Context as Key: The Protection of Personal Integrity by Means of the Purpose Limitation Principle

Heidi Beate Bentzen*

Abstract
One of the core principles of European Union data protection law, the purpose limitation principle, holds that personal data must be processed for specified, explicit, legitimate purposes, and not used in manners incompatible with those purposes. How the principle emerged around the world, how the two dimensions of the principle – purpose specification and compatibility – is to be understood in European Union data protection law, taking into account both Court of Justice of the European Union and European Court of Human Rights jurisprudence, and how the principle relates to people’s expectations of respect for context, is explored in this chapter. Respect for individuals’ reasonable expectations, respect for context, and the purpose limitation principle’s compatible use dimension are often touted as separate notions, yet, as argued in this chapter, their natures intertwine and these facets may aid in assessing compatibility in a manner that preserves social expectations.

Keywords
Purpose – Limitation – Principle – Specification – Compatibility – Context

* Norwegian Research Center for Computers and Law, Faculty of Law, University of Oslo, Norway. Affiliated researcher at HeLEX Centre for Health, Law and Emerging Technologies, University of Oxford, UK. Email: h.b.bentzen@medisin.uio.no. The author wishes to thank Professors Lee Andrew Bygrave and Dag Wiese Schartum for their valuable discussions and document review. This chapter reports research conducted as part of the ‘Governance of Health Data in Cyberspace’ project. The project is a joint undertaking between the University of Oxford, the University of Iceland, Uppsala University and the University of Oslo. In addition to the named author and individuals, the following individuals have contributed to the chapter through group discussion and peer support: Sarah Coy, Eik Haraldsdóttir, Jennifer Viberg Johansson, Guðbjörg Andrea Jónsdóttir, Jane Kaye, Deborah Mascalzoni, Salvór Nordal, Nisha Shah and Jorien Veldwijk. This work was supported by NordForsk grant number 81105 and the Economic and Social Research Council (part of UK Research and Innovation), and by the Research Council of Norway grant number 238999.
1. Introduction

Processing of health data in cyberspace can cause concern because digital networks enable data generated in one context subsequently to be used for other purposes, across geographical borders and contextual boundaries. Projects such as the care.data initiative proposed by the National Health Service in England where the plan was to regularly upload data from patients’ medical records to a central database to be used by academic institutions and commercial organizations, sparked public outcry due to a lack of transparency regarding the data processing and poor communication, contravening social expectations about secondary use of existing data.\(^1\) It may further have contributed to the concern that data is used for secondary purposes for which it is indeed relevant, but unsuited: the data is correct and is not being misapplied, but the decisional quality may be lacking.\(^2\) In contrast, Genomics England, a commercial entity, is rapidly rolling out personalized medicine in the clinic and facilitating widespread reuse of health and genetic data with the help of a supportive society.\(^3\) The Chair of the Ethics Advisory Committee for Genomics England, Professor Mike Parker, suggests that embedding ethics can make the difference between success and failure, and may explain why the 100,000 Genomes Project is a success while care.data failed.\(^4\) This suggests that elements of the context, such as embedded ethics or respect for social expectations, may influence people’s perceptions of risk and trustworthiness.

Both examples relate to one of the core principles of European Union (EU) data privacy law, the purpose limitation principle, also known as the purpose specification principle or the finalité principle after the French *le principe de finalité*. It holds that personal data must be processed for specified, legitimate purposes, and not used in manners incompatible with those purposes.\(^5\)

---

As elaborated further below, the principle is really a cluster of at least two sub-principles: purpose specification and compatibility. Purpose specification entails as detailed in Section 4 that the purpose must be specified, explicit, and legitimate, while compatibility entails that later purposes must be compatible with the original purpose.

The principle is internationally considered as a fundamental and important principle in the field of data protection law. The purpose limitation principle contributes to other EU data protection principles such as transparency and accountability; to predictability and foreseeability; and it is a pre-requisite for applying data quality requirements such as adequacy, relevance, proportionality, and accuracy. It entails that data controllers – those determining the purposes and means of the personal data processing – must have foresight as new purposes can only be added at a later stage within the parameters of compatibility. These firm boundaries protect the integrity – a person’s state of intact, harmonious functionality based on other persons’ respect for him/her – and private life of individuals. They also prevent the data accumulation one associates with a surveillance society – data cannot be stored just in case it may come in useful in the future.

The purpose limitation principle aims to protect people by limiting data about them being used in a way or for purposes they find unexpected or inappropriate. The European Data Protection Board (EDPB) predecessor, the Article 29 Working Party, emphasized the individual’s expectations about the purposes for which the data will be used in relation to the purpose limitation principle, stating that “[t]here 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.”

---

6 Rt. 2013 p. 143 A and Landsorganisasjonen i Norge (LO) vs. Avfallsservice AS (The Norwegian Supreme Court) paragraph 47.
7 ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 03/2013 on purpose limitation (WP 203) (2013) 11, 14, 18.
10 A29WP Opinion 03/2013, 11.
11 A29WP Opinion 03/2013, 4.
Respect for individuals’ reasonable expectations, respect for context, and the purpose limitation principle’s compatible use dimension are often touted as separate notions, yet, as argued in this chapter, their natures intertwine and these facets may aid in assessing compatibility in a manner that preserves social expectations. A comprehensive overview and analysis of the purpose limitation principle in EU law will be provided in Sections 4 and 5 below, taking into account both the jurisprudence and research on the topic before concluding with an assessment of the social expectations and respect for context as it relates to purpose limitation in Section 6.

The Court of Justice of the European Union (CJEU) has in settled case-law confirmed that fundamental rights form an integral part of the general principles of law.\(^\text{12}\) Article 6(3) of the Treaty on European Union confirms that the fundamental rights enshrined in the European Convention on Human Rights (ECHR) constitute general principles of EU law, and Article 52(3) of the Charter of Fundamental Rights of the European Union (Charter) provides that the rights contained in the Charter that correspond to rights in the ECHR are to have the same meaning and scope as those laid down by the ECHR. As such, the CJEU draws inspiration from international treaties for the protection of human rights on which the Member States have collaborated or to which they are signatories, and the ECHR has special significance in this respect.\(^\text{13}\) Consistency between the Charter and the ECHR is ensured, without the autonomy of EU law and that of the CJEU being adversely affected.\(^\text{14}\) Article 6(2) of the Treaty on European Union states that the EU shall accede to the ECHR, however, negotiations are still ongoing, and

\(^{12}\) C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Court of Justice of the European Union (Grand Chamber)) para 98.


