Article 29 Working Party
Overview of results of public consultation on Opinion on legitimate interests of the data controller (Opinion 06/2014)

14 November 2014

1. Background and introduction

The Article 29 Data Protection Working Party launched a public consultation following the adoption on 9 April 2014 of Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7(f) of Directive 95/46/EC. The deadline for comments was extended until 27 June 2014.

The Working Party received 16 replies, from 6 EU-wide business and industry associations and 5 national associations (UK, Germany) representing the e-commerce, advertising & marketing, insurance, media and newspapers, as well as research sectors; 2 US organisations representing global businesses; and 3 companies active in the field of credit rating, energy savings, and IT security:

- The Industry Coalition for Data Protection, a coalition of 16 EU level associations covering all areas of the digital economy
- EMOTA, the European Multi-channel and Online Trade Association
- FEDMA, the Federation of European Direct and Interactive Marketing
- EMMA, the European Magazine Media Association, and ENPA, the European Newspaper Publishers' Association
- EFAMRO, the European Research Federation
- Insurance Europe
- The Information Accountability Foundation
- The Centre for Information Policy Leadership
- The UK Advertising Association
- The Association of British Insurers
- The Institute of Practitioners in Advertising (IPA), UK
- The German Insurance Association (GDV)
- The German Magazine Publishers Associations (VDZ) and the Federation of German Newspaper Publishers (BDZV)
- Experian
- Opower (web-based software provider in the field of energy)
- Symantec

The Working Party published all replies on its website. This document provides an overview of the most relevant comments received, as well as a concise response,

addressing comments on the general approach taken in the Opinion, but also more specific comments including on some of the examples relating to research, direct marketing and processing for journalistic purposes.

At this stage, the Working Party does not think it is necessary to revisit the text of the adopted Opinion itself. The Working Party and its members, however, will endeavour to consider the issues raised in the comments when implementing the guidance provided in the Opinion and may also consider providing further guidance on selected topics in due course as appropriate. More generally, the Working Party will continue to consider seeking input from relevant stakeholders and the public at large in its future work, as appropriate.

2. General overview and key points of endorsement

Most stakeholders welcomed the general approach and main lines of the Opinion, as well as the fact that a consultation took place. In particular, the replies indicate the following key points of endorsement:

- Stakeholders welcome the public consultation and would like this practice to be continued for other opinions. They would, more broadly, also welcome other forms of dialogue with stakeholders.
- Stakeholders also welcome the efforts aiming at ensuring a harmonised interpretation and application of Article 7 of Directive 95/46/EC.
- Stakeholders welcome the recognition that the legitimate interest is an important legal ground for processing personal information, which is of equal importance to the other grounds mentioned in Article 7.
- Stakeholders agree that an exhaustive list of legitimate interests is an impractical solution, but that an explanation how to apply the Article 7(f) balancing test in different contexts is useful. Sufficient flexibility and a case by case approach are essential elements of the legitimate interests ground to be applied properly.
- Stakeholders recognise that accountability is a critical element to the balancing process, in terms of facilitating that the balancing test be appropriately carried out to assess whether Article 7(f) may be relied on as the legal ground for processing in particular cases.
- Stakeholders recognise that the scalability of documentation requirements is essential. Documentation requirements should not result in or create unnecessary legal and bureaucratic burdens.

3. Specific comments

Stakeholders also raised a number of more specific comments. The Working Party selected some of the comments it considers as most relevant, often those showing concerns shared by a number of organisations which responded to the consultation. Each of these key comments will be set out briefly below, along with a brief reaction by the Working Party.

3.1. Should the balancing test, in general, weigh in favour of the data subject or the controller?

Stakeholder comment

- The balancing test must reflect a genuine balance and should not be weighed in favour of the data subject to the detriment of the controller.

- In particular, the scope of considerations on behalf of the data subject should not be broadened by including all 'interests' of the data subject (including when the data subject engages in illegal activities) while at the same time narrowing the scope of considerations on behalf of the controller to 'compelling' legitimate interests.

