Automated Decision-Making Under the GDPR:

Practical Cases from Courts and Data Protection Authorities

FUTURE OF PRIVACY FORUM

MAY 2022

AUTHORED BY

Sebastião Barros Vale and Gabriela Zanfir-Fortuna

for the Future of Privacy Forum

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

FPF Europe maintains strong partnerships across the EU through its convenings and knowledge-sharing with policymakers and regulators. This transatlantic engagement helps regulators, policymakers, and staff at European Union data protection authorities better understand the technologies at the forefront of data protection law. By building this bridge between European and U.S. data protection cultures, FPF hopes to build a common data protection language. Learn more about FPF Europe by visiting fpf.org/about/EU.

TABLE OF CONTENTS

BACKGROUND AND OVERVIEW

The European Union's (EU) General Data Protection Regulation (GDPR) establishes one of its foundational rationales in Recital 4, stating that "the processing of personal data should be designed to serve mankind." This refers to any processing of personal data, from its collection to its various uses, as simple as keeping a record about one's purchases at their favorite grocery store and as complex as using personal data for automated decision-making, such as pre-screening candidates for a job through the use of algorithms, or having personal data result from complex processing, like creating a profile of the customer of a grocery store on the basis of their purchase history.[1] The same underlying rationale of the GDPR applies if personal data are in any way processed as part of an Artificial Intelligence (AI) or Machine Learning (ML) application[2] — either as input or output of such processing.

While all the provisions of the GDPR apply to such complex processing of personal data — from the obligation of the controller to have a lawful ground for processing in place,[3] to the obligation to ensure that the processing is done fairly and transparently[4], to more technical obligations like ensuring an adequate level of data security[5] and ensuring that the protection of personal data is baked into the design of a processing operation,[6] one particular provision of the GDPR is specifically applicable to decisions "based solely on automated processing [of personal data — *n.*], including profiling, which produces legal effects" concerning an individual "or similarly affects" that individual: Article 22.

This provision enshrines one of the "rights of the data subject,"[7] particularly "the right not to be subject to a decision based solely on automated processing" which has a legal or similarly significant effect on the individual. All automated-decision making (ADM) that meets these criteria as defined in Article 22 GDPR is referred to as "qualifying ADM" in this Report.

Even if apparently introduced in the GDPR to respond to the current age of algorithms, AI and ML systems, this provision has in fact existed under the former EU Data Protection Directive adopted in 1995, and has its roots in a similar provision of the first French data protection law adopted in the late 1970s (see Section 1.1 of the Report). However, it has only scarcely been enforced under previous law. Cases started to pick up after the GDPR became applicable in 2018, also considering that automated decision-making is becoming ubiquitous in daily life, and it now looks like individuals are increasingly interested in having their right under Article 22 applied.

This Report outlines how national courts and Data Protection Authorities (DPAs) in the EU/European Economic Area (EEA) and UK have interpreted and applied the relevant GDPR provisions on ADM so far, as well as the notable trends and outliers in this respect. To compile the Report, **we have looked into publicly available judicial and administrative decisions and regulatory guidelines across EU/EEA jurisdictions and the UK,** which was a member of the EU until December 2020 and whose rules on ADM are still an implementation of the GDPR at the time of writing this Report. To complement the facts of the cases discussed, we have also looked into press releases, annual reports and media stories.

This research is limited to documents released until April 2022, and it draws from more than 70 cases — 19 court rulings and more than 50 enforcement decisions, individual opinions or general guidance issued by DPAs, — from a span of 18 EEA Member-States, the UK and the European Data Protection Supervisor (EDPS). The main cases and documents used for reference are listed in Annex I. The Report primarily contains case summaries, as well as relevant guidelines, with the cases explored in detail being numbered consistently so that all the notes on a particular case can be easily identified throughout the document (e.g. Case 3 will be referred to several times, under different sections).

The cases we identified often stem from situations of daily life where ADM is increasingly playing a significant role. For instance, one cluster of cases envisages students and educational institutions. These cases vary from the use of live Facial Recognition technologies to manage access on school premises and recording of attendance, to online proctoring and further to fully automated grading based on the individual profile of a student, but also on the profile of their school district, as a substitute of highschool graduation exams during the COVID-19 pandemic.

Another significant cluster of cases has at its core the situation of gig workers and the way they are being distributed shifts, gigs, income and penalties through their respective platforms. A significant number of cases challenge automated credit scoring. The way in which governments distribute social benefits, like unemployment, and manage tax avoidance and potential fraud is increasingly subject to more cases — individual challenges or ex officio investigations. We also encountered cases where the underlying ADM was challenged in situations like the issuing of gun licenses, scraping publicly available sources to build an FR product, or profiling of prospective clients by a bank.

