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

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.

PAGES 7-15 OMMITTED

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.

PAGES 30-54 OMMITTED

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.