Tilburg University

Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles

Gil Gonzalez, Elena; de Hert, Paul

Published in:
ERA Forum

DOI:
[10.1007/s12027-018-0546-z](https://doi.org/10.1007/s12027-018-0546-z)

Publication date:
2019

Document Version
Version created as part of publication process; publisher's layout; not normally made publicly available

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):
Gil Gonzalez, E., & de Hert, P. (2019). Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles. *ERA Forum*, 2019(4), 597–621.
<https://doi.org/10.1007/s12027-018-0546-z>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles

Elena Gil González & Paul de Hert

ERA Forum

Journal of the Academy of European Law

ISSN 1612-3093

ERA Forum

DOI 10.1007/s12027-018-0546-z

Your article is protected by copyright and all rights are held exclusively by Europäische Rechtsakademie (ERA). This e-offprint is for personal use only and shall not be self-archived in electronic repositories. If you wish to self-archive your article, please use the accepted manuscript version for posting on your own website. You may further deposit the accepted manuscript version in any repository, provided it is only made publicly available 12 months after official publication or later and provided acknowledgement is given to the original source of publication and a link is inserted to the published article on Springer's website. The link must be accompanied by the following text: "The final publication is available at link.springer.com".

Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles

Elena Gil González¹ · Paul de Hert^{2,3}

© Europäische Rechtsakademie (ERA) 2019

Abstract This contribution looks at the legal grounds for data processing ('when is one allowed to collect and use data on others?') according to the General Data Protection Regulation (GDPR). It then addresses the specific regime for profiling both by solely automated and non-automated means. What is the most suitable lawful basis for this specific, sometimes controversial kind of processing?

The vagueness and subjectivity of various relevant GDPR provisions in this matter can undermine legal certainty. Data protection principles such as transparency and overall fairness as enshrined in Article 5 GDPR may in this case serve as a resort to identify appropriate checks and balances. Additional understanding can be found outside data protection legislation—for instance, in competition law.

Keywords Consent · Fairness · GDPR · Legitimate interest · Profiling

E.G. González is visiting researcher at Instituut voor Informatierecht (IViR), Universiteit van Amsterdam, funded by the 2018 CEINDO CEU-Banco Santander grant.

✉ E. Gil González
ele.gil.ce@ceindo.ceu.es

P. de Hert
paul.de.hert@uvt.nl

¹ PhD candidate, CEINDO - CEU San Pablo University (Madrid), Madrid, Spain

² Professor, Vrije Universiteit Brussels (LSTS), Brussels, Belgium

³ University of Tilburg (TILT), Tilburg, The Netherlands

1 Introduction and structure

Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR)¹ aims to harmonise data protection legislation across EU member states, enhancing individuals' rights. The text consists of 99 articles preceded by 173 recitals, and has been directly applicable in EU Member States since 25 May 2018. The GDPR applies to organisations established in the EU as well as organisations operating outside the EU which offer goods or services to, or monitor the behaviour of, individuals in the EU.² It applies to organisations processing personal data which have an establishment within the EU and also those organisations which operate outside the EU but offer goods or services to, or monitor the behaviour of, individuals in the EU.

Our article is structured as follows.³ We begin by reviewing the provisions in the GDPR that identify a limited set of (six) legal grounds for lawful processing of personal data. Without any such grounds there is simply no acceptable licence for a person to process data of others (Sect. 2). In our section we pay special attention to two of these grounds—consent and legitimate interests. The main problems relating to these are set out and some practical examples are given to identify best practices.

We then turn to profiling and the process of creating profiles (Sect. 3). It is essential to understand the existence of different types of profiles, as the risks deriving from each may not be the same. The subsequent sections of our contribution analyse the relevant legal provisions and GDPR terms ('automated' and 'non-automated' '-making') decision-making and also discuss relevant GDPR principles (laid down in Article 5 GDPR), such as paying transparency and fairness, to add additional understanding of the GDPR provisions (Sects. 4 and 5).

To better apprehend the function and importance of fairness, we look at the meaning of this concept, present in and outside data protection law. We focus on the presence and the role of the concept in competition law relating to the current digital marketplace (Sect. 6), which is heavily reliant on extensive use of personal data. In a last section, we conclude that the vagueness and subjectivity of certain concepts in the GDPR can undermine subjects' rights. In these situations, fairness may serve as a last resort for providing checks and balances. An understanding of the concept of fairness gains in authority when bridging the fields of data protection and competition law (Sect. 7).

2 Legal grounds for the processing of personal data according to the GDPR

2.1 General discussion of the six legal grounds for processing data (Article 6(1) GDPR)

The principles of European data protection law are listed in Article 5 GDPR. No less than three principles are enshrined in Article 5(1)(a), according to which personal

¹Regulation (EU) 2016/679, General Data Protection Regulation [43].

²Art. 2 GDPR.

³An earlier version of this paper was presented at the *ERA Brussels Annual Conference on EU Data Protection Law (DPL)* in April 2018.

Fig. 1 The right to erasure, to portability and to object under different legal bases

	Right to erasure	Right to portability	Right to object
Consent			X but right to withdraw consent
Contract			X
Legal obligation	X	X	X
Vital interest	X	X	
Public task		X	
Legitimate interests		X	

data must be ‘processed lawfully, fairly and in a transparent manner in relation to the data subject’.

Article 6 expands on the first principle, that of lawfulness, and provides six grounds for lawful processing: the consent of the data subject (6(1)(a)), the necessity of the performance of a contract (6(1)(b)), the necessity to comply with a legal obligation on the controller (6(1)(c)), the necessity to protect the vital interests of the data subject (6(1)(d)), the necessity to perform a task carried out in the public interest or the exercise of official authority (6(1)(e)), and necessity in the legitimate interest of the controller or another third party (6(1)(f)). These six grounds have remained mainly unchanged from those in Directive 95/46,⁴ and any processing operation must be based in at least one of these grounds.

The idea of European data protection law here is quite remarkable: the GDPR not only requires a legal ground for processing activities, but also serves as a legal basis by enumerating six possible grounds for processing activities. Controllers who cannot identify a specific legal ground for their activities outside the realm of the GDPR can turn to the GDPR and try to rely on one of the six grounds listed in Article 6.

No single basis is better than others, and there is no hierarchy among the six grounds. However, the selection of a ground needs to be done with care, as different legal grounds give rise to different rights under the GDPR (see Fig. 1). The controller must determine the lawful basis before processing starts, and document it. This step is important, as it will be difficult to swap between different grounds at a later point and doing so may involve a breach of the GDPR.

Additionally, it is crucial that the controller informs the outside world in a clear and transparent way which lawful ground is being used for the processing, according to Articles 13–14 GDPR. Therefore, the selection of the best-suited lawful basis should be part of the data governance strategy of an organisation and be carefully assessed between all relevant stakeholders in the decision-making process (such as the legal department, the IT Department and the data protection officer—where applicable—within an organisation).

⁴Directive 95/46 [19].

2.2 The requirement of necessity when invoking the legal grounds

The literal wording of Article 6 reveals that, except for Article 6(1)(a) (consent), all other legal grounds require that processing be ‘necessary’.

