

00569/13/EN
WP 203

Opinion 03/2013 on purpose limitation

Adopted on 2 April 2013

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

Table of contents

Executive Summary 3
I. Introduction 4
II. General observations and policy issues 6
II.1. Brief history 6
II.2. Role of concept 11
II.2.1. First building block: purpose specification 11
II.2.2. Second building block: compatible use 12
II.3. Related concepts 13
II.4. Context and strategic consequences 14
III. Analysis of provisions 15
III.1. 'Specified, explicit and legitimate' purposes 15
III.1.1. Purposes must be specified 15
III.1.2. Purposes must be explicit 17
III.1.3. Purposes must be legitimate 19
III.2. Assessment of compatibility 20
III.2.1. General framework for compatibility assessment 21
III.2.2. Key factors to be considered during the compatibility assessment 23
III.2.3. Further processing for historical, statistical or scientific purposes 28
III.2.4. Article 13 of the e-Privacy Directive on unsolicited communications 34
III.2.5. Big data and open data 35
III.2.6. Consequences of incompatibility 36
III.3. Exceptions under Article 13 of the Directive 37
IV. Conclusions 38
IV.1. Analysis of the current legal framework 38
IV.2 Recommendations for the future 41
Annex 1: Proposed amendments 43
Annex 2: Big data and open data 45
Big data 45
Open data 48
Annex 3: Practical examples to illustrate purpose specification 51
Annex 4: Practical examples to illustrate the compatibility assessment 56

Executive Summary

This Opinion analyses the principle of purpose limitation. It provides guidance for the principle's practical application under the current legal framework, and formulates policy recommendations for the future.

Purpose limitation protects data subjects by setting limits on how data controllers are able to use their data while also offering some degree of flexibility for data controllers. The concept of purpose limitation has two main building blocks: personal data must be collected for 'specified, explicit and legitimate' purposes (purpose specification) and not be 'further processed in a way incompatible' with those purposes (compatible use).

Further processing for a different purpose does not necessarily mean that it is incompatible: compatibility needs to be assessed on a case-by-case basis. A substantive compatibility assessment requires an assessment of all relevant circumstances. In particular, account should be taken of the following key factors:

- the relationship between the purposes for which the personal data have been collected and the purposes of further processing;
- the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;
- the nature of the personal data and the impact of the further processing on the data subjects;
- the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

Processing of personal data in a way incompatible with the purposes specified at collection is against the law and therefore prohibited. The data controller cannot legitimise incompatible processing by simply relying on a new legal ground in Article 7. The purpose limitation principle can only be restricted subject to the conditions set forth in Article 13 of the Directive.

This analysis also has consequences for the future. Article 6(4) of the proposed Data Protection Regulation provides a broad exception from the requirement of compatibility, which would severely restrict its applicability and risk eroding this key principle. The WP29 therefore recommends that the proposed paragraph 4 should be deleted. Further, to provide more legal certainty, the WP29 recommends that legislators adopt the above list of relevant factors in order to assess compatibility. Although this presentation of key factors is not fully exhaustive, it attempts to highlight the most typical factors that may be considered in a balanced approach: neither too general so as to be meaningless, nor too specific so as to be overly rigid.

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

The principle of 'purpose limitation'

Article 6(1)(b) of Directive 95/46/EC[1] (the 'Directive') lists the purpose limitation principle among the key data protection principles. It provides that personal data must be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'.

Specification of purpose is an essential first step in applying data protection laws and designing data protection safeguards for any processing operation. Indeed, specification of the purpose is a pre-requisite for applying other data quality requirements, including the adequacy, relevance, proportionality and accuracy of the data collected and the requirements regarding the period of data retention. The principle of purpose limitation is designed to establish the boundaries within which personal data collected for a given purpose may be processed and may be put to further use. The principle has two components:

- the data controller must only collect data for specified, explicit and legitimate purposes, and
- once data are collected, they must not be further processed in a way incompatible with those purposes.

When we share personal data with others, we usually have an expectation about the purposes for which the data will be used. There is a value in honouring these expectations and preserving trust and legal certainty, which is why purpose limitation is such an important safeguard, a cornerstone of data protection. Indeed, the principle of purpose limitation inhibits 'mission creep', which could otherwise give rise to the usage of the available personal data beyond the purposes for which they were initially collected.

On the other hand, data that have already been gathered may also be genuinely useful for other purposes, not initially specified. Therefore, there is also a value in allowing, within carefully balanced limits, some degree of additional use. The prohibition of 'incompatibility' in Article 6(1)(b) does not altogether rule out new, different uses of the data – provided that this takes place within the parameters of compatibility.

---

[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).

The principle of purpose limitation - which includes the notion of compatible use - requires that in each situation where further use is considered, a distinction be made between additional uses that are 'compatible', and other uses, which should remain 'incompatible'. The principle of purpose limitation is designed to offer a balanced approach: an approach that aims to reconcile the need for predictability and legal certainty regarding the purposes of the processing on one hand, and the pragmatic need for some flexibility on the other.

Need for a more consistent and harmonized approach across Europe

The principle of purpose limitation continues to be considered as sound and valid. However, lack of harmonised interpretation has led to divergent applications of the notions of purpose limitation and incompatible processing in the different Member States, especially in comparison to other principles. For example, in some Member States the concepts of purpose limitation and incompatible processing are inherently linked to other concepts such as fairness, transparency or lawfulness. Consequently, while in some cases the outcome of the analysis based on these divergent approaches may ultimately be the same, these divergent approaches may also lead to different views on what data controllers can do with information they have already collected for a particular purpose or set of purposes.

This diversity has also been noted in the review of the Directive.[2] In this context, various studies have observed that the wording of the purpose-limitation principle is very open-ended, which leaves the concept susceptible to different interpretations[3].

The lack of a consistent approach may weaken the position of data subjects and may also impose unnecessary regulatory burdens on businesses and other organisations operating across borders. This has gradually become a more serious concern as the volume of data and their global availability have increased exponentially and the processing of personal data has become an increasingly prominent feature of modern society, both in on-line and off-line environments.

It is therefore particularly timely, as work towards a new general Data Protection Regulation continues, that the purpose limitation principle – the important role it has and its relationship with the other data protection principles – be more clearly understood. This is why the Article 29 Working Party ('WP29'), 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[4] - committed to draft this Opinion.

---

2 On 25 January 2012, the 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' (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).

3 See, for example, 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.

4 See Work programme 2012-2013 of the Article 29 Data Protection Working Party adopted on 1 February 2012 (WP 190).

Implementation of 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 the Directive[5]. Potential changes to the existing legal framework will take some time, and therefore clarifying the current notion of 'purpose limitation' and its main elements has its own virtues and advantages. For this reason, a key objective of this Opinion is to provide a common, consistent European approach, clarify the role and 'raison d'être' of the purpose limitation principle, and offer guidance and best practice regarding its practical application.

Secondly, clarifying the existing provisions will help expose which areas need improvement. Thus, building on the analysis, the Opinion will also formulate policy recommendations to assist policy makers as they consider changes to the data protection legal framework.

This is all the more important as the proposed data protection legal framework, while leaving the wording of the principle of purpose limitation itself unchanged compared with the text of Article 6(1)(b) of the Directive, also proposes some new provisions. These new provisions, in particular, Article 6(4) of the proposed Data Protection Regulation, would, if adopted, risk eroding this key principle.[6] It is therefore essential to assess the exact scope and function of this principle, at a time where discussions on the new legal framework are still open.

Structure of the Opinion

After an overview of the history and role of purpose limitation in data protection legislation, the Opinion will examine the different elements and requirements for purpose limitation under national law implementing the Directive and the e-Privacy Directive[7]. This analysis is illustrated with practical examples based on national experience. The analysis supports the recommendations in the final part of this Opinion on the interpretation of the purpose limitation principle in the current regulatory framework. At the same time, it also helps provide policy recommendations for policy makers to consider in the context of the review of the Directive.

II. General observations and policy issues

II.1. Brief history

This Section provides an overview of how the right to privacy and the right to the protection of personal data have evolved, starting with the early international instruments on human rights. The overview focuses on how the concept of purpose limitation has developed. It

---

5 Such as Opinion 15/2011 on the definition of consent, adopted on 13.07.2011 (WP187), 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).

6 See Section II.1, pages 10-11, 'Perspectives for the future', as well as Section III.2.6, and Section IV for further detail on the proposed Data Protection Regulation.

7 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.07.2002, p 37), as amended by Directives 2006/24/EC and 2009/136/EC.

explains in particular how this concept was first used as a requirement in the context of derogations to privacy rights, and subsequently developed into a full principle in the data protection context. The summary focuses on the European Union but also touches on relevant international developments.

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 of the 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.

The concepts of legal basis and purpose limitation, which were to become the cornerstones of data protection law, thus, started to take shape, and were further developed in the privacy case law of the European Court of Human Rights ('ECHR'). In the course of time, the ECHR also developed the test of 'reasonable expectations of privacy' to help decide whether there had been an interference with the right to privacy[8]. The Court has furthermore progressively extended the protection of private life, including the protection of personal data, from cases of collection and filing of personal information by secret services (Rotaru, Amann), to the most recent cases where the Court applied the safeguards to the work environment (Copland) and to public places (Gillan and Quinton v. UK)[9].

Convention 108

The Council of Europe's Convention 108[10], opened for signature in 1981, introduces the concept of the protection of personal data. Thereby, it elaborates on a more comprehensive and proactive approach where the notion of 'purpose limitation' is clearly established as one of the essential principles of data protection. This represents an important step forward: a legal basis and specification of a legitimate purpose are now required in all circumstances where personal data are processed, both in the private and public sector.

---

8 See, for instance, ECtHR, 15 June 1992, *Lüdi V. Suisse*, (no 12433/86, A-238); ECtHR 25 June 1997, *Halford v. The United Kingdom* (no. 20605/92, 1997-III).

9 ECtHR 4 May 2000, *Rotaru v. Romania* (no. 28341/95, Reports of Judgments and Decisions 2000-V); ECtHR 16 February 2000, *Amann v. Switzerland* (no. 27798/95, Reports of Judgments and Decisions 2000-II); ECtHR 3 April 2001, *Copland v. The United Kingdom* (no. 62617/00 Reports of Judgments and Decisions 2007-I); ECtHR 12 January 2010, *Gillan and Quinton v. The United Kingdom* (no 4158/05, Reports of Judgments and Decisions 2010).

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

Convention 108 follows on from the Council of Europe ('CoE') Resolutions (73) 22 and (74) 29[11]. These early texts already provide some elements of what will later become key building blocks of the right to the protection of personal data, including the principle of purpose limitation.

CoE Resolution (73) 22 requires the information to be 'appropriate and relevant with regard to the purpose for which it has been stored' and - in the absence of 'appropriate authorisation' - prohibits its use 'for purposes other than those for which it has been stored' as well as its 'communication to third parties'.[12]

For the public sector, CoE Resolution (74) 29 takes a somewhat different approach. While similar general rules require 'the information stored' to be 'appropriate and relevant to the purpose for which it has been stored', there is a specific provision which allows a change of purpose under some conditions. Data may be used 'for purposes other than those which have been defined' if such an exception is 'explicitly permitted by law, is granted by a competent authority, or the rules for the use of the electronic data bank are amended'.[13]

Following on from these early texts, Article 5 of Convention 108 establishes the fundamental principles of data protection law, including lawfulness, fairness and proportionality, but also purpose specification and the requirement that the purpose must be legitimate. It also introduces the notion of incompatibility. The data cannot be used 'in a way incompatible' with the specified purposes. Article 9 of Convention 108 allows derogations from this provision only if 'provided for by law' and further provided that this is 'necessary in a democratic society', in close analogy to the language used in Article 8 of the ECHR.

Since the adoption of Convention 108, the concept of purpose limitation appears to have been recognised as an essential element in instruments that developed later on.[14] The wording 'in a way incompatible' has also been taken on board in the Directive, and it has so far not been challenged in the current revision of Convention 108.

---

[11] Committee of Ministers Resolution (73) 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector, adopted on 26 September 1973, and Committee of Ministers Resolution (74) 29 on the protection of privacy of individuals vis-à-vis electronic data banks in the public sector, adopted on 20 September 1974.

[12] See Annex, Sections 2 and 5.

[13] See Annex, Sections 2(c) and 3(c). It is worth mentioning that the notion of 'change of purpose', subject to similar additional safeguards, is also used and permitted in Article 6 of Regulation (EC) 45/2001 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 ('Regulation 45/2001'). Article 6(1) provides that [p]ersonal data shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the internal rules of the Community institution or body'.

[14] Since Convention 108 was opened for signature in 1981, the Council of Europe produced nineteen recommendations, resolutions or reports to provide further, more specific guidance on the interpretation of Convention 108 with regard to specific sectors (e.g. insurance, banking, health, police, scientific research and statistics, telecommunication, privacy on the internet), specific techniques or technologies (smart cards, video surveillance, direct marketing, profiling), specific categories of data (biometric), or other areas of concern ('communication to third parties of personal data held by public bodies'). Several of these documents address issues related to purpose limitation and compatible use. A compilation of CoE texts on data protection are available at: http://hub.coe.int/c/document_library/get_file?uuid=1d807537-6969-48e5-89f4-48e3a3140d75&groupId=10227 .

OECD Guidelines[15]

The OECD Guidelines, prepared in parallel with Convention 108 and adopted in 1980, share the same ideas of purpose specification and incompatibility, although the concept of incompatibility[16] is defined in a different way.

Purposes must be specified no later than at the time of the collection. The Guidelines allow the 'subsequent use' of the data for different purposes so long as those are not incompatible with the initial purposes and are specified on each occasion of change of purpose. The guidelines mention two exceptions to the requirement of compatible use: 'with the consent of the data subject' or 'by the authority of law'[17].

Despite the differences in the concept of compatible use, and the exceptions available, it is important to highlight that the purpose limitation principle - as a building block of the data protection system - also appears to be a stable element in the international context and is not challenged in the current review of the OECD Guidelines.

Directive 95/46/EC

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

The wording of the purpose limitation principle was not identical in all these instruments and the authors of the Directive also made their own choices at the time. This included a general decision not to separate private and public data processing activities, which means that purpose specification requirements apply to both without distinction.

The Directive added a new requirement to purpose specification, not yet present in either Convention 108 or the OECD Guidelines: the purpose must be 'explicit'[18].

The Directive also introduced a provision for further processing of data for historical, statistical or scientific purposes; these are not considered as incompatible provided that the Member States ensure appropriate safeguards. This is not entirely new: CoE Resolution (73) 22, and CoE Resolution (74) 29 already contain provisions on statistical use. Convention 108 also provides an exception for use of data for statistics or scientific research[19].

The Directive also allows Member States to restrict the scope of certain rights and obligations including the principle of purpose limitation in Article 6(1)(b) provided that such a restriction constitutes a necessary measure to safeguard certain important interests[20]. This provision follows the same logic as Article 9 of Convention 108.

---

15 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

16 Paragraph 9 of the Guidelines.

17 Paragraph 10 of the Guidelines.

18 Article 6(1)(b) of the Directive.

19 Article 9(3) of the Convention. This provision applies 'where there is obviously no risk of an infringement of the privacy of the data subjects'. Paragraph 55 of the Explanatory Memorandum to the OECD Guidelines also mentions that 'the authority of law' may provide 'that data which have been collected for purposes of administrative decision-making may be made available for research, statistics and social planning'.

20 Article 13 of the Directive.

Implementation of the Directive

A study entitled 'Evaluation of the implementation of the Data Protection Directive'[21] underlines that the implementation of the provisions of the Directive on purpose limitation is sometimes unsatisfactory, including, among other things, safeguards for further processing of data for research purposes. In the technical analysis of the transposition of the Directive in the Member States[22], the Commission gives further details on the implementation of Article 6.

The analysis explains that while laws in most Member States set out the purpose specification and limitation principles in similar terms to the ones used in the Directive, the flexibility of these principles, in fact, has led to divergent applications. The divergences touch upon several aspects of the concept. Member States apply different tests to analyse the notions of purpose specification and incompatible use. In some countries, specific rules may apply to the public sector. In others, purposes may sometimes be defined in very broad terms. The approaches in the different Member States also vary as to how the purposes are made explicit, for example, whether specification of purpose is required in the notification to the data protection authority or in the notice to the data subject.[23] The rules concerning the change of purpose, including for research and statistical purposes, also vary considerably, as they do in terms of the requirement of safeguards for these specific uses.

As to the notion of incompatible use, the study notes that the test to determine incompatibility varies from 'reasonable expectations' of the data subject (in certain cases in Belgium) to application of balancing tests (Germany and the Netherlands), or it is intimately linked to other safeguarding principles of transparency, lawfulness and fairness (UK and Greece).

The Charter of Fundamental Rights

The European Union Charter of Fundamental Rights ('the Charter') was initially proclaimed in Nice in 2000. Since the Lisbon Treaty entered into force on 1 December 2009, the Charter, pursuant to the new Article 6 of the Treaty on European Union ('TEU'), enjoys 'the same legal value as the Treaties'. The Charter enshrines data protection as a fundamental right under Article 8, which is distinct from respect for private and family life under Article 7. This feature sets the Charter apart from other key human rights instruments, which - for the most part - treat the protection of personal data as an extension of the right to privacy. This evolution is clearly visible when comparing the 2000 Charter with the 1950 ECHR.[24]

The Charter clearly establishes the principle of purpose limitation, specifying that personal data must be processed 'fairly for specified purposes'. As a separate and distinct requirement, the Charter also lays down the requirement for a legitimate basis for the processing. In

---

21 See Annex 2 of the Impact Assessment to the Commission's data protection reform package, cited in footnote 2 above.

22 Analysis and impact study on the implementation of Directive EC 95/46 in Member States. See http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf .

23 The UK specifies several options. It is also notable that paragraph 54 of the Explanatory Memorandum to the OECD Guidelines provides that 'specification of purposes can be made in a number of alternative or complementary ways, e.g. by public declarations, information to data subjects, legislation, administrative decrees, and licenses provided by supervisory bodies'.

24 As explained above, the ECHR does not contain an explicit and autonomous right to data protection. Rather, data protection in the context of the ECHR emerged from the jurisprudence of the European Court of Human Rights in Strasbourg as an aspect of privacy protection.

particular, it provides that personal data must be processed: 'on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[25]

Perspectives for the future

In conclusion, the history of the purpose limitation concept, both in the EU and beyond (see developments in the OECD and in the Council of Europe), shows that purpose specification and compatible use are essential principles in the system of data protection. In addition, today, when three key data protection instruments are under review (Convention 108, OECD Guidelines and the Directive) there is a consensus on the importance of keeping these principles as fundamental requirements to be met when personal data are processed.