\(^{14}\) Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net (C-511/18 and C-512/18), French Data Network (C-511/18 and C-512/18), Fédération des fournisseurs d’accès à Internet associatifs (C-511/18 and C-512/18), Igwan.net (C-511/18) v Premier ministre (C-511/18 and C-512/18), Garde des Sceaux, ministre de la Justice (C-511/18 and C-512/18), Ministre de l’Intérieur (C-511/18), Ministre des Armées (C-511/18), interveners: Privacy International (C-512/18), Center for Democracy and Technology (C-512/18), and Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l’Homme ASBL, VZ, WY, XX v Conseil des ministres, interveners: Child Focus (C-520/18) (Court of Justice of the European Union (Grand Chamber)) para 128.
the EU had not acceded yet.\textsuperscript{15} Hence, and as stated by the CJEU most recently in \textit{Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems}, the ECHR does not yet constitute a legal instrument which has been formally incorporated into EU law.\textsuperscript{16}

Nevertheless, the provisions of the EU data protection instruments must be interpreted in light of fundamental rights in so far as the provisions govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy.\textsuperscript{17} Therefore, when applying the provisions in Directive 95/46/EC in for instance the case of \textit{Rechnungshof v Österreichischer Rundfunk and Others}, the Court first ascertained whether there was an interference with private life, and if so, whether that interference was justified from the point of view of Article 8 of the ECHR.\textsuperscript{18}

In the the joined cases of \textit{La Quadrature du Net and Others, French Data Network and Others and Ordre des barreaux francophones et germanophone and Others}, CJEU in Grand Chamber stated that account must be taken of the corresponding rights of the ECHR for the purpose of interpreting the Charter, as the minimum threshold for protection.\textsuperscript{19} According to Article 52(3) of the Charter, the Union is not prevented from providing more extensive protection. The EDPB therefore considers also the jurisprudence of the ECtHR, “to the extent that the Charter as interpreted by the CJEU does not provide for a higher level of protection which prescribes other

\begin{itemize}
  \item[\textsuperscript{17}] Joined Cases C-465/00, C-138/01 and C-139/01 \textit{Rechnungshof (C-465/00) and Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kaltenleutgeben, Land Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG, and between Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) and Österreichischer Rundfunk} (Court of Justice of the European Union) para 68.
  \item[\textsuperscript{18}] Ibid para 72.
  \item[\textsuperscript{19}] \textit{La Quadrature du Net} para 128.
\end{itemize}
requirements than the ECtHR case law”.20

Similarly, the jurisprudence included below will encompass both CJEU and the European Court of Human Rights (ECtHR) judgments. Case law databases have been searched for jurisprudence related to purpose limitation, and the cases have been subdivided into two categories, either relating to purpose specification or compatibility. This sheds further light on the content of these two dimensions of the purpose limitation principle in EU data protection law and provides practical guidance when assessing similar cases. Though the jurisdictional scope is that of the countries which have implemented the EU General Data Protection Regulation 2016/679 (GDPR), it is necessary to first take a wider jurisdictional view to understand what category of principle the purpose limitation principle is (Section 2), and how it evolved into the EU data protection principle it is today (Section 3).

2. What is a principle

Principles are ambiguities in data protection law. The term is used as a reference for overarching norms, but these can be ethical, political, legal or social. The purpose limitation principle is a legal principle, but it may build upon or benefit from being supplemented by ethical, political, and/or social norms.

*Ethical* or moral principles – foundational principles about right and wrong and baseline guiding principles – may be quite abstract. Ethics crosses jurisdictional boundaries, and the principles may need to be modified before being suited as legal principles or rules. The ethical principle of autonomy is for instance expressed legally in the South African Constitution, but strongly modified to account for the Ubuntu notion of solidarity.21 Often, ethical principles will be expressed as political principles in soft law before making its way into hard law.

The principles set forth in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980, including that of purpose limitation, have served as highly

---


influential political principles and points of reference, and have led the Guidelines to achieve an impact not commonly associated with soft law instruments, but more akin to a hard law effect. As the first internationally agreed statement on the core data protection principles, it has served as a basis for national laws, other international instruments, for policies, and self-regulation.\textsuperscript{22} It has influenced the development of data protection law around the world; particularly Japan, Australia, New Zealand, Canada, and Hong Kong.\textsuperscript{23} The principles have provided a vocabulary and a starting point for international conversations. This is visible on both a political, system, and individual level. The predecessor to the GDPR, Directive 95/46/EC, drew inspiration from the OECD Guidelines.

The GDPR offers legal principles, primarily in Article 5, amongst those the purpose limitation principle. It is common to distinguish between legal principles and rules.\textsuperscript{24} This distinction is also evident in the GDPR itself, for instance in Recital 17, which refers to the “principles and rules established in this Regulation”. Legal principles are typically more overarching and abstract than rules.\textsuperscript{25} However, the GDPR is in itself so general and abstractly formulated that this distinction is not always clear.\textsuperscript{26} The notion of compatibility in the purpose limitation principle is for instance elaborated on in the rule in Article 6(4). Many of the rules in the GDPR pertain to one or more of the principles, and can be seen as expressions and specifications of them, such as Article 25.\textsuperscript{27} The principles in the GDPR are furthermore legal rules in their own

\begin{itemize}
\item \textsuperscript{23} See BYGRAVE (2014) 50-51 for details on the various legal instruments around the world inspired by the OECD Guidelines.
\item \textsuperscript{25} OLGA MIRONENKO ENERSTVEDT, ‘Aviation security and protection of individuals: Technologies and legal principles’ (2016) 186-191.
\item \textsuperscript{27} This description is not necessarily given by the GDPR, but by other EU laws, see e.g. Recital 97 of the European Communications Code 2018.
\end{itemize}
right, and can also function as guiding standards for interest-balancing processes.\textsuperscript{28} Additionally, and similarly to the OECD Guidelines, the principles in the GDPR have a political function and provide guidance for drafting of new data protection rules, both within the EU and internationally.

Furthermore, \textit{social} principles can govern the flow of personal data. Philosopher Helen Nissenbaum, whose seminal theory on contextual integrity is explored in more detail in Section 6 below, refers to social norms related to data sharing as context-relative informational norms.\textsuperscript{29} These norms define and sustain activities, relationships and interests, protect against harm and balance the distribution of power.\textsuperscript{30} Such norms are historically, geographically and culturally responsive, and evolve over time and between societies.\textsuperscript{31}

The purpose limitation principle in the GDPR is a legal principle. As the historical overview in Section 3 will show, the legal principle has evolved from ethical and political principles that have served as a starting point for international conversations. Even with a fully elaborated purpose limitation principle as we now have in the GDPR, we must ensure convergence with social principles to prevent individuals from experiencing data processing as a privacy violation, and we will return to this topic in Section 6.

### 3. The evolution of the purpose limitation principle across the world

To understand the ideas the purpose limitation principle in the GDPR build on, one must take account of the work of the early committees across the world that first formulated principles along the lines of the purpose limitation principle, and examine which ideas they drew upon. This fills a knowledge gap in the literature, providing an overview of the evolution of the purpose limitation principle and thus a better understanding of the principle as currently formulated in the GDPR.

