privacy and data protection impact assessment (under Article 33 of the proposed Regulation) will only be necessary when a processing operation presents specific risks to the rights and freedoms of data subjects. In these cases, the assessment under Article 7(f) could become a key part of this broader impact assessment.

Step 7: What if the data subject exercises his/her right to object?

- Where only a qualified right to opt-out is available as a safeguard (this is explicitly required under Article 14(a) as a minimum safeguard): in case the data subject objects to the processing, it should be ensured that an appropriate and user-friendly mechanism is in place to re-assess the balance as for the individual concerned and stop processing his/her data if the re-assessment shows that his/her interests prevail.
- Where an unconditional right to opt-out is provided as an additional safeguard (either because this is explicitly required under Article 14(b) or because this is otherwise deemed a necessary or helpful additional safeguard): in case the data subject objects to the processing, it should be ensured that this choice is respected, without the need to take any further step or assessment.

Annex 2. Practical examples to illustrate the application of the Article 7(f) balancing test

This Annex provides examples with regard to some of the most common contexts in which the issue of legitimate interest in the meaning of Article 7(f) may arise. In most cases, we grouped together two or more related examples that are worth comparing under a single heading. Many of the examples are based on actual cases, or elements of actual cases handled by data protection authorities in the different Member States. However, we have sometimes changed the facts to some degree to help better illustrate how to carry out the balancing test.

The examples are included in order to illustrate the *thinking process* - the method to be used to carry out the multi-factor balancing test. In other words, the examples are *not* meant to provide a *conclusive* assessment of the cases described. Indeed, in many cases, by changing the facts of the case in some way (for example, if the controller were to adopt additional safeguards such as more complete anonymisation, better security measures, and more transparency and more genuine choice for the data subjects), the outcome of the balancing test could change.[116]

This should encourage controllers to better comply with all horizontal provisions of the Directive and offer additional protection where relevant based on privacy and data protection by design. The greater care controllers take to protect personal data overall, the more likely it is that they will satisfy the balancing test.

Exercise of the right to freedom of expression or information[117], including in the media and the arts

Example 1: NGO republishes expenses of Members of Parliament

A public authority publishes - under a legal obligation (Article 7(c)) - expenses of members of parliament; a transparency NGO, in turn, analyses and re-publishes data in an accurate, proportionate, but more informative annotated version, contributing to further transparency and accountability.

Assuming the NGO carries out the re-publication and annotation in an accurate and proportionate manner, adopts appropriate safeguards, and more broadly, respects the rights of the individuals concerned, it should be able to rely on Article 7(f) as a legal ground for the processing. Factors such as the nature of the legitimate interest (a fundamental right to freedom of expression or information), the interest of the public in transparency and accountability, and the fact that the data have already been published and concern (relatively

[116] Applying correctly Article 7(f) may raise complex issues of assessment, and to help guide the assessment, specific legislation, case law, jurisprudence, guidelines, as well as codes of conduct and other formal or less formal standards may all play an important role.

[117] On freedom of expression or information, see page 34 of the Opinion. Any relevant derogations under national law for processing for journalistic purposes under Article 9 of the Directive must also be taken into account when assessing these examples.

less sensitive) personal data related to the activities of the individuals relevant to the exercise of their public functions[118], all weigh in favour of the legitimacy of the processing. The fact that the initial publication has been required by law, and that individuals should thus expect their data would be published, also contribute to the favourable assessment. On the other side of the balance, the impact on the individual may be significant, for example, because of public scrutiny, the personal integrity of some individuals may be questioned, and this may lead, for instance, to loss of elections, or in some cases to a criminal investigation for fraudulent activities. The factors above, taken together, however, show that on the balance, the controller's interests (and the interests of the public to whom the data are disclosed) override the interests of the data subjects.