However, even if the principle of purpose limitation itself seems stable, its precise meaning, including any exceptions to it, is now subject to discussion. The fact that purpose specification and legitimacy are two different and cumulative requirements, which is confirmed explicitly by Article 8 of the Charter, is challenged in the proposed Data Protection Regulation[26]. Under the proposed framework, data processing for incompatible use is allowed provided a new legal ground is available: if so, the further processing would be considered as a new data processing operation disconnected from the original purpose. This change of purpose would be possible under any of the legal grounds of Article 6(1) except for the legitimate interests of the controller[27]. This new development further justifies the present work, which aims at clarifying the exact scope and function of this important principle.

II.2. Role of concept

Purpose specification is an essential condition to processing personal data and a prerequisite for applying other data quality requirements. Purpose specification and the concept of compatible use contribute to transparency, legal certainty and predictability; they aim to protect the data subject by setting limits on how controllers are able to use their data and reinforce the fairness of the processing. The limitation should, for example, prevent the use of individuals' personal data in a way (or for further purposes) that they might find unexpected, inappropriate or otherwise objectionable. At the same time, the notion of compatible use also offers some degree of flexibility for data controllers.

To aid the analysis of the concept of purpose limitation, the two main building blocks of the concept: 'purpose specification' and 'compatible use', will be briefly described.

II.2.1. First building block: purpose specification

Collection for 'specified, explicit and legitimate' purposes

Article 6(1)(b) of the Directive requires that personal data should only be collected for 'specified, explicit and legitimate' purposes. Data are collected for certain aims; these aims are the 'raison d'être' of the processing operations. As a prerequisite for other data quality requirements, purpose specification will determine the relevant data to be collected, retention

---

[25] See Article 8(2) of the Charter.
[26] See footnote 2 above.
[27] Article 6(4) of the proposed Data Protection Regulation.

periods, and all other key aspects of how personal data will be processed for the chosen purpose/s.

First, any purpose must be **specified**, that is, sufficiently defined to enable the implementation of any necessary data protection safeguards, and to delimit the scope of the processing operation. When and how this specification takes place will be discussed in Section III.1.1.

Second, to be **explicit**, the purpose must be sufficiently unambiguous and clearly expressed. Comparing the notion of 'explicit purpose' with the notion of 'hidden purpose' may help to understand the scope of this requirement, as will be discussed further in Section III.1.2.

Third, purposes must also be **legitimate**. This notion goes beyond the requirement to have a legal ground for the processing under Article 7 of the Directive and also extends to other areas of law. Purpose specification under Article 6 and the requirement to have a legal ground under Article 7 are thus two separate and cumulative requirements[28].

The use of the term 'legitimate' in Article 6 provides a link to Article 7 but also to broader legal principles of applicable law, such as non-discrimination. The notion of legitimacy must also be interpreted within the context of the processing, which determines the 'reasonable expectations' of the data subject. This will be discussed further in Section III.1.3.

Pre-requisite for other data quality requirements

When applying data protection law, it must first be ensured that the purpose is specific, explicit and legitimate. This is a prerequisite for other data quality requirements, including adequacy, relevance and proportionality (Article 6(1)(c)), accuracy and completeness (Article 6(1)(d)) and requirements regarding the duration of retention (Article 6(1)(e)).

In cases where different purposes exist from the beginning and different kinds of data are collected and processed simultaneously for these different purposes, the data quality requirements must be complied with separately for each purpose.

If personal data are further processed for a different purpose:

- the new purpose/s must be specified (Article 6(1)(b)), and
- it must be ensured that all data quality requirements (Articles 6(1)(a) to (e)) are also satisfied for the new purposes.

II.2.2. Second building block: compatible use

Article 6(1)(b) of the Directive also introduces the notions of 'further processing'[29] and 'incompatible' use, and requires that further processing must not be incompatible with the purposes for which personal data were collected. In particular, Article 6(1)(b) requires that personal data should not be 'further processed in a way incompatible' with those purposes and recital 28 states that the 'purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified'.

---

[28] Article 8(2) of the Charter also makes it clear that the requirement of purpose specification is a separate, cumulative requirement that applies in addition to the requirement of an appropriate legal ground.

[29] On the notion of 'further processing', see Section III.2.1.

The prohibition of incompatible use sets a limitation on further use. It requires that a distinction be made between further use that is 'compatible', and further use that is 'incompatible' and therefore prohibited. The general framework and specific criteria that will help make this assessment will be discussed extensively in Section III.2.

In this context, in Section III.2.3 we will also deal with the specific provision in Article 6(1)(b) on 'further processing for historical, statistical or scientific purposes'. It is not clear from the text of Article 6(1)(b) alone whether this specific provision should be seen as an *exception* to the general prohibition of incompatible use in order to give a privileged position to 'historical, statistical or scientific purposes' or as a *specification* of the general rule, while not excluding that other cases could also be considered as 'not incompatible'. The analysis in this Opinion firmly supports this second view: the specific provision could give rise to more general criteria for compatibility (e.g. potential impact on the data subject, and appropriate safeguards).

This leads to a more prominent role in our analysis for different kinds of safeguards, including technical and organisational measures to ensure functional separation, such as full or partial anonymisation, pseudonymisation, aggregation of data, and privacy-enhancing technologies (see further in Section III.2).

II.3. Related concepts

Transparency

There is a strong connection between transparency and purpose specification. When the specified purpose is visible and shared with stakeholders such as data protection authorities and data subjects, safeguards can be fully effective. Transparency ensures predictability and enables user control.

Predictability

If a purpose is sufficiently specific and clear, individuals will know what to expect: the way data are processed will be predictable. This brings legal certainty to the data subjects, and also to those processing personal data on behalf of the data controller.

Predictability is also relevant when assessing the compatibility of further processing activities. In general, further processing cannot be considered predictable if it is not sufficiently related to the original purpose and does not meet the reasonable expectations of the data subjects at the time of collection, based on the context of the collection.[30]

[30] That said, there may be situations where the data initially collected for one purpose or set of purposes may nevertheless be subsequently used for different purposes (or for the same purposes but in novel ways) even if such further use could not have met the original expectations of the data subjects. In these situations, additional safeguards, for example, informed consent of the data subjects, may help ensure that the further processing meets the expectations of the data subjects at the time of further use.

User control

User control is only possible when the purpose of data processing is sufficiently clear and predictable. If data subjects fully understand the purposes of the processing, they can exercise their rights in the most effective way. For instance, they can object to the processing or request the correction or deletion of their data.

As will be developed below, this does not mean that the presented purpose should always be trusted as the actual and effective one, as there may be a discrepancy between what is claimed and what is pursued in practice by the data controller. Ultimately, compliance with other data protection requirements, such as the necessity and relevance of data, will always need to be measured against the actual purpose.

II.4. Context and strategic consequences

The objective of this Opinion is to clarify the purpose limitation principle and to provide guidance on its practical application. This should be done in order to help clearly delimit the use of personal data, primarily in the interest of data subjects, but also to allow for the necessary flexibility to data controllers, and to improve predictability and legal certainty in the interest of all stakeholders.

Several elements lead to the need for an in-depth analysis of the concept of purpose limitation:

- The way in which it has been implemented in Member States, which has led to a diversity of interpretations. A clear common understanding of the concept will better ensure its effective application in practice - in the interest of all concerned - and will also help in finding the best way forward in the new legislative framework.

- The context of processing activities today. The development of new technologies results in increasingly more data being available, for a great diversity of purposes.

- Current trends for reuse of data by the private sector ('big data') but also 'open data' and 'data sharing' initiatives proposed by many governments, including EU legislative initiatives, are of particular relevance here.[31]

With the development of multifunctional use of data, it becomes all the more relevant to gain a good understanding of the role and the meaning of the principle of purpose limitation. One of the most dangerous pitfalls would be to reject or weaken the concept simply because its implementation has been too diverse and there is no general understanding of the notion, or because the reality of data processing has changed, and it is a challenge to apply a valid concept to a changed reality.

It should be kept in mind that processing of personal data has an impact on individuals' fundamental rights in terms of privacy and data protection. This impact on the rights of individuals must necessarily be accompanied by a limitation of the use that can be made of

---

[31] In this context, it is to be recalled that purpose limitation applies not only to personal data held by the private sector but also to personal data held by the public sector. In addition, the principle of purpose limitation continues to apply to personal data even if such data have been made publicly available. For more detail on 'big data' and open data', see Section III.2.5 and Annex 2.

the data, and therefore by a limitation of purpose. An erosion of the purpose limitation principle would consequently result in the erosion of all related data protection principles.

III. Analysis of provisions

III.1. 'Specified, explicit and legitimate' purposes

Article 6(1)(b) of the Directive requires that personal data must be collected for 'specified, explicit and legitimate' purposes. These three requirements are analysed below.

III.1.1. Purposes must be specified

What is purpose specification and why is it necessary?

Personal data must be collected for specified purposes. The controller must therefore carefully consider what purpose or purposes the personal data will be used for, and must not collect personal data which are not necessary, adequate or relevant for the purpose or purposes which are intended to be served.

Purpose specification lies at the core of the legal framework established for the protection of personal data. In order to determine whether data processing complies with the law, and to establish what data protection safeguards should be applied, it is a necessary precondition to identify the specific purpose(s) for which the collection of personal data is required. Purpose specification thus sets limits on the purposes for which controllers may use the personal data collected, and also helps establish the necessary data protection safeguards.

Purpose specification requires an internal assessment carried out by the data controller and is a necessary condition for accountability. It is a key first step that a controller should follow to ensure compliance with applicable data protection law. The controller must identify what the purposes are, and must also document, and be able to demonstrate, that it has carried out this internal assessment.

At what time should the purposes be specified?

Article 6(1)(b) of the Directive requires that personal data be 'collected' for specified, explicit and legitimate purposes.[32] Thus, it can be inferred that the purposes must be specified prior to, and in any event, not later than, the time when the collection of personal data occurs.

How precisely, and in how much detail, should the purpose be specified?

The purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied.

---

[32] See also recital 28, which says that purposes 'must be determined at the time of collection of the data'.

For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'.[33] That said, the degree of detail in which a purpose should be specified depends on the particular context in which the data are collected and the personal data involved. In some clear cases, simple language will be sufficient to provide appropriate specification, while in other cases more detail may be required.[34]

The fact that the information must be precise does not mean that longer, more detailed specifications are always necessary or helpful. Indeed, a detailed description may at times even be counter-productive. This may particularly be the case if the written, detailed specifications of purpose are overly legalistic and provide disclaimers rather than helpful information to data subjects and other stakeholders.[35]

In light of this, the approach of a 'layered notice' to data subjects often works well, especially on the Internet, and has thus been recommended in many situations by the WP29[36]. This means that key information is provided to data subjects in a very concise and user-friendly manner, while additional information (perhaps via a link to a more detailed description of the processing on another Internet page) is provided for the benefit of those who require further clarification.[37]

What if personal data are collected for more than one purpose?

Personal data can be collected for more than one purpose. In some cases, these purposes, while distinct, are nevertheless related to some degree. In other cases the purposes may be unrelated. A question that arises here is to what extent the controller should specify each of these distinct purposes separately, and how much additional detail should be provided.[38]

For 'related' processing operations, the concept of an overall purpose, under whose umbrella a number of separate processing operations take place, can be useful.[39] That said, controllers should avoid identifying only one broad purpose in order to justify various further processing activities which are in fact only remotely related to the actual initial purpose.

Ultimately, in order to ensure compliance with Article 6(1)(b), each separate purpose should be specified in enough detail to be able to assess whether collection of personal data for this purpose complies with the law, and to establish what data protection safeguards to apply[40].

---

33 See Annex 3, examples 7 and 8.

34 See Annex 3, examples 1, 3 and 13.

35 See Annex 3, example 12.

36 See, for example, WP29 Opinion 10/2004 on More Harmonised Information Provisions (WP100) and WP29 Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) (WP160).

37 See Annex 3, examples 9 and 10.

38 In this context it is relevant to mention that Article 18 of the Directive requires Member States to provide that the controller 'must notify the supervisory authority ... before carrying out ... operations intended to serve a single purpose or several related purposes.' This provision introduces the notion of 'related purposes'. In some Member States, for example, in Belgium, related purposes can be notified to the data protection authority in the same form.

39 See Annex 3, example 11.

40 If personal data are processed for several purposes, all requirements of Article 6 apply to each purpose separately. Thus, not all data collected for one purpose may always be relevant, necessary, and not excessive for all other (related or unrelated) purposes, defined at the time of original collection or later on. This will

III.1.2. Purposes must be explicit

What does 'explicit' mean and why is it necessary?

Personal data must be collected for explicit purposes. The purposes of collection must not only be specified in the minds of the persons responsible for data collection. They must also be made explicit. In other words, they must be clearly revealed, explained or expressed in some intelligible form. It follows from the previous analysis that this should happen no later than the time when the collection of personal data occurs.

The ultimate objective of this requirement is to ensure that the purposes are specified without vagueness or ambiguity as to their meaning or intent. What is meant must be clear and should leave no doubt or difficulty in understanding. The specification of the purposes must, in particular, be expressed in such a way so as to be understood in the same way not only by the controller (including all relevant staff) and any third party processors, but also by the data protection authorities and the data subjects concerned. Particular care should be taken to ensure that any specification of the purpose is sufficiently clear to all involved, irrespective of their different cultural/linguistic backgrounds, level of understanding or special needs.[41]

The requirement that the purposes be specified 'explicitly' contributes to transparency and predictability. It allows unambiguous identification of the limits on how controllers are able to use the personal data collected, with a view to protecting the data subjects. It helps all those processing data on behalf of the controller, as well as data subjects, data protection authorities and other stakeholders, to have a common understanding of how the data can be used. This, in turn, reduces the risk that the data subjects' expectations will differ from the expectations of the controller.

In many situations, the requirement also allows data subjects to make informed choices – for example, to deal with a company that uses personal data for a limited set of purposes rather than with a company that uses personal data for a wider variety of purposes.

As background, we note that the word 'explicit' has not been translated with identical meaning into the different language versions of the Directive.[42] In some versions the requirement appears to focus more clearly on the end result: on the objective that the purposes must be unambiguous, and that they must be understood in the same way by all concerned. In other versions, the focus is on the method of how this end result is to be achieved: on the requirement that the purposes must be clearly expressed and explained.

---

therefore require a case-by-case analysis, at the initial stage as well as at any further stage in time when a new purpose is envisaged.

41 See Annex 3, examples 2 and 4.

42 The same Latin root is used in several languages including English, Italian and French as 'explicit', 'explicite' and 'esplicite'. The original Latin verb from which these adjectives all originate is 'explicare', with the meaning of 'unfold, unravel, explain', and thus appears to imply a requirement that the purposes must be expressed and explained in some form. Other language versions focus on the requirement of the end-result, that the specification of the purposes must be unambiguous. See, for example, the German 'eindeutig' and the Hungarian 'egyértelmű', which can be translated as 'unambiguous', and do not necessarily require that the purposes must also be 'expressed' in any way. However, the Dutch 'uitdrukkelijk omschreven' is again similar to 'explicit'.

A common ground amongst these different approaches is that as much information needs to be expressed and communicated as is necessary to ensure that everyone concerned has the same, unambiguous understanding of the purposes of the processing.[43]

In what form, and to whom, should the purposes be made explicit?

The requirement for the purposes to be explicit is distinct from the requirement of information to be given to the data subject (Articles 10 and 11 of the Directive) and the requirement to notify the supervisory authority (Article 18). Nevertheless, all three requirements are closely related and each serves, as one of its main objectives, the purpose of transparency.

Expressing the purposes under the meaning of Article 6(1)(b) may be accomplished in different ways. These include, for example, describing the purposes in a notice provided to the data subjects, in a notification provided to the supervisory authority, or internally in the information provided to a data protection officer. Some national laws specifically provide that both notices and notifications are acceptable forms of complying with the requirement of making the purposes of the processing explicit, but that they are not the only possibilities.[44]

The OECD Guidelines emphasise flexibility and specifically mention[45] that the 'specification of purposes can be made in a number of alternative or complementary ways, e.g. by public declarations, information to data subjects, legislation, administrative decrees, and licenses provided by supervisory bodies'. What matters is the quality and consistency of the information provided.

In terms of accountability, specification of the purpose in writing and production of adequate documentation will help to demonstrate that the controller has complied with the requirement of Article 6(1)(b). It would also allow data subjects to exercise their rights more effectively – for example, it would provide proof of the original purpose and allow comparison with subsequent processing purposes.

Specifying the purposes in writing can be helpful, or even necessary, in many circumstances. In particular, nowadays, many data processing activities happen in a complex, opaque, and ambiguous context, especially on the Internet. In those situations, special care is needed to unambiguously specify the purposes.[46]

That said, at times, context and custom may make it clear enough to all involved, including those processing the data as well as the data subjects, how the personal data will be used. If this is possible without risking uncertainty and ambiguity,[47] Article 6(1)(b) may sometimes be satisfied by expressing the essential elements only.[48] However, in those situations, more detailed information should still be provided to those who want it.

Provision of detailed information to the data subjects may not always be necessary in simple and straightforward cases where the data subject can already, and without any doubt,

---

43 See Annex 3, examples 5 and 6.
44 This is the situation in the UK, for example.
45 See paragraph 54 of the Explanatory Memorandum to the Guidelines.
46 See Annex 3, examples 1, 2, 3, 8, 13 and 14.
47 Subject to other possible requirements under Articles 10, 11 and 18 of the Directive.
48 See Annex 3, examples 5 and 6.

unambiguously determine the purposes of the processing from the context and custom.[49] National data protection laws may also provide exceptions from the notification requirements in certain situations.

What happens in case of serious shortcomings?

It is possible that a controller could fail to comply with the requirements of Article 6(1)(b) of the Directive: for example, if it does not specify the purposes of the processing in sufficient detail or in a clear and unambiguous language. In other situations, the information provided may not correspond to the facts of the case, or it could contain inconsistencies about the purpose (e.g. as between the notice to data subjects and the notification to the supervisory authority). There may also be cases where a detailed, legalistic data protection notice includes unfair, surprising, or unilateral terms and conditions about the purposes for which data may be used, which do not fully match the reasonable expectations of the data subjects.

It is crucial to consider the consequences of such shortcomings. It is important to emphasize that a failure to state, or accurately state the purpose or purposes for processing does not mean that the data controller can process personal data for any and all purposes at its discretion, or that it is free to determine the purposes based on its subjective expectations or unilateral interpretation of inconsistent information. Neither does it mean that a carefully crafted document prepared by the controller's lawyers (for example, data protection notices that are misleading or contain unfair contractual terms) can legitimize processing for the described purposes in these situations. In such cases it will be necessary to reconstruct the purposes of the processing, keeping in mind the facts of the case.