The foundation of purpose limitation as it is now expressed in the GDPR was laid as least as

\begin{itemize}
  \item \textsuperscript{28} BYGRAVE (2014) 145.
  \item \textsuperscript{29} HELEN FAY NISSENBAUM, \textit{Privacy in context : technology, policy, and the integrity of social life} (Stanford Law Books 2010) 3.
  \item \textsuperscript{30} Ibid.
  \item \textsuperscript{31} Ibid.
\end{itemize}
far back as in 1950 in relation to Article 8 of the ECHR, and developed by the accompanying case law of the ECtHR.\textsuperscript{32,33} Article 8 reads:

«Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.»

Thus, interference requires justification and legal basis. When assessing this, the ECtHR examines the context the data processing is taking place in and the individual’s reasonable expectations based on the purpose of the data processing.\textsuperscript{34} This formed a starting point for the principle of purpose limitation because a legitimate purpose cannot be determined without a legal basis which at the same time sets limits to the interference.\textsuperscript{35}

The ECHR is not the only human rights instrument to ensure a right to privacy with aspects relevant for how the purpose limitation principle came to be formulated in the GDPR. All EU Member States are parties to the 1966 International Covenant on Civil and Political Rights (ICCPR). Article 17 of the ICCPR reads:

\textsuperscript{32} A29WP Opinion 03/2013, 7.
\textsuperscript{33} German administrative courts, primarily the Prussian Oberverwaltungsgericht, developed a proportionality test in the late nineteenth century where measures by the police required a lawful purpose, and a proportionality between the intrusiveness on an individual’s liberty or property and the means to be applied. For more detail, see DIETER GRIMM, ‘Proportionality in Canadian and German Constitutional Jurisprudence’ (2007) 57 University of Toronto Law Journal 383-397, 384-387.
“1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.”

Similar to the ECHR, interference requires justification and legal basis according to the ICCPR. The United Nations Human Rights Committee (HRC) has specified that every individual should have the right to ascertain for what purposes personal data is stored in automatic data files.\textsuperscript{36} The HRC has furthermore stated that effective measures have to be taken by States to ensure that information about a person’s private life is never used for purposes incompatible with the Covenant.\textsuperscript{37}

The Younger Committee in Great Britain conducted a privacy study in 1972 in which one of the recommended safeguards was that “[i]nformation should be regarded as held for a specific purpose and not to be used, without appropriate authorization, for other purposes”.\textsuperscript{38} When the House of Commons considered the Younger Report, one of the comments was that

“…Government data banks in certain respects have sold information for commercial purposes – for example to provide address lists for purposes other than that for which the information was originally obtained. A considerable question therefore arises, (…) what controls there are for its use for a purpose other than that for which it was obtained…”\textsuperscript{39}

\textsuperscript{36} UN HUMAN RIGHTS COMMITTEE (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (8 April 1988) 10.

\textsuperscript{37} Ibid.


\textsuperscript{39} HOUSE OF COMMONS MRS. SHIRLEY WILLIAMS, Privacy (Younger Report) – in the House of Commons at 12:00 am on 13th July 1973. Available at <https://www.theyworkforyou.com/debates/?id=1973-07-13a.1955.6#g1973.1>
A year later, in 1973, the United States Department of Health, Education and Welfare recommended the enactment of a Federal “Code of Fair Information Practice” for all automated personal data systems.\textsuperscript{40} The Code rests on five principles given legal effect as safeguard requirements. One of the principles – perhaps even the core one – is that “[t]here must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent”.\textsuperscript{41} One of the objectives is to prevent data processing to which an individual may seriously object, the report noting that any personal data used outside its appropriate context is a potential source of harm to individuals.\textsuperscript{42}

The compatible use dimension of the purpose limitation principle is evident in both the Younger Report and the Code of Fair Information Practice. The Fair Information Practice Principles went on to inspire the Privacy Act of 1974 in the United States.\textsuperscript{43} In the years to follow, several US laws incorporated the purpose limitation principle.\textsuperscript{44} However, the U.S. does not operate with a fully fledged purpose limitation principle similar to European legal versions.\textsuperscript{45}

In 1973, the Council of Europe Resolution 73 (22), which applied to electronic data banks in the private sector, provided that information be “appropriate and relevant with regard to the purpose for which it has been stored” and prohibited processing “for purposes other than those for which it had been stored”.\textsuperscript{46} The following year, the Council of Europe Resolution 74 (29), which applied to electronic data banks in the public sector, likewise required the data processing to be “appropriate and relevant to the purpose for which it has been stored”, but allowed data processing for other purposes if an exception is “explicitly permitted by law, is granted by a

\textsuperscript{40} UNITED STATES DEPARTMENT OF HEALTH, AND WELFARE (1973).

\textsuperscript{41} Ibid xx, 41.

\textsuperscript{42} Ibid 62, 80.


\textsuperscript{45} BYGRAVE (2014) 110.

\textsuperscript{46} A29WP Opinion 03/2013, 8.
Building on these Resolutions, in 1981, the Council of Europe’s Convention 108 for the Protection of Individuals with regard to automatic processing of personal data established purpose limitation as one of the essential principles of data protection. All EU Member States have ratified the Convention, which was the first legally binding international data protection instrument. Article 5(b) of Convention 108 stated that “Personal data undergoing automatic processing shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes”. According to the accompanying explanatory report, the reference to “purposes” in Article 5(b) was meant to indicate that it should not be allowed to store data for undefined purposes. However, it was acknowledged that the way in which the legitimate purpose is specified may vary with national legislation.

Convention 108 was modernised in 2018, including a further elaboration of the purpose limitation principle. The Modernised Convention is convergent with the EU data protection framework, and the European Council has adopted a decision authorizing EU Member States to ratify it. Article 5(4)(b) of the Modernised Convention 108 states that:

“Personal data undergoing processing shall be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes”.

47 Ibid.
49 Ibid. Note also the Explanatory report paragraph II: “The text of the explanatory report prepared by the committee of experts and submitted to the Committee of Ministers of the Council of Europe, as amended by the CDCJ does not constitute an instrument providing an authoritative interpretation of the text of the Convention, although it might be of such nature as to facilitate the understanding of the provisions contained therein.”
50 Ibid 41.
51 The Modernised Convention has not yet entered into force. It opened for signatures 10 October 2018. As of 15 May 2021, 39 Council of Europe member States and 4 non-member States (Argentina, Mauritius, Tunisia and Uruguay) have signed, and there are 10 member state and 1 non-member state ratifications.
Underlining the connection between the purpose limitation principle and the principle of transparency, the Modernised Convention 108 also provides in Article 8(1)(b) that the controller informs the data subject of the purpose of the intended processing.