To assess this notion of necessity (stronger than for example ‘just reasonable’), one should note whether the controller can reasonably achieve the same purpose without such processing or by a less intrusive means, by ensuring proportionality between the processing and the purpose.

Although consent may seem to be the only legal ground which does not require necessity, it actually does involve necessity to a certain degree, as valid consent for the purposes of the GDPR is given for a specific purpose, and the processing must be necessary in relation to that purpose, according to Article 5(1)(c).⁵

The foregoing shows the centrality of the concept of necessity in Article 6 GDPR and the centrality of the requirement for the lawful processing of personal data.

The prerequisite of necessity also appears in the EU Charter of Fundamental Rights⁶ and the European Convention on Human Rights (ECHR),⁷ both of which require that any interference or limitation to the right to privacy and data protection be ‘necessary’. However, the European Data Protection Supervisor has stated that they are not equivalent, arguing that the ‘necessity of processing operations in EU secondary law and necessity of the limitations on the exercise of fundamental rights refer to different concepts’.⁸

In the following sections we will focus consent and legitimate interests as two important grounds for lawful processing. We will come back to the notion of necessity when discussing the ground of legitimate interests.

2.3 Consent: only valid when respecting four requirements the (Article 6(1)(a) GDPR)

Consent has become a cornerstone of data protection across the EU.⁹ However, reliance on consent is not always the best option. Indeed, it is only appropriate if the controller can offer genuine choice, control and responsibility to individuals over the use of their personal data. If the controller would process personal data even without a user’s agreement, then asking for consent ‘is misleading and inherently unfair’.¹⁰ In such case, the controller may prefer reliance on legitimate interests in order to maintain the option of demonstrating that it is complying with the reasonable expectations of subjects and that the processing is not unfair.

The requirements for establishing consent under the GDPR have been tightened beyond those in Data Protection Directive 45/96 (the EU predecessor of the GDPR), making the establishment of valid consent harder to achieve. In what follows, we

⁵Hildebrandt [26].

⁶Charter of Fundamental Rights of the European Union [13].

⁷Convention for the Protection of Human Rights and Fundamental Freedoms [14].

⁸European Data Protection Supervisor (EDPS) [20].

⁹For a deeper understanding of this legal ground, see Kosta [33].

¹⁰Information Commissioner’s Office [30].

Fig. 2 Example of a tracking wall from the online content provider Medium

identify the most important requirements that consent must involve in order to be valid under the GDPR.

First, consent need to be freely given, specific, informed and unambiguous (Article 4). The requirement for free consent means giving people genuine control over how their data is used. As such, the controller must allow for separate consents for different processing operations¹¹ and consent to giving more data than necessary must not be a condition for the provision of a contract.¹² So, no bundled consent!

As examples of such bundled consent, one may refer to the so-called ‘tracking walls’ (see Fig. 2), functionalities that operate in online environments and present users with a ‘take-it-or-leave-it’ choice between privacy and access to a service (for instance when you are denied access to a website if you do not provide consent for non-necessary cookies being stored in your device).¹³

Interesting to better understand the tracking walls-problem is the recent is the recent official warning by the Information Commissioner’s Office—the UK data protection authority—to the Washington Post.¹⁴ The Washington Post cookie banner only allows users to access the service without being tracked by third-parties under the premium subscription option, while both the free service access and the basic subscription option require providing consent for non-necessary processing of data for third-party tracking (see Fig. 3).

Secondly, the requirement of informed consent is linked to the data protection principles of fairness, transparency spelled out in Article 5 GDPR and the information requirements set in Articles 13 and 14 GDPR (which oblige the controller to inform about, among others, the purpose of processing, and the lawful basis or existence of automated decision-making). In online environments this is normally done through privacy notices, which have long been accused of being too complex, long, and using legalistic jargon, and therefore, not being understandable for the average user. This leads to the provision of consent which does not reflect a real choice on the part of the individual. Kirsten Martin discusses ‘designed obscurity’¹⁵—situations where controllers create an illusion of complexity and intricacy—whereas *Reiden-*

¹¹Recital 43 GDPR and Art. 29 Working Party [2].

¹²Art. 7(4) GDPR and Art. 29 Working Party [2].

¹³In addition to the requirements of consent provided for in the GDPR, the future e-Privacy Regulation (which at the time of writing is undergoing its drafting process) is likely to address tracking walls by imposing a ban on them.

¹⁴*Privacy & Information Security Law Blog* [42].

¹⁵*Martin* [37].

Fig. 3 Example of a tracking wall from the online version of the newspaper Washington Post

berg et al. had already made the point that when notices are so vague, they are in practice equivalent to lack of notice.¹⁶

The solution for this was seen in the requirements for concise and easy to-understand-information.¹⁷ However, some authors have argued simplified language cannot provide enough detail to give complete information.¹⁸ Additionally, changes in technologies and in the new data ecosystem cause new additional troubles for companies in providing online notices. Examples are the small screens of internet of things devices,¹⁹ black box algorithms in machine learning²⁰ and the unpredictability of the results of big data which create a lack of knowledge of the secondary uses of the data.

Thirdly, consent must also be unambiguous and require a positive act of opting in to GDPR specific rules out pre-ticked boxes²¹—presented separately from other terms and conditions. The data subject retains in any event a right to withdraw consent (Article 7).

Lastly, special categories of data require explicit consent, which needs to be expressed in writing, rather than by any other positive action (Article 9).

Even when they are complex, privacy notices are still useful even if only to provide advanced readers and data protection authorities with details off the processing. Additionally, several solutions and models have been proposed to manage the difficulties of providing consent. Culnan and Bruening²² propose a model based on an

¹⁶Reidenberg, Russell, Callen, Qasir, and Norton [44].

¹⁷Kuner et al. [34].

¹⁸This issue was christened ‘the paradox of transparency’ by Baroccas and Nissebaum [4].

¹⁹Culnan and Bruening [16].

²⁰Pasquale [41], Diakopoulos [18], Moerel and Prins [38] and Kuner et al. [34].

²¹Recital 32 GDPR.

²²Culnan and Bruening [16].

Fig. 4 Information Commissioner's Office privacy policy. The ICO uses a creative combination of video and images in its privacy policy

environment of transparency, where transparency is tackled not only by means of notices but through a variety of approaches (*i.e.*, just-in-time notices, images, icons or sounds as well as public awareness, so as to instil a better understanding of the data ecosystem at large). Other authors argue in favour of reserving consent only for those uses of data that derive from what is reasonably expected,²³ so that individuals will pay more attention whenever consent is required of them.

Some of these models, suggestions and practices are being considered nowadays. For instance, Recital 60 GDPR already promotes the use of icons, the Information Commissioner's Office uses a combination of video, images and layered informa-

²³Baroccas and Nissebaum [4]; World Economic Forum and The Boston Consulting Group [50].