While the publicly specified purpose is the main indicator of what the data processing will actually aim at, it is not an absolute reference: where the purposes are specified inconsistently or the specified purposes do not correspond to reality (for instance in case of a misleading data protection notice), all factual elements, as well as the common understanding and reasonable expectations of the data subjects based on such facts, shall be taken into account to determine the actual purposes.[50]

III.1.3. Purposes must be legitimate

Legitimacy is a broad requirement

Personal data must be collected for legitimate purposes. This requirement goes beyond a simple cross-reference to Article 7 of the Directive, which outlines the 'criteria for making data processing legitimate' and lists six different legal grounds for processing personal data, ranging from consent of the data subject to a balance of interests test.

In order for the purposes to be legitimate, the processing must - at all different stages and at all times - be based on at least one of the legal grounds provided for in Article 7.[51] However, the requirement that the purposes must be legitimate is broader than the scope of Article 7. In

---

[49] Articles 10 and 11 of Directive 95/46/EC provide a specific exception from the notice requirement for cases in which the data subject 'already has' the information.

[50] In addition, infringement of the requirements of Article 6(1)(b) of the Directive may also have other serious consequences. For example, it may lead to a ban on such processing or to other legal sanctions to be imposed by the competent data protection authority.

[51] The same goes for Article 8(1)-(4) of the Directive concerning 'special categories of data', where applicable.

addition, Article 6(1)(b) also requires that the purposes must be in accordance with all provisions of applicable data protection law, as well as other applicable laws such as employment law, contract law, consumer protection law, and so on.

The requirement of legitimacy means that the purposes must be 'in accordance with the law' in the broadest sense. This 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.[52]

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.

The legitimacy of a given purpose can also change over time, depending on scientific and technological developments, and changes in society and cultural attitudes.

Examples to illustrate how purpose specification is carried out in practice are provided in **Annex 3.**

III.2. Assessment of compatibility

Article 6(1)(b) of the Directive provides that personal data collected for one or more purposes shall 'not be further processed in a way incompatible with those purposes'.

This Section will discuss how to assess whether further processing is compatible with the purposes specified at collection.

This will be done by first providing a general framework for a 'compatibility assessment' (Section III.2.1), and then explaining the most common factors that should be considered in the assessment (Section III.2.2).

Next, we will consider a few specific applications of the compatibility assessment: further processing for historical, statistical or scientific purposes (Article 6(1)(b) of the Directive) (Section III.2.3); the case of unsolicited communications (Article 13 of the e-Privacy Directive) (Section III.2.4) and 'open data' and 'big data' initiatives (Section III.2.5).

Finally, Section III.2.6 will set out the consequences of incompatibility.

---

[52] See Annex 3, example 15.

III.2.1. General framework for compatibility assessment

The notion of 'further' processing

It is helpful to first clarify what constitutes 'further processing'. As explained earlier, it follows from Article 6(1)(b) and recital 28 of the Directive that the purposes of processing must be specified prior to, and in any event, not later than, the time when the collection of personal data occurs.

When setting out the requirement of compatibility, the Directive does not specifically refer to processing for the 'originally specified purposes' and processing for 'purposes defined subsequently'. Rather, it differentiates between the very first processing operation, which is collection, and all other subsequent processing operations (including for instance the very first typical processing operation following collection - the storage of data).

In other words: any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered 'further processing' and must thus meet the requirement of compatibility.

The notion of incompatibility

Rather than imposing a requirement of compatibility, the legislator chose a double negation: it prohibited incompatibility. By providing that any further processing is authorised as long as it is *not incompatible* (and if the requirements of lawfulness are simultaneously also fulfilled), it would appear that the legislators intended to give some flexibility with regard to further use. Such further use may fit closely with the initial purpose or be different. The fact that the further processing is for a *different* purpose does not necessarily mean that it is automatically *incompatible*: this needs to be assessed on a case-by-case basis, as will be shown below.

In some situations, this additional flexibility may be needed to allow for a change of scope or focus in situations where the expectations of society - or of the data subjects themselves - have changed about what additional use the data may be put to. It is also possible that when initially specifying the purpose, neither the controller nor the data subject thought additional purposes would be necessary, although it subsequently transpired that the data could indeed be very useful for other things. In some of these (and similar) situations, a change of purpose may be permissible, and further processing may be considered not incompatible, provided that the compatibility test is satisfied.

A purely formal or a substantive compatibility assessment?

The nature of the assessment to be carried out by the data controller (but also by the data protection authority when assessing compliance) is decisive. In very brief terms, it can take two different forms. The compatibility test could be formal or substantive:

- A formal assessment will compare the purposes that were initially provided, usually in writing, by the data controller with any further uses to find out whether these uses were covered (explicitly or implicitly).
- A substantive assessment will go beyond formal statements to identify both the new and the original purpose, taking into account the way they are (or should be) understood, depending on the context and other factors.

While the first method may at first sight seem more objective and neutral, it risks being too rigid, building too much on formal text. By doing so, it may encourage controllers to specify the purpose in increasingly more legalistic ways, with a view to ensure a margin for further data processing rather than to protect the individuals concerned.

The second method is more flexible and pragmatic, but also more effective: it may also enable adaptation to future developments within the society while at the same time continuing to effectively safeguard the protection of personal data. A major issue is then of course to identify the criteria that will help to assess at what point a different purpose becomes an incompatible purpose. This will be the subject of Section III.2.2, where the relevant criteria and their practical use will be discussed.

Different scenarios and needs for assessment

Before turning in more detail to the factors that should be taken into account in the compatibility assessment, it may be useful to highlight that in practice there may be different scenarios for this assessment. Some situations will require little or no analysis, others a more thorough assessment, as illustrated below:

- *Scenario 1: Compatibility is prima facie obvious:* Further processing may be found compatible, because data are processed specifically to achieve the purposes clearly specified at collection, and in a way customary to achieve those purposes. As such, the processing clearly meets the reasonable expectations of the data subjects, even if not all details were fully expressed at the start.

Example: A customer contracts an online retailer to deliver an organic vegetable box each week to their home. After initial 'collection' of the customer's address and banking information, these data are 'further processed' by the retailer each week for payment and delivery. This obviously complies with the principle of purpose limitation and requires no further analysis.

- *Scenario 2: Compatibility is not obvious and needs further analysis:* There may be a 'connection' between the specified purpose and the way the data are subsequently processed; the purposes are related but not fully matching. It is also possible that the data are further used for different and not directly related purposes. In all these cases there is a need to assess a number of relevant factors, including among other things, the relationship between the initial purpose and the purpose of the further processing, and the context in which the data were collected. In principle, the greater the distance between the initial purpose specified at collection and the purposes of further use, the more thorough and comprehensive the analysis will have to be, and there may be a number of additional criteria that will need to be assessed. In these situations, there may also be a need to include additional safeguards to compensate for the change of purpose (e.g. to provide additional information and explicit options for the data subject).

Example: The vegetable box retailer wishes to use the customer's email address and purchase history to send them personalized offers and discount vouchers for similar products including its range of organic dairy products. He also wishes to provide the customer's data including their name, email address, phone number, and purchase history to a business contact which has opened an organic butchery business in the neighbourhood. In both cases, the retailer cannot assume that this further use is compatible and some additional analysis is necessary, with the possibility of different outcomes (e.g. in case of 'internal' use or transfer of data[53]).

- *Scenario 3: Incompatibility is obvious:* If data are processed in a way or for additional purposes that a reasonable person would find not only unexpected, but also obviously inappropriate or otherwise objectionable, and the processing clearly does not meet the expectations of a reasonable person in the situation of the data subject, it is highly likely to be considered incompatible. Only in marginal cases of doubt, would further analysis be useful.

Example: The vegetable box customer also buys a range of other organic products on the retailer's website, some of which are discounted. The retailer, without informing the customer, has implemented an off-the-shelf price-customization software solution, which - among other things - detects whether the customer is using an Apple computer or a Windows PC. The retailer then automatically gives greater discounts to Windows users. In this case, the further use of available data and the unfair collection of additional information, both for an unrelated purpose (allowing secret 'price discrimination'), are problematic.

The above scenarios underline the need for a limited number of key factors that can help to focus a compatibility assessment, as well as the need for a pragmatic approach that allows the use of practical assumptions ('rules of thumb') based on what a reasonable person would find acceptable under any given circumstances.

III.2.2. Key factors to be considered during the compatibility assessment

Member States have developed a number of useful criteria, in specific legal provisions and in practice, to assess the compatibility between the purposes specified at collection and the way in which the data are further processed. These criteria are already widely used in practice and allow the identification of a limited number of common key factors:

a) the relationship between the purposes for which the data have been collected and the purposes of further processing

This factor is perhaps the most obvious one as the compatibility assessment is, first of all, about the relationship between the initial purpose and the purpose of further processing as already briefly touched on above. This should not only be seen as a *textual* issue, i.e. how the language of the initial purpose compares to the purposes of further processing. In fact, it may be that in practice only limited, if any, text has been used to express the initial purposes (see Section III.1). The focus should rather be on the *substance* of the relationship between the purposes of collection and the purposes of further processing.

---

[53] See also Section III.2.4 on unsolicited communications and Article 13 of the e-Privacy Directive.

This may cover situations where the further processing was already more or less implied in the initial purposes, or assumed as a logical next step in the processing according to those purposes, as well as situations where there is only a partial or even non-existent link with the original purposes. In any case, the *greater* the distance between the purposes of collection and the purposes of further processing, the more problematic this would be for the compatibility assessment.[54]

As previously highlighted in the context of purpose specification, it is always necessary to take account of the factual context and the way in which a certain purpose is commonly understood by relevant stakeholders in the various situations under analysis.

b) the context in which the data have been collected and the reasonable expectations of the data subjects as to their further use

The second factor focuses on the specific context in which the data were collected and the reasonable expectations of the data subjects as to their further use based on that context. In other words, the issue here is what a reasonable person in the data subject's situation would expect his or her data to be used for based on the context of the collection.[55]

An important aspect of this is the *nature* of the relationship between the controller and the data subject. This requires not only a review of any legal statements made, but also consideration of what would be customary and generally expected practice in the given context, and in the given (commercial or other) relationship. In general, the more unexpected or surprising the further use is, the more likely it is that it would be considered incompatible.[56]

An assessment of the nature of this relationship should also include an investigation into the balance of power between the data subject and the data controller. In particular, it should be noted whether the data subjects, or any third parties on their behalf, were *obliged* to provide the data under law.[57] Alternatively, the collection could have been based on a contractual relationship. In this case, the nature of the contract and the balance of power between the data subject and the data controller (for example, how easy was it for the data subject to terminate that contract and seek an alternative service-provider) should be examined.[58] If the further processing was based on consent, an assessment should be made as to what extent the consent was freely given, and on the precision of its terms.[59] In general, the compatibility assessment will need to be more stringent if the data subject was not given sufficient freedom of choice, if the terms of any consent were unspecific, and/or if the further use is considered objectionable.

In all these cases, it is also important to consider whether the status of the data controller[60], the nature of the relationship or the service provided[61], or the applicable legal

---

54 See Annex 4, in particular, examples 1, 2 and 3.
55 See Annex 4, among others, examples 1 and 2.
56 See Annex 4, in particular, examples 8 and 9.
57 See Annex 4, in particular, examples 2, 17, 18, 19, 20, 22.
58 See Annex 4, in particular, example 8.
59 See Annex 4, in particular, examples 7, 8, 9 and 10.
60 Such as, for example, an attorney or a physician.
61 Such as, for example, cloud computing services for personal document management, email services, diaries, e-readers equipped with note-taking features, and various life-logging applications that may contain very personal information.

or contractual obligations (or other promises made at the time of collection) could give rise to reasonable expectations of stricter confidentiality and stricter limitations on further use.[62] In general, the more *specific* and *restrictive* the context of collection, the more limitations there are likely to be on further use.[63] Here again, it is necessary to take account of the factual context rather than simply rely on text in small print.

In assessing the context in which data were collected and the reasonable expectations of the data subject as to their use, due attention should also be given to the *transparency* of the processing (including the type and content of the information initially or subsequently provided to the data subject)[64], as well as whether the further processing was based on provisions of law.[65] In the latter case, legal security and predictability in general might suggest that the further use is appropriate, even if the data subjects might not have been aware of all the consequences involved.[66]

c) the nature of the data and the impact of the further processing on the data subjects

The third factor focuses on the nature of the data and the impact of the further processing on the data subjects. This is a fairly common approach in data protection law which has after all been designed to *protect* individuals against the *impact* of improper or excessive use of their personal data. The nature of the data processed plays a critical role in all its provisions. It would therefore be important to evaluate whether the further processing involves sensitive data, either because they belong to the special categories of data under Article 8 of the Directive[67], or for other reasons, as in the case of biometric data, genetic information, communication data, location data, and other kinds of personal information requiring special protection.[68] In general, the more sensitive the information involved, the narrower the scope for compatible use would be.[69]

In assessing the impact of the further processing, both positive[70] and negative consequences should be taken into account. These may include potential future decisions or actions by third parties[71], and situations where the processing may lead to the exclusion or discrimination of individuals.[72] In addition to adverse outcomes that can be specifically

---

62 In some cases, the context of collection may suggest a complete prohibition of any further use beyond a specific, pre-defined purpose.

63 See Annex 4, in particular, examples 4 and 16.

64 See Annex 4, in particular, examples 5, 9, 10, 12. It should be kept in mind that the requirement to provide clear information to data subjects is a horizontal one. Still, the better a controller complies with all requirements of the Directive, the more likely it is that a further use may be considered compatible.

65 i.e. legal provisions, describing further phases of the purpose for which data were *originally* collected, as clearly distinguished from legal provisions which might legitimate *incompatible* use under certain circumstances (see Section III.3).

66 See Annex 4, in particular, examples 3 and 11.

67 Special categories of data include 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership', 'data concerning health or sex life', and 'data relating to offences and criminal convictions'.

68 It may also be relevant to consider whether the data subject is a child or otherwise belongs to a more vulnerable segment of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly.

69 See Annex 4, in particular, examples 4, 12, 14, 16, 17, 18. However, it cannot be excluded that even highly sensitive personal data may be further processed, provided that the processing meets the criteria for compatibility assessment, and in particular, the reasonable expectations of the data subjects are respected.

70 See Annex 4, in particular, examples 6 and 11.

71 See Annex 4, in particular, examples 1, 2, 12, 13, 17, 18, 19, 20, 21, and 22.

72 See Annex 4, in particular, examples 5, 13, 14, 18, and 19.

foreseen, emotional impacts also need to be taken into account, such as the irritation, fear and distress that may result from a data subject losing control over personal information, or realising that it has been compromised.

Relevant impact in a larger sense may also involve *the way in which* data are further processed: such as whether the data are processed by a different controller in another context with unknown consequences, whether the data are publicly disclosed or otherwise made accessible to a large number of persons, or whether large amounts of personal data are processed or combined with other data (e.g. in case of profiling, for commercial, law enforcement or other purposes), particularly if such operations were not foreseeable at the time of collection.[73]

The relevant consequences might therefore vary from targeted and well defined to more general and unpredictable with a variable scale or scope. Again, in general, the more negative or uncertain the impact of further processing might be, the more unlikely it is to be considered as compatible use. The availability of alternative methods to achieve the objectives pursued by the controller, with less negative impact for the data subject, would certainly have to be a relevant consideration in this context.[74]

d) the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects

An inherent characteristic of a multi-factor assessment is that deficiencies at certain points may in some cases be compensated by a better performance on other aspects. This is why the fourth and last factor looks at the safeguards that have been applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

Appropriate additional measures could thus, in principle, serve as 'compensation' for a change of purpose[75] or for the fact that the purposes have not been specified as clearly in the beginning as they should have been. This might require technical and/or organisational measures to ensure functional separation (such as partial or full anonymisation, pseudonymisation, and aggregation of data), but also additional steps taken for the benefit of the data subjects, such as increased transparency, with the possibility to object or provide specific consent. Whether the result is acceptable will depend on the compatibility assessment as a whole (i.e. including those measures and their effect on the other aspects mentioned above).

If the purposes have changed or have not been specified clearly, a first necessary (but not always sufficient) condition towards ensuring compatibility is to re-specify the purposes. Often it is also necessary to provide additional notice to the data subjects and – depending on the circumstances and the legal basis of the further processing – it may be necessary to provide an opportunity to allow them to opt-in or opt-out.[76]

---

[73] See Annex 4, in particular, examples 5, 9, 10, 19, 20, 21, 22.

[74] See Annex 4, in particular, examples 4, 5, 6, 12 and 13.

[75] This follows implicitly from the specific provision on further processing for historical, statistical or scientific purposes in Article 6(1)(b) of the Directive (see Sections II.2.2 and III.2.3).

[76] If required, the data protection authority must also be notified.

In some cases, requesting a specific separate consent for the new processing may, in particular, help compensate for the change of purpose.[77] That is, a new legal basis under Article 7(a) can, in some situations, contribute to compensate for the incompatibility. It is important to reiterate, however, that the requirements of compatibility under Article 6(1)(b) and the requirement of an appropriate legal basis under Article 7 are cumulative. That is, a new legal basis alone cannot legitimize an otherwise incompatible further use.

In addition, the implementation of additional technical and organisational measures may be particularly important. The identification of the relevant measures is facilitated if certain basic goals of data protection and data security are taken into account. The classic goals of data security are availability, integrity and confidentiality. To meet data protection requirements effectively, the data protection goals of transparency, isolation and 'intervenability' should be considered as well.[78]

When trying to identify technical and organisational measures that qualify as appropriate safeguards to compensate for the change of purpose, the focus often lies with the notion of isolation[79]. Examples of the relevant measures may include, among other things, full or partial anonymisation, pseudonymisation, or aggregation of the data, privacy enhancing technologies, as well as other measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation'). These measures are particularly relevant in the context of further use for 'historical, statistical or scientific purposes', as will be developed below.[80]

Although this presentation of key factors is not fully exhaustive, it attempts to highlight the typical issues that may be considered in a balanced approach; neither too general so as to be meaningless, nor too specific so as to be overly rigid. As shown above, each factor may be further developed into more detailed or more specific criteria. As technology, society and business practices continue to evolve, it is possible that certain factors may become more or less important, and may require specific attention when assessing compatibility.

It should be emphasised that the assessment of compatibility will often imply a multi-criteria evaluation. While there may be cases where not all the considerations mentioned above will be relevant, typically the assessment will require the evaluation of a number of relevant factors applied in a cumulative way. Their different weight will therefore have an impact on the global assessment.

Practical examples to illustrate the compatibility assessment on the basis of these factors are provided in **Annex 4**.

---

77 See Annex 4, and compare, in particular, examples 7 and 8.

78 See Opinion 05/2012 of the WP29 on Cloud Computing adopted on 1 July 2012 (WP 196), in particular, Section 3.4.

79 See Section 3.4 of Opinion 05/2012 on Cloud Computing just referred to. In addition, it should be noted that in Germany the broader concept of 'unlinkability' has been introduced into legislation and is promoted by the Conference of Data Protection Commissioners.