Several soft law instruments also include the purpose limitation principle, chief among them the aforementioned 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which were prepared in parallel with Convention 108. Several EU Member States are also OECD members, and additionally, the European Commission takes part in the work of the OECD for the benefit of all EU Member States. The OECD Guidelines included in Article 9 a Purpose Specification Principle and in Article 10 a Use Limitation Principle. The OECD Guidelines were revised in 2013, however, these provisions remain unchanged. The 2005 Asia-Pacific Economic Cooperation (APEC) Privacy Framework was modelled on the 1980 OECD Guidelines, with the purpose limitation principle in paragraphs 15b and 19. Following the OECD Guideline revision, APEC updated its Privacy Framework in 2015, with the purpose limitation provisions now in paragraphs 21b and 25. Another soft law instrument, the United Nations Guidelines for the Regulation of Computerized Personal Data Files was adopted in 1989, and included in Article 3 the principle of the purpose-specification. Though some instruments may operate with less stringent versions of the purpose limitation principle, the territorial scope of these soft law instruments show that across the world, purpose limitation is considered one of the building blocks of data protection legislation.

In the European Union, Directive 95/46/EC drew inspiration from Convention 108 and the OECD Guidelines, but added a requirement to purpose specification in Article 6(1)(b) that the purpose must be explicit. An EU directive is binding as to the results to be achieved, but leaves to the national authorities the choice of form and methods for implementing it. Consequently, the “Evaluation of the implementation of the Data Protection Directive” revealed divergent

---


54 Article 288 of the Treaty on the Functioning of the European Union.
applications and use of different tests of the purpose limitation principle in Member States. Variations were detected between sectors; in how purposes are made explicit and how broadly they may be defined; the rules concerning change of purpose; and the test to determine incompatibility.

Article 8 of the Charter, initially proclaimed in 2000, enshrines a right to the protection of personal data. Article 8(2) of the Charter establishes the principle of purpose limitation:

“Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.”

Thus, the Charter presents purpose specification and legitimacy as two separate, cumulative requirements. However, the Charter only partially establishes the purpose limitation principle, as compatibility is not explicitly mentioned.

The purpose limitation principle was challenged by the proposal for a new European Union General Data Protection Regulation where data processing for incompatible use was allowed if a new legal ground was available. The European Data Protection Supervisor (EDPS) reacted strongly, emphasizing that the requirement of compatible use and the requirement of lawfulness are cumulative, also referencing Article 5 of Convention 108. The Article 29 Data Protection Working Party suggested amendments to the proposed regulation that would restore the functioning of the requirement of compatible use and the lawfulness of processing as cumulative requirements.

---

56 A29WP Opinion 03/2013, 10 and ibid.
57 A29WP Opinion 03/2013, 11.
58 THE EUROPEAN DATA PROTECTION SUPERVISOR, Opinion of the European Data Protection Supervisor on the data protection reform package (7 March 2012) para 123.
59 A29WP Opinion 03/2013, 43-44.
In an effort to harmonize European Union data protection legislation further, the GDPR started to apply and replaced Directive 95/46/EC in 2018. Purpose limitation is explicitly mentioned as one of the principles relating to processing of personal data in Article 5(1)(b):

“Personal data shall be:
collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’)”

Furthermore, Recital 39 of the GDPR clarifies the time when the purpose needs to be determined: “the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data”.60

Thus, it is clear from this evolutionary overview that the purpose limitation principle in the GDPR is a fully fledged version of the principle, encompassing both the purpose specification and the compatible use dimension. It is convergent with how the principle is expressed in other legally binding data protection instruments in EU Member States, but it exceeds some of them by providing the data subject with additional protection.

4. The dimensions of the purpose limitation principle and relevant case law

The purpose limitation principle in the GDPR has two main dimensions: it entails that data should be collected for specified, explicit, legitimate purposes (the purpose specification dimension), and not be used in manners incompatible with these purposes (the compatible use

---

60 Recitals do not have independent legal value, but can be used to help interpret and determine the nature of a provision and expand an ambiguous provision’s scope. Recitals cannot be used to derogate from provisions or to restrict unambiguous provisions. See TADAS KLIMAS and JURATE VAICIUKAITE, ‘The Law of Recitals in European Community Legislation’ (2008) 15:1 ILSA Journal of International & Comparative Law 61, 63 and LLIO HUMPHREYS and others, ‘Mapping Recitals to Normative Provisions in EU Legislation to Assist Legal Interpretation’ JURIX 41-49, 42-44.
Each dimension will be elaborated on in the following, informed by CJEU and ECtHR jurisprudence as to the detailed content of the dimension.

a. Purpose specification

The purpose is the reason why the personal data is processed. Purpose specification encompasses three aspects: the purpose must be 1) specified; 2) explicit; and 3) legitimate.

To specify the purpose means to set it precisely and fully, and well enough to allow for assessment of legal compliance and implementation of necessary data protection measures and realization of data subject rights. Undefined purposes do not enable precise delimiting of the scope of the processing. Hence, the explanatory report to the Modernised Convention 108 stresses that “it is not permitted to process data for undefined, imprecise or vague purposes”. Even though the purpose cannot be undefined, there is room for some generality and vagueness. In relation to Directive 95/46/EC, “for commercial purposes” was mentioned as an example of a too general and vague purpose that would not fulfill the requirement that the purpose be specified. The Article 29 Working Party provided further examples such as “future research”, “marketing purposes” and “IT-security purposes”. Another of the Working Party’s examples of vague purposes, “improving users’ experience”, was employed by Google when it consolidated its services under one account and one privacy policy, resulting in fines from the Spanish DPA.

---

63 Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe Treaty Series - No. 223, 10 October 2018) 48. Recall that the Modernised Convention 108 is not yet in force, but it will be a legally binding instrument similar to Convention 108, though updated and convergent with the GDPR.
64 COMMISSION OF THE EUROPEAN COMMUNITIES, Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(92) 422 final—SYN 287, 15 October 1992) 15.
65 A29WP Opinion 03/2013, 16.
The purpose must be explicitly stated and sufficiently clear; there can be no hidden purposes.\(^67\) This entails expressing or explaining the purpose in a manner that ensures unambiguous understanding by all concerned, irrespective of linguistic or cultural diversity.\(^68\)

Finally, the purpose must be legitimate. In Article 6(1)(b) of Directive 95/46/EC, there were subtle, yet significant language differences between for instance the French version in which the purpose was described as having to be “légitimes” and the German version which used the term “rechtmäßige”. Hence, the German version was more narrowly formulated, and more similar to the OECD Guidelines which use the term “lawful”. In Article 5(1)(b) of the GDPR, also the German version now uses the wider term “legitime”. The Article 29 Working Party describes legitimacy as a broad requirement that goes beyond having a legal ground for the processing, stating that “[i]t also extends to other areas of law and must be interpreted within the context of the processing”, and specifying that “[w]ithin 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”.\(^69\) In the same vein, the explanatory report to the Modernised Convention 108 mandates that in the assessment of what constitutes a legitimate purpose “a balancing of all rights, freedoms and interests at stake is made”.\(^70\) Bygrave illustrates that most data protection codes comprehend legitimacy primarily in terms of procedural norms, meaning that the processing purposes fall naturally within the ordinary and lawful ambit of the controller’s activities.\(^71\) Further, there is overlap between the various principles in Article 5. Article 5(1)(a) regarding lawfulness, fairness and transparency is an overarching norm that embraces and generates the other principles in Article 5 – including purpose limitation – at the same time as it constitutes something over and above the latter.