Working Party response

- The Working Party fully agrees that the balancing test must be a genuine one and should not be presumed to be weighed in favour of either the data subject or the data controller. Indeed, it is only on a case by case basis that an assessment can be made of whether the legitimate interests of the controller are 'overridden' by the interests of the data subject. The interests of the data controller and the data subject must both be genuinely taken into account in a fair and reasonable way, with no partiality to 'either side'.
- The Working Party has only highlighted the full scope of the balancing test and not broadened or narrowed any part of it. More specifically, it did not suggest that the interest of the controller must always be 'compelling'. Indeed, there may be situations where both the interests of the data controller and those of the data subject are fairly inconsequential, and the balance nevertheless is struck in favour of the controller (e.g. sending a pizza coupon via direct postal marketing to existing customers, subject to Article 14(b) right to object. See Scenario 1 on page 31 of the Opinion).
- The Working Party further acknowledges that there may be strong cases for a data controller to claim that its legitimate interest overrides the interests of data subjects whom it suspects are engaged in illegal or criminal activities (e.g. insurance fraud, hacking into IT systems). However, even individuals who are found guilty of illegal or criminal activities are entitled to protection, especially with regard to their privacy and other fundamental rights and should not be subjected to disproportionate interference with their rights.[1] Further, in these situations, the data processed may not only concern those individuals who actually commit illegal or criminal activities, but also many other parties who may not have done anything wrong at all. Hence the Working Party emphasises that in these situations also, the controller has to make a careful analysis taking into account all relevant factors under the balancing test. In fact, in these situations, where the stakes are high, the proportionality of the measures, as well as the safeguards offered by the data controllers continue to play a crucial role.

3.2. How comprehensive should the balancing test be?

Stakeholder comment

- A balancing process that is relatively simple but has integrity, should normally be the regulatory goal.
- Data protection authorities should assess the legitimacy of relying on Article 7(f) as the legal basis for carrying out the processing in light of the facts known at the time, and not require data controllers to take an over-elaborate approach.
- Analysis needs to involve a 'family of processing', not each individual processing activity on too granular a basis. Balancing can be applied to programmes, not individual processes. (For example, an organisation could describe the balancing

[1] The Working Party also notes that lawful processing of criminal data also require the fulfilment of all other requirements of data protection law beyond satisfaction of the balancing test based on Article 7(f), including, in particular, the requirements of Article 8(5), as implemented into national law.

process for all of its fraud-protection measures as a whole, rather than for each individual activity.)

Working Party response

- The Working Party agrees that accountability, including appropriate procedures to carry out the balancing test, is a critical element if the data controller is to demonstrate that Article 7(f) can be relied on. The more a data controller is able to demonstrate that it has put in place appropriate measures to ensure compliance, the more likely that the data protection authorities will view the assessment favourably.
- The Working Party also agrees that any review should not be speculative, but should assess risks in light of the known facts (or foreseeable ones) at the time. However, trends that can be foreseen - for example, advances in analytics and big data or increased risk of re-identification of data subjects - must be taken into account. Any procedural framework for accountability must be designed in such a way that the controller should be able to update the data protection safeguards in light of new circumstances, whenever this is necessary – 're-adjusting' the balancing test when necessary and perhaps coming to a different conclusion. In some cases, for example, in the case of making anonymised data publicly available, or sharing pseudonymised data with a large number of partners, particular attention should be paid to the potential harm to data subjects resulting from the fact that data that was thought to be non-identifiable later turns out to be re-identifiable.
- As regards the level of detail: we cannot rule out the fact that in some cases analysis may be performed for a 'family of processing', for example, in routine cases that are standard industry practice and where there is detailed guidance already set forth in codes of conducts or guidelines by data protection authorities. However, in other situations - for example, where a complex and novel algorithm is used to build a comprehensive profile of data subjects - there may be a need for more detailed and more specific analysis. In any event, there must be sufficient detail to allow data controllers to carry out the balancing test and for data protection authorities to verify this if necessary, in particular allowing assessment of whether the proposed measures are adequate to protect the interests of the data subjects in light of the specific circumstances of the data processing involved.
- Indeed, if the assessment is not carried out in sufficient detail, a high-risk processing (e.g. a processing that is more intrusive and/or may have more significant consequences for the individuals concerned) might be 'concealed' or not sufficiently assessed within a relatively low-risk 'family' of processing, and this in turn may lead to a partial or inadequate application of the balancing test in Article 7(f). To illustrate, a specific fraud-prevention measure that may lead to the controller excluding customers from using a service for a period of time (e.g. a number of years) needs to be evaluated on its own merits and should not be simply lumped together, and implicitly authorised, along with another fraud prevention measure that may involve different, and perhaps less invasive processing activities, and/or may result in different, and perhaps less severe, consequences, for example, may only lead to demanding payment in advance from certain customers.
- In the end, it is the results that count and internal procedures should be designed in such a way so as to deliver results, and continue to do so in the face of continuously changing circumstances.