Example 2: Local councillor appoints his daughter as special assistant

A journalist publishes a factually accurate, well-researched article in a local online newspaper about a local councillor revealing that he has only attended one of the last eleven council meetings and he is unlikely to be re-elected because of a recent scandal involving the appointment of his seventeen-year-old daughter as a special assistant.

A similar analysis as in *Example 1* also applies here. On the facts, it is in the legitimate interests of the newspaper in question to publish the information. Even though personal data has been revealed about the councillor, the fundamental right to freedom of expression and to publish the story in the newspaper is not overridden by the right to privacy of the councillor. This is because the privacy rights of public figures are relatively limited in respect of their public activities and because of the special importance of freedom of expression – especially where publication of a story is in the public interest.

Example 3: Top search results continue to show minor criminal offence

The on-line archive of a newspaper contains an old article concerning an individual, once a local celebrity, captain of a small town amateur football team. The individual is identified with his full name, and the story relates to his involvement in a relatively minor criminal proceeding (drunk and disorderly behaviour). The criminal records of the individual are now clean and no longer show the past offence for which he served his sentence several years ago. What is most disturbing for the individual is that by searching his name with common search engines online, the link to this old piece of news is among the first results concerning him. Notwithstanding his request, the newspaper refuses to adopt technical measures, which would restrict the broader availability of the piece of news related to the data subject. For example, the paper refuses to adopt technical and organisational measures that would aim - to the extent technology allows - limiting access to the information from external search engines using the individual's name as a search category.

This is another case to illustrate the possible conflict between freedom of expression and privacy. It also shows that in some cases additional safeguards - such as ensuring that, at least in case of a justified objection under Article 14(a) of the Directive, the relevant part of the

[118] It cannot be excluded that some expenses may reveal more sensitive data, such as health data. If this is the case, these should be edited out of the dataset before it is published in the first place. It is good practice to take a 'proactive approach' and give individuals an opportunity to review their data before their publication and to clearly inform them about the possibilities and modalities of publication.

newspaper archives will no longer be accessible by external search engines or the format used to display the information will not allow search by name - may play a key role in striking an appropriate balance between the two fundamental rights concerned. This is without prejudice to any other measures that might be taken by search engines or other third parties.[119]

Conventional direct marketing and other forms of marketing or advertisement

Example 4: Computer store advertises similar products to clients

A computer store obtains from its customers their contact details in the context of the sale of a product, and uses these contact details for marketing by regular mail of its own similar products. The shop also sells products on-line and sends out promotional emails when a new product line comes into stock. Customers are clearly informed about their opportunity to object, free of charge and in an easy manner when their contact details are collected, and each time a message is sent, in case the customer did not object initially.

The transparency of the processing, the fact that the customer can reasonably expect to receive offers for similar products as a client of the shop, and the fact that he/she has the right to object helps strengthen the legitimacy of the processing and safeguard individuals' rights. On the other side of the balance, there appears to be no disproportionate impact on the individual's right to privacy (in this example we assumed that there are no complex profiles created by the computer shop of its consumers, for example, using detailed analysis of click-stream data).

Example 5: On-line pharmacy performs extensive profiling

An online pharmacy carries out marketing based on the medicines and other products customers have purchased, including products obtained by prescription. It analyses this information – combined with demographic information about customers – for example, their age and gender – to build up a 'health and wellbeing' profile of individual customers. Click-stream data is also used, which is collected not only about the products the customers purchased but also about other products and information they were browsing on the website. The customer profiles include information or predictions suggesting that a particular customer is pregnant, suffering from a particular chronic illness, or would be interested in purchasing dietary supplements, suntan lotion or other skin-care products at certain times of the year. The online pharmacy's analysts use this information to offer non-prescription medicines, health supplements and other products to particular individuals by email. In this case the pharmacy cannot rely on its legitimate interests when creating and using its customer profiles for marketing. There are several problems posed by the profiling described. The information is particularly sensitive and can reveal a great deal about matters that many individuals would expect to remain private.[120] The extent and manner of profiling (use of click-stream data, predictive algorithms) also suggest a high level of intrusiveness. Consent based on Article 7(a) and Article 8(2)(a) (where sensitive data are involved) could, however, be considered as an alternative where appropriate.