80 See Annex 4, in particular, examples 14 and 15.

III.2.3. Further processing for historical, statistical or scientific purposes

Article 6(1)(b) of the Directive contains a specific provision on further processing for 'historical, statistical or scientific purposes'.[81] This provision, read together with the relevant recitals, allows further processing of data for historical, statistical and scientific research as long as the controller compensates for this change by implementing 'appropriate safeguards' and in particular by ensuring that the data will not be used to support measures or decisions regarding any particular individuals.

Objective of the provision on processing for 'historical, statistical or scientific purposes'

The provision contributes to greater legal certainty. It should not be read as providing an overall exception from the requirement of compatibility, and it is not intended as a general authorisation to further process data in all cases for historical, statistical or scientific purposes. Just like in any other case of further use, all relevant circumstances and factors must be taken into account when deciding what safeguards, if any, can be considered appropriate and sufficient. In addition, as in other situations, a separate test must be carried out to ensure that the processing has a legal basis in one of the grounds listed in Article 7 and complies with other relevant requirements of the Directive.

As noted in recital 29, the purpose of the safeguards is typically to 'rule out' that the data will be used to support measures or decisions regarding any particular individual. The term ‘rule out’ suggests that the safeguards should indeed be strong enough to exclude or at least minimise any risks to the data subjects.[82]

In order to ensure appropriate safeguards, the term 'measures or decisions' should be interpreted in the broadest sense. First, they should be understood to cover any 'measures or decisions' irrespective of whether they are taken by the controller or by anyone else. Second, 'measures or decisions' do not only cover formal decisions and measures in a formal procedure. In other words: any relevant impact on particular individuals - either negative or positive - should be avoided.

Under the current framework, it is up to each Member State to specify what safeguards may be considered as appropriate. This specification is typically provided in legislation, which could be precise (e.g. national census or other official statistics) or more general (most other kinds of statistics or research). In the latter case, this leaves room for professional codes of conduct and/or further guidance released by the competent data protection authorities.

---

[81] Pursuant to Article 6(1)(b) further processing of data for these purposes 'shall not be considered as incompatible provided that Member States provide appropriate safeguards'. Recital 29 further provides that 'these safeguards must in particular *rule out* the use of the data in support of measures or decisions regarding any particular individual'. Article 11(2) and recital 40 with regard to notice to data subjects are also relevant in this respect. Recital 40 provides that 'it is not necessary to [provide notice to the data subject] if the data subject already has the information' and that 'there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate effort, which could be the case *where processing is for historical, statistical or scientific purposes*; whereas, in this regard, the number of data subjects, the age of the data, and any *compensatory measures* adopted may be taken into consideration'

[82] In this respect it is worth recalling Article 9(3) of Convention 108, referred to in footnote 19, which also allows further use for statistics or scientific research but only in cases where ‘there is obviously no risk of an infringement of the privacy of the data subjects’.

Diversity of the situations covered and the safeguards to be applied

The provision covers a broad range of processing activities. Whereas some processing may serve important public interests, there are many other types of activities - outside the scope of 'public interests' - that may also fall under this provision.

'Statistical purposes' in particular, cover a wide range of processing activities, from commercial purposes (e.g. analytical tools of websites or big data applications aimed at market research[83]) to public interests (e.g. statistical information produced from data collected by hospitals to determine the number of people injured as a result of road accidents).

Processing for 'historical' purposes can also have specific characteristics and this may require a different set of safeguards. Member States often have specific laws governing access to national archives, archives on recent history of particular interest (such as archives evidencing oppressive regimes), and court files kept by the judiciary. These laws often call for safeguards beyond anonymisation or pseudo-anonymisation, including appropriate security measures and restrictions on access.

Although historians are often more interested in facts than in the precise identity of the individuals concerned (and for these cases anonymised or pseudonymised data may often be appropriate), in some cases, the research may focus on specific individuals, such as historical figures or family history. It may also be that researchers wish to use historical data that pose little or no risk to persons concerned, due to the lapse of time since the data were collected.[84]

As regards 'scientific' purposes, there may also be a need to access different kinds of data. Some research may require raw microdata, which are only partially anonymised or pseudonymised. In some cases, the research purposes involved can only be fulfilled if the pseudonymisation is reversible: for example, when research subjects need to be interviewed at a later stage in a longitudinal study. Other research, however, may require less detail, and therefore allow a higher level of aggregation and anonymisation. Further, publication of research results should, as a rule, be possible in such a way that only aggregated and/or otherwise fully anonymised data will be disclosed.

Finally, as will be shown below, it will also be relevant to distinguish between situations where the further processing will be carried out by the initial data controller and those where personal data will be transferred to a third party. In this context, some research projects may require very precise protocols (rules and procedures) to ensure a strict functional separation between participants in the research and outside stakeholders. This may include technical and organisational measures, such as securely key-coding the personal data transferred and prohibiting outside stakeholders from re-identifying data subjects (as in the case of clinical trials and pharmaceutical research) and possible other measures.

---

83 For big data and open data, see Section III.2.5 and Annex 2.

84 In this context, however, it should be kept in mind that some data (for example, criminal records) may continue to have an adverse impact on a data subject even after many decades, and may, for example, continue to stigmatise an individual and hinder his/her rehabilitation. Moreover, information that a deceased individual has been a secret agent or collaborator of an oppressive regime, a paedophile, perpetrator of crimes, suffered from a mental illness giving rise to a stigma, or suffered from a hereditary disease, may also have a negative impact on the family (e.g. surviving spouse, children, or other descendants) of the deceased individual.

Considering the diversity of potential situations, it is all the more important to once again follow the generally applicable multi-factor approach in order to identify the appropriate safeguards.

The concept of 'functional separation'

When it comes to the safeguards to be adopted, the notion of functional separation may be of particular relevance. This means that data used for statistical purposes or other research purposes should not be available to 'support measures or decisions' that are taken with regard to the individual data subjects concerned (unless specifically authorized by the individuals concerned). To comply with this requirement, controllers need to guarantee the security of the data, and take all other necessary technical and organisational measures to ensure functional separation.

As will be discussed later, full or partial anonymisation, in particular, can be relevant to the safe use or sharing of data within organisations, particularly large ones with diverse functions. When full anonymisation and use of aggregated data (at a sufficiently high level of aggregation) are not possible, data will often at least need to be partially anonymised (e.g. pseudo-anonymised, key-coded, and stripped of direct identifiers) and additional safeguards may also be required, as will be discussed below.

Different scenarios require different safeguards

Once again, it is helpful to distinguish different scenarios for further analysis:

- Scenario 1: unidentifiable personal data: data are anonymised or aggregated in such a way that there is no remaining possibility to (reasonably) identify the data subjects.

- Scenario 2: indirectly identifiable personal data: lower level of aggregation, partial anonymisation, pseudonymisation or key-coded data.

- Scenario 3: situations where directly identifiable personal data are needed due to the nature of the research.[85]

As a general rule, this leads to the following considerations:

1) Full anonymisation (including a high level of aggregation) is the most definitive solution. It implies that there is no more processing of personal data and that the Directive is no longer applicable.[86]

---

[85] Article 2(a) of the Directive defines 'personal data' as 'any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity'. See also Opinion 4/2007 on the concept of personal data, adopted on 20.06.2007 (WP 136), especially on p. 12-21 (discussing 'pseudonymised data', 'key-coded data' and 'anonymous data' on p. 18-21). The issue of information '*relating to*' an individual is discussed on p. 9-12.

[86] The term 'full' or 'complete anonymisation' is used in this Opinion to refer to data that can no longer be considered 'personal data' under Article 2(a) of the Directive. See also Opinion 4/2007 of the WP29 referred to in the previous footnote.

Full anonymisation may, however, not be possible due to the nature of the processing (e.g. where there may be a need to re-identify the data subjects or a need to use more granular data that, as a side effect, may allow indirect identification). Furthermore, anonymisation is increasingly difficult to achieve with the advance of modern computer technology and the ubiquitous availability of information. Full anonymisation would also require, for instance, that any reasonable possibility of establishing a link with data from other sources with a view to re-identification be excluded. However, re-identification of individuals is an increasingly common and present threat.[87] In practice, there is a very significant grey area, where a data controller may believe a dataset is anonymised, but a motivated third party will still be able to identify at least some of the individuals from the information released.[88] Addressing and regularly revisiting the risk of re-identification, including identifying residual risks, therefore remains an important element of any solid approach in this area.

2) Partial anonymisation or partial de-identification may be the appropriate solution in some situations[89] when complete anonymisation is not practically feasible. In these cases, various techniques (including pseudo-anonymisation[90], key-coding[91], keyed-hashing, using rotating salts, removal of direct identifiers and outliers, replacing unique IDs, introduction of 'noise', and others) should be used to reduce the risk that data subjects can be re-identified, and subsequently, that any measures or decisions can be taken in their regard. In addition, there will also often be a need to complement these techniques with other safeguards in order to adequately protect the data subjects.[92] These include data minimisation, as well as appropriate organisational and technical measures, including effective 'data silo'-ing, to ensure functional separation.

3) Directly identifiable personal data may be processed only if anonymisation or partial anonymisation is not possible without frustrating the purpose of the processing, and further provided that other appropriate and effective safeguards are in place.

---

87 See, for example, 'Transparent Government, Not transparent Citizens', a report prepared for the UK Cabinet office by Kieron O'Hara of Southampton University in 2011, in which the author warned of the ability to identify individuals from anonymised data, using, among others, 'jigsaw identification' and saying that there are no complete technical solutions to the de-anonymisation problem. Available at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/transparency-and-privacy-review-annex-b.pdf

88 At present, there is no comprehensive guidance on anonymisation at European level. The WP29 is currently preparing a guidance document on open data, which will address, among other things, some issues related to anonymisation. The WP29 may also provide further guidance in due course on anonymisation techniques more generally. These documents are expected to be adopted in the course of 2013. For guidance at the national level, see the 'Anonymisation code of practice' issued by the Information Commissioner's Office in the UK in November 2012, available at: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx.

89 Whether a certain degree of partial anonymisation or de-identification is sufficient as a safeguard depends on the context, including all relevant criteria mentioned in Section III.2.2.

90 It is important to emphasize that partial anonymisation is not a synonym for pseudo-anonymisation or for key-coding personal data. In addition to pseudo-anonymisation (of which key-coding is a classic example), additional anonymisation techniques may often need to be used.

91 In this context the WP29 emphasises the importance of the security of key-coding measures. For example, in case of clinical trials, the use of initials and date of birth as coding mechanisms should be avoided because this method would allow for a fairly easy identification of patients. A better practice is to apply more secure key-coding measures, for example, randomly allocated numbers.

92 In any event, key-coded or otherwise pseudonymised, or partially anonymised personal data - so long as the possibility of re-identification exists, with reasonable means, to be applied by the controller or any third party - continues to be considered personal data, and thus, requires appropriate protection.

Importance of additional safeguards beyond anonymisation

The above analysis shows that anonymisation is a key tool in achieving functional separation, and although it is highly recommended, it does have its challenges and limits. The analysis also shows that once the first assessment has been completed in terms of the possibilities and limits of effective de-identification, the second step of applying additional safeguards will often need to follow.

As essential guidance, it should be kept in mind that the easier the data subject can be identified, the more additional safeguards will be needed. That said, the compatibility assessment cannot be reduced to these two factors and steps alone: as in any other case, it must also include all the other relevant key factors mentioned in Section III.2.2. For example, in general, the more sensitive the data and the more consequential potential adverse impact on the data subject if identified would be, the more should be done to limit the possibilities of re-identification and the more additional safeguards may be required.

Among the appropriate safeguards which may bring additional protection to the data subjects, the following could be considered:

- taking specific additional security measures (such as encryption);
- in case of pseudonymisation, making sure that data enabling the linking of information to a data subject (the keys) are themselves also coded or encrypted and stored separately;
- entering into a trusted third party (TTP) arrangement in situations where a number of organisations each want to anonymise the personal data they hold for use in a collaborative project;[93]
- restricting access to personal data only on a need-to-know basis, carefully balancing the benefits of wider dissemination against the risks of inadvertent disclosure of personal data to unauthorised persons. This may include, for example, allowing read only access on controlled premises. Alternatively, arrangements could be made for limited disclosure in a secure local environment to properly constituted closed communities. Legally enforceable confidentiality obligations placed on the recipients of the data, including prohibiting publication of identifiable information, are also important. It is important to note that in high-risk situations, where the inadvertent disclosure of personal data would have serious or harmful consequences for individuals, even this type of access or restriction may not be suitable.

In addition,

- further processing of personal data concerning health, data about children, other vulnerable individuals, or other highly sensitive information should, in principle, be permitted only with the consent of the data subject[94];
- any exceptions to this requirement for consent should be specified in law, with appropriate safeguards, including technical and organisational measures to prevent undue impact on the data subjects (in case of doubt, the processing should be subject to prior authorisation of the competent data protection authority); exceptions should only apply with regard to

---

[93] This model is increasingly being used to facilitate the large-scale research using data collected by a number of organisations. Trusted third parties can be used to link datasets from separate organisations, and then create anonymised records for researchers.

[94] The processing should also respect other relevant legislation (e.g. relating to clinical trials).

research that serves an important public interest, and only if that research cannot possibly be carried out otherwise.[95]

Articles 6(2) and 83 of the proposed Data Protection Regulation

Articles 6(2) and 83 of the proposed Data Protection Regulation address the issue of further use for historical, statistical or scientific research purposes.[96] These articles take a somewhat similar approach to the above analysis by requiring anonymisation, or if that is not possible, depending on the nature of the processing, at least some degree of de-identification. However, they also differ in some crucial ways.

Article 6(2) of the proposed Data Protection Regulation (under the heading: 'lawfulness of processing') provides that '[p]rocessing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83'.

Article 83(1) in turn provides that 'within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if: (a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject; (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner'.

A crucial difference of this approach compared to the analysis provided in this Opinion is that Articles 6(2) and 83 do not mention any further safeguards, such as additional technical or organisational measures to ensure functional separation, or other safeguards that would contribute to transparency or choice. In addition, this provision does not imply or make clear that further use for historical, statistical or scientific research purposes is subject to the same general multi-factor compatibility assessment under Section III.2.2 as all other further use.[97]

Further, these provisions also confuse two different concepts: the notion of 'compatibility' under Article 5(b) of the proposed Data Protection Regulation and the notion of 'lawful ground' under Article 6. As explained earlier, these two requirements are cumulative. Processing of personal data for the purposes of historical, statistical or scientific research must be based on one of the legal grounds (points a to f), in any event. Article 83 may help assess under what conditions further use may be compatible (and more generally, what safeguards must be applied in case of any processing for historical, statistical or scientific purposes) but cannot provide a substitute for an appropriate lawful ground for the processing.

For these reasons, the WP29 recommends that the Commission and the legislators reconsider the language of both Articles 6(2) and 83 of the proposed Data Protection Regulation (see also Section IV.2).

---

95 See also amendments 334-342 of the Draft report of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) dated 16.1.2013 (2012/0011(COD) ('Draft LIBE Committee Report').

96 See also Article 81(2) on the further use of health data.

97 Appropriate safeguards play a key role in this assessment, but which safeguards are appropriate will depend on the context, the nature of the data and the impact of further processing on the data subjects, if measures to ensure functional separation are not fully effective. See also Articles 11(2) and 13(2) of the current Directive.

III.2.4. Article 13 of the e-Privacy Directive on unsolicited communications

The e-Privacy Directive complements the Directive by providing specific provisions for the electronic communication sector, notably for the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks.[98] One of those specifications relates to the subject of this Opinion and helps to illustrate the general assessment of compatibility as discussed above.

Article 13 of the e-Privacy Directive sets forth a basic rule of prior ('opt-in') consent for certain kinds of unsolicited communications (i.e. the use of automatic calling systems, fax and email) for the purposes of direct marketing. An exception is created in Article 13(2) for existing relationships, i.e. cases where a business has previously provided a product or service to an individual, in the context of which the individual provided his/her email address, and where an unsolicited email is subsequently sent by the controller to advertise its own 'similar' products or services. Unsolicited emails sent under this exception must, however, provide the customer with an opportunity to 'opt-out' of future emails.

This provision illustrates how the reasonable expectations of the data subject and the context of the data collection may impact on the assessment of both the legal grounds and the compatibility of the processing. The requirements for data controllers are different depending on the context in which personal data have been collected: in principle, the use of automated calling systems, fax and e-mail for direct marketing is subject to the prior consent of the data subject. A specific safeguard is therefore required to ensure the lawfulness of the processing. This is not the case, however, when the data subjects' details have been obtained from the customer at the time they were sold a product or service, and when the purpose of the processing is the direct marketing of products or services similar to those bought by the customer, provided the marketing is done by the controller itself and for its own products and services.

The further use of data for marketing purposes may in both cases be lawful, but subject to different safeguards, depending on the context of the data collection and on the relationship between the data subjects and the controllers, as well as their expectations concerning this relationship. It is worth noting that Article 13 is apparently based on the notion that some means of communication are inherently more intrusive than others and should therefore only be allowed subject to additional safeguards.

More traditional means of direct marketing, such as the use of surface mail for the sending of personalised messages for commercial, political or charitable purposes, remain outside the scope of Article 13 and should therefore be considered under the provisions of the general Directive.

In the light of the general analysis in Section III.2.2 of this Opinion it would seem that at least some distinction should be made between:

- direct mailings in the context of existing relationships to provide information on new offerings or other relevant opportunities;

---

[98] Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002, p. 37, as amended by Directive 2009/136/EC of the European Parliament and the Council of 25 November 2009, OJ L 337, 18.12.2009, p. 11.

- similar direct mailings, but now based on sensitive personal data, and/or automated profiles using more intrusive data analytics tools[99];
- the sharing of information with data brokers or other third parties in order to develop more effective segmentation in direct mailings.

In this context, it should also be noted that Article 14(b) of the Directive provides for the right for data subjects to object - free of charge - to *any processing* of their personal data for the purposes of direct marketing, without further consideration of the circumstances. This *absolute* right to object can only serve its purpose, subject to adequate transparency as to its existence and the ways to exercise it. It is therefore essential that reasonable infrastructure (such as, for example, a 'Robinson list' or other mail preference service) be created and maintained so that this right can be effectively exercised.

III.2.5. Big data and open data

Big data

Big data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed (hence the name: analytics[100]) using computer algorithms. Big data can be used to identify more general trends and correlations but it can also be processed in order to directly affect individuals.

With all its potential for innovation, big data may also pose significant risks for the protection of personal data and the right to privacy. How the general compatibility assessment and the specific provisions on 'further processing for historical, statistical or scientific purposes' can be applied to big data, including appropriate safeguards that may help data controllers meet the compatibility test, will be further discussed in Annex 2.