3.3. How should transparency be best achieved?

Stakeholder comment

- Transparency needs to be effective and workable.
- Mandatory or proactive publication of assessments by controllers may create a disincentive to rely on this legal basis because of the number and volume of such publications.
- An alternative approach might be to recommend that data controllers, whether in their privacy policy or otherwise, publish general criteria that they apply when relying on the legitimate interests ground for processing.

Working Party response

- The Working Party agrees that transparency needs to be effective and workable and that the obligations on the controller should not be unduly burdensome.
- However, if insufficient information is provided or '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 ... will ... not fulfil the requirements of .... Article 7(f) in terms of reasonable expectations of the data subject and an overall acceptable balance of interests' (see page 44 of the Opinion). This illustrates the connection between Article 10 (information to be given to the data subject) and Article 7.
- Indeed, as emphasised by the Working Party on numerous occasions, there are many innovative ways to provide effective notice to data subjects, in a user-friendly way, often in a layered manner that is manageable to comprehend by the data subjects and at the same time feasible to provide for the data controllers. The amount of information that needs to be provided to data subjects depends on the circumstances of the case, but in any event, must be sufficient to allow a reasonable person in place of the data subject to be fully empowered to make a decision whether or not to object to the processing under Article 14(a) where that right applies.

3.4. When should an unconditional opt-out be provided?

Stakeholder comment

- Some commentators assert that unconditional opt-out is not always feasible (e.g. as regards fraud prevention and detection by insurers or credit rating agencies, or processing for purposes of IT security).
- There has also been some criticism of 'blurring' the line between opt-out and Article 7(a) consent.

Working Party response

- The Working Party agrees that an unconditional opt-out, while it may work very well in certain situations (e.g. some direct marketing not requiring Article 7(a) consent), may not work in other situations, for example, in some cases of fraud prevention where – in reality – legitimate processing would be prevented if it had to be carried out either on the basis of consent or subject to such an opt-out.
- Providing data subjects with unconditional opt-out is thus not a panacea for all situations. Rather, it is a tool that may be helpful to strike the right balance in certain situations. It may enable controllers to carry on their business in a way that is not objectionable to the vast majority of data subjects, while at the same time, it caters for the needs of those who prefer to keep their information more private, or who may be more risk-averse when it comes to allowing access to their personal data.
- It is important to recognise the difference between the legal grounds of Article

7(f) – legitimate interests – and Article 7(a) – consent. The Working Party's intention is certainly not to 'blur' the lines between Article 7(a) consent and opt-out under Article 7(f), but rather to provide a compromise solution, for cases where reliance on Article 7(a) may be too burdensome for data controllers or otherwise not appropriate for a public policy purpose, while recognising that at the same time, the right to object under Article 14(a), which is still subject to many conditions, may not always prove fully sufficient to protect the rights of data subjects.