[119] See also Case C-131/12 Google Spain v Agencia Española de Proteccion de Datos, currently before the Court of Justice of the European Union.

[120] Beyond any restrictions posed by data protection laws, advertisement of prescription products is also strictly regulated in the EU, and there are also some restrictions regarding advertisement on non-prescription drugs. Further, the requirements of Article 8 on special categories of data (such as health data) must also be considered.

Unsolicited non-commercial messages, including for political campaigns or charitable fundraising

Example 6: Candidate in local election makes targeted use of electoral register

A candidate in local election uses the electoral register[121] to send an introduction letter promoting her campaign for the upcoming elections to each potential voter in her election district. The candidate uses the data obtained from the electoral register only to send the letter and does not retain the data once the campaign has ended.

Such use of the local register is in the reasonable expectations of individuals, when it takes place in the pre-election period: the interest of the controller is clear and legitimate. The limited and focused use of the information also contributes to tip the balance in favour of the legitimate interest of the controller. Such use of electoral registers may also be regulated by law at national level, in a public interest perspective, providing for specific rules, limitations and safeguards with regard to the use of the electoral register. If this is the case, compliance with these specific rules is also required to ensure the legitimacy of the processing.

Example 7: Non-profit-seeking body collects information for targeting purposes

A philosophical organisation dedicated to human and social development decides to organise fundraising activities based on the profile of its members. To this end, it collects data on social networking sites by means of ad-hoc software targeting individuals who 'liked' the organisation's page, 'liked' or 'shared' the messages the organisation posted on its page, regularly viewed certain items or re-tweeted the organisation's messages. It then sends messages and newsletters to its members according to their profiles. For example, elderly dog owners who 'liked' articles on animal shelters receive different fundraising appeals from families with small children; people from different ethnic groups also receive different messages.

The fact that special categories of data are processed (philosophical beliefs) requires compliance with Article 8, a condition which seems to be met as the processing takes place in the course of the legitimate activities of the organisation. However, this is not a sufficient condition in this case: the way data are being used exceeds the reasonable expectations of individuals. The amount of data collected, the lack of transparency about the collection and the reuse of data initially published for one purpose for a different purpose contribute to the conclusion that Article 7 (f), cannot be relied on in this case. The processing should therefore not be allowed except if another ground can be used, for instance the consent of individuals under Article 7(a).

[121] It is assumed that in the Member State where the example applies an electoral register is established by law.

Enforcement of legal claims, including debt collection via out-of-court procedures

Example 8: Dispute on quality of renovation work

A customer disputes the quality of kitchen renovation work and refuses to pay the full price. The building company transfers the relevant and proportionate data to his lawyer in order that he could remind the customer of payment and negotiate a settlement with the customer if he continues to refuse to pay.

In this case, the preliminary steps taken by the building company using basic information of the data subject (e.g. name, address, contract reference) to send a reminder to the data subject (directly or via its lawyer as in this case) may still fall within the processing necessary for the performance of the contract (Article 7(b)). Further steps taken,[122] including the involvement of a debt collection agency, should however be assessed under Article 7(f) considering, among others, their intrusiveness and impact on the data subject as will be shown in the following example.

Example 9: Customer disappears with car purchased on credit

A customer fails to pay for the instalments that are due on an expensive sports car purchased on credit, and then 'disappears'. The car dealer contracts a third-party 'collection agent'. The collection agent carries out an intrusive 'law-enforcement style' investigation, using, among others, practices such as covert video-surveillance and wire-tapping.

Although the interests of the car dealer and the collection agent are legitimate, the balance does not tip in their favour because of the intrusive methods used to collect information, some of which are explicitly prohibited by law (wire-tapping). The conclusion would be different if, for instance, the car dealer or the collection agent only carried out limited checks to confirm the contact details of the data subject in order to start a court procedure.