<h2>Introduction</h2> <p>Our registered users ("Members") share their professional identities, engage with their network, exchange knowledge and professional insights, post and view relevant content, learn and find business and career opportunities. Content and data on some of our Services is viewable to non-members ("Visitors").</p> <p>We use the term "Designated Countries" to refer to countries in the European Union (EU), European Economic Area (EEA), and Switzerland.</p>		<p>We are a social network and online platform for professionals. People use our Services to find and be found for business opportunities and to connect with others and information. Our Privacy Policy applies to any Member or Visitor to our Services.</p>
<h2>Services</h2> <p>This Privacy Policy applies to LinkedIn.com, LinkedIn-branded apps, Slideshare, LinkedIn Learning and other LinkedIn-related sites, apps, communications and services ("Services"), including off-site Services, such as our ad services and the "Apply with LinkedIn" and "Share with LinkedIn" plugins, but excluding services that state that they are offered under a different privacy policy.</p>		<p>This Privacy Policy, including our Cookie Policy applies to your use of our Services.</p>

Fig. 5 LinkedIn's privacy policy. Regardless of other considerations about its content, LinkedIn's privacy policy serves as a good example on how to provide detailed information in the left column and shorter and simpler information in the right column, using plain language that is understandable and avoids reading fatigue

Fig. 6 Instagram's privacy options. Instagram tricks users into syncing all their contacts with the app when picking a username by using unnoticed lettering for the more protective option

tion for its privacy notice²⁴ and LinkedIn provides layered information using plain language (see Figs. 4, 5 and 6).

2.4 Legitimate interests for processing personal data and its three-step assessment (Article 6(1)(f) GDPR)

2.4.1 General introduction to legitimate interests

The concept of a 'legitimate interest' may be among the most confusing in the data protection framework, loved, and loathed in equal measure. In the next paragraphs we will try to shed some light on this notion. Article 6(1)(f) GDPR provides for the lawfulness of processing when it

²⁴The Information Commissioner's Office privacy notice can be found here: <https://ico.org.uk/global/privacy-notice/>.

‘is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child’.

Article 6.1.f GDPR also adds that this basis is not applicable to the processing carried out by public authorities in the performance of their tasks.

Legitimate interest is not a new concept. It was found in Article 7 of the former Data Protection Directive 95/46. The current wording is substantially unchanged²⁵ — which means that it uses ambiguous terms that may create uncertainty and need interpretation.²⁶ However, there is (limited) experience gained in the lifetime of the Directive together with the case law of the European Court of Justice²⁷ Article 6(1)(f) GDPR also includes some new, useful clarifications: first, the explicit requirement for stricter protection when the data subject is a child, and second, the exclusion of this ground for public authorities in the performance of their tasks. However, public authorities can still use legitimate interests as a basis for activities other than their official tasks.

In line with the principles of transparency and fairness, when the controller applies legitimate interests as the basis for processing, it must inform the data subject about the legitimate interests being pursued either by the controller itself or by a third party (Articles 13(1)(d) and 14(2)(b)).

The use of Article 6(1)(f) as the lawful basis for the processing of personal data requires what has been recognised as a three-step assessment, which, ultimately, must be assessed on a case-by-case basis.²⁸ First, there must be an interest on the part of the controller or a third party, which must be legitimate. Secondly, a necessity test must be passed. Thirdly, a balancing test must be applied, weighing on one side the legitimate interests of the controller or a third party and on the other side the interests and rights of data subjects.

Neither the Directive nor the GDPR provide any indications as to how to apply this basis, and in particular, how to perform the balancing test. Regarding the circumstances where legitimate interests may be relied upon, the GDPR provides slightly more direction. Recitals 47–50 provide some examples of cases where there may be a possibility for basing processing on legitimate interests, such as the prevention of fraud (Recital 47), direct marketing (Recital 47), the transmission of personal data among a group of organisations for internal administrative purposes (for instance, for the processing of employees’ data (Recital 48), ensuring network and IT secu-

²⁵For a further analysis of legitimate interests see *Ferretti* [21]. *Ferretti* argues in favour of a restrictive interpretation of legitimate interests as a lawful basis for processing in order to provide what he called a ‘rights’ perspective (*i.e.*, a people’s rights protective approach).

²⁶*Ferretti* [21].

²⁷For case law on the balancing test, see Cases C-13/16 *Rigas* [7], C-398/15 *Manni* [9], C-212/13 *Rynes* [8], JoinedJ cases C-468/10 and 469/10 *ASEF and FECEMD* [10]. For a further review of case law on legitimate interests see *Nymity* and the *Future for Privacy Forum* [40].

²⁸This test has been widely recognised among different stakeholders. See Art. 29 Working Party [3]; *European Data Protection Supervisor (EDPS)* [20]; *Kamara and de Hert* [32].

rity (Recital 49)²⁹ or the indication done by the controller of possible criminal acts or threats to public security which may require the subsequent transmission of the relevant personal data to a competent authority (Recital 50)).

In any case, these are examples where legitimate interests ‘may’ apply, however, this cannot be always be seen as automatically applicable. Even in these circumstances, the data controller must conduct an assessment to probe whether Article 6(1)(f) applies to its specific situation.

2.4.2 The 3 steps: what is a legitimate interest, when is there necessity and how to balance?

In general terms, interest is the broad value or intention the controller wants to fulfil with the processing and will be legitimate when it respects all relevant laws (and not merely data protection laws). It must be real, present, and clearly articulated so as to allow the balancing test to be carried out.³⁰ For instance, an interest in profiling a customer in order to engage in further actions like sending advertisements would be an interest on the part of the controller. However, a broad statement that an economic benefit would be obtained would not qualify as a valid interest.³¹ This brings us again to the central notion of necessity as discussed *above* (Sect. 2.2).

Assessment of the existence of a necessity involves evaluating whether the processing of data is directly linked to accomplishing the legitimate interest and whether there is a way which is less intrusive upon the rights of individuals to achieve the same goal.³² This does not require the processing to be absolutely indispensable: if there is another way to pursue the same objective but which requires a disproportionate effort, then the processing may be deemed necessary.³³ The boundaries to what is necessary in each case will be much related to the principles relating to the processing of personal data, provided in Article 5 GDPR, such as lawfulness, fairness, data minimisation and integrity.³⁴

The last step is the balancing test, as between the legitimate interests of the data controller or third party and the interests or fundamental rights and freedoms of the data subject (which do not need to be legitimate. Thus, for instance, a subject could argue the use of his image obtained from a surveillance camera engaging in incorrect behaviour cannot be used to dismiss him). When doing the balancing of interests, the controller must still comply with the principles of the GDPR. This means that the controller must refrain, for instance, from trying to provide an unfair result to the balance and from acting in a biased way so as to favour his own interests.

The balancing must consider the whole context of the processing, and in particular the nature of the interests (such as types of interests and data, vulnerability of

²⁹For further analysis on the importance of processing personal and other types of data for security purposes see *Hoffman and Rimo* [27].

³⁰Art. 29 Working Party [3].

³¹*Data protection Network* [17].

³²*European Data Protection Supervisor (EDPS)* [33]; *Information Commissioner's Office* [28].

³³*Data protection Network* [17].