Open data

Open data projects take accessibility of information processed by public bodies to a whole new level. Such projects often involve (i) making entire databases available (ii) in standardised electronic format (iii) to any applicant without any screening process (iv) free of charge and (v) for any commercial or non-commercial purposes under an open license. This new form of accessibility is the main purpose of open data, but it is not without risks if applied indiscriminately and without appropriate safeguards.

While it is not easy to reconcile the two concerns of unrestricted information reuse and purpose limitation, it is important to note that any information relating to an identified or identifiable natural person, be it publicly available or not, constitutes personal data. Moreover, the mere fact that such data has been made publicly available does not lead to an exemption from data protection law. The reuse of personal data made publicly available by the public sector, thus remains subject in principle to the relevant data protection law.

---

[99] On big data and analytics, see further Section III.2.5 and Annex 2.
[100] Analytics is the discovery and communication of meaningful patterns in data.

Annex 2 will also analyse and illustrate how the general compatibility assessment, as well as the specific provisions on 'further processing for historical, statistical or scientific purposes' can be applied to open data, and recommend appropriate safeguards that may help public sector bodies that release data, and data controllers who reuse it, to meet the compatibility test.

III.2.6. Consequences of incompatibility

Incompatible processing cannot be remedied simply by adopting a new legal ground

Failure to comply with the compatibility requirement set forth in Article 6(1)(b) of the Directive has serious consequences: the processing of personal data in a way incompatible with the purposes specified at collection is unlawful and therefore not permitted.

In other words, the data controller cannot simply consider the further processing as a new processing activity disconnected from the previous one and circumvent this prohibition by using one of the legal grounds in Article 7 to legitimise the processing. As explained above, the requirements under Article 6 and Article 7 are cumulative: both must be met simultaneously.

Legalising an otherwise incompatible data processing activity simply by changing the terms of a contract with the data subject, or by identifying an additional legitimate interest of the controller, would go against the spirit of the purpose limitation principle and remove its substance.[101]

Incompatibility under the proposed Data Protection Regulation

To be clear on this point is all the more important as Article 6(4) of the proposed Data Protection Regulation proposes to provide a very broad exception from the requirement of compatibility, which would severely restrict its applicability. The text proposed by the Commission provides that '[w]here the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract'.[102]

This text would, in effect, mean that it would always be possible to remedy the lack of compatibility by simply identifying a new legal ground for the processing. The only legal ground which could not in itself be sufficient to compensate for incompatibility would be the 'legitimate interest' of the controller under point (f).

---

[101] As explained before, this does not mean that the initial purpose of the processing operation can never change: in some situations, after assessment of all relevant factors, including the availability of safeguards and/or the availability of an appropriate new legal basis to compensate for the change of purpose, the controller may find that further processing for a changed purpose can comply both with the compatibility requirement and the requirement of a legal ground under Article 7.

[102] Article 7 of the Directive provides that personal data may be processed only on the basis of one of six grounds: (a) consent; (b) performance of a contract; (c) compliance with a legal obligation; (d) protection of the vital interests of the data subject; (e) a task carried out in the public interest or in the exercise of official authority; (f) legitimate interests pursued by the controller or by a third party (except where such interests are overridden by the fundamental rights and freedoms of the data subject).

The WP29 therefore recommends that the proposed paragraph 4 should be deleted. This is because the prohibition of incompatible use and the requirement of a legal basis under Article 7 of the Directive are cumulative requirements. Therefore, for a change of purpose, one of the legal grounds (points a to f) needs to apply anyway. The Directive, which is currently in effect, does in principle not allow for a change of purpose without a favourable outcome of a compatibility assessment, and this level of protection should be maintained in the proposed Data Protection Regulation as well.[103]

Enforcement of the purpose limitation principle

Data protection authorities have an essential role in ensuring compliance with this principle. In accordance with the national law implementing the Directive, they have effective powers of intervention, including the ordering of blocking, erasure or destruction of data, or imposing a ban on processing. Action can also (often in a first phase) consist of warning or admonishing the controller, while legal proceedings may also remain a possible option.

Depending on national law, sanctions can also consist of administrative fines. The proposed Data Protection Regulation aims at harmonising this aspect of enforcement procedures, with highest potential fines of up to 1 000 000 euros or 2% of the annual turnover[104].

III.3. Exceptions under Article 13 of the Directive

The scope of the purpose limitation principle can only be restricted in specific cases as defined in Article 13 of the Directive (or Article 15 of the e-Privacy Directive where applicable). This means that if the compatibility assessment shows that the processing is incompatible, the only grounds on which it can be carried out must be based on those specific provisions.

Article 13 of the Directive provides that 'Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Article 6 (1) … when such a restriction constitutes a necessary measure to safeguard ... national security; defence; public security; the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; an important economic or financial interest of the Member State or the European Union ... ; a monitoring, inspection or regulatory function ... and the protection of the data subject or of the rights and freedoms of others ....'.[105]

The limited scope of exceptions confirms that it is not possible to legitimise incompatible processing of personal data simply by relying on one of the grounds listed in Article 7. This is all the more so since the legislative measures adopted under Article 13 of the Directive must be interpreted restrictively as they are introduced by way of exception to the general

---

[103] See Amendment 103 of the Draft LIBE Committee Report.

[104] See Article 79 of the proposed Data Protection Regulation. In this respect, the WP29 highlights that Article 79 as proposed appears to have a gap and not cover the purpose limitation principle (for that matter, it also appears not to cover, or not cover in full, the other crucial data quality principles listed in paras (a) to (f). This should be remedied by making Article 79 either less detailed and less prescriptive or by specifically adding Article 5 to the provisions for which the highest fines may - in some situations - be appropriate. In this perspective, see also amendment 321 of the Draft LIBE Committee Report.

[105] See also Article 9 of Convention 108.

principles of Article 6. Therefore, a legislative measure providing for a legal obligation under Article 7 would not necessarily be sufficient to make processing compatible.

While the legislator has an essential role to play, it is also subject to a number of strict conditions:
- First, the measure must be aimed at safeguarding specific and important public interests, as listed above, including public security, important economic or financial interests of the Member State or the European Union, and crime prevention.
- Second, a qualified test must be applied, to ensure that the legislative measure meets the criteria that allow derogating from a fundamental right. There are two aspects to this test: on the one hand the measure must be sufficiently clear and precise to be foreseeable, and on the other hand it must be necessary and proportionate, consistent with the requirements developed by the European Court of Human Rights[106].

In practice, it is not sufficient for such a law to only mention the final objectives of the legislative measure and designate the controller of the processing. It should, at least, also specifically describe the objectives of the relevant data processing, the categories of personal data to be processed, the specific purposes and means of processing, the categories of persons authorised to process the data, the procedure to be followed for the processing, and the safeguards against any arbitrary interference by public authorities.[107]

IV. Conclusions

This Opinion provides an analysis of the concept of purpose limitation. The objective of this exercise is twofold. First, it aims to clarify the purpose limitation principle and offer guidance on its practical application under the current legal framework. Second, it highlights areas for further improvements and formulates policy recommendations to assist policy makers as they consider changes to the current data protection legal framework.

IV.1. Analysis of the current legal framework

The concept of purpose limitation plays a crucial role in the application of the Directive. It is an essential first step in applying data protection laws since it constitutes a pre-requisite for other data quality requirements including the adequacy, relevance, proportionality and accuracy of the data collected, along with the rules surrounding data retention periods. It contributes to transparency, legal certainty and predictability and aims to protect the data subjects by setting limits on how controllers are able to use their data. At the same time, it is also designed to offer some degree of flexibility for the data controller.

The concept of purpose limitation has two main building blocks: the personal data must be collected for 'specified, explicit and legitimate' purposes (purpose specification) and not be 'further processed in a way incompatible' with those purposes (compatible use).

---

[106] See Section II.1 on ‘Brief History’.
[107] See Annex 4, in particular, examples 17, 18, 19, 20, 22.

First building block: 'specified, explicit and legitimate' purposes

With regard to purpose specification, the WP29 highlights the following key considerations:

- Purposes must be *specific*. This means that - prior to, and in any event, no later than the time when the collection of personal data occurs - the purposes must be precisely and fully identified to determine what processing is and is not included within the specified purpose and to allow that compliance with the law can be assessed and data protection safeguards can be applied.

- Purposes must be *explicit,* that is, clearly revealed, explained or expressed in some form in order to make sure that everyone concerned has the same unambiguous understanding of the purposes of the processing irrespective of any cultural or linguistic diversity. Purposes may be made explicit in different ways.

- There may be cases of serious shortcomings, for example where the controller fails to specify the purposes of the processing in sufficient detail or in a clear and unambiguous language, or where the specified purposes are misleading or do not correspond to reality. In any such situation, all the facts should be taken into account to determine the actual purposes, along with the common understanding and reasonable expectations of the data subjects based on the context of the case.

- Purposes must be *legitimate*. Legitimacy is a broad requirement, which goes beyond a simple cross-reference to one of the legal grounds for the processing referred to under Article 7 of the Directive. It also extends to other areas of law and must be interpreted within the context of the processing. Purpose specification under Article 6 and the requirement to have a lawful ground for processing under Article 7 of the Directive are two separate and cumulative requirements.

- If personal data are further processed for a different purpose
  - the new purpose/s must be specified (Article 6(1)(b)), and
  - it must be ensured that all data quality requirements (Articles 6(1)(a) to (e)) are also satisfied for the new purposes.

Second building block: compatible use

- Article 6(1)(b) of the Directive also introduces the notions of 'further processing' and 'incompatible' use. It requires that further processing must not be incompatible with the purposes for which personal data were collected. The prohibition of incompatible use sets a limitation on further use. It requires that a distinction be made between further use that is 'compatible', and further use that is 'incompatible', and therefore, prohibited.

- By prohibiting incompatibility rather than requiring compatibility, the legislator seems to give some flexibility with regard to further use. Further processing for a different purpose does not necessarily and automatically mean that it is incompatible, as compatibility needs to be assessed on a case-by-case basis.

- In this context, the WP29 emphasises that the specific provision in Article 6(1)(b) of the Directive on 'further processing for historical, statistical or scientific purposes' should be seen as a specification of the general rule, while not excluding that other cases could also

be considered as 'not incompatible'. This leads to a more prominent role for different kinds of safeguards, including technical and organisational measures for functional separation, such as full or partial anonymisation, pseudonymisation, aggregation of data, and privacy-enhancing technologies.

Compatibility assessment

- The nature of the compatibility assessment is decisive. In comparison to a purely formal assessment which focuses on declared purposes and therefore risks being too rigid, a substantive assessment takes into account the way purposes should be understood. This substantive assessment offers more flexibility while at the same time effectively safeguarding the personal data.

- A substantive compatibility assessment requires an assessment of all relevant circumstances of the case in order to determine whether any further use may be considered compatible. Account should be taken in particular of the following key factors:

  - the relationship between the purposes for which the personal data have been collected and the purposes of further processing;
  - the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;
  - the nature of the personal data and the impact of the further processing on the data subjects;
  - the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

Specific applications of the compatibility assessment

- The approach and general framework for the compatibility assessment outlined above should also apply to 'further processing for historical, statistical or scientific purposes' and with regard to Article 13 of the e-Privacy Directive on unsolicited communications. These provisions are true specifications of the general framework for a compatibility assessment.

- The WP29 also calls attention to some of the challenges in applying the compatibility test to big data and open data. Here, perhaps even more so than elsewhere, there is a need for a rigorous but balanced and flexible application of the compatibility test to ensure it can be applied in our modern, networked society.

Consequences of incompatibility

- Failure to comply with the compatibility requirement set forth in Article 6(1)(b) of the Directive has serious consequences: the processing of personal data in any way that is incompatible with the purposes specified at collection is unlawful and therefore not permitted.

- In other words, the data controller cannot simply consider the further processing as a new processing activity disconnected from the previous one, and circumvent this prohibition by using one of the legal grounds in Article 7 to legitimise the processing.

Exceptions under Article 13 of the Directive

- The scope of the purpose limitation principle can only be restricted in specific cases as defined in Article 13 of the Directive (or Article 15 of the e-Privacy Directive where applicable). This means that if the compatibility assessment shows that the processing is incompatible, the only grounds on which it can be carried out must be based on those provisions.

- A legislative measure providing for a legal obligation under Article 7 would not *per se* be sufficient to make processing compatible. While the legislator has an essential role to play, it is also subject to a number of strict conditions:

  - First, the measure must be aimed at safeguarding specific and important public interests.

  - Second, a qualified test must be applied, to ensure that the legislative measure meets the criteria that allow derogating from a fundamental right: The measure must be sufficiently clear and precise to be foreseeable, and it must be necessary and proportionate.

IV.2 Recommendations for the future

The WP29 hopes that the above analysis clarifies the scope and functioning of purpose limitation, which is a key principle of data protection. This analysis also has consequences for the future as even if the principle of purpose limitation itself seems stable, its precise meaning, including any exceptions to it, is now subject to discussion.

In particular, Article 6(4) of the proposed Data Protection Regulation, attempts to provide a very broad exception from the requirement of compatibility, which would severely restrict its applicability. This text would in effect mean that it would always be possible to remedy the lack of compatibility by simply identifying a new legal ground for the processing. The only legal ground which could not in itself be sufficient to compensate for incompatibility would be the 'legitimate interest' of the controller under point (f).

These new provisions would, if adopted, risk eroding this key principle. The WP29 therefore recommends that the proposed paragraph 4 should be deleted. This is because the prohibition of incompatible use and the requirement of a legal basis under Article 7 of the Directive are cumulative requirements. Therefore, for a change of purpose, one of the legal grounds (points a to f) needs to apply anyway. The Directive, which is currently in effect, does in principle not allow for a change of purpose without a favourable compatibility assessment, and this level of protection should be maintained in the proposed Data Protection Regulation as well.

Further, to complement the existing general and concise provisions on the purpose limitation principle, and to provide for more legal certainty, the WP29 recommends the adoption of the provisions set out in Annex 1 to this Opinion.

The proposed provisions aim to provide a non-exhaustive list of the relevant factors that should be assessed to determine whether any further use may be considered compatible. Although this presentation of key factors is not fully exhaustive, it attempts to highlight the

typical factors that should be considered in a balanced approach: neither too general so as to be meaningless, nor too specific so as to be overly rigid.

Finally, and for similar reasons, the WP29 proposes to delete Article 6(2), which attempts to provide a new legal ground for all processing for historical, statistical or scientific research (subject to the conditions and safeguards referred to in Article 83 but not subject to a broader compatibility assessment). This provision may be replaced by a similar, but more nuanced provision in Article 5, which discusses the 'principles relating to personal data processing'. A proposed amendment to this effect is also set forth in Annex 1 to this Opinion.

Additional text in Article 83 or in appropriate recitals could help clarify what safeguards may be required in case of processing for historical, statistical or scientific purposes. These safeguards could apply both for initial processing and further processing for these purposes. However, concrete recommendations for specific provisions would go beyond the scope of this Opinion.

Annex 1: Proposed amendments

Article 5 ***Principles relating to personal data processing***	
Personal data must be: (a) (.....) (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c-f) (.....)	***1.*** Personal data must be: (a) (.....) (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c-f) (.....)
	2. When assessing whether further processing of personal data is incompatible with the purposes for which those data have been collected, within the meaning of point (b) of paragraph 1, account shall be taken in particular of: ***(a) the relationship between the purposes for which the personal data have been collected and the purposes of further processing;*** ***(b) the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;*** ***(c) the nature of the personal data and the impact of the further processing on the data subjects;*** ***(d) the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.***
	3. Further processing of personal data which is necessary for the purposes of historical, statistical or scientific research, shall not be considered as incompatible, subject to the conditions and safeguards referred to in Article 83 and provided that appropriate measures are applied to prevent any undue impact on the data subjects.

Justification

To complement the existing provision on purpose limitation, and to provide for more legal certainty, a list of relevant factors should be taken into account when assessing whether any further processing is compatible with the purposes of data collection. A specific provision on historical, statistical or scientific research is required to ensure that appropriate safeguards will continue to be applied in this context.

Article 6 ***Lawfulness of processing***	
1. Personal data shall be lawful only if and to the extent that at least one of the following applies: (a) - (f) (.....)	***No change***
2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.	***Deleted***
3. (.....)	***2. (.....)***
4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms or general conditions of a contract.	***Deleted***
4. (.....)	***3. (.....)***

Justification

The deletion of paragraphs 2 and 4 ensures that the requirement of compatible use in Article 5 and the lawfulness of processing under Article 6 continue to function as cumulative requirements and that the current level of protection is maintained in the proposed Data Protection Regulation.

Annex 2: Big data and open data

Big data

What is 'big data' and 'big data analytics'?

As briefly highlighted in Section III.2.5, 'Big data' refers to the exponential growth in availability and automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed using computer algorithms. Big data relies on the increasing ability of technology to support the collection and storage of large amounts of data, but also to analyse, understand and take advantage of the full value of data (in particular using analytics applications). The expectation from big data is that it may ultimately lead to better and more informed decisions.

There are numerous applications of big data in various sectors, including healthcare, mobile communications, smart grid, traffic management, fraud detection, marketing and retail, both on and offline. Big data can be used to identify general trends and correlations but its processing can also directly affect individuals. For example, in the field of marketing and advertisement, big data can be used to analyse or predict the personal preferences, behaviour and attitudes of individual customers and subsequently inform 'measures or decisions' that are taken with regard to those customers such as personalised discounts, special offers and targeted advertisements based on the customer's profile.[108]

What are the risks and challenges posed by big data to the right to the protection of personal data and to privacy?

Despite its potential for innovation, big data may also pose significant risks for the protection of personal data and the right to privacy. In particular, big data raises concerns about:

- the sheer scale of data collection, tracking and profiling, also taking into account the variety and detail of the data collected and the fact that data are often combined from many different sources;
- the security of data, with levels of protection shown to be lagging behind the expansion in volume;
- transparency: unless they are provided with sufficient information, individuals will be subject to decisions that they do not understand and have no control over;
- inaccuracy, discrimination, exclusion and economic imbalance (as will be discussed further below); and
- increased possibilities of government surveillance.

The type of analytics application used can lead to results that are inaccurate, discriminatory or otherwise illegitimate. In particular, an algorithm might spot a correlation, and then draw a statistical inference that is, when applied to inform marketing or other decisions, unfair and discriminatory. This may perpetuate existing prejudices and stereotypes, and aggravate the problems of social exclusion and stratification.

---

[108] Currently, the fundamental business model of the Internet appears to be financing products and services with targeted advertisements: the value of these ads directly correlates with the amount and richness of the information collected from the users. See Opinion 2/2010 of 22 June 2010 of the WP29 on online behavioural advertising (WP 171).