Prevention of fraud, misuse of services, or money laundering

Example 10: Verification of clients' data before opening of a bank account

A financial institution follows reasonable and proportionate procedures - as per non-binding guidelines of competent government financial supervisory authority - to verify the identity of any person seeking to open an account. It maintains records of the information used to verify the person's identity.

The interest of the controller is legitimate, the processing of data involves only limited and necessary information (standard practice in the industry, to be reasonably expected by data subjects, and recommended by competent authorities). Appropriate safeguards are in place to limit any disproportionate and undue impact on the data subjects. The controller can therefore rely on Article 7(f). Alternatively, and to the extent that the actions taken are specifically required by applicable law, Article 7(c) could apply.

[122] There is currently, among the different Member States, a degree of variance as to which measures may be considered necessary for the performance of a contract.

Example 11: Exchange of information to fight money laundering

A financial institution - after obtaining advice of the competent data protection authority – implements procedures based on specific and limited criteria to exchange data regarding suspected abuse of anti-money laundering rules with other companies within the same group, with strict limitation on access, security, and prohibition of any further use for other purposes.

For reasons similar to those explained above, and depending on the facts of the case, the processing of data could be based on Article 7(f). Alternatively, and to the extent that the actions taken are specifically required by applicable law, Article 7(c) could apply.

Example 12: Black list of aggressive drug-addicts

A group of hospitals create a joint black list of 'aggressive' individuals in search of drugs, with the aim of prohibiting them access to all medical premises of the participating hospitals.

Even if the interest of the controllers in maintaining safe and secure premises is legitimate, it has to be balanced against the fundamental right of privacy and other compelling concerns such as the need not to exclude the individuals concerned from access to health treatment. The fact that sensitive data are processed (e.g. health data related to drug addiction) also supports the conclusion that in this case the processing is unlikely to be acceptable under Article 7(f).[123] The processing might be acceptable if it were to be for instance regulated in a law providing for specific safeguards (checks and controls, transparency, prevention of automated decisions) ensuring that it would not result in discrimination or violation of fundamental rights of individuals[124]. In this latter case, depending on whether this specific law requires or only permits the processing, either Article 7(c) or Article 7(f) may be relied on as a legal ground.

Employee monitoring for safety or management purposes

Example 13: Working hours of lawyers used both for billing and bonus purposes

The number of billable hours worked by lawyers at a law firm is processed both for billing purposes and for determination of annual bonuses. The system is transparently explained to employees who have an explicit right to express disagreement with the conclusions in terms of both billing and bonus payment, to be then discussed with their management.

The processing appears necessary for the legitimate interests of the controller, and there does not appear to be a less intrusive way to achieve the purpose. The impact on employees is also limited due to the safeguards and processes put in place. Article 7(f) could therefore be an appropriate legal ground in this case. There may also be an argument to support that processing for one or both purposes is also necessary for the performance of the contract.

[123] The requirements of Article 8 on special categories of data (such as health data) must also be considered.

[124] See the Working document on Black Lists (WP 65) adopted on 3 October 2002.

Example 14: Electronic monitoring of internet use[125]

The employer monitors internet use during working hours by employees to check they are not making excessive personal use of the company's IT. The data collected include temporary files and cookies generated on the employees' computers, showing websites visited and downloads performed during working hours. The data is processed without prior consultation of data subjects and the trade union representatives/work council in the company. There is also insufficient information provided to the individuals concerned about these practices.

The amount and nature of the data collected represents a significant intrusion into the private life of the employees. In addition to proportionality issues, transparency about the practices, closely linked to the reasonable expectations of the data subjects, is also an important factor to be considered. Even if the employer has a legitimate interest in limiting the time spent by the employees visiting websites not directly relevant to their work, the methods used do not meet the balancing test of Article 7(f). The employer should use less intrusive methods (e.g. limiting accessibility of certain sites), which are, as best practice, discussed and agreed with employees' representatives, and communicated to the employees in a transparent way.