³⁴*Kamara and de Hert* [32].

the individuals), the impact of the processing and the safeguards implemented by the controller. Consequently, some scholars argue that a legitimate interest is the most appropriate basis for standard innocuous business practices.³⁵ Others go beyond this and state that, due to the need of a balancing test, Article 6(1)(f) GDPR is a more protective basis for individuals' rights than consent, therefore, arguing in favour of legitimate interests being used as a basis for the processing of electronic communications personal data.³⁶

Special relevance acquires the reasonable expectations of the data subject³⁷ which may be different depending on the relationship between the controller and the individual.³⁸ For instance, a person that is already a customer of a Chinese food restaurant (and therefore has a prior relationship with the controller), would reasonably expect the restaurant to keep his or her name and home address for future delivery orders.

Additionally, great importance has the further processing of the data for secondary purposes other than those which triggered the collection of the data, for instance, to conduct profiling, to mine data or any other objective. In this line, the concept of compatible purposes is of crucial, together with transparency and purpose limitation principles.³⁹

3 Profiling, definition and distinctions

3.1 What is it? (Article 4.4 GDPR)

Nowadays, the development of technologies enabling for higher volumes of data storing, faster transmission and computing power and more sophisticated analysis make it easier to collect more and more varied data and to extract relations from it, allowing for the creation of more precise profiles. The uses of profiles are many, and their greatest opportunities are description and, overall, prediction of behaviours for purposes ranging from credit scoring to direct marketing and criminal behaviour.

While profiling activities have enormous benefits, they can also create risks, in particular when they are used without the knowledge of the individuals concerned, a situation that clearly undermines fairness.

³⁵ Van der Sloot and Borgesius [46].

³⁶ Centre for Information Policy Leadership (CIPL) [12]. The report makes an argument in favour of enabling the use of legitimate interest as a basis for the processing of electronic communications personal data (both content and metadata), contrary to the position taken by the ePrivacy proposed Regulation, which allows for the processing on this data with the consent of the user but not under the legitimate interest of the service provider. Specifically, the report asserts that, in practice, individual privacy rights may ultimately benefit from a strong protection if an organization relies on legitimate interests for processing personal data, including electronic communications data. This is because where a company relies on Art. 6(1)(f) GDPR, it must implement additional measures to pass the balancing test. On the other side, it is argued in the report, although consent gives individuals the highest level of control over their personal data (or at least, in theory), it may not always result in a better protection of their rights in practice.

³⁷ Recital 47.

³⁸ Kamara and de Hert [32].

³⁹ Art. 5 GDPR.

Article 4(4) GDPR defines profiling as ‘any form of *automated processing* of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, *in particular to analyse or predict* aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements’ (emphasis added).

The Council of Europe has defined the concept of profile as ‘the set of characteristics specific to a group of individuals and, consequently, to each individual belonging to the group’. In this regard, profiling is defined as ‘applying to a particular individual the profile of a group with which he or she can be identified through the data collected on him or her. This operation will result in the creation of new characteristics relating to the identified or identifiable individual who has been profiled in this way (. . .). *Profiling therefore creates new personal data*’ (emphasis added).⁴⁰

The foregoing teaches us that profiling activities require a degree of automation. One of their main uses is the prediction of behaviours and patterns, for which they can be read as creating personal data. The Council of Europe clarifications suggest that where a combination of characteristics allow us to create a profile for a group of people, all those characteristics will define every individual within that group. This will certainly not be the case for all profiles (see the discussion on distributive group profile below in this section *below*). In many cases, profiling requires a statistical extrapolation which leads to partially accurate and partially inaccurate results, a fact that both the data controller and the decision-maker need to bear in mind.

3.2 Useful distinction: individual profiling and group profiling

Profiling activities can be classified according to the subject to which they refer—*i.e.*, a single individual or a group.⁴¹ Individual profiling targets one specific person with the aim of identifying him or discovering characteristics about him, for instance, through device fingerprinting. On the other hand, group profiling deals with a set of people who share certain characteristics or patterns. Sometimes, profiling seeks to discover unknown patterns within a known community (for instance, a political party). At other times, profiling identifies that a group of people, who did not previously form a community, share some patterns that were not known, correlating with other facts, (for instance, that couples who have children between 1 and 3 years old and who live in a certain neighbourhood have a certain probability of buying one six-pack of beer every two weeks).

In this latter case, the identified group of people who share patterns are couples that have children between 1 and 3 years old and that live in a certain neighbourhood, whereas the correlation found among them is their beer consumption habit.

Our interest lies specially in these group profiles, which are the outcome of three technical stages.⁴²

⁴⁰Council of Europe [15].

⁴¹Lammerant and de Hert [35].

⁴²See, among others, Council of Europe [15]; Lammerant and de Hert [35]; Vedder [48]; Gil González [22].

First, the collection of data, which nowadays is done mostly on a large scale, which is then digitalised, enriched and coded to be then stored in a data warehouse. The resulting data may be nominative, coded or anonymised.⁴³ It may consist of the contents of a shopping basket, a telecommunications bill, a list of trips on public transport. In addition, the collected data is prepared for the subsequent analysis that will take place.

Secondly, the analysis of the data by means of data mining techniques to search for correlations and patterns among individual behaviours and characteristics and the creation of specific profiles. For example, what link can be made *a priori* between residence in a particular postal code area, the consumption of beer, the monthly rent and the ability to repay a loan? Additionally, statistics are used to calculate a probability for the correlations found.

For instance, if a person lives in certain location, buys beer more than twice a week, and his rent is under X euros per month, he can be categorised under the below-35-single-male profile, and the data shows that people in that group have a probability of 27% for falling behind with a payment.

This is a reversal of traditional data analysis, where the hypothesis would be chosen first and then the data queried to test the hypothesis.⁴⁴

Thirdly, whereas in the second phase profiles are created, the third stage involves using them for profiling of other individuals. That is, the third stage involves drawing inferences and deducing characteristics or behavioural variables referring to the past, present or future from some other variables we can observe on the individual. For instance, if we observe a person who shares the characteristics of our below-35-single-male profile, we would assume his default rate is also 27%. With that information, the controller can take decisions about the person.⁴⁵ As a matter of fact, this involves a margin of error of assigning characteristics to a person that do not really define him or her but are rather those of the group to which he or she has been included (the profile group), regardless of whether he or she ever defaulted on a loan before, or has savings.

The banking sector uses profiling and data mining extensively to assess customer risk (*i.e.*, creating credit scoring), which refers to future behaviour. To do this, the banking institutions analyse large quantities of customers' data and their repayment history to identify the characteristics that serve as a proxy for finding correlations and to identify who repays and who fails to repay due. That

⁴³Regardless of whether data is anonymised, the mere collection of data that is personal makes the data protection framework applicable. In addition, when considering large or rich datasets, as is often the case nowadays, together with powerful analytical tools, the process of anonymising data gives rise to serious concerns. Therefore, the most common approach is to consider that this stage involves coded data (*i.e.*, pseudonymised data) rather than anonymised data. Consequently, data protection rules must be respected during this process.

⁴⁴Information Commissioner's Office [28]; Gil González [22].