Further, and more broadly, the availability of large datasets and sophisticated analytics tools used to examine these datasets may also increase the economic imbalance between large corporations on one hand and consumers on the other.[109] This economic imbalance may lead to unfair price discrimination with regard to the products and services offered, as well as highly intrusive, disruptive, and personalised targeted advertisements and offers. It could also result in other significant adverse impacts on individuals, for example, with regard to employment opportunities, bank loans, or health insurance options.

What safeguards would make the further use of personal data for analytics compatible?

As in other cases of compatibility assessment, all relevant factors described in Section III.2.2 should be considered, including the relationship between the purposes, the context of collection, the reasonable expectations of the data subjects, the nature of the personal data and the impact on the data subjects. It is also important to assess the safeguards adopted to ensure fair processing and to prevent any undue impact. In addition, the specific provisions relating to 'historical, statistical or scientific purposes'[110] are also relevant.

In order to identify what safeguards are necessary, it may be helpful to make a distinction between two different scenarios. In the first one, the organisations processing the data want to detect trends and correlations in the information. In the second one, the organisations are interested in individuals.

In the first scenario, the concept of *functional separation*[111] is likely to play a key role, and the extent to which this may be achieved could be an important factor in deciding whether further use of the data for (marketing or other) research can be considered compatible. In these cases, data controllers need to guarantee the confidentiality and security of the data, and take all necessary technical and organisational measures to ensure functional separation.[112]

The second potential scenario is when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform 'measures or decisions' that are taken with regard to those customers.

In these cases, free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible. Importantly, such consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research.[113]

---

[109] This may be the case, irrespective of whether the companies involved have a monopoly or dominant position on the market. However, a dominant position clearly decreases the choices of data subjects to seek alternative service providers, and therefore, can be a relevant factor when measuring potential negative impact on a data subject.

[110] See Section III.2.3.

[111] See Section III.2.3.

[112] See Annex 4, in particular, example 15.

[113] It cannot be excluded, however, that in some cases, based on an informed debate of the societal benefits of some uses of big data, a Member State of the European Union may decide that due to compelling public interest, exceptions may be laid down in binding legislation (see Section III.3). In addition, in some cases, and subject to transparency and additional safeguards, tracking and profiling may also be permissible to prevent fraudulent use of the services offered.

For the consent to be informed, and to ensure transparency, data subjects/consumers should be given access to their 'profiles', as well as to the logic of the decision-making (algorithm) that led to the development of the profile. In other words: organisations should disclose their decisional criteria.[114] This is a crucial safeguard and all the more important in the world of big data.[115] More often than not, it is not the information collected in itself that is sensitive, but rather, the inferences that are drawn from it and the way in which those inferences are drawn, that could give cause for concern.[116] Further, the source of the data that led to the creation of the profile should also be disclosed.

Considering the risk of inaccurate inferences in particular, it is also crucial that data subjects/consumers are able to correct or update their profiles if they choose to do so. This may also benefit data controllers who will be able to base their (marketing or other) decisions on more accurate information.

Further, in many situations, safeguards such as allowing data subjects/customers to have direct access to their data in a portable, user-friendly and machine-readable format may help empower them, and redress the economic imbalance between large corporations on one hand and data subjects/consumers on the other. It would also let individuals 'share the wealth' created by big data and incentivise developers to offer additional features and applications to their users.[117]

For example, access to information about energy consumption in a user-friendly format could make it easier for households to switch tariffs and get the best rates on gas and electricity, as well as enabling them to monitor their energy consumption and modify their lifestyles to reduce their bills as well as their environmental impact.

Allowing data portability could enable businesses and data-subjects/consumers to maximise the benefits of big data in a more balanced and transparent way. It can also help minimise unfair or discriminatory practices and reduce the risks of using inaccurate data for decision-making purposes, which would benefit both businesses and data-subjects/consumers.

---

[114] See also Recommendation CM/Rec(2010)13 of 23 November 2010 of the Council of Europe Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

[115] See Annex 4, in particular, examples 9 and 10.

[116] One of the challenges in this respect is to ensure maximum disclosure while at the same time not infringing any legal requirements protecting trade secrets (and other intellectual property rights where relevant). However, we emphasise that any claims to the 'proprietary' nature of the information cannot provide an undue limitation to the requirements of disclosure under data protection law. Again, a balanced approach is needed, but one that fully respects fundamental rights.

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

Open data

What are the key challenges of open data to data protection?

As briefly outlined in Section III.2.5, open data projects take accessibility of information processed by public bodies to a whole new level. Such projects often involve (i) making entire databases available (ii) in standardised electronic format (iii) to any applicant without a screening process, (iv) free of charge, and (v) for any commercial or non-commercial purposes under an open license. This new form of accessibility is the main purpose of open data, and a key driver for innovation, but it is not without risks if applied indiscriminately and without appropriate safeguards.

In Opinion 7/2003, the WP29 provided guidance on the application of the current data protection framework to the reuse of public sector information (PSI) when it includes personal data. The WP29 Opinion shows that applying the current legal framework for data protection to PSI reuse raises a number of issues.

One of the main concerns is that in some cases it is not easy to implement the principle of purpose limitation effectively in case of PSI reuse. On the one hand, the very idea and driving force for innovation behind the concept of 'open data' and PSI reuse is that the information should be available for reuse for innovative new products and services, and thus, for purposes that are not previously defined and cannot be clearly foreseen. On the other hand, purpose limitation is a key data protection principle and requires that personal data that have been collected for a specific purpose should not at a later stage be used for another, incompatible purpose.

The challenge is to clearly define, in advance, the personal data that could be made publicly available, and to establish appropriate data protection safeguards, in order to ensure legal certainty while allowing innovation and reuse for any (lawful) purpose.

In this respect it is important to recall that any information relating to an identified or identifiable natural person, be it publicly available or not, constitutes personal data. Moreover, the mere fact that such data has been made publicly available does not lead to an exemption from data protection law. The reuse of personal data made publicly available by the public sector, thus remains subject, in principle, to the relevant data protection law.

Different scenarios require different safeguards

As in all other cases of compatibility assessment, all relevant factors described in Section III.2.2 should be considered. In order to identify what safeguards are necessary, it may again be helpful to make a distinction between different scenarios.

In some cases, the public sector body disclosing the data and the potential re-users of the data are interested in statistical use of the data: for example, they want to detect or present trends and correlations in the data. In other cases, there may be a 'market demand' for more granular data or for directly identifiable personal data and therefore, full anonymisation is not possible due to the nature and purposes of reuse. The different types of scenarios pose different challenges and require different safeguards.

As a general 'rule of thumb': while most data can be released for reuse in sufficiently aggregated or otherwise effectively anonymised form, open data initiatives will often not be appropriate for granular research data or for directly identifiable personal data, which will require a more cautious approach.

In many situations, anonymisation may help public sector bodies comply with data protection law whilst at the same time enabling them to make the necessary data available for reuse. Indeed, when this is possible, 'complete' anonymisation (and a high level of aggregation) of personal data is the most definitive solution to minimize the risks of inadvertent disclosure. Anonymisation should be done prior to making the data available for reuse - by the data controller or by a trusted third party.

However, as explained in Section III.2.3, re-identification of individuals is an increasingly common and present threat, and there is a significant grey area where it is difficult to assess in advance if re-identification may be possible. It is very important to take great care, at the initial stage of producing, disclosing and making available for reuse, any information derived from personal data, even when this is ultimately presented in the form of an anonymised dataset.[118]

For this reason, it is important to conduct an effective *data protection impact assessment* to decide what data may be made available for reuse, and at what level of anonymisation and aggregation. Such a robust and detailed impact assessment should be completed *prior* to the disclosure of information and making it available for reuse.

It is important that the analysis is not monopolized by any interested parties, and that the outcome is not pre-determined. Such an exercise therefore demands the participation of diverse stakeholders, including not only the data controller wishing to release the data, but also those demanding the data, and who therefore can provide context for the discussion, as well as representatives of individuals whose personal data are at stake.

When anonymised datasets are released, the risk assessment should include tests to assess re-identifiability, for example, penetration or 'pen' testing. Data controllers must be aware of the risk of re-identification and that this risk can change over time, e.g. powerful data analysis techniques that were once rare are now commonplace. Therefore, organisations should carry out a periodic review of their policy on the release of data and of the techniques used to anonymise it, based on current and foreseeable future threats.

Unless data can be fully anonymised, data protection law continues to apply. This means, among other things, that the public release of the information must be 'compatible' with the initial purposes of data collection under Article 6(1)(b) of the Directive. In addition, there must also be an appropriate legal basis for the processing under Article 7(a) to (f) of the Directive (for example, consent, or necessity to comply with the law).

With regard to directly identifiable personal data or not sufficiently anonymised datasets, in general, an even more cautious approach is needed. Once personal data are publicly available for reuse, it will be increasingly difficult, if not impossible, to have any form of control on the nature of potential further use, be it for historical, statistical, scientific or other purposes. This is especially the case if the data are available in digital, searchable and machine readable

---

[118] See Annex 4, in particular, example 14.

format and have been published on the internet, Hence, the selection of the information that will or will not be made publicly available becomes all the more important.

An in-depth data protection impact assessment must therefore be carried out, and - as a rule - alternatives should be sought. Making data available for reuse under an open license should be avoided unless it can be clearly demonstrated that compliance with data protection law can be effectively ensured.

That said, it cannot be excluded that a data protection impact assessment may conclude that the data may be opened up and made publicly available following the principles of 'open data'. For these cases, a rigorous licensing regime should be put in place, which must also be stringently enforced to ensure that the data will not be used for incompatible purposes (for example, for unsolicited commercial messages or otherwise in a way that the data subjects would find unexpected, inappropriate or otherwise objectionable).

Of course, publication of the data and any further use must, in these cases, always have to have an appropriate legal basis (e.g. consent or requirement of law) under Article 7(a) to (f) of the Directive.

Annex 3: Practical examples to illustrate purpose specification

The following examples illustrate the ways in which purpose specification is carried out in practice. The examples serve to highlight the diversity of situations and the flexibility and scalability needed for the effective implementation of the principle. They also identify common concerns and provide guidance on how to specify the purposes in different contexts.

As will be illustrated, the overall context, and in particular the reasonable expectations of the data subjects and the extent to which the parties concerned have a common understanding of the purposes of the processing, will determine, to a large extent, the level of detail necessary.

Examples 1-4: How purposes are specified needs to be adapted to the context

The level of detail to be provided may vary and needs to be adapted to the situation, as illustrated in the following examples:
- a local shop selling to local people in a small town and collecting only limited information about its customers would not need to specify the purposes in as much detail as a large retail company selling goods via a website all across Europe and using complex analytics to inform personalised offers and targeted advertisements;
- a social networking website operating across Europe will need to give particular attention to the way it specifies its purposes and the clarity of the information it provides, as it targets a broad user group across different cultures;
- if a data controller provides different services (for example, email, social networking, and photograph, video and music uploads), oversimplification should be avoided: sufficient granularity will be needed to make sure that all the different purposes are sufficiently clear for the users;
- a government website providing advice to the elderly or the mentally ill, a gaming website aimed at teenagers, and a government agency processing the personal data of asylum applicants, all need to take into consideration the respective age, special needs, nationality and culture of the individuals they are targeting.

Examples 5-6: More detail is needed in case of ambiguities and for processing beyond what is customary in a given context

In situations where the purposes of processing can be clearly derived from the context, usually less detail is required. However, even here, more precise and detailed information is necessary where ambiguities arise, as illustrated in the following cases:
- A small local trader is contracted to deliver and install a heating system at a customer's home, and to provide annual maintenance. The company collects information such as name, address, and telephone number of the customer in order to deliver and install the system, and to schedule annual maintenance. This could happen without extensive data protection disclosure to the data subjects as details may be implied from context, custom, and the nature of the underlying economic transaction. However, if any ambiguity arises, for example, as to whether the company also intends to send advertisements regarding its other services (or the services of other companies) to the customer, this should be specifically disclosed to the data subjects.[119]

[119] In this respect, see also Section II.2.4 on unsolicited communications.

- A candidate's CV is to be used by a potential employer for assessment of his/her professional experience in a current recruitment procedure. This is self-explanatory. However, if the CV is also intended to be used for internal mobility schemes, promotion exercises, or further recruitment procedures, this should be specified.

Examples 7-8: Purposes that are too vague or too general

Vague or general purposes such as 'improving users' experience', 'marketing', 'IT-security' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'. However, the degree of detail in which a purpose should be specified depends on the particular context in which the data are collected and the personal data involved. To illustrate:

- A small but exclusive boutique specialising in 'bespoke dresses and unique accessories' relies on word of mouth advertising. The only direct marketing tool it uses is a glossy annual catalogue that goes to the home addresses of its 200 customers in paper form. When signing up to the catalogue (and as clearly noted in the catalogue itself), the customers are informed that they can unsubscribe from the mailing list at anytime: in person, in writing, via email or by calling the shop. They are also advised that their data will not be shared with others and will only be used for sending the catalogue. This is sufficient specification of the purposes in this simple context.[120]
- The above example can be contrasted with that of a large retail company selling goods via a website all across Europe and using complex analytics to inform personalised offers and targeted advertisements. In this case, the purposes must be specified in a much more detailed and comprehensive way, including, among other things, 'the way in which' personal data are processed. The decisional criteria used for customer profiling must also be disclosed.[121]

Examples 9-10: Layered notice

A layered notice is often a workable way to provide key information to data subjects in a very concise and user-friendly manner, while also supplying additional information on the next 'layer' for the benefit of those who require further clarification.

- A government department uses a CCTV system to protect its buildings, and combines two methods to provide information to the public: (i) it places on-the-spot notices to immediately alert the public to the fact that monitoring takes place and provide them with essential information about the processing, and (ii) it posts on its intranet and internet sites the public version of its video-surveillance policy. This post is easy to find: the on-the-spot notice already contains the link and it can also be found by putting the name of the organisation and the words 'CCTV' or video-surveillance' in search engines. The notice is easy to read and provides comprehensive information.
- A website aimed at a teenage audience offers a collaborative mapping tool to plan and post running routes. While the default setting is for the posted routes to remain private (for safety and security reasons), the users may also decide to share their running routes with their 'friends' or even post the routes publicly. Before saving a route in the system, a message pops up and asks the user whether he/she wants to share the information, with three choices: 'no, please keep it private', 'yes, share with my friends' and 'yes, post publicly'. The 'no, please keep it private' box is pre-ticked and the message also contains a link entitled 'read more about how to protect your privacy on the map'. Next to the choice of 'yes, post publicly', a

[120] See also Section II.2.4 on unsolicited communications.

[121] On customer profiling, see also examples 9 (Secret algorithms predict pregnancy of customers from purchasing habits) and 10 (Special offer for a lawn-mower) in Annex 4 discussing the compatibility assessment.

triangular danger icon is displayed. By clicking on it, the risks associated with public postings are highlighted. Further information on the website provides all elements of a data protection notice in more detail and in a language adapted to the audience. It also contains tips and advice, for example, that users should generally avoid posting running routes publicly, and if they do so, are advised to take sensible precautions. In particular, they are advised to avoid mapping their home and school addresses, posting routes that are going through deserted areas, indicating their age and sex, or posting their photos. They are also advised to use pseudonyms.

Example 11: Breaking down more general purposes into 'sub-purposes'

It is generally possible to break a 'purpose' down into a number of sub-purposes.
- For example, processing an individual's claim for a social benefit could be 'broken down' into verifying his or her identity, carrying out various eligibility checks, checking other benefit agencies' records, etc.
- The concept of an overall purpose, under whose umbrella a number of separate processing operations take place, can be useful. This concept can be used, for example, when providing a layered notice to the data subject. More general information can be provided in the first instance about the 'overall purpose', which can be complemented with further information. Breaking down the purposes is also necessary for the controller and those processing data on its behalf in order to apply the necessary data protection safeguards.

Example 12: General terms and conditions of a retail bank

A traditional retail bank specifies in its general terms and conditions that it will process clients' personal data in order to provide the financial services requested and to provide information on other services which clients may be interested in. It will also use the data to prevent fraud and abuse of the financial system, and to comply with legal obligations requiring that certain information is reported to the competent public authorities. This approach gives rise to several comments:
- First, it seems that 'providing the financial services requested' as a primary purpose is both clear and precise enough for most clients to understand the basic scope of the processing.[122]
- Second, the other purposes mentioned may - as discussed in Section III.2 - either be compatible with the primary purpose, or be imposed by law, but although providing some basic information, they are too general to serve as a useful specification of purpose.
- Third, it is doubtful whether inclusion of these additional items in the general terms and conditions will bring any more flexibility for further use for the data controller, considering that additional use is not necessary for the execution of the contract, and the client has not unambiguously consented.

[122] Of course, in its internal procedures, the bank must still define the purposes more specifically so as to ensure it can apply the necessary safeguards. Further information may also need to be provided to the data subjects, for example, where information obtained from the customer using a particular service will subsequently be used in another context. Such use may or may not be appropriate depending on the specific context. Even if permissible, such a combination of data may require additional safeguards. For example, there must be strict rules in place governing whether or not, and under what conditions, a bank which has both an insurance business and a retail banking business may use information obtained in one capacity for use in the other (see also Section III.2).

Example 13: Population registers

- In many countries, population register systems (many of which originated several centuries ago) have been developed to include some or all of the events covered by civil registration (such as births, deaths, marriages, divorces, adoptions, etc), but also a wider range of events, such as change of address. These registries are typically used to provide reliable information about the population that can be used for a variety of public purposes, such as planning; budgeting and taxation; issuing identification documents; establishing eligibility to vote; access to education, health care, social insurance, welfare and pension systems; and determining eligibility for military service.
- Both the content and use of these registries are usually regulated under specific laws. Although broad umbrella provisions often appear in those laws, such as 'information can be used for any public task', they also contain detailed legal provisions to provide legal certainty. These provisions specify in what situations and for what purposes the data may be used, and who may have access to it.
- The registries also form the basis for e-government services. With increasing tendencies towards government data sharing, it is becoming more and more important that clear, specific and proportionate legal rules are in place to clarify how information contained in population registers and other government databases may be used, shared, and safeguarded. The challenge is to define these rules in such a manner that they provide sufficient legal certainty without being overly rigid.

Example 14: Data sharing among competent authorities across EU Member States

- There is a growing tendency towards administrative cooperation among various competent authorities in Member States, for example, in the area of law enforcement (such as the Schengen Information System), customs (Customs Information System), consumer protection (Consumer Protection Cooperation System), asylum applications (EURODAC), visa applications (Visa Information System) or on broader internal market issues (Internal Market Information System).
- Just as in the case of intra-government data sharing, it is becoming increasingly important that clear, specific and proportionate legal rules are in place. These rules should clarify what data are to be used, shared, exchanged or stored and for what purposes. They should also specify who has access to what information, how the security of the IT systems is ensured, and what additional safeguards may apply.