Whistle-blowing schemes

Example 15: Whistleblowing scheme to comply with foreign legal obligations

An EU branch of a US group establishes a limited whistle-blowing scheme to report serious infringements in the field of accounts and finance. The entities of the group are subjected to a code of good governance that calls for strengthening procedures for internal control and risk management. Because of its international activities, the EU branch is required to supply reliable financial data to other members of the group in the US. The scheme is designed to be compliant with both US law and the guidelines provided by the national data protection authorities in the EU.

Among the safeguards, employees are given clear guidance as to the circumstances in which the scheme should be used, through training sessions and other means. Staff are warned not to abuse the scheme – for example by making false or unfounded allegations against other members of staff. It is also explained to them that if they prefer they can use the scheme anonymously or if they wish they can identify themselves. In the latter case, employees are informed of the circumstances in which information identifying them will be fed back to their employer or passed-on to other agencies.

If the scheme were required to be established under EU law or under the law of an EU Member State, the processing could be based on Article 7(c). However, foreign legal obligations do not qualify as a legal obligation for purposes of Article 7(c), and therefore, such an obligation could not legitimise the processing under Article 7(c). However, the processing could be based on Article 7(f), for example, if there is a legitimate interest in guaranteeing the stability of financial markets, or the fight against corruption, and provided

[125] A few Member States consider that some limited electronic monitoring may be 'necessary for the performance of a contract', and therefore, may be based on the legal ground of Article 7(b) rather than 7(f).

that the scheme includes sufficient safeguards, in accordance with guidance from the relevant regulatory authorities in the EU.

Example 16: 'In-house' whistle-blowing scheme without consistent procedures

A financial services company decides to set up a whistle-blowing scheme because it suspects widespread theft and corruption amongst its staff and is keen to encourage employees to inform on each other. In order to save money, the company decides to operate the scheme in-house, staffed by members of its Human Resources department. In order to encourage employees to use the scheme it offers a cash 'no questions asked' reward to employees whose whistle-blowing activities lead to the detection of improper conduct and the recovery of monies.

The company does have a legitimate interest in detecting and preventing theft and corruption. However, its whistle-blowing scheme is so badly designed and lacking in safeguards that its interests are overridden by both the interests and right to privacy of its employees – particular those who may be the victim of false reports filed purely for financial gain. The fact that the scheme is operated in-house rather than independently is another problem here, as is the lack of training and guidance on the use of the scheme.

Physical security, IT and network security

Example 17: Biometric controls in a research laboratory

A scientific research laboratory working with lethal viruses uses a biometric entrance system due to the high risk to public health in case these viruses were to escape the premises. Appropriate safeguards are applied, including the fact that biometric data are stored on personal employee cards and not in a centralised system.

Even if data are sensitive in the broad sense, the reason for their processing is in the public interest. This and the fact that risks of misuse are reduced by appropriate use of safeguards make Article 7(f) an appropriate basis for the processing.

Example 18: Hidden cameras to identify smoking visitors and employees

A company makes use of hidden cameras to identify employees and visitors who smoke in unauthorised areas of the building.

While the controller has a legitimate interest to ensure compliance with non-smoking rules, the means used to reach this end are - generally speaking - disproportionate and unnecessarily intrusive. There are less intrusive and more transparent methods (such as smoke detectors and visible signs) available. The processing thus fails to comply with Article 6, which requires data to be 'not excessive' in relation to the purposes for which they are collected or further processed. At the same time, it will probably fail to meet the balancing test of Article 7.