⁴⁵On the contrary, merely selecting individuals on the basis of their real characteristics cannot be deemed as profiling. For instance, if a financial institution selects customers with an income of over 8000 euros/month and with assets valued at over one million euros and groups all these customers together, the bank has not engaged in profiling but rather in a mere selection, which does not involve a margin of error.

way, when a new customer applies for a loan, the bank gathers data about him or her to calculate his credit score. This score represents a probability of the individual having certain characteristics previously observed in other customers, and as such, entails a margin of error.

3.3 Useful distinction: distributive group profiles and non-distributive group profiles

Among group profiles, we need to further differentiate between distributive and non-distributive profiling, defined by *Vedder* two decades ago.⁴⁶

First, distributive group profiles are those which assign certain properties to members of a group in such a way that these properties are unconditionally manifested in all those members, as if they were a matter of fact. Therefore, in these cases, group profiles are applied to the members of the group as if they were individual profiles.⁴⁷

Non-distributive group profiles work differently. They are framed in terms of probabilities and comparisons between members of the group and the group as a whole as against other groups. The result of this is that not every individual member in the group will present all the characteristics, but they may be treated as if they did.

For instance, a banking institution may deny a loan on the basis of the low credit score assigned to an individual due to the fact that he or she has been characterised as belonging to a group profile of individuals linked to bad creditor qualities. This may happen regardless of whether the individual is a clear exception to that group and has never failed on an instalment before, which may lead to discrimination issues.

In words of *Vedder*, ‘the information contained in the profile or generalisation envisages individuals as members of groups; it does not envisage the individuals as such’.⁴⁸

It is this use of non-distributive group profiles which can lead to the highest risks of unfairness. Fairness implies, in brief, considering how the processing may affect the individual and justify any adverse impact,⁴⁹ as well as acting as promised (that and is, in accordance with the information provided as required by the rights of Articles 13 and 14 GDPR). To ensure fair processing when undertaking profiling, the controller should use appropriate mathematical or statistical procedures for the profiling, implement appropriate measures to detect and correct inaccuracies and prevent discriminatory outcomes.⁵⁰

Recent case law has taken account of this risk regarding group profiling. The Finnish National Non-Discrimination and Equality Tribunal determined⁵¹ that a per-

⁴⁶ *Vedder* [48].

⁴⁷ *Lammerant and de Hert* [35].

⁴⁸ *Vedder* [48].

⁴⁹ *Information Commissioner's Office* [29].

⁵⁰ Recital 71.

⁵¹ Case C-216/2017 *National Non-Discrimination and Equality Tribunal of Finland*, EU:C:2017:216:TOC [39].

son was discriminated against when applying for a consumer credit because no individual assessment of his solvency was carried out. Only general information was taken into account (such as age, gender, place of residence and native language) to give the subject a certain solvency score. At the same time, the bank institution ignored information regarding the person's own credit behaviour and creditworthiness even though these factors would have favoured extending credit to him. The Court considered that even if an individual score is made up of statistical variables, the score in question was not an individual assessment based on the income level and financial status of the person in question, but a case of statistical profiling, which was mainly based on reasons related to grounds of discrimination. This is the first legal decision concerning discrimination in automated credit granting.

Let us now return to European data protection law. Of special importance for the legal guarantees foreseen in this body of law is a distinction based on process: challenges, risks and consequences of profiling activities may depend on whether the process is carried on using solely using automated means or not. This fact therefore deserves special attention.

After analysing the processes for profiling, the following sections will be devoted to studying the interplay of the lawful grounds for processing personal data and the different types of profiling recognised in the GDPR depending on their effects over individuals.

4 Solely automated decision-making (profiling) with legal or similarly significant effects

4.1 Starting point: Article 22 GDPR

Article 22.1 GDPR establishes that individuals '*have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*'.

There is an exception to this provision (under Article 22(2)) where automated decision-making is necessary either for entering into or the performance of a contract, where there is explicit consent on the part of the data subject or where it is authorised by law (*e.g.*, for the prevention of fraud).⁵² Noticeably, legitimate interest is not a lawful ground for this kind of decision or profiling, (although it can legitimate less intrusive profiling activities falling outside Article 22).⁵³

⁵²Recital 71.

⁵³Some voices have arisen that seem to criticize this provision. See, as an example, the *Centre for Information Policy Leadership (CIPL)* [11]. The report highlights the fact that legitimate interests are not among the lawful basis for automated decision-making including profiling, while valid consent may prove difficult to be obtained: 'How can consent be 'specific, informed and unambiguous' if an organization may not be fully aware of how collected data will be used, or of all subsequent purposes of processing at the time of collection?'.

In case of necessity for a contract or consent, the controller must guarantee, at least, the following to the subject: the right to obtain human intervention, the right of the individual to express his or her point of view and the right to contest the decision (Article 22(3)).

Thus, automated profiling is not permitted unless one of the three exceptions can be called upon. In two of the three, the use of automated profiling is only allowed for when suitable measures are taken. However, the provision of such suitable measures can be challenging to apply, as will be discussed later on. Apart from problems with checks and balances, there are problems concerning the narrow scope of the prohibition (see also *below*), but also with the legitimacy of these three exceptions themselves, and problems with the way in which data subjects should be informed about the use of automated profiling.

Take for example the first exception, namely, the *necessity* of the processing for the performance of a contract. This can itself raise several discussions about the scope of the exception itself. For instance, ‘is extensive automated profiling necessary to obtain a loan from a bank?’. Regarding the exception of consent, the assessment of its validity given needs to be based, among other factors, on the issue of whether the consent given was sufficiently informed. For that, the user will count on the information offered to him before the automated decision-making (based on Arts. 13–14). These articles establish the duty of informing beforehand about ‘the *existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*’ (emphasis added).

The wording of Articles 13, 14 and 22, in our view, uses ambiguous terms that can compromise the effectiveness of the GDPR to ensure protection for individuals.

4.2 The information loophole in Articles 13–14 due to ambiguous terminology

First, the controller may face difficulties in providing prior information, particularly as regards the logic involved and the consequences envisaged, due to the use of complex analytical methods.

Second, the information must be provided ‘at the time when personal data are obtained’, in the event that personal data is obtained from the data subject himself (Article 13(1)) or within a reasonable time frame, at the time of the first communication or when the data is disclosed to another recipient, in case the data is not obtained from the subject (Article 14(3)). This excludes, for instance, the possibility of informing, even in generic terms, about new data obtained about subjects due to data mining or inferences⁵⁴ and therefore, about the consequences of the processing of this new data.⁵⁵

Additionally, this obligation refers to Article 22(1) and (4). Therefore, this is to be interpreted as meaning that decisions and profiling falling under Article 22(2) (*i.e.*,

⁵⁴ Gil González [23].

⁵⁵ It is also arguable whether the controller is compelled to inform about inferred data under Art. 15.b on the ‘categories of personal data’ concerned or under Art. 15(3) ‘the controller shall provide a copy of the personal data undergoing processing’.

those necessary for a contract, for which consent was provided or because authorised by law) must not be informed about? If this is the case, the height where we set the bar to consider valid consent was given, or whether the processing is necessary for the performance of a contract will be crucial. However, as the necessity test is done by the controller in first instance, there may be incentives to promote lack of transparency and fairness.⁵⁶

4.3 Two problems with regard to the prohibition in Article 22(1) GDPR

Article 22 gives individuals the right to oppose to fully automated decisions which may have legal or similar significant consequences over them.⁵⁷ Two main sets of issues arise here.