Example 15: Illegitimate purposes - racial profiling of customers

A business segments its customers into two groups based on ethnic profiles: it charges higher prices for ‘white’ as opposed to ‘Asian’ customers. This is done in a non-transparent way to hide the practices, by applying different personalised discounts to the coupons sent to customers with Asian surnames. No information is provided to the customers beyond the notice that 'loyalty card data may be used for marketing purposes'.

- Apart from the other issues the case may raise, this example illustrates that the requirement for the purposes to be legitimate is broad: for example, it also prohibits the processing of data for purposes that may result in discriminatory practices.
- The case also illustrates the importance of transparency to ensure fair processing: had the

business prominently displayed on its front door a notice advising that there would be a 10% discount for everyone with Asian origin (or 10% mark-up for all non-Asian customers), the discriminatory effect would have surely been evident for everyone (and would have also likely driven away all non-Asian customers).

Annex 4: Practical examples to illustrate the compatibility assessment

The following examples illustrate the ways in which a substantive, multi-factor compatibility assessment may be carried out in very different situations. To better guide the reader, the examples - in general - move from relatively simple and straightforward cases towards more complex ones that require a more nuanced compatibility assessment. On some occasions two or more related examples that are worth comparing are grouped together.

Situations where various safeguards are required will also be discussed, as will situations where further processing is likely to be incompatible, and may only be carried out under the strict provisions of Article 13 of the Directive. Examples will come from both the private and public sectors, and will also cover government data sharing. Many of the examples are based on actual cases, or elements of actual cases handled by data protection authorities in the different Member States. However, the facts have sometimes been changed to some degree to help better illustrate the concept and methodology for compatibility assessment.

Regarding the nature of the examples, it is important to underline that they are included in order to illustrate the *thinking process* - the method in which the multi-factor compatibility assessment is to be carried out. In other words, the examples are *not* meant to provide a *conclusive* assessment of the cases described. Indeed, in many cases, by changing the facts of the case in some way (for example, if the controller were to adopt additional safeguards such as more complete anonymisation, better security measures, and more transparency and genuine choice for the data subjects), the outcome of the compatibility assessment could change.

This should also encourage controllers to better comply with all horizontal provisions of the Directive: the greater care they take to protect personal data overall, the more likely it is that any further use they contemplate may be considered compatible.

Example 1: Chatty receptionist caught on CCTV

A company installs a CCTV camera to monitor the main entrance to its building. A sign informs people that CCTV is in operation for security purposes. CCTV recordings show that the receptionist is frequently away from her desk and engages in lengthy conversations while smoking near the entrance area covered by the CCTV cameras. The recordings, combined with other evidence (such as complaints), show that she often fails to take telephone calls, which is one of her duties.

Apart from any other CCTV concerns that may be raised by this case, in terms of the compatibility assessment it can be accepted that a reasonable data subject would assume from the notice that the cameras are there for security purposes only. Monitoring whether or not an employee is appropriately carrying out her duties, such as answering phone calls, is an unrelated purpose that would not be reasonably expected by the data subject. This gives a strong indication that the further use is incompatible. Other factors, such as the potential negative impact on the employee (for example, possible disciplinary action), the nature of the data (video-footage), the nature of the relationship (employment context, suggesting imbalance in power and limited choice), and the lack of safeguards (such as, for example, notice about further purposes beyond security) may also contribute to and confirm this assessment.

Example 2: Breathalyser checks working hours

A public transport company requires bus drivers, each day before starting their shift, to blow into a breathalyser in order to check for the presence of alcohol. The time and date of the test is recorded, along with information on whether the test was successfully passed. This procedure is integrated with an entry-exit system. When bus drivers start their work shift, they are required to hold their magnetic ID card at the breathalyser module and then blow into the breathalyser. The purpose of the collection and further processing of these data, as specified in law and also notified to the employees, is to check that the drivers do not have an unauthorized amount of alcohol in their bodies during the work shift, which is a legal requirement in the country in question. However, unbeknownst to the drivers, the breathalyser system is also used to check if drivers have fulfilled their work time obligations (i.e. whether they have arrived punctually at the start of their shift).

Apart from any other concerns over labour law practices that this case may raise, in terms of compatibility it can be said that a reasonable data subject would assume that the breathalysers are there to check the presence of alcohol, and not for the entirely unrelated purpose of checking whether drivers arrive late at work. This gives a strong indication that further use is incompatible. Other factors, such as the potential negative impact on the employee (for example, possible disciplinary action), the sensitive nature of the data, the legal obligation for the employee to provide the data, the imbalance of power between the data subject and the employer, and the lack of safeguards (such as, for example, notice about further purposes beyond checking alcohol limits) may contribute to and confirm this assessment.

Example 3: Security clearance certificates stored to evidence and audit departmental compliance

In order to protect classified information, a government department requires some of its employees to pass a security clearance procedure in order to evidence that they have the required level of trustworthiness. The security clearance procedure is regulated by law and is carried out by another government department. The resulting 'clean' (i.e. approved) security clearance certificates are stored by the government department which requested the clearance, as evidence that it is complying with the requirements. Certificates are stored for the duration of employment (and a fixed, limited time afterwards) to allow for auditing compliance with the security clearance requirements internally as well as by a third government department. These purposes, as well as the retention periods, are clearly identified, set forth in legislation, and also communicated to staff. The 'clean' certificates provide no additional information beyond the fact that the screening procedure has been successfully carried out.

Without analysing any other aspects of this case, in terms of compatibility it can be said that the purpose of keeping the 'clean' certificates for audits stems from and is in furtherance of the original purpose of obtaining the certificates for security clearance reasons: the auditing is in place in order to verify that the necessary security clearances have been obtained. This gives some (not in itself conclusive) indication towards compatibility and may suggest that the data subjects should expect some degree of data storage for purposes of auditing. Other aspects of the procedure, such as the fact that predictability and legal certainty are assured by detailed provisions in legislation, and that the data subjects are clearly informed in advance, may also contribute toward compatibility. Although the nature of the data would be highly sensitive if

also 'negative certificates' were stored, potential impact on data subjects is limited by the fact that - in the scenario described - only 'clean' security certificates are stored.

Example 4; 'Get Well Quick' breaks

A doctor's wife runs a small independent travel agency. The doctor provides his wife with details of patients who have recently been discharged from hospital. His wife uses the information to send the patients offers for her 'Get Well Quick' range of recuperative seven-day breaks.

Given the sensitivity of health information, and the special legal protection it is afforded both through data protection and other elements of the law (e.g. professional ethics and confidentiality rules), the use of that information for a commercial purpose not directly related to the health-care provided, as well as the transfer of this data to a third party (the doctor's wife), raises immediate concerns over compatibility.

This example is typical of the multi-factor assessment. The fact that the secondary purpose is not directly related to the provision of health-care (which was the primary purpose of the data collection), and the sensitive nature of the medical data, both support the assessment of incompatibility. Based on this, and considering the professional obligations of confidentiality placed upon the doctor, it could be reasonably assumed by the patient that the data were collected specifically (and only) in order to provide health-care.

In addition, - and apart from any other issues this case raises - the fact that there is a transfer of personal data to a third party (the doctor's wife), also contributes to the assessment of incompatibility, as does the doctor's ethical obligation not to take commercial advantage of patients in vulnerable situations. The availability of alternative, less intrusive means of achieving the objective of advertising the 'Get Well Quick' breaks (e.g. placing holiday brochures in the doctor's waiting room, if this is allowed under ethical rules) also suggests that this processing is likely to be incompatible.[123]

Example 5: A public-private partnership: lovers of fatty food told to eat less

A supermarket takes part in a new public health initiative promoted by the government's Department of Wellbeing. The supermarket uses its already available analytics software and customer purchasing database (obtained via its 'loyalty card' system) to identify customers that buy excessive amounts of alcohol or large quantities of high-fat foods. It then sends out leaflets prepared by another private government partner to these customers' home addresses. The leaflets provide nutritional and lifestyle advice and offer appointments at a local 'well-being' clinic, which also participates in the government campaign. The data subjects are not informed of this initiative prior to the supermarket sending out the leaflets, and the initiative itself is not defined in law.

Using customer-purchasing data for an unrelated purpose raises significant compatibility issues that require careful analysis. This is especially the case in this example, given that the

[123] See also Section III.2.4 on unsolicited commercial messages.

project is being carried out for public interest purposes, and involves a voluntary government partnership with private sector entities. First, supermarkets have no formal role, statutory responsibility, or legal obligation in respect of safeguarding public health. Whilst educating customers may be a useful objective in itself, it is not closely related to the primary purpose of selling products, and cannot provide a justification for the further processing. Indeed, it is highly unlikely that customers would expect their data to be used (and to be mined using analytics tools) in this way.

The nature of the data and the way in which they are used to classify customers as 'high-risk individuals' (who need help with their obesity or alcohol problems) is a key factor that contributes towards incompatibility. While the data in themselves (e.g. purchasing a piece of chocolate or can of beer on a particular day) are by no means sensitive, the inferences that can be drawn from them are. The potential impact on the customers will depend on various factors: while some customers may find the leaflets helpful, other may feel singled out, annoyed, pressurised, or discriminated against. This negative impact may be heightened by the lack of transparent information made available to the data subjects about the way in which their information is being used and why they are receiving the brochures.

Further, alternative methods (such as making the leaflets available at the point of sale or within other areas of the supermarket) would be a much less intrusive, and perhaps more effective way of achieving the intended purposes. Alternatively, customers could be offered a clear and specific (opt-in) choice on whether they agree to the supermarket mining their data for the purpose of providing them with nutritional advice. They could also be asked to confirm whether they are happy for this information to be transferred to other campaign partners under clearly specified purposes.

Example 6: Safe internet training for children

Following a public campaign about safe use of the internet, a school decides to forward the contact information of all school children aged 8 to 13 and their parents to a non-profit organisation running an innovative and highly effective government-subsidised workshop that teaches children how to use the internet safely. The non-profit organisation then sends leaflets to the parents and children, inviting them to register for the workshop.

Despite good intentions, the further use and transfer of the children's data raises compatibility issues. Rather than transferring the data without permission automatically, alternative methods could have been used, such as informing the parents and/or the children directly about the training sessions. This example highlights that the compatibility assessment cannot be reduced to a mechanical check, and requires a common sense approach. Sometimes several factors may indicate compatibility, but one or two other crucial considerations will suggest incompatibility. In this case, the educational goals of the workshop are closely related to the educational objectives of the school, and use of the data for organising the workshop would not necessarily be problematic in itself, especially in light of the potential positive impact on the pupils. However, the fact that the data are being unnecessarily transferred to a third party where other direct means of communication are available, suggests incompatibility.

Example 7: Consent for use of holidays photographs to promote a website

A small tour operator specialising in mountain trekking organises a holiday program for a group of eight participants. During the holidays, lots of photos are taken by the manager of the company who is a keen photographer and has also been serving as a tour guide and overall organiser for the trip. Many of the photos are subsequently shared among the participants via password-protected access on a photo-sharing website, with the understanding that photos may be used for personal and non-commercial purposes only.

Two years later, the manager nevertheless wishes to use a handful of these photos on the company's new website to promote its holiday program. The photos are inoffensive but somewhat intimate as they artistically capture private moments and emotions while trekking at high altitudes. During a reunion, the manager asks the individuals whose photos he wishes to use, to consent to him uploading the pictures on the website. Some participants give informed, unambiguous and explicit consent (to make sure the consent is properly evidenced, the manager drafts a simple but clear document, which is then signed by all those who consented). Others prefer their photos not to be uploaded on the website. Subsequently, the manager only uploads those photos for which the individuals concerned gave their consent.

Although the purpose of the processing has changed significantly, this use can be considered compatible because extra safeguards were put in place to ensure that appropriate information was provided, and consent obtained, for the further processing. This simple and straightforward scenario helps to illustrate that in some cases, even when a reasonable person would not usually expect such further use (like having their private and intimate photos put on a commercial website for promotional reasons), a change of purpose is possible, subject to appropriate safeguards - in this case, freely given and informed consent.

Example 8: Photo-sharing website changes privacy policy

A market-leading social networking and photo-sharing site allows its users to upload photos for personal use and share them with selected 'friends'. The privacy notice reassures customers that the photos will only be shared 'with whom you want, when you want'. Two years later, the company changes its privacy policy. In an email it notifies its customers that a new privacy policy will come into effect and unless they remove their photos within 30 days, they will be deemed to have consented to giving the site a license to use all uploaded photos for any purpose, including, but not limited to, promotion of the website. A detailed license agreement and privacy policy are provided in a link to the email as well as via the site whenever the customer visits it. The customer must accept these documents by clicking 'I accept' before being allowed to continue browsing the website.

This further use of the photos - besides raising other data protection concerns such as validity of the consent, proportionality, and legitimacy - also raises compatibility issues. The change clearly could not have been expected by the customers who have by now uploaded two years' worth of their photos online with the understanding that they will only be shared 'with whom [they] want, when [they] want'. The purpose of the initial processing (allowing customers to share their photos with their friends) is clearly unrelated to the - excessive - further use by the company. The context and the specific assurances given in advertising the services at the time of the initial collection also confirm the assessment of incompatibility.

The nature of the data is also a factor that supports incompatibility: although many of the photos uploaded on the site might be innocuous, others can be more intimate, perhaps embarrassing, or simply badly taken. They can also be misinterpreted, if taken out of context. Further, the thought that the photos may be used for promotional or other purposes may have a stifling effect of self-censorship on what people might post on the website, which could be classed as a potential impact on the data subject. The balance of power between the consumers and the photo-sharing website, and lack of suitable alternatives for photo-sharing services, may also contribute to the conclusion that consent alone, collected in this form and under these circumstances, is unlikely to be sufficient to compensate for this excessive and unexpected change of purpose.

Example 9: Secret algorithms predict pregnancy of customers from purchasing habits

A department store uses loyalty card data to analyse the purchasing habits of its clients, to identify new marketing trends, and also to make special offers and send discount coupons to its customers. The innovative analytics software used by the department store predicts with a high degree of probability whether a female customer is pregnant and by how many months. This information is used to adapt marketing offers to their profile. No specific information is provided to the customers when they register for a loyalty card. The detailed terms and conditions (which are available on the department store's website) only mention that 'loyalty card data may be used for marketing purposes, including providing customers with special offers and discount coupons'. The department store receives a complaint from the father of a teenage girl who finds out that she is three months pregnant following suspicions about the increased amount of pregnancy-related advertisements arriving in the mailbox of the family home.

The above scenario immediately raises clear privacy concerns: some pregnant women, especially those in the early stages of their pregnancy, may want to keep the news to themselves and/or to a very close circle of family and friends. The way in which the profiling is carried out (secret algorithms to predict pregnancy) is obviously one that many customers would find unexpected, inappropriate and objectionable. The problem is less related to the nature of the data collected (which may be non-intrusive in itself) but rather to the way the data is combined, further processed, and used to predict a general profile (pregnancy and number of months) using a secret and objectionable algorithm.

On balance, and apart from any other issues that this case may raise, there is a strong indication of incompatibility primarily due to the manner in which the data are processed and the lack of safeguards (such as transparency, as well as genuine and informed consent). This case can be contrasted with the next one, which is also about customer profiling, but in a more socially acceptable way.

Example 10: Special offer for a lawnmower

A national retail chain selling gardening supplies and do-it-yourself equipment offers its customers a loyalty card for a modest annual subscription fee, which allows a 10% discount on all purchases made using the card. There is an informative privacy notice on the company's website, and a shorter version is also provided to customers who sign up for the loyalty card, with some explicit options to choose from.

The notice is clearly written and mentions, among other things, that if the customer opts in to option (a) 'I want my purchase history to be stored online so that I can receive personalised discounts', then the purchase history may be used to 'analyse purchasing patterns and make special personalised offers to loyal customers'. Alternatively, the notice explains that the customer can still keep her loyalty card and thereby still get the 10% discount (and all other general discounts), but by choosing option (b) 'I want my details to be kept private and receive general discounts only' she may choose not to be subject to profiling and not to receive personalised offers and discounts. More details are provided both on-line and off-line.

One spring day a loyal customer and keen gardener, who opted in for personalised discounts, receives a special offer by post: 30% off the price of a brand new, less noisy and more energy efficient lawnmower, just as her old one starts to give her some trouble.

She is interested and goes on-line to find out more about the offer. Each card-holder has access not only to personalised recommendations and special offers, but also to their purchase history for the past five years - information that the store retains as a default setting. The site has many user-friendly features to analyse the purchases made and to recommend additional items a customer might like. It also has a prominently featured informative article about the ways in which analytics software works, which highlights common practices in the industry, that are also used by the gardening store. For example, the article explains that special offers for items previously purchased by the customer will be sent around the time when customers might want to start thinking about replacing their old models.

The article also explains that the discount applied will be customised based on various factors such as the average monthly spend of the customer in the store (the more they spend, the bigger the discount), the up-take of previous special offers, and other similar indicators that are described transparently and in detail. This transparency has already led to jokes on the 'forum' part of the website about the average time it takes for particular lawnmowers to break down, and to the sharing of strategies and tips on how to 'trick' the system and get a better discount. For example, many customers now specifically click on discounted items on the website to show they shop around and thus, suggest that they will react well to a bigger discount.

The site also allows a customer's purchase history to be downloaded in a standard format. Some customers, for example, may decide to integrate this data into an (independently purchased) software tool they use to plan and analyse their personal finances.

Just as in the previous example relating to pregnancy prediction, this case requires a complex analysis of the details, which a short summary could not cover. Nevertheless, it is worth comparing the two cases, which display many similarities but also many differences. Both cases involve customer profiling for marketing purposes, but common sense suggests that while the first case is clearly objectionable to most people, the second one appears to be much less problematic.

Ultimately the most striking element of the first case is the unexpected, uncanny ability of the algorithm to predict pregnancy from seemingly innocuous purchasing data. In contrast, the gardening store appears to profile its customers in a much more predictable (even convenient) and reasonable way: an offer for a new lawnmower comes when it is time to replace the old one. There is nothing surprising or objectionable in the special offer received or in the way the company calculates the timing of the offer. The key differences are in the way in which

the algorithms are designed: whether they meet the general reasonable expectations of the public or whether there is something objectionable or unfair about them.

In this respect it is also important to emphasise that tracking and profiling for marketing purposes can usually only be considered as compatible use if there is a lawful basis for the processing such as genuine, unambiguous, freely given and informed consent. In the second case, the gardening store seems to have made significant efforts to ensure transparency and provide an informed choice to its customers. These safeguards, in turn, can contribute to predictability, and confirm reasonable expectations. They can also help to ensure overall fairness and minimise any unexpected and objectionable impact on the data subjects. Indeed, if a company has to disclose its decisional criteria - its algorithm for profiling - it is much less likely that it will use unfair or objectionable methods.