\(^{67}\) A29WP Opinion 03/2013, 12, 17-19.
\(^{68}\) Ibid 39.
\(^{69}\) Ibid 39, 20.
\(^{70}\), Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 48.
\(^{71}\) BYGRAVE (2014) 155-156.
ECtHR and CJEU jurisprudence demonstrate non-compliance with purpose specification in the fields of intelligence and surveillance.

The concurring opinion in the Rotaru v. Romania Grand Chamber judgment is one example of ECtHR case law linking Article 8 of the ECHR to the purpose specification dimension of the purpose limitation principle, as it raised doubts about whether the interference with the applicant’s rights pursued a legitimate aim: “To refer to the more or less indiscriminate storing of information relating to the private lives of individuals in terms of pursuing a legitimate national security concern is, to my mind, evidently problematic.”

The ECtHR ruled that there had been a violation of Article 8 ECHR in Szabó and Vizzy v. Hungary. The Court provided clarification on the term “in accordance with the law” in Article 8 § 2 ECHR, illustrating the link between quality and purpose specification, as a law of sufficient quality will need to be specified enough to provide delimiting of the data processing purposes. The Court acknowledges that there is also a need to “avoid excessive rigidity and to keep pace with changing circumstances”. However, the law must indicate the scope of discretion and the manner of its exercise with sufficient clarity.

Also the Court of Justice of the European Union has ruled general and indiscriminate national legislation to be in breach of purpose specification. The Grand Chamber case of Digital Rights Ireland Ltd v. Minster for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others – where the Court found an entire Directive invalid – can serve as an example in this regard. Likewise, in both the Grand Chamber case of Tele2

---

73 Szabó and Vizzy v. Hungary Application no. 37138/14 (European Court of Human Rights (Fourth Section)) para 89.
74 Ibid para 59.
75 Ibid para 64.
76 Ibid para 65.
Sverige AB v. Post- og telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others and the Grand Chamber case of Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, the Court precluded national legislation which provided for general and indiscriminate data retention, noting that clear and precise rules and limits, would have been acceptable.\textsuperscript{78} All cases highlight the link between the principle of purpose limitation and the principle of proportionality. In the the Joined Cases of La Quadrature du Net, the Court in Grand Chamber provided a generous margin of appreciation for processing for national security purposes. Where there exists “genuine and present or foreseeable” national security threats, the Court found that, subject to safeguards, EU law does not preclude indiscriminate retention of telecommunications data “for a limited period of time”.\textsuperscript{79}

Additional examples of non-compliance with purpose specification can be found in jurisprudence relating to criminal justice and health.

The ECtHR Grand Chamber case of S. and Marper v. the United Kingdom concerned indefinite retention by the criminal justice system of fingerprints, cell samples, and DNA profiles of persons suspected, but not convicted of criminal offences.\textsuperscript{80} The Court noted that “the mere

\begin{footnotesize}
\begin{enumerate}
\item Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB (C-203/15) v. Post- och telestyrelsen, and Secretary of State for the Home Department (C-698/15) v. Tom Watson, Peter Brice, Geoffrey Lewis, interveners: Open Rights Group, Privacy International, The Law Society of England and Wales ECLI:EU:C:2016:970 (Court of Justice of the European Union (Grand Chamber)) paras 63, 105-112. C-623/17 Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service (Court of Justice of the European Union (Grand Chamber)).
\item La Quadrature du Net paragraph 229.
\item The Court considered cellular samples personal data within the meaning of the Council of Europe Data Protection Convention 108, see S. and Marper v. the United Kingdom Applications nos. 30562/04 and 30566/04 (European Court of Human Rights Grand Chamber) 68. This was a controversial finding at the time, and if still upheld, even more so today when the GDPR has harmonized the understanding of the definition of personal data within the EU, excluding human biological samples from the definition of personal data. For a legal analysis of human biological samples versus personal data, see LEE A. BYGRAVE, ‘The Body as Data? Biobank Regulation via the ‘Back Door’ of Data Protection Law’ 2 Law, Innovation and Technology 1-25, HEIDI BEATE BENTZEN, ‘Biologisk materiale som personopplysning’ (2013) 115 Lov og Data 12, and WORKU GEDEFA URGESSA,
\end{enumerate}
\end{footnotesize}
retention and storing of personal data by public authorities, however obtained, are to be regarded as having a direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data”.

The domestic law should “ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored”.

It should also afford adequate guarantees that personal data is efficiently protected against misuse and abuse. The Court goes on to add that this is “especially valid as regards the protection of special categories of more sensitive data (...) and more particularly of DNA information, which contains the person’s genetic make-up of great importance to both the person concerned and his or her family”.

The Court referred to the lack of purpose specificity by concluding that “the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard.”

Hence, the retention constituted a disproportionate interference with the applicants’ right to respect for private life not necessary in a democratic society, and thus a violation of Article 8.

In *L.H. v. Latvia* the ECtHR recalled that the protection of personal data, and in particular medical data, is of fundamental importance to the right to respect for private life.

Latvian law lacked sufficient precision, it simply “did not limit in any way the scope of private data that could be collected”, leading the Inspectorate of Quality Control for Medical Care and Fitness for Work (“MADEKKI”) to collect the applicant’s medical data from three medical institutions.

---

81 S. and Marper 121.
82 Ibid paragraph 103.
83 Ibid.
84 Ibid. The Court referred to Recommendation No. R (92) 1 of the Committee of Ministers on the use of analysis of DNA within the framework of the criminal justice system.
85 Ibid paragraph 125.
86 Ibid paragraphs 125-126.
87 *L.H. v. Latvia* Application no. 52019/07 (European Court of Human Rights (Fourth Section)) paragraph 56.
indiscriminately.\textsuperscript{88} The Court found this to be a violation of Article 8 ECHR.

Purpose specification was also one of the principles mentioned as relevant by the ECtHR to take into consideration in relation to the governance of monitoring of internet use and electronic communications in the workplace in the Grand Chamber case of \textit{Bărbulescu v. Romania}.\textsuperscript{89} However, the Court did not elaborate further on the concept of purpose specification.