First, many profiling activities may fall outside the scope of Article 22, due to the ambiguity of the definition in this provision. Some effects will be clearly significant (such as the denial of a loan), but other effects may not be as clear (for instance, being granted a loan with an interest rate higher than what would have been granted by using non-solely automated means). Would this trigger the rights and measures of Article 22? The issue is emphasised by the information asymmetries caused by the inefficiencies of Articles 13–14, which account for the only information the user will have on most occasions.

Second, what qualifies as solely automated decision has also raised discussion.⁵⁸ For instance, imagine a human intervention that is not intended to question any decision, or done by a person with no special education to understand how the model works. Would this leave the decision out of the scope and guarantees of Article 22? Logic may respond with a negative answer, although these are all issues that will need to be solved during the life of GDPR.

4.4 Suitable measures in case automated profiles are used in exceptional cases (Article 22(3) GDPR)

As mentioned, when one of the exceptions applies, the data controller is required to implement ‘suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part

⁵⁶In its report, the *Centre for Information Policy Leadership* (CIPL) [11] also expresses the difficulties for meeting the requirement of transparency and information with respect to decisions made by complex algorithms, which cannot be often anticipated. In addition, the report states that, in technically complex scenarios where surprising correlations are found, such as when artificial intelligence is being applied, it turns difficult to know in advance what qualifies as ‘necessary’ for the purpose of the processing, or even what are the purposes of the processing, as these may change as the machine learns.

⁵⁷It is not clear whether this Art. indeed sets a right to object or a prohibition on the controller. On the one hand, the wording of the Art. states that it is a right, and it is located in Chapter 3 GDPR, entitled ‘Rights of the data subject’, which would mean that the provision only applies if actively invoked by the data subject. On the other hand, the Art. 29 Working Party interpreted it as a general prohibition. This discussion, however, is beyond the scope of this paper.

⁵⁸*Veale and Edwards* [47].

of the controller, to express his or her point of view and to contest the decision' (Article 22(3) GDPR).⁵⁹

Obtaining human intervention is one of the key elements here. However, in order for it to be an effective and valid measure, the person must be relevant in the reviewing process. An artificial intervention that does not consider how the decision was made and question it is not valid. Some factors that can be taken into account here are assessing whether the human has the authority to change the machine-made decision, and assessing whether he or she has the knowledge to do so.

The other two suitable measures mentioned in Article 22.3—expressing one's point of view and contesting the decision—would very much depend on the information the data subjects count on. Therefore, the transparency principle together with the information obligations turn out to be very significant to the effective exercise of the guarantees.

4.5 Special categories of data can never be used, unless there is consent or public interest (Article 22.4 GDPR)

Automated decisions can never be based on the processing of special categories of personal data, unless there is explicit consent or substantial public interest, and there are suitable measures to safeguard the data subject's rights and freedoms and legitimate interests (Article 22.4).

This includes not only data obtained directly from the data subject, but also derived or inferred data. This is relevant since the profiling activity can use non-special categories of data as an input to infer special categories of data. Consider, for instance, the possibility of inferring someone's state of health from his or her shopping data combined with nutritional data. The same can happen with other special categories of data, such as political convictions, religious beliefs or sexual orientation.⁶⁰

5 Not solely automated decision-making (profiling)

After our discussion of group profiling (Sect. 4) and the focus of the GDPR on automated—decision-making based on profiles (Sect. 5), let us now turn to decision-making and profiling activities not based solely on automated processing or not producing legal or similar significant effects (in other words, those not falling within Article 22).

These practices are not governed by a prohibition and can be grounded under any of the lawful legal grounds in Article 6 discussed *above* (Sect. 2). Article 29 Working Party has specifically acknowledged that profiling carried out under these circumstances can be based on Article 6(1)(f) (the ground of legitimate interest).

⁵⁹Recital 71 mentions a right to obtain an explanation of the decision reached which is not included in Art. 22. This discordancy has triggered numerous debates about the existence or not of a right to an explanation. An exhaustive discussion about this can be found in *Wachter, Mittelstadt and Floridi* [49]; *Malgieri and Comandé* [36] and *Goodman and Flaxman* [24].

⁶⁰Art. 29 Working Party [1].

Regardless of the ground relied upon, duties to inform under Articles 13–14 are once again imposed. However, this time, individuals are not entitled to be informed about the existence of automated decisions (those which exist, but do not cause, *at least in the eyes of the controller*, legal or significant effects); their logic or for the future foreseen. Nor may they request human intervention, express their opinion or challenge the decision.

The foregoing profiling-friendly regime might cause concerns whenever profiling is done under the legitimate interest basis. In this case, the controller is the one carrying out its own self-assessment to decide if Article 6(1)(f) may apply, as well as self-assessing whether the profiling or decision is automated or (even more relevantly, due to the degree of subjectivity), the effects are significant. Will an automated profiling activity which aims at identifying consumption patterns so as to offer targeted discounts to people be regarded as having significant effects?

In any event, the principles of transparency and lawfulness still apply and serve as a boundary for abusive practices. The ICO has actually argued that fair processing is sufficient to address the legal and ethical challenges of new technologies.^{61,62}

In addition, if the profiling activities are challenged and subsequently found not to be grounded in a lawful basis, controllers face the highest tier of sanctions under the GDPR. This may serve as a counterbalance against bad practices. This can be the case when the necessity test is not passed (for every Article 6 ground apart from consent), when the balancing test is not fairly done (for the legitimate interests) or when users have not provided free, informed and unambiguous consent.

The WP29 has provided guidance on some of the factors to be considered in the balancing of interests. These include the level of detail of the profile, its impact over individuals and safeguards put in place to ensure fairness, non-discrimination and accuracy. For all that, it states ‘it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive processing and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering’.⁶³

6 Bringing in principles (transparency and fairness) and competition law to get the balance right

In the foregoing text, we saw several problems with the GDPR regime for profiles—such as the scope of the prohibition of Article 22; the way in which users must be presented with the information regarding automated means for profiling; and the use of ambiguous terminology in the GDPR provisions. For this, we believe that the principles of transparency and the fairness of Article 5 GDPR may act as interpretative principles and therefore provide for a remedy.

⁶¹ Information Commissioner’s Office [28].

⁶² For a critical analysis of the ICO’s report on fairness and the GDPR, see Butterworth [5].

⁶³ Art. 29 Working Party [1].

Interestingly, the notion of fairness is not exclusive to data protection law, but also underpins competition law and can serve a bridge between these different arenas. Indeed, data protection and competition law can be linked, specifically in relation to the concept of fairness and the legal grounds for processing personal data. *Kalimo and Majcher* argue⁶⁴ that the digital economy companies usually provide a service in exchange for user consent to process personal data, which creates a commercial relationship between the provider and the individual, subject to the Treaty on the Functioning of the European Union (TFEU). The concept of fairness would allow, for instance, the argument that where a company provides information about its terms of service in a way that is difficult to understand, consent has not been obtained in accordance with the GDPR. This creates a competition law issue, as this establishes the requirement to act on the basis of fair trading conditions.