Scientific research

Example 19: Research on effects of divorce and parental unemployment on children's education attainment

Under a research programme adopted by the government, and authorised by a competent ethics committee, research is performed into the relationship between divorce, parental unemployment and children's educational attainment. While not classified as 'special categories of data', the research is nevertheless focusing on issues that for many families, would be considered very intimate personal information. The research will allow special educational assistance to be targeted at children who may otherwise fall into absenteeism, poor educational attainment, adult unemployment and criminality. The law of the Member State concerned explicitly allows processing of personal data (other than special categories of data) for research purposes, provided the research is necessary for important public interests, and carried out subject to adequate safeguards, which are then further detailed in implementing legislation. This legal framework includes specific requirements but also an accountability framework that allows for assessment on a case-by-case basis of the permissibility of the research (if carried out without the consent of the individuals concerned) and the specific measures to be applied to protect the data subjects.

The researcher runs a secure research facility and, under secure conditions, the relevant information is provided to it by the population registry, courts, unemployment agencies, and schools. The research centre then 'hashes' individuals' identities so that divorce, unemployment and education records can be linked, but without revealing individuals' 'civic' identities – e.g. their names and addresses. All the original data is then irretrievably deleted. Further measures are also taken to ensure functional separation (i.e. that data will only be used for research purposes) and reduce any further risk of re-identification.

Staff members working at the research centre receive rigorous security training and are personally - possibly even criminally - liable for any security breach they are responsible for. Technical and organisational measures are taken, for example, to ensure that staff using USB sticks could not remove personal data from the facility.

It is in the legitimate interests of the research centre to carry out the research, in which there is a strong public interest. It is also in the legitimate interests of the employment, educational and other bodies involved in the scheme, because it will help them to plan and deliver services to those that most need them. The privacy aspects of the scheme have been well designed and the safeguards that are in place mean that the legitimate interests of the organisations involved in carrying out the research are not overridden by either the interests or privacy rights of the parents or children whose records formed the basis of the research.

Example 20: Research study on obesity

A university wants to carry out research into levels of childhood obesity in several cities and rural communities. Despite generally having difficulties gaining access to the relevant data from schools and other institutions, it does manage to persuade a few dozens of school teachers to monitor for a period of time children in their classes who appear obese and to ask them questions about their diet, levels of physical activity, computer-game use and so forth. These school teachers also record the names and addresses of the children interviewed so that an online music voucher can be sent to them as a reward for taking part in the research. The

researchers then compile a database of children, correlating levels of obesity with physical activity and other factors. The paper copies of the completed interview questionnaires – still in a form that identifies particular children – are kept in the university archives for an indefinite period of time and without adequate security measures. Photocopies of all questionnaires are shared on request with any MD or PhD student of the same and of partner universities across the world who show interest in further use of the research data.

Although it is in the legitimate interests of the university to carry out research, there are several aspects of the research design that mean these interests are overridden by the interests and rights to privacy of the children. Besides the research methodology, which is lacking in scientific rigour, the problem emanates in particular from the lack of privacy enhancing approaches in the research design and the broad access to the personal data collected. At no point are children's records coded or anonymised and no other measures are taken to ensure either security of the data or functional separation. Valid Article 7(a) and Article 8(2)(a) consent is not obtained, either, and it is not clear that it has been explained to either the children or their parents what their personal data will be used for or with whom it will be shared.

Foreign legal obligation

Example 21: Compliance with third country tax law requirements

EU banks collect and transfer some of their clients' data for purposes of their clients' compliance with third country taxation obligations. The collection and transfer is specified in and takes place under conditions and safeguards agreed between the EU and the foreign country in an international agreement.

While a foreign obligation in itself cannot be considered a legitimate basis for processing under Article 7(c), it may well be if such obligation is upheld in an international agreement. In this latter case, the processing could be considered necessary for complying with a legal obligation incorporated into the internal legal framework by the international agreement. However, if there is no such agreement in place, the collection and transfer will have to be assessed under Article 7(f) requirements, and may only be considered permissible provided that adequate safeguards are put in place such as those approved by the competent data protection authority (see also *Example 15* above).