In \textit{Deutsche Post AG v. Hauptzollamt Köln} the CJEU found the personal data in question to be processed for specified, explicit, and legitimate purposes.\textsuperscript{90} Tax identification numbers were collected by employers to ensure compliance with income tax legislation, and the employer obligation to deduct tax.\textsuperscript{91} Subsequent collection of personal data by customs authorities was necessary for those authorities to comply with a legal obligation to make a decision on applications for Authorized Economic Operator status.\textsuperscript{92}

ECtHR and CJEU jurisprudence both show general and indiscriminate legislation or data collection to constitute a lack of purpose specification. Though some generality or vagueness is permitted, the purpose must be specified well enough to allow for assessment of legal compliance, implementation of necessary measures, and realization of rights.

b. Compatible use

The compatible use dimension is that later purposes must be compatible with the original purpose. The data subject should not find the further processing unexpected, inappropriate or otherwise objectionable.\textsuperscript{93} By ensuring compatible use, the transparency, legal certainty,
predictability and fairness of the data processing is respected.\textsuperscript{94} If the purpose is incompatible, the processing is unlawful, unless Article 6(4) applies. To be able to properly assess compatibility, also subsequent purposes must therefore be specified.

Compatible use tends to be phrased as a double negation; incompatibility is prohibited.\textsuperscript{95} This gives some flexibility as a purpose can be different without necessarily being incompatible, and the flexibility may to a certain degree also accommodate society’s and data subjects’ changing expectations.\textsuperscript{96} The Article 29 Working Party favored a substantive compatibility assessment, as opposed to a formal compatibility assessment in which the initial purposes on paper are compared to the further uses to determine if these uses are explicitly or implicitly covered.\textsuperscript{97} This is because a substantive assessment goes beyond the formalities, and consider also the context and how the purposes are or should be understood on that basis.\textsuperscript{98} As such, it is less rigid and legalistic, and – importantly – the flexibility and pragmatism it offers leads to it being more effective as it can adapt to societal developments while safeguarding the personal data.\textsuperscript{99} A formal assessment could, on the other hand, encourage controllers to specify the purpose in a legalistic manner that would ensure a wide margin for further data processing, rather than focusing on protection of the data subject.\textsuperscript{100}

It is crucial to know when one crosses the boundary in which a different purpose becomes an incompatible purpose. Article 6(4) and Recital 50 GDPR offers guidance. Based on a more elaborate list by the A29WP, Article 6(4) offers five criteria to consider when assessing compatibility.\textsuperscript{101} The controller must consider any link between the original and later purpose, the context in which the data has been collected, the nature of the data, possible consequences of the intended future processing for data subjects, and the existence of appropriate safeguards.

\begin{flushright}
\textit{Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)}
\end{flushright}

\textsuperscript{94} Ibid.
\textsuperscript{95} A29WP Opinion 03/2013, 21.
\textsuperscript{96} Ibid.
\textsuperscript{97} PARTY 21-22.
\textsuperscript{98} Ibid.
\textsuperscript{99} Ibid.
\textsuperscript{100} Ibid.
\textsuperscript{101} Ibid 40.
The consequence of incompatibility is that the personal data cannot be processed unless Article 6(4) applies, as elaborated below in Section 5. One cannot simply find a new lawful basis for the processing as that would render the purpose limitation principle without substance.

The concept of compatible use is well elaborated on in the explanatory report to the CoE Modernized Convention 108, relevant as the GDPR to a large extent is modeled on the original Convention 108:

«In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data is initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia, any link between those purposes and the purposes of the intended further processing; the context in which the personal data has been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to its further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.»\textsuperscript{102}

Despite the ECHR not explicitly mentioning compatibility, ECtHR jurisprudence often addresses the issue. This is because the ECtHR refers to the individual’s reasonable expectations, and both purpose specification and compatibility are subelements of the assessment.\textsuperscript{103} For instance, unforeseen publication of personal data conflicts with the individual’s reasonable expectations.\textsuperscript{104}

In the ECtHR case of \textit{Z v. Finland}, the applicant’s identity and HIV infection was disclosed in a text of a court’s judgment made available to the press. The criminal proceedings had been against her husband. The Court remarked that the protection of personal data, not least medical data, is of fundamental importance to the enjoyment of the right to respect for private and family life. Going on, the Court noted: “Respecting the confidentiality of health data is a vital principle

\textsuperscript{102} Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 49.
\textsuperscript{103} VON GRAFENSTEIN, 426-428.
\textsuperscript{104} Ibid. See also \textit{Peck v. the United Kingdom} Application no. 44647/98 (European Court of Human Rights) paras 60-61.
in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. 105 Otherwise, people may be deterred from seeking treatment, not only endangering their own health, but that of the community if their disease is transmissible. 106 In particular, the disclosure of HIV status may, the Court noted, “dramatically affect his or her private and family life, as well as social and employment situation, by exposing him or her to opprobrium and the risk of ostracism”. 107 Therefore, any State measures compelling disclosure of HIV status without the individual’s consent “call for the most careful scrutiny on the part of the Court, as do the safeguards designed to secure an effective protection.” 108 The Court did “not find that the impugned publication was supported by any cogent reasons”, and, accordingly, that there had been a violation of the applicant’s right to respect for private and family life not necessary in a democratic society. 109

Armonas v. Lithuania and Biriuk v. Lithuania concerned the same newspaper story. 110 The biggest Lithuanian daily newspaper ran a frontpage story about AIDS in Lithuanian villages. In the article, two people who had not consented to being part of the story were identified by full names and residences as being HIV positive. Medical personnel from an AIDS center and a hospital confirmed their diagnoses. One of the applicants was described as “notoriously promiscuous”, and the second applicant was said to have two illegitimate children with the first applicant. Information intended for provision of medical treatment was hence used to create a sensationalist tabloid media story. This latter purpose was not found acceptable, and the Court again noted the negative impact the disclosure could have on the willingness of others to take HIV tests and seek treatment.

Colorful descriptions were also provided of the applicant in Mockutė v. Lithuania, where a physician without the applicant’s consent explained on national television that the applicant suffered acute psychosis after having attended a meditation center where the followers held sex

105 Z v. Finland Application no. 22009/93 (European Court of Human Rights) 95.
106 Ibid.
107 Ibid.
108 Ibid.
109 Ibid.
110 Armonas v. Lithuania Application no. 36919/02 (European Court of Human Rights) and Biriuk v. Lithuania Application no. 23373/03 (European Court of Human Rights).
orgies, and was currently undergoing psychiatric treatment at the hospital.\textsuperscript{111} The ECtHR found that the disclosure was not in accordance with the law. And in \textit{Peck v. the United Kingdom}, disclosure of CCTV footage of the applicant cutting his wrists by the Municipal Council to the media, was found to constitute a violation of Article 8.\textsuperscript{112}

In the ECtHR case of \textit{M.S. v. Sweden}, the compatible use dimension of the purpose limitation was used to ascertain the limits of a patient’s consent and her justified expectations to the processing of medical data about her.\textsuperscript{113} Medical data was shared by a hospital with a national social security office in order to ascertain whether the applicant qualified for injury compensation. The Court noted that the data processing served a different purpose and entailed an interference, but found the reason for disclosure relevant and sufficient, the measure was proportional to the legitimate aim pursued, and effective and adequate safeguards were in place.