Illustrative in this regard is the *AstraZeneca* antitrust case,⁶⁵ where the CJEU found the company had violated the TFEU due to its manifestly misleading information and lack of transparency. This is in fact similar to the notion of a ‘bundling prohibition’, which originated from German competition law and has been observed in Article 7.4 GDPR.

The requirement to request consent to the processing of personal data as a condition for accessing a service has led to calls in favour of data-free services. Only time will tell whether the market extensively incorporates this idea of data-free services. For the time being, some examples can already be found, as shown both in Fig. 7 and in the Washington Post example discussed *above* (Sect. 2.3).⁶⁶

Fairness also influences the concepts of proportionality and necessity found in data protection law, which, as already mentioned, are vital in assessing the best lawful basis for processing under the GDPR.

The same may be said regarding the reinforcement of data protection consent through the prohibition in competition law on the abuse of dominant positions.⁶⁷ The data economy is characterised by very few but big market players (such as Google and Facebook) with a high share in the market for digital services which are essential in our current society. Therefore, data subjects/consumers may not have a real choice regarding providing freely given consent.⁶⁸

An instance of this is the Dutch Data Protection Authority investigation of Google⁶⁹ for combining personal data obtained using various services of the company (its internet search engine, video streaming webpage, web browser, online maps, e-mail) for profiling activities and personalised services and ads. The investigation concluded that no valid consent was granted, since it was not unambiguous or sufficiently informed. Likewise, legitimate interests could not

⁶⁴Kalimo and Majcher [31].

⁶⁵Case C-457/10, *AstraZeneca* [6].

⁶⁶*Privacy & Information Security Law Blog* [42].

⁶⁷*Graef, Clifford and Valcke* [25].

⁶⁸However, one must keep in mind that competition law prohibits the abuse of market power, not market power in itself, so that an assessment on whether the personal data price was fair or not is needed.

⁶⁹*The Netherlands, Autoriteit Persoonsgegevens*, z2013-00194 [45].

Fig. 7 Example of service which offers money-free and data-free options

be a valid ground because Google's interest did not outweigh the data protection rights of the users. The balance of interests involved consideration of the nature of the data (much of which was sensitive, such as payment information, location data, and information on surfing behaviour across multiple websites), the diversity of services, the lack of adequate and specific information, and interestingly, the considerable share of the market of the services in the country. This rendered it almost impossible for a user to have a digital presence without coming across Google's services (even if only through third-party websites and cookies). In this case, therefore, typical competition law concepts such as market share were considered by the authority to construe its arguments under data protection laws.

7 Conclusion: reading principles together with provisions to apply the legal grounds and the profiling mechanisms correctly

We have first looked at the legal grounds for data processing according to Article 6 of the 2016 General Data Protection Regulation (GDPR), namely, the data subject's consent, the necessity for the performance of a contract/for a compliance with legal obligation/to protect vital interests, for the performance of a task carried out in the public interest or exercise of official authority/necessity for a legitimate interest pursued by a controller or by a third party.

We have paid special attention to the grounds of unambiguous consent and legitimate interests, accompanying this is a legal analysis with practical examples. In

relation to them, we have noted where the GDPR has introduced changes in relation to the previous Data Protection Directive 95/46, such as the stronger information requirements in the GDPR or the call for express consent or the right to withdraw consent. We have also seen where the GDPR has remained substantially unchanged—for instance, in the wording regarding what constitute legitimate interests—which means that the previous case law of the European Court of Justice is still useful under the GDPR.

We then addressed the topic of profiling. After looking at individual and group profiling, we focused on the legal regime applying to these under the GDPR, which depends on whether profiling is done by solely automated means or not. Article 22 sets a general prohibition on decision-making processes including profiling carried on under solely automated methods with legal or similarly significant effects. This prohibition is followed by three exceptions as set in Article 22(2): the data subject's explicit consent, the necessity for the performance of or entering into a contract, and the authorisation by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. In the first two cases, the controller must also guarantee that the subject will have a right to have a human review of the decision, to express his or her own point of view and to appeal the decision. On the other hand, decisions that are not solely automated or do not produce significant effects, fall outside the scope of Article 22, its prohibition and safeguards, and can, for instance, be based on legitimate interests.

Regardless of whether the processing falls in Article 22 or not, we have argued that the vagueness and subjectivity of the concepts used in the GDPR can undermine subjects' rights and data protection principles in practice. For instance, regarding the scope of Article 22 itself, the meaning of what is *solely* automated or what are *significant* effects is not clear. This may cause many processes to fall beyond the scope of Article 22 and its safeguards. Additionally, the duty of the controller in the case of automated decisions to inform the subject beforehand about the *logic involved* and the *envisaged consequences* can become very challenging in practice due to the complexity of the analytics and decision-making techniques.

To offset these drawbacks, we looked at how the principles of transparency and overall fairness, as enshrined in Article 5 GDPR may serve as a last resort to identify the appropriate checks and balances. In particular, the concept of fairness is to be interpreted with regard to the concepts of necessity and proportionality, which are at the root of the choice of the best-suited lawful basis for processing under GDPR. Moreover, the principle of fairness is not unique to data protection law but present in other fields such as competition law. Therefore, solutions to data protection issues can be found outside data protection legislation, for instance in competition law. In order to clarify that this is not merely theoretical reasoning, but an argument that can be applied in fact, we have presented two court decisions as example. The first one was a data protection case which took into account competition law concepts, and the second one was a competition law judgment which considered data protection notions.

In any case, the adjustment of this is burdensome according to a more flexible or stricter interpretation will need to be assessed on a case by case basis. This will come