Finally, the nature of the data may also play a role in the assessment. Although detailed patterns about the purchase of gardening tools and supplies may reveal significant information about individuals, in general, this will not be as sensitive as the type of inferences that could be made from knowing what particular websites they visit, the books or films they rent/ purchase, or the items they buy from a pharmacy.

Example 11: Car manufacturer uses public vehicles registry data to notify car owners of malfunction and recall the cars

A car manufacturer identifies a significant malfunction in a series of cars, which could lead to serious car accidents. Under national product safety legislation, the manufacturer is required to recall all cars purchased from the relevant series and inform customers 'by all reasonable means' of the malfunction. National legislation fails to provide further detail on exactly how car owners should be notified, but a practice has developed whereby - upon request - the national vehicle registration service (which is run by a public service body) provides an updated list of all concerned car owners to the manufacturer. Legislation on vehicle registration also fails to provide specific provisions.

According to this practice, the transfer is documented in a standard contract developed by the national vehicle registration service which provides strict conditions on the use of the data. The contract, among other things, prohibits the use of the data for additional purposes (such as marketing). Other safeguards, such as technical and organisational measures to protect the security of the data are also adequately addressed and implemented.

This example requires a detailed assessment. First, the up-to-date information in the vehicle registry is likely to be a much more reliable source of contact details for current owners than any other sales data that might be held by the manufacturer. Therefore, it is in the direct interests of the data subjects themselves (as well as the general public) for them to be contacted by the most reliable means, in order to minimise the risk of any potential accidents. This is a strong and obvious indicator towards compatibility. Second, although legislation may not be sufficiently specific on what public vehicle registry information can be used for, it is not too far-fetched to argue that the use of registration data for this purpose may be to some extent expected, or at least not inappropriate or objectionable. This factor also supports the assessment of compatibility.

Based on these considerations, the use of registration data by the vehicle registry for this purpose is likely to be considered compatible: further use appears to be for a somewhat

related, perhaps even reasonably expected purpose, in the clear interests of the data subjects (thus, with a positive impact on them). The nature of the data (i.e. who owns a particular car) is not overly sensitive (although not trivial), which also confirms the analysis.

Some doubts may arise because of the additional element of the data transfer to a third party (car manufacturer). The transfer may have some risks, although these are probably relatively limited. In particular, the manufacturer might misuse the data for additional purposes (such as direct marketing) or may simply not take good care of the information, and fail to ensure its security. For this reason, the contractual safeguards mentioned above play an important role.

In this case, on balance, and also considering the significant positive impact on the data subjects, it can be considered that the use is likely to be compatible. However, for purposes of legal certainty and predictability, it would be desirable to update the legislative provisions so they clearly allow data transfer from the registry to the manufacturer in such situations, and to provide the necessary safeguards which are currently only covered by a contractual arrangement.

Example 12: Transfer of results of pre-employment medical examination

Two government departments (A and B) each have their own separate organisational structures and recruitment procedures, which are to some extent harmonised, based on general governmental guidelines. Each department requires candidates, once they have been offered their first jobs within the department, to pass a pre-employment medical exam to test their fitness for the job. The test is carried out by an external medical service provider. Department A selects a candidate for a job, but the candidate fails to pass the medical test, and thus, fails to get the job.

Two years later, the candidate gets a job offer from Department B. In order to save costs and also to speed up the procedure, the two departments and the medical service provider have an undocumented and informal arrangement in place for sharing medical certificates that are not too old (usually less than two or three years). Accordingly, Department B contacts the external medical service provider to check if the candidate has already passed an exam in the past three years, and if so, whether they could forward the certificate of fitness. Neither Department A nor B informed the data subject that his medical certificates could be transferred between the two departments. Department B receives the certificate - and as it is negative - rejects the application. The candidate complains about the transfer of her personal data.

In addition to any other concerns this scenario may raise, it is clear that there is an issue about compatibility. Although the purposes are to some extent similar (both cases relate to a pre-employment exam carried out by a government department), they can also be distinguished. This is especially so as the two departments both have their own separate human resources organisation and procedures. In general, it can also be said that a reasonable person would not have expected that he would be rejected a job offer based on a medical exam that he failed two years earlier, when applying for a different job at a different organisation (even if both departments were parts of the same overall governmental structure of the country in question).

Lack of transparency (no clear information to the data subject about what her data can be used for), and lack of predictability and legal certainty (no formal inter-department agreements or legal provisions addressing the informal ad hoc arrangements foreseen for sharing the medical

certificates between the two departments) also contribute to the assessment of incompatibility. Finally, both the nature of the data (medical data suggesting lack of fitness to work) and the potential impact (refusal of employment) confirm the assessment.

It could be added that - if the two departments wished to share results in order to cut costs - they would have been able to use alternative and less intrusive methods, and could have applied additional safeguards. For example - and although consent may not necessarily be an adequate legal basis for the transfer of negative certificates, considering the vulnerable situation of the data subject - an arrangement could have been made that only positive medical exam results would be transferred, (thus not risking any negative impact on the data subject and allowing him a second chance in case of application for a different department).

This could have been clearly foreseen in formal arrangements between the two departments, and could also have been made subject to the clear and informed consent of the data subject. This informed consent could feasibly be given on the occasion of the first medical exam and could cover use of the 'clean' certificates for a reasonable period of time (for example, two years).

Example 13: Housing Department needs access to data for fire protection

A local authority has a Grants Department that processes individual tenants' claims for housing assistance grants. It is aware of a problem in its area of large older houses being illegally converted into multiple occupancy flats without the necessary fire safety precautions being in place. The Grants Department has been asked by its Housing Department if its database of claimants could be used to detect cases where a number of individuals are claiming grants for the same property – because this would be indicative of multiple-occupancy.

The use of the data for this purpose raises compatibility issues. The purposes of processing are not strictly related: grant applications and fire protection are two separate issues, although it can also be said that the authority has a broad statutory responsibility in respect of both the safety of domestic dwellings in its area and in ensuring tenants claiming social assistance are in adequate accommodation. There is also clearly a public interest in the health and safety of dwellings and their occupants – in this case it is difficult to envisage how else the Housing Department could find out whether a single property has been converted into a multiple occupancy one, short of asking everyone by mail and hoping for a good response rate.

In terms of nature of the data, this may be sensitive as we are talking about potential offences: failure to put in place the necessary fire safety precautions. As for the impact, this is mixed: on one hand, tenants may benefit from increased fire safety precautions that will ultimately no longer be ignored. On the other hand, they might also face penalties that they have ignored the fire safety rules thus far. Further, in terms of reasonable expectations and legal certainty, normally it would be difficult to conclude that the use of the grant data for fire precaution purposes was foreseeable and predictable.

For these reasons, this may be a borderline case for compatibility assessment. If feasible, additional arrangements could be put in place, such as, for example, clearly informing the tenants of their fire safety obligations when they apply for the grant, and advising them, while giving them a reasonable deadline to act, that should they fail to do so, their data will be transferred to the Housing Department.

Example 14: Victims of rape

A report on crime is published on a government website including detailed statistical data on victims of rape and sexual assault in a predominantly conservative neighbourhood. The data was published by a government department in order to raise awareness of this problem. The department lacked the appropriate statistical and data protection expertise and has not put in place a sufficient procedure to ensure that the data are completely anonymised. As a result, some data that the department believed were anonymised nevertheless enabled relatives of these women to identify them. As a consequence, several women suffered severe prejudice and were rejected by their community. One victim committed suicide.

This example serves primarily to illustrate the importance of a careful impact assessment and adequate technical and organisational procedures (e.g. penetration testing to establish the possibilities of re-identification, and stakeholder involvement to ensure all concerns are taken into account) in order to prevent any undue impact in all cases where anonymised datasets derived from personal data are concerned. This is particularly important in cases where data are published on the internet, but may also be relevant in other circumstances.

The example also highlights the need to consider the nature of the data and the potential impact on the data subjects. In this case, all factors support the assessment of incompatible use. Although it could be reasonably expected that the data would be used for statistical purposes, data subjects also would have expected (especially considering the highly sensitive nature of the data, the vulnerability of the victims involved and the gravity of the possible consequences), that anonymisation would be 'foolproof' and would categorically rule out any possibility of re-identification. The safeguards were, thus, insufficient.

Example 15: Mobile phone locations help inform traffic calming measures

The Department for Transport has asked a telecommunications company whether it can use the company's mobile phone location data. in order to calculate the speed at which the phones – and therefore the vehicles they are contained in – are moving over various routes. The mobile phone data reveals that speeding is common on certain stretches of road. This is then used to plan traffic-calming measures, which are later shown to have led to a significant reduction in road traffic accident fatalities in the area. The mobile phone data are effectively anonymised prior to disclosure to the Department of Transport to ensure that the risk of re-identification of the data subjects is minimal. A careful impact assessment is made, penetration tests are carried out, and stakeholders are consulted. In this scenario we assume that all facts confirm very low or minimal risks of re-identification and relatively low impact on the data subjects if it nevertheless happens.

This scenario requires a detailed compatibility assessment. Telecoms data initially collected for a specific purpose are now used for different (road traffic related) purposes. Most people would not commonly expect their data to be used in this way. This may give an initial strong indication that the purposes are incompatible. The relative sensitivity of the mobile location data collected may also support this assessment.

However, in this case, prior to its use/disclosure for the secondary purpose, the data is effectively anonymised. Therefore, although the two purposes are different, and provided the anonymisation is performed adequately (so the information no longer constitutes personal

data or falls into a borderline zone with very low risks of re-identification) this reduces any concerns regarding incompatible processing. Nevertheless, additional safeguards, such as full transparency about the processing will be still recommended. In particular, if complete anonymisation cannot be ensured and some risks remain, this should be disclosed - as a rule, and unless an exemption under Article 13 could apply, informed consent will be required.

Example 16: Patients vouching for an alternative medical practitioner

An alternative medical practitioner specialising in acupuncture treatment has a small but successful practice in a small town servicing a local and regional clientele. On his website, with informed consent of the data subjects, a number of testimonials are listed, many with photographs, full names, contact information and detailed descriptions of the medical conditions that have been cured, and all with emphatic recommendations. The website is local and receives little traffic other than by word of mouth.

A large international on-line 'health-food' business is selling a variety of supplements and vitamins over the internet in the country in question. It uses a powerful web crawler application that searches the web and extracts information about potential customers who have publicly stated they suffer from certain common medical conditions or otherwise appear to be interested in health food or supplements. The application then creates a database of these contacts and uses it to send unsolicited email messages containing advertisements.

Apart from any other concerns this scenario may raise, the example illustrates that although personal data have been posted on the internet, this does not mean that the information no longer deserves protection. Indeed, in the circumstances of this case, the further processing raises serious issues of compatibility. First, there is obviously little similarity between the purposes for which the data subject provided his or her information (to give recommendations for a medical professional) and the purposes for which the on-line business wishes to use it (marketing). Although data subjects may have understood that they took some risks by making their data public on the internet, this certainly does not mean that they have authorised in any way the use of their data for an unrelated and incompatible purpose.

The nature of the data (sensitive medical data) also contributes to the assessment of incompatibility. Finally, although the impact will often be no more than the receipt of a few unsolicited communications, in some cases, (and depending on the type of medical condition involved), this may cause more serious distress. On balance, the processing would seem to be incompatible.

Example 17: Data Retention Directive[124]

A telecommunications company is required by law (national law implementing the Data Retention Directive) to store certain data for its subscribers for one year: amongst other information, the date, time and duration of every telephone call is recorded, as well as the telephone numbers that were dialled for further use in counter-terrorism and the investigation of other serious criminal activity. Extracts from the data are routinely made available to the law enforcement services for these purposes.

[124] The Data Retention Directive (Directive 2006/24/EC) was adopted on 15 March 2006 and published in OJ 2006, L105/54.

This further processing is a clear example of incompatible purpose. First, the further processing is not related in any way to the primary purpose of delivering telecommunications services to subscribers and is imposed by the government (in this case, on the basis of an EU directive). Secondly, ordinary citizens going about their business would have reasonable expectations of privacy regarding whom they speak to on the telephone, when they do so, for how long, and at which location. They could also reasonably assume that this information is not retained for law enforcement purposes. Other issues, such as the fact that they had little or no choice to 'provide' the data, the confidential nature of the data, and the fact that large amounts of data are processed about the data subject, also confirm the assessment of incompatibility. Finally, the fact that the impact on the data subjects may be particularly severe (criminal prosecution) reinforces this analysis.

Considering the incompatibility, the only possibility to nevertheless lawfully retain and process data for these further purposes must be based on Article 13 of the Directive (as specified in Article 15 of the e-Privacy Directive). Indeed, the retention of telecommunication data for law enforcement purposes has been initially 'legitimised' through a legislative measure, the Data Retention Directive. The question is whether this legislative measure fulfils the qualified test that aims to ensure that the restriction to fundamental rights is foreseeable as well as necessary and proportionate. The relevant case is currently before the European Court of Justice.

Example 18: Fingerprints of asylum seekers used for law enforcement purposes

European Union law requires that asylum seekers be fingerprinted so that their identity can be unambiguously identified. A database ('EURODAC') has been established to contain the fingerprints. The objective of this system is to prevent asylum seekers from filing multiple asylum applications in different Member States simultaneously.

An amendment to the relevant EU Regulation proposes that law enforcement authorities should be allowed to access the fingerprint database. As in the cases above, the initial purposes of the database and the further purposes for which access is sought are entirely unrelated. The nature of the data and the potential impact on the data subjects also both strongly suggest incompatibility. Just because the data has already been collected, it should not be used for another purpose which may have a far-reaching negative impact on the lives of individuals.

To intrude upon the privacy of individuals and risk stigmatising an already vulnerable population (asylum-seekers) requires strong justification and sufficient reasons why asylum seekers should be singled out for such treatment. This should only be possible, if at all, subject to the strict conditions of Article 13.

Example 19: passenger name records ('PNR')

An international agreement between the EU and the US on the processing and transfer of Passenger Name Record (PNR) data requires the transfer of certain booking details ('PNR data') by European airlines to the US authorities, as part of the measures used in the fight against terrorism and other serious forms of crime.

The data, such as flight details, credit card numbers, and contact information, are initially collected for a commercial purpose, but subsequently, based on the agreement, are transferred

to serve entirely different (anti-terrorism and law enforcement) purposes. The transfer of such data to a third country government may not be reasonably expected by data subjects, especially if they have not done anything wrong and are not under any particular suspicion or investigation.

These factors strongly indicate incompatibility. The nature of the data (relatively sensitive as it may indicate movements, relationships, affiliations, and also include financial data and contact information), the way in which it is processed (secret algorithms and hidden profiling) and the high potential impact on data subjects (denial of boarding, increased scrutiny at airports, arrests, criminal penalties or worse) all indicate that the further use is incompatible, and only permissible subject to the strict conditions set forth in Article 13 of the Directive.

Example 20: Smart metering data used for tax purposes and to detect indoor cannabis factories

Smart meters have recently been rolled out in households in a certain EU country. They provide detailed and remote electricity readings. The meters have been introduced primarily for reasons relating to energy efficiency and environmental concerns. The detailed readings are needed both for the efficient management of the smart grid (i.e. smart electricity network) and to bill the customers according to dynamic time of use tariffs.

The tax authorities wish to have bulk access to the data in order to detect whether any houses or apartments that are declared unoccupied actually have people residing in them. Law enforcement also wishes to mine the data in order to detect secret indoor cannabis factories. As an alternative, they are considering a partnership with energy companies whereby it would be the companies who would help identify specific violations of tax or criminal law. In that approach, data would be transferred to the tax authorities and law enforcement more selectively, on the basis of a risk analysis and profiling carried out by the energy companies, which would result in a selection of data subjects with an increased risk of rule violation.

In both cases, as with the previous examples, commercial data provided for an entirely unrelated purpose are to be used for law enforcement or tax purposes. Such use may not be reasonably expected by the data subjects, especially if they have not done anything wrong and are not under any particular suspicion or investigation. These factors strongly indicate incompatibility.

The nature of the data (electricity load profiles allow detailed inferences about what individuals do in the privacy of their own homes), the way in which it is processed (secret algorithms and hidden profiling) and the significant potential impact on the data subjects (tax consequences, administrative penalties, arrest, criminal sanctions) all indicate that the further use is incompatible. Therefore, it could only be permissible, subject to the strict conditions set forth in Article 13 of the Directive.

Example 21: Smart metering data mined to detect fraudulent energy use

This example refers to the same scenario with recent roll-out of smart metering systems and smart grid in an EU Member State.

The electricity network operator, who also operates the smart metering system in the country in question, wishes to implement an intelligent system, including an analytics tool, to detect

anomalies in usage patterns, which may give reasonable suspicion of fraudulent use (for example, tampering with the meters). The network operator consults both the regulatory authorities responsible for the electricity grid and the data protection authorities, and discusses its plans with them in detail. Further to their suggestions, it puts in place a number of additional safeguards to minimize the risks of any undue impact on the data subjects. This includes technical and organisational measures, fair and effective procedures to correct any inaccurate results, and transparency towards the data subjects.

In contrast to the other examples above, the present compatibility assessment suggests that the further processing for fraud prevention stems from, and is in furtherance of, the initial purposes of providing energy to the customers and charging them for the energy they use. Customers could reasonably expect that their provider will take reasonable and proportionate measures to prevent fraudulent use of the energy, in the interest not only of the energy company, but also those customers that are paying their bills correctly. Although the nature of the data remains sensitive and the potential impact on the data subjects high (contractual penalties for misuse and possible criminal sanctions), the close connection between the purposes, the reasonable expectations of the data subjects, and the additional safeguards applied, appear to confirm compatibility on balance.

Example 22: Transactions in EU climate change registry used to detect VAT fraud

The European Union has a system of emission trading in place (the EU Emissions Trading System or 'ETS') to help meet EU greenhouse gas emissions reduction targets under the Kyoto Protocol. Europol, national law enforcement authorities and tax authorities have access to this database, among other purposes, in order to carry out data mining operations aimed at catching certain types of VAT fraud.

As with the previous examples, commercial data provided for an entirely unrelated purpose are also being used for law enforcement or tax purposes. Use of such data may not be reasonably expected by the data subjects, especially when they have not done anything wrong and are not under any particular suspicion or investigation. These factors strongly indicate incompatibility. The nature of the data is a mitigating circumstance in the compatibility assessment, as individuals are acting in their professional capacity (trading emissions at the marketplace). Nevertheless, the way in which the data is processed (secret algorithms and hidden profiling) and the significant potential impact on data subjects (tax consequences, administrative penalties, arrest, criminal sanctions) indicate that the further use is incompatible, and only permissible subject to the strict conditions set forth in Article 13 of the Directive.