Our analysis will show that the GDPR as a whole is relevant for ADM cases and has been effectively applied to protect the rights of individuals in such cases, even in those situations where the ADM at issue does not meet the high threshold established by Article 22 GDPR, and the right not to be subject to solely automated decision-making is not applicable. For instance, without even analyzing whether Article 22 applies in those cases — Courts and DPAs have found that the deployment of live FR applications to manage access to school premises and monitor attendance was unlawful under other provisions of the GDPR because it did not have a lawful ground for processing in place and it did not respect the requirements of necessity and proportionality, thus protecting the rights of students in France and Sweden (see Cases 30 and 31).

A comparative reading of relevant cases will also show how complex transparency requirements are considered in practice, being effectively translated into a right of individuals to receive a high level explanation about the parameters that led to an individual automated decision concerning them or about how profiling applied to them.

The principles of lawfulness and fairness are applied separately in ADM related cases, with the principle of fairness gaining momentum in enforcement. For instance, in one of the most recent cases enshrined in the Report, the Dutch DPA found that the algorithmic system used by the government to automatically detect fraud in social benefits requests breached the principle of fairness, since the processing was considered “discriminatory” for having taken into account the dual nationality of the people requesting childcare benefits.

Another important point that surfaced from our research is that when enforcers are assessing the threshold of applicability for Article 22 (“solely” automated, and “legal or similarly significant effect” of ADM on individuals), the criteria used are increasingly sophisticated as the body of case-law grows. For example, Courts and DPAs are looking at the entire organizational environment where an ADM is taking place, from the organization structure, to reporting lines and the effective training of staff, in order to decide whether a decision was “solely” automated or had meaningful human involvement. Similarly, when assessing the second criterion for the applicability of Article 22, enforcers are looking whether the input data for an automated decision includes inferences about the behavior of individuals, and whether the decision affects the conduct and choices of the persons targeted, among other multi-layered criteria.

Finally, we should highlight that in virtually all cases where an ADM process was found to be unlawful, DPAs went beyond issuing administrative fines by also ordering specific measures which varied in scope: orders to halt practices, orders to delete the illegally collected personal data, orders to prohibit further collecting personal data.

All of the sections of the Report are accompanied by summaries of cases and brief analysis pointing out commonalities and outliers. The Report initially explores the context and key elements of Article 22 and other relevant GDPR provisions that have been applied in ADM cases, all of them reflected in concrete examples (Section 1). Then, it delves into how the two-pronged threshold required by Article 22 GDPR has been interpreted and applied in practice (Section 2). Finally, Section 3 brings forward how Courts and DPAs have applied Article 22 in sectoral areas, namely in employment, live facial recognition and credit scoring matters. The Conclusion will lay out some of the identified legal interpretation and application trends that surface from our research and highlight remaining areas of legal uncertainty that may be clarified in the future by regulators or the CJEU (Section 4).

1. THE FUNDAMENTALS OF ARTICLE 22 GDPR

Article 22

Automated individual decision-making, including profiling

1. *The data subject shall 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.*
2. *Paragraph 1 shall not apply if the decision:*
   - *(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
   - *(b) is authorised 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; or*
   - *(c) is based on the data subject's explicit consent.*
3. *In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall 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 of the controller, to express his or her point of view and to contest the decision.*
4. *Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.*

1.1 ADM provisions have been enshrined in data protection laws since the 1970s

The effects of Automated Decision Making and profiling on individuals have been one of the key concerns of legislators as far back as the 1970s, from the very emergence of automation and computers. The way they dealt with this concern was by proposing and adopting data protection legislation, with strong principles and rights for individuals. For instance, the **French Data Protection Act of 1978** specifically prohibited **ADM in the context of judicial, administrative, or private decisions** involving assessment of human behavior that would profile or define the personality of the individual,[8] while granting individuals a right to know and a right to challenge the information and the reasoning used by automated processing affecting them.[9] In 1995, the EU aimed to harmonize national data protection laws in its Member States through the Data Protection Directive, and included a provision similar to the one in the French law, resulting in Article 15 on "Automated individual decisions."[10]

The right not to be subject to solely automated decision-making as provided by Article 22 of the GDPR replicates this right and adds to it. While the core of the right is the same ("not to be subject to a decision which produces legal effects" concerning the individual "or significantly affects" them, and "which is based solely on automated processing of data"), there are a few differences between Article 15 DPD and Article 22 GDPR.

First, the DPD did not mention individual consent as an exemption for controllers who wished to conduct such ADM, providing contract and legal obligations as the only permissible grounds. Second, the DPD specifically referred to automated processing intended to evaluate certain aspects about targeted individuals, language which has been transposed into the current definition of profiling under the GDPR. In any case, for ADM to be covered by Article 22 GDPR, it does not need to entail any form of profiling, which was not the case under Article 15 DPD.