over time from national authorities, from national courts, and in the last resort, from the European Court of Justice. In addition, guidelines provided by data protection authorities and the European Data Protection Board will prove useful. The interplay of rights and concepts across legal frameworks will also present opportunities for further discussion by legal scholars.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. Article 29 Working Party: Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP 251 rev. 01) (2018). Available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
2. Article 29 Working Party: Guidelines on consent under Regulation 2016/679 (WP 259 rev. 01) (2018). Available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
3. Article 29 Working Party: Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46 (WP 217) (2014). Available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
4. Barocas, S., Nissebaum, H.: Big data's end run around anonymity and consent. In: Lane, J., Stodden, V., Bender, S., Nissenbaum, H. (eds.) *Privacy, Big Data and the Public Good*. Cambridge University Press, Cambridge (2014)
5. Butterworth, M.: The ICO and artificial intelligence. The role of fairness in the GDPR framework. *Comput. Law Secur. Rev.* (2018). Available at: <https://reader.elsevier.com/reader/sd/F4A2552841043362FF7A3BB9555F86DC14B1A531E9EDFDA585EEE202EA038D31B5878BDFC85756C5661695A4956A63BD>
6. C-457/10, AstraZeneca, ECLI:EU:C:2012:770
7. Case C-13/16 Rigas, ECLI:EU:C:2017:336
8. Case C-212/13 Ryneš, ECLI:EU:C:2014:2428
9. Case C-398/15 Manni, ECLI:EU:C:2017:197
10. Cases C-468/10 and 469/10 ASNEF and FECMD, ECLI:EU:C:2011:777
11. Centre for Information Policy Leadership: *Delivering Sustainable AI Accountability in Practice*. First Report: Artificial Intelligence and Data Protection in Tension (2018)
12. Centre for Information Policy Leadership: *The ePrivacy Regulation and the EU. Charter of Fundamental Rights* (2018)
13. Charter of Fundamental Rights of the European Union [2000] OJ L C 364/01
14. Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14, Rome, 4 November 1950
15. Council of Europe: The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec (2010) 13 and explanatory memorandum (2010). Available at: <https://rm.coe.int/16807096c3>
16. Culnan, M.J., Bruening, P.: Privacy notices limitations, challenges, and opportunities. In: Selinger, E., Polonetsky, J., Tene, O. (eds.) *The Cambridge Handbook of Consumer Privacy* (2018)
17. Data protection Network: Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation (version 2.0) (2018). Available at: <https://www.fairtrade.org.uk/~media/FairtradeUK/Resources%20Library/Data%20Protection%20Network%20-%20Guidance%20on%20the%20use%20of%20legitimate%20interest.pdf>
18. Diakopoulos, N.: *Algorithmic-accountability: the investigation of Black Boxes*. Tow Center for Digital Journalism (2014)
19. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31
20. European Data Protection Supervisor (EDPS): *Developing a toolkit for assessing the necessity of measures that interfere with fundamental rights* (2016). Available at: https://edps.europa.eu/sites/edp/files/publication/16-06-16_necessity_paper_for_consultation_en.pdf

21. Ferretti, F.: Data protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights? *Common Mark. Law Rev.* **51**(3), 843 (2014)
22. Gil González, E.: Big data y datos personales: ¿es el consentimiento la mejor manera de proteger nuestros datos? *Diario La Ley*, ISSN 1989-6913, No. 9050 (2017)
23. Gil González, E.: Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías big data y de aprendizaje computacional. *Revista Internacional de Transparencia* **5** (2017)
24. Goodman, B., Flaxman, S.: European Union regulations on algorithmic decision-making and a “right to explanation”. *AI Mag.* **38**(3) (2017)
25. Graef, I., Clifford, D., Valcke, P.: Fairness and enforcement: bridging competition, data protection and consumer law. Forthcoming in *International Data Privacy Law* (2018). Available at: https://www.researchgate.net/publication/326668711_Fairness_and_Enforcement_Bridging_Competition_Data_Protection_and_Consumer_Law_forthcoming_in_International_Data_Privacy_Law_2018
26. Hildebrandt, M.: Privacy as protection of the incomputable self: from agnostic to agonistic machine learning. DRAFT PAPER for the International Conference ‘The Problem of Theorizing Privacy’, submitted for publication in the special issue of *Theoretical Inquiries in Law (TIL)*, and defended at PLSC-Europe (2018). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081776
27. Hoffman, D.A., Rimo, P.A.: It takes data to protect data. In: Selinger, E., Polonetsky, J., Tene, O. (eds.) *The Cambridge Handbook of Consumer Privacy* (2018). Available at: <https://www.yvtlfi.fi/en/index/opinionsanddecisions/decisions.html>
28. Information Commissioner’s Office: Big data, artificial intelligence, machine learning and data protection (version 2.2) (2017). Available at: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>
29. Information Commissioner’s Office: Guide to the General Data Protection Regulation (2018). Available at: <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>
30. Information Commissioner’s Office: Lawful basis for processing, consent (2018). Available at: <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent-1-0.pdf>
31. Kalimo, H., Majcher, K.: The concept of fairness: linking EU competition and data protection law in the digital marketplace. *Eur. Law Rev.* **42**(2), 210 (2017). Available at: https://www.researchgate.net/publication/317217197_The_concept_of_fairness_Linking_EU_competition_and_data_protection_law_in_the_digital_marketplace
32. Kamara, I., de Hert, P.: Understanding the balancing act behind the legitimate interest of the controller ground. A pragmatic approach. In: Selinger, E., Polonetsky, J., Tene, O. (eds.) *The Cambridge Handbook of Consumer Privacy* (2018)
33. Kosta, E.: *Consent in European Data Protection Law*. Martinus Nijhoff Publishers, Leiden (2013)
34. Kuner, C., Svantesson, D., Kate, F.H., Lynskey, O., Millard, C.: Machine learning with personal data: is data protection law smart enough to meet the challenge? *Int. Data Priv. Law* **7**(1), 1 (2017)
35. Lammerant, H., de Hert, P.: Predictive profiling and its legal limits: effectiveness gone forever? In: van der Sloot, B., Broeders, D., Schrijvers, E. (eds.) *Exploring the Boundaries of Big Data*. Amsterdam University Press, The Hague/Amsterdam (2016)
36. Malgieri, G., Comandé, G.: Why a right to legibility of automated decision-making exists in the general data protection regulation. *Int. Data Priv. Law* **7**(4), 243 (2017)
37. Martin, K.: Privacy notices as tabula rasa: an empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. *J. Public Policy Mark.* **34**(2), 210 (2015)
38. Moerel, L., Prins, C.: Privacy for the homo digitalis: proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things. *SSRN Electronic Journal* (2016)
39. National Non-Discrimination and Equality Tribunal of Finland. C-216/2017
40. Nymity and Future for Privacy Forum: Processing personal data on the basis of legitimate interests under the GDPR: practical cases (2018). Available at: https://info.nymity.com/hubfs/Landing%20Pages/Nymity%20PF%20-%20Legitimate%20Interests%20Report/Deciphering_Legitimate_Interests_Under_the_GDPR.pdf?hsCtaTracking=9cf491f2-3ced-4f9c-9ffa-5d73a77a773e%7C7469b2ec-e91c-4887-b5db-68d407654e23
41. Pasquale, F.: *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press, Cambridge, London (2015)

42. Privacy & Information Security Law Blog: UK ICO Issues Warning to Washington Post Over Cookie Consent Practices, November 21 (2018)
43. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free Government of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1
44. Reidenberg, J., Russell, N., Callen, A., Qasir, S., Norton, T.: Privacy harms and the effectiveness of the notice and choice framework. 2014 TPRC Conference Paper, Fordham Law Legal Studies Research Paper No. 2418247 (2014). http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2418247
45. The Netherlands, Autoriteit Persoonsgegevens, z2013-00194, Google. English (non-official) translation available at: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf
46. Van der Sloot, B., Borgesius, F.: The EU General Data Protection Regulation: a new global standard for information privacy (Working draft)
47. Veale, M., Edwards, L.: Clarity, surprises, and further questions in the Article 29 working party draft guidance on automated decision-making and profiling. *Comput. Law Secur. Rev.* **34**(2), 398 (2018)
48. Vedder, A.: KDD: the challenge to individualism. *Ethics Inf. Technol.* **1**(4), 275 (1999)
49. Wachter, S., Mittelstadt, B., Floridi, L.: Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *Int. Priv. Data Law* **7**(2), 76 (2016)
50. World Economic Forum and The Boston Consulting Group: Rethinking Personal Data: Strengthening Trust (2012)