Example 22: Transfer of data on dissidents

Upon request, an EU company transfers data of foreign residents to an oppressive regime in a third country that wishes to access data of dissidents (e.g. their email traffic data, email content, browsing history, or private messages in social networks).

In this case, unlike in the previous example, there is no international agreement that would allow for applying Article 7(c) as a legal ground. Besides, several elements argue against Article 7(f) as an appropriate ground for processing. Although the controller may have an economic interest in ensuring that it complies with foreign government requests (otherwise it might suffer less favourable treatment by the third country government compared to other companies), the legitimacy and proportionality of the transfer is highly questionable under the EU fundamental rights framework. Its potentially huge impact on the individuals concerned

(e.g. discrimination, imprisonment, death penalty) also greatly argue in favour of the interests and rights of the individuals concerned.

Reuse of publicly available data

Example 23: Rating of politicians[126]

A transparency NGO uses publicly available data on politicians (promises made at the time of their election and actual voting records) to rate them based on how well they kept their promises.

Even if the impact on politicians concerned may be significant, the fact that processing is based on public information and in relation to their public responsibilities makes, with a clear purpose of enhancing transparency and accountability, the balance tips in the interest of the controller[127].

Children and other vulnerable persons

Example 24: Information website for teenagers

An NGO website offering advice to teenagers regarding issues such as drug abuse, unwanted pregnancy and alcohol abuse collects data via its own server about visitors to the site. It then immediately anonymises these data and turns them into general statistics about which parts of the website are most popular among visitors coming from different geographical regions of the country.

Article 7(f) could be used as a legal ground even if data concerning vulnerable individuals are concerned, because the processing is in the public interest and strict safeguards are put in place (the data are immediately rendered anonymous and only used for the creation of statistics), which helps tipping the balance in favour of the controller.

Privacy by design solutions as additional safeguards

Example 25: Access to mobile phone numbers of users and non-users of an app: 'compare and forget'

Personal data of individuals are processed to check whether they had already granted unambiguous consent in the past (i.e., 'compare and forget' as a safeguard).

An application developer is required to have the data subjects' unambiguous consent for processing their personal data: for example, the app developer wishes to access and collect the entire electronic address book of users of the app, including the mobile phone numbers of contacts that are not using the app. To be able to do this, it may first have to assess whether

[126] See and compare also with Example 7 above.

[127] As in *Examples 1 and 2*, we assumed that the publication is accurate and proportionate - lack of safeguards and other factors may change the balance of interests depending on the facts of the case.

the holders of the mobile phone numbers in the address books of users of the app have granted their unambiguous consent (under Article 7(a)) for their data to be processed.

For this limited initial processing (i.e., short-term read access to the full address book of a user of the app), the app developer may rely on Article 7(f) as a legal ground, subject to safeguards. These safeguards should include technical and organisational measures to ensure that the company only uses this access to help the user identify which of his contact persons are already users, and which therefore had already granted unambiguous consent in the past to the company to collect and process phone numbers for this purpose. The mobile phone numbers of non-users may only be collected and used for the strictly limited objective of verifying whether they have granted their unambiguous consent for their data to be processed, and they should be immediately deleted thereafter.

Combination of personal information across web services

Example 26: Combination of personal information across web services

An internet company providing various services including search engine, video sharing, social networking, develops a privacy policy which contains a clause that enables it 'to combine all personal information' collected on each of its users in relation to the different services they use, without defining any data retention period. According to the company, this is done in order to 'guarantee the best possible quality of service'.

The company makes some tools available to different categories of users so that they can exercise their rights (e.g. deactivate targeted advertisement, oppose to the setting of a specific type of cookies).

However, the tools available do not allow users to effectively control the processing of their data: users cannot control the specific combinations of their data across services and users cannot object to the combination of data about them. Overall, there is an imbalance between the company's legitimate interest and the protection of users' fundamental rights and Article 7(f) should not be relied on as a legal ground for processing. Article 7(a) would be a more appropriate ground to be used, provided that the conditions for a valid consent are met.