Several other ECtHR judgments also deal with medical information being disclosed for other than the initial purpose. In \textit{Avilkina and Others v. Russia}, a violation of Article 8 was found as the medical records of three Jehovah’s Witnesses were disclosed from the hospital where they had refused blood transfusions to Russian prosecution authorities.\textsuperscript{114} In \textit{Panteleyenko v. Ukraine}, the ECtHR found a violation of Article 8 when confidential information obtained from a hospital regarding the applicant’s mental state and psychiatric treatment was disclosed at a public court hearing.\textsuperscript{115} A violation was likewise found in \textit{L.L. v. France} where the applicant’s medical records without his consent had been submitted to and used by the courts in divorce proceedings.\textsuperscript{116}

In the ECtHR case of \textit{Surikov v. Ukraine}, an employee issued the human resources department of the company Tavrida with his military identification card, in accordance with applicable law.\textsuperscript{117} The card included a reference to an Article of the Diseases and Handicap Schedule, on

\textsuperscript{111} Mockuté v. Lithuania Application no. 66490/09 (European Court of Human Rights).

\textsuperscript{112} Peck v. the United Kingdom Application no. 44647/98 (European Court of Human Rights).


\textsuperscript{114} Avilkina and Others v. Russia Application no. 1585/09 (European Court of Human Rights).

\textsuperscript{115} Panteleyenko v. Ukraine Application no. 11901/02 (European Court of Human Rights).

\textsuperscript{116} L.L. v. France Application no. no. 7508/02 (European Court of Human Rights).

\textsuperscript{117} Surikov v. Ukraine Application no. 42788/06 (European Court of Human Rights).
the basis of which the applicant had been deemed unfit for military service. The company obtained and included this health data in the applicant’s personnel file. Tavrida later used the information for an unrelated purpose when assessing and turning down the applicant’s applications for promotions. The Court considered this a disproportionate interference with the applicant’s right to respect for private life, not necessary in a democratic society.\textsuperscript{118} The Court also found that disclosure of the data to third parties in relation to the promotion assessment were not necessary in a democratic society.\textsuperscript{119}

\textit{Radu v. the Republic of Moldova} concerned a similar case, where the ECtHR found a hospital’s disclosure of medical information to the Police Academy where the applicant worked not to be in accordance with the law.\textsuperscript{120} In \textit{P.T. v. the Republic of Moldova}, the Court found the inclusion of a legal reference to the applicant’s HIV positive status on a military exemption certificate which he had to present to various authorities to be issued a national identity card to constitute a violation of Article 8.\textsuperscript{121}

Article 7 of the Charter corresponds to Article 8 of the ECHR, whereas Article 8 of the Charter is only based on it.\textsuperscript{122} In contrast to the ECtHR’s consideration of the individual’s reasonable expectations, the CJEU considers the data protection instruments provided for by Article 8 of the Charter and the secondary law specifying and extending these when assessing compatibility.\textsuperscript{123}

In the CJEU case of \textit{Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT)}, the authority for working conditions (ACT) requested access to the company Worten’s record of working time for the purpose of monitoring national Portuguese legislation relating to working conditions.\textsuperscript{124} The Court found that the purpose limitation principle does not preclude national legislation, provided that it is necessary for the purposes

\begin{itemize}
\item \textsuperscript{118} Ibid para 89.
\item \textsuperscript{119} Ibid para 94.
\item \textsuperscript{120} \textit{Radu v. the Republic of Moldova} Application no. 50073/07 (European Court of Human Rights).
\item \textsuperscript{121} \textit{P.T. v. the Republic of Moldova} Application no. 1122/12 (European Court of Human Rights).
\item \textsuperscript{122} VON GRAFENSTEIN 175.
\item \textsuperscript{123} Ibid 428.
\item \textsuperscript{124} C-342/12 \textit{Worten – Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT)} (Court of Justice of the European Union (Third Chamber)) paragraph 2.
\end{itemize}
of the performance by that authority of its task. However, it is clear that there are limits for what the Court will accept even when the secondary data use has a legislative basis, as illustrated for instance by the Grand Chamber case of Tele2 Sverige AB mentioned above.

The General Court case of HJ v. EMA concerned documents in the applicant’s personal file being made accessible to any member of staff at the European Medicines Agency for six weeks. In the applicant’s opinion, this constituted processing for purposes other than those for which the documents were collected, without the change in purpose having been expressly authorized. According to the applicant, the sensitive data content of the documents called into question her integrity, thus causing her real, non-material harm. The EMA was ordered to pay compensation for non-material harm.

Regrettably, in the past, the CJEU has avoided bringing clarity to the purpose limitation principle where it had opportunity to do so. The case of Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others is illustrative. It concerned the transmission of income data from the national Romanian tax administration agency (ANAF) to the national Romanian health insurance fund (CNAS). The applicants claimed that the income data was transmitted and used for other purposes than those for which it had initially been disclosed to ANAF. This was done on the basis of an internal ANAF-CNAS protocol, without the applicants’ prior notification or their express consent. A new case specifically concerning purpose limitation has been referred to the CJEU in 2021, the case of Digi Távközlési és Szolgáltató Kft. v. the Hungarian DPA.

---

125 Ibid para 45.
126 C-683/13 Pharmacontinente – Saúde e Higiene SA, Domingos Sequeira de Almeida, Luís Mesquita Soares Moutinho, Rui Teixeira Soares de Almeida, André de Carvalho e Sousa v Autoridade para as Condições do Trabalho (ACT) (Court of Justice of the European Union (Eight Chamber)) paras 12-13.
127 Tele2 Sverige AB para 119.
128 T-881/16 HJ v European Medicines Agency (The General Court (Fourth Chamber)).
129 C-201/14 Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF) (Court of Justice of the European Union (Third Chamber)).
130 C-77/21 Digi Távközlési és Szolgáltató Kft. v. the Hungarian DPA (Court of Justice of the European Union).
But both the CJEU and the ECtHR have assessed purpose compatibility, and though the ECtHR has done so through the lens of reasonable expectations with compatibility as a subcriterion, both Courts find unexpected new uses to constitute a violation.\textsuperscript{131}

5. Further processing for incompatible and \textit{a priori} compatible purposes

In two cases, Article 6(4) GDPR allows for further processing for incompatible purposes: if the data subject consents or if the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1). These objectives include \textit{inter alia} national security or important objectives of general public interest such as public health.