- A similar solution based on the data subject's unconditional right to object to processing free of charge, already exists for traditional direct marketing under Article 14(b). The Working Party suggests that there may be other situations where – as a matter of good practice – the provision of an unconditional and easy way to exercise the right to opt-out would help strike the right balance between the interests of data subjects and data controllers.

3.5. Can direct marketing be based on Article 7(f) or should it always be based on consent?

Stakeholder comment

- It is claimed that some of the examples in relation to direct marketing activities (in particular scenario 2 of the example on page 32 of the Opinion) and the conclusions on p. 45-47 are unbalanced. It is also suggested that these examples seem to put forward a view that online advertising and marketing cannot be carried out under the legitimate ground for processing personal information, which should not be the case.

Working Party response

- The intention of the Working Party with the three 'pizza examples' in scenarios 1, 2 and 3 was to provide introductory illustrations of the wide spectrum of facts and circumstances that may need to be taken into account when carrying out the Article 7(f) balancing test. These scenarios provide some 'good' and some 'bad' examples; these examples are what they are: just illustrations. The examples are not intended to claim that advertising and marketing (whether online or off-line) can never be carried out under Article 7(f). Indeed, scenario 1 shows that it can, at least in some situations. The examples were also meant to illustrate that it is too simplistic to say that Article 7(f) can or cannot be relied on to legitimise processing – it depends on the circumstances, including the type of marketing being carried out and its effect on the data subjects. [2]

[2] As explained in the Opinion - see in particular, pages 45-47: *Illustration: the evolution in the approach to direct marketing* - for a number of specific situations, the legislators have provided for the requirement for consent (with specific exceptions to allow a certain degree of flexibility). In other situations, in the absence of legislative guidance, a case by case analysis is necessary to assess whether Article 7(f) - often combined with some form of a right to object or opt-out as a safeguard - is appropriate to be relied on, or whether an Article 7(a) consent is required to make the processing legitimate.

3.6. Concerns relating to advanced analytics and profiling: should the preliminary research phase be treated differently from subsequent application of the research?

Stakeholder comment

- Some call for a two-phased approach that separates the research that may lead to new insights and the application of those insights, whereby it may be appropriate for the discovery phase to be conducted under the legitimate interest legal basis, while the application of any results may require a different legal basis.
- They urge the Working Party to consider whether the potential benefits of discovering new insights by using advanced analytic processes against large data sets can be addressed as part of the legitimate interest discussion and whether analytics can be given more neutral treatment.
- They argue that protection of a data subjects' rights in big data situations can be maintained using principles of accountability.

Working Party response

- In principle, it is helpful to analyse, distinguish, and fully cover both scenarios when assessing to what extent and subject to what safeguards processing may come under Article 7(f). However, this should not provide a blanket authorisation under Article 7(f) for all research activities that may lead to new insights. This will be subject to the same rigorous assessment on a case by case basis under the Article 7(f) balancing test as all other processing.
- The Working Party also notes that if the activity involves further use of existing personal data for a different purpose, it should also be assessed whether the further use is compatible. For more explanation of this please refer to the Working Party's Opinion on purpose limitation (Opinion 3/2013), especially Section III.2.3 on 'Further processing for historical, statistical or scientific purposes'. Safeguards, especially those ensuring functional separation, when appropriate, may also play an important role here, but may not always be feasible. The Working Party recognises that the early and thorough deployment of privacy-enhancing techniques can reduce the risk of individuals' rights being unduly interfered with and therefore, in general, it makes it more likely that data controllers can rely on Article 7(f) subsequently.

3.7. When can research be based on Article 7(f) and when should it require consent?

Stakeholder comment

- In example 19, researchers and their clients most likely would be able to rely on Article 7(f) in the preparatory or design phase of a research project before data collection by interview takes place.
- Example 20 on research on p. 65-66 should be withdrawn as the processing would require the consent of the data subjects under Articles 7(a) and 8(2)(a). Failure to clearly establish the informed consent of the participants in the study would be in clear breach of the established self-regulatory rules of the research sector. The situation described under example 20 would be considered to be unethical by professional researchers.