Furthermore, some incompatible purposes are \textit{a priori} considered compatible with the initial purposes. These include archiving purposes in the public interest, scientific or historical research or statistical purposes, see Article 5(1)(b) GDPR. Such processing must be in accordance with Article 89(1), which mandates appropriate safeguards and allows derogations from various data subject rights.

The main challenge with considering the mentioned purposes compatible, is that the GDPR does not include definitions of said purposes, only vague guidance in the Recitals. Without a definition of for instance “scientific research”, there is a risk that unethical practices or a wider range of practices may enjoy more lenient data protection obligations than intended by the legislator. The elements the CJEU and the ECtHR use to assess what constitutes scientific research are the role of the entity where the activity takes place, the role of the individual carrying out the activity, and adherence to quality standards such as scientific methodology and scientific publication.\textsuperscript{132} Elsewhere, I recommend a fourth criterium, that the activity is

\textsuperscript{131} Also national courts have addressed purpose limitation. In Norway, a European Economic Area member which has implemented the GDPR and previously Directive 95/46/EC, a Supreme Court judgment entailed a sharpening of the purpose limitation’s compatible use dimension. The Supreme Court stressed that the fact that the data has already been gathered is not in itself an argument for allowing new processing, see Rt. 2013 p. 143 para 48.

\textsuperscript{132} HEIDI BEATE BENTZEN, ‘In the Name of Scientific Advancement: How to Assess what Constitutes 'Scientific Research' in the GDPR to Protect Data Subjects and Democracy’ in GEORGIOS TERZIS; DARIUSZ
conducted in an ethical manner. The United Nations Special Rapporteur on the Right to Privacy, Joseph Cannataci, provides the most extensive definition of scientific research in his Recommendation on the protection and use of health-related data, including *inter alia* the four mentioned criteria. The lack of definition of the *a priori* compatible purposes in the GDPR constitutes a potential risk to data subjects.

The EDPB has signalled that it will provide guidance on whether a lawful basis is still required for the new *a priori* compatible data processing purpose. A29WP was clear that a lawful basis would still be required, also for further processing for these purposes. Regardless of which conclusion the EDPB reaches in its future guidance, it stresses that the controller remains subject to all other obligations under data protection law, including fairness, necessity, proportionality, and data quality.

The issue has received substantial scholarly attention. It is stated in Recital 50 that when the purposes are compatible, a separate legal basis is not required. Even though the statement has no equivalent in Article 6(4), some argue that Recital 50 should be understood to mean that compatible purposes do not require its own lawful basis in Article 6(1). Others argue that after compatibility is established, a lawful basis for the new data processing must be sought in Article 6(1). A third view, provided by Kotschy, is that Recital 50 is to be understood as referring to the transfer of data to a new processing purpose, and the legal basis for the transfer is the same.

---

KLOZA; ELŻBIETA KUŻELEWSKA & DANIEL TROTTIER (ed), *Disinformation and Digital Media as a Challenge for Democracy* (Intersentia 2020).

133 Ibid.


135 29WP Opinion 03/2013, 33.


as for the initial processing. However, further processing for the new purpose requires a lawful basis in Article 6(1). The advantage of the third view is that it provides an explanation for why the sentence is included in Recital 50, and an interpretation that is in line with that of the Article 29 Working Party in its 2013 guidance on the matter.

6. Conclusion: the utility and value of the purpose limitation principle

The philosophical theory of contextual integrity developed by Helen Nissenbaum is that adequate privacy protection is tied to specific context norms, and that data processing should be context appropriate and obey the governing norms of distribution within that context. Hence, the theory is based on the idea of appropriate personal data flow. Appropriateness is dependent on whether the data flow conforms to legitimate, contextual informational norms. Specifically, the theory of contextual privacy utilizes three parameters for prescribing information flow: 1) actors (sender, subject, recipient); 2) information types; and 3) transmission principles. According to Nissenbaum’s theory, we judge an information flow based on how it conforms to expectations of flow within a given context. Your expectations for how health data flows from your physician is (likely) different from your expectations for how the same data would flow from a journalist. If data you had only shared with your physician ended up in the newspaper, you would (likely) consider that a privacy violation. If the journalist published health data you had chosen to share with her, you would probably not consider that a privacy violation. Note that the sensitivity of the data can be the same, but the context provides different expectations, though some might see sensitivity as a function of context.

The theory of contextual privacy shares similarities with the principle of purpose limitation, which, as mentioned above, aims to protect people by limiting data about them being used in a way or for purposes they find unexpected or inappropriate. Respect for individuals’

---

138 KOTSCHY, 76.
139 Ibid.
141 HELEN NISSENBAUM ‘Measuring privacy’, 13-14.
142 Ibid 14.
143 Ibid.
144 Ibid.
145 A29WP Opinion 03/2013 p. 11.
expectations and respect for the context in which the data was collected or generated are increasingly mentioned in legal instruments and accompanying reports and guidelines. Article 6(4)(b) GDPR lists as a criterion for assessing compatibility “the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller”, with Recital 50 elaborating that “in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use” must be considered. Similarly, the ECtHR considers the individual’s reasonable expectations when assessing purpose limitation.

Nissenbaum’s theory also shares a similarity with the GDPR as such: By defining privacy as contextual integrity, a sharp difference between giving up privacy and giving up data is revealed. The free movement of data within the European Union is an objective of the GDPR alongside the protection of fundamental rights and freedoms, in particular the right to the protection of personal data. As such, also the GDPR prescribes to a scenario in which giving up personal data is fine, while giving up privacy is not.

Empirical data protection research emphasizes this point. People do not mind sharing personal data about themselves, or for the personal data to be reused for other purposes, provided that they consider the data sharing to be appropriate. Quantitative data from discrete choice experiments in Europe show that respondents’ willingness to share pseudonymized health data depend on the contextual properties of the data collection setting. For reuse of the data, respondents prefer national authorities and academic researchers over pharmaceutical or technological companies to be the new user, and they do not want the reuse to be for marketing or promotional purposes. It is worth noting that much of the data processing pharmaceutical companies conduct, is a priori considered compatible with the initial purposes, such as scientific research. Therefore, for-profit pharmaceutical companies may find themselves in a situation where they process data legally, yet the data subjects may experience the processing as a privacy violation. In contrast to the GDPR, people do not feel that anonymization makes reuse acceptable, and in addition to being informed of the reuse and being able to either consent

147 JENNIFER JOHANSSON and others, ‘Publics’ preferences for sharing health data: a discrete choice experiment’ JMIR Preprints. 14/04/2021:29614
148 Ibid
or opt-out, they request additional governance in the form of an oversight or review board to govern data reuse.149

Hence, the purpose limitation principle must itself consider the context it functions within. Specifically, respect for social principles and context norms will help determine the individual’s reasonable expectations of the data processing and any subsequent reuse. Only then can we rest assured that the data processing is not just legally, but also societally acceptable.

149 Ibid.