Working Party response

- The intention of the Working Party was to show that in some cases, and subject to a number of safeguards, such as those described in example 19, it is possible to rely on Article 7(f) for all or part of a research project**. T**he Working Party recognises though that there are different forms of research – posing different privacy risks – and acknowledges the importance of consent in some scenarios. It

also notes that beyond the requirement of 'consent' as a matter of data protection law, consent may also be required as a matter of other laws, regulations, and codes of conduct governing the research process more broadly, as is often the case, for example in medical research. In many situations, such as in medical research, consent may be crucial in terms of empowering individuals in respect of more sensitive personal information, furthering transparency and developing engagement between researchers and data subjects.

- Example 20 describes a situation illustrating what can go wrong in a research project. Apart from many other design flaws in the research, the example is also meant to illustrate that in this specific situation, consent would have been required, and the legitimate interest ground would have been inappropriate. (In addition to obtaining valid consent, all the other compliance problems would have had to be sorted out.)

3.8. When does a regulatory requirement/guidance constitute a legal obligation under Article 7(c) and when should the controller rely on Article 7(f) instead as a legal ground?

Stakeholder comment

- The Opinion should recognise that regulatory obligations can also be (legally) mandatory. For example, if the relevant supervisory authority in a Member State issues a regulatory requirement, insurers have to abide by it.

Working Party response

- This issue is addressed in Section III.2.3 of the Opinion, when discussing Article 7(c). In broad policy terms, the Working Party recognises that compliance with relevant regulatory obligations is – in a regulated sector, in general – in a data controller's legitimate interest. This could include compliance with 'softer' forms of regulation such as industry codes of practice or authoritative regulatory recommendation. However, whether Article 7(c) or 7(f) applies, in essence depends on the facts of the case.
- The Opinion explains on page 20 that '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 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 '

3.9. How broad is the Article 9 exception for journalistic purposes?

Stakeholder comment

- Some commentators suggest that in examples 2 and 3 on p. 58-59, Article 7(f) should not be applied to processing for journalistic purposes, as such processing benefits from an exemption under Article 9.
- They further suggest that the application of Article 7(f) to journalistic data processing, as outlined in Opinion 06/2014, implies a very problematic threat to press freedom by demanding data protection control over press and other media.

Working Party response

- It should be emphasised that Article 9 does not provide a blanket exemption for journalistic activities from any and all data protection requirements. It merely allows Member States to put in place exemptions or derogations from certain parts of the Directive.
- As pointed out in footnote 80 on page 35 of the Opinion, Article 9 of the Directive (under the title *Processing of personal data and freedom of expression*) allows (but does not require) 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'.
- Member States have significant discretion with regard to the exemptions and derogations they wish to provide for journalistic activities. For example, they may, if they so wish, entrust the supervision of compliance of the press with data protection requirements to an independent supervisory body other than the national data protection authority, or provide specific rules regarding the accuracy of personal data reported in news coverage. However, these exceptions and derogations must be 'necessary' and not go beyond their intended objective: to reconcile the right to privacy with the rules governing freedom of expression.
- In any event, these exemptions and derogations must also be set forth in binding national law, which, in turn, should strike the appropriate balance between privacy and the rules governing freedom of expression. It was beyond the scope of the Working Party's Opinion to provide an authoritative exposition of the functioning of Member States' national laws relating to journalistic purposes, and their interaction with Article 7(f) and other provisions of the Directive.
- Rather than being inappropriate, a balancing test under Article 7(f) (or a similar balancing test under national law in case of a derogation), lies at the heart of reconciling two great fundamental freedoms, the right to privacy and the right to freedom of expression. Neither has primacy over the other, and reconciling them often requires a careful and nuanced analysis.