Case 1: Statistical analyses of defendants in criminal cases are not qualifying ADM

Case law interpreting Article 15 of the 1995 Data Protection Directive is scarce. One of the few judicial decisions of note is a 1998 ruling from the French Supreme Court (*Cour de Cassation*), in which the Court held that Article 15 did not apply to the use of statistical comparisons of a defendants' professional activities (medical acts performed and fees charged) with that of colleagues from the same profession — in the case at hand, other masseur-physiotherapists — in a specific criminal case, by means of computer systems. In the particular criminal case, the Court found that the statistical analyses had not been conducted in such a way as to define the profile or personality of the persons concerned in the proceedings.[11]

Case 2: Personalized rates for users of a car sharing service are qualifying ADM

Much later, in January 2018, the Italian DPA (*Garante*) found that a controller who offered personalized rates to the users of its car sharing service, on the basis of their collected habits and characteristics, was profiling data subjects for the purposes of the Italian law which transposed Article 15 DPD. During the respective administrative procedure, the defendant disagreed, arguing that there was no "categorization" of the service's users, as the data used for the rates' calculation were not permanently associated with the subjects. The DPA dismissed the defendant's arguments, stating that it was undeniable that, in this case, there was: a) personal data processing; b) based solely on automated processing; and c) aimed at defining the profile or personality or at analyzing habits or consumption choices of individuals.[12] This decision — which led to a 60.000 EUR administrative fine — was confirmed by the Italian Supreme Court (Corte Suprema de Cassazione) in November 2021. In the appeal procedure, the Supreme Court sided with the *Garante,* as it held that processing personal data through an algorithm to calculate a personalized rate is considered profiling, even if the data is not attributable to the data subject nor stored by the controller.[13]

In another consequential case of applying Article 15 DPD, the French Data Protection Authority (CNIL) found that the University admission system used in France breached the right not to be subject to ADM as provided by the DPD and ordered universities to put in place a procedure which involved meaningful human intervention (see Case 25 below).

1.2 The EDPB interprets Article 22 as an a *priori* prohibition on engaging in qualifying ADM

EU Member-States transposed Article 15 DPD into their national legal systems in considerably different ways. While some (like Belgium) framed their national ADM provisions as a qualifying ADM prohibition, others (like Sweden) saw Article 15 as requiring Member-States to grant individuals a right to opt-out from ADM. The text of Article 22 GDPR was intended to lay down a uniform set of rules on ADM across the EU and to settle these diverging readings. **The issue of the nature of Article 22 — whether it is a prohibition (with exceptions) or a right for individuals to exercise in order to be effective — still sparks academic debate.**[14] And this debate is of consequence: if Article 22 provides for a prohibition, then controllers must *a priori* abstain from engaging in qualifying ADM unless one of the exceptions applies. Whereas if Article 22 provides for a right that needs to be exercised, then controllers can engage in qualifying ADM regarding an individual until that individual specifically requests not to be subject to it.[15]

While the academic debate is ongoing, the EDPB has taken the view that Article 22 provides for a prohibition, by stating in an Opinion from 2018 that:

"The term *right* in the provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing. This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data."[16]

Like for other provisions of EU law, the CJEU has ultimate authority to interpret Article 22 GDPR, but it has not yet adjudicated on its content. Questions for a preliminary ruling to

clarify the content and scope of Article 22 GDPR have been sent to the CJEU in 2021 by the Administrative Court of Wiesbaden (Germany) in the SCHUFA case (C-634/21), and by the Vienna Regional Administrative Court (Austria) in February 2022. The former is further explored in Section 3.3 (as Case 39), and the latter in Section 1.6.c (as Case 14) below.

1.3 There are three conditions that trigger the applicability of Article 22 GDPR

For Article 22(1) GDPR to apply, there are three cumulative conditions that need to be met by the processing of personal data underlying the automated decision-making: the processing needs to underpin (a) a decision (b) based solely on automated processing or profiling (c) that has legal or similarly significant effects on an individual ("data subject").

a) The first element requires the existence of a "**decision**" as the result of the underlying data processing operation, which involves taking a particular resolution regarding a person, formal enough to be "distinguished from other steps that prepare, support, complement or head off decision-making."[17]

b) Regarding the requirement that such a decision is "**based solely on automated processing,**" the EDPB has clarified that this means that no human has **meaningful** involvement in the decision-making process. In its dedicated Guidelines on ADM and Profiling, the EDPB does not give a concrete example of a system where this may happen. It merely mentions an "automated process" that "produces what is in effect a recommendation concerning a data subject."[18] This example is very broad and it could potentially capture systems as varied as automated recommendation for interviewing a job applicant, to automated recommendation for receiving a credit or not, to other automated recommender systems. The EDPB adds that if a "human being reviews and takes account of other factors in making the final decisions," then that ADM is not "based solely" on automated processing. Further, controllers cannot avoid Article 22 by having a human merely rubber-stamp machine-based decisions, without actual authority or competence to alter their outcome.[19] By contrast, if the automated process at hand merely provides input for a decision to be ultimately taken by a human, the processing underlying it is not in the scope of Article 22(1) GDPR.[20] Courts across the EU have found that some (often limited) degree of human involvement in a number of disputed cases was enough to set aside the application of the provision (see Section 2.1 below).

The third condition refers to the nature of the **effects** that these automated decisions must have on individuals: "legal effects" or "similarly significant effects." According to the EDPB, a decision has legal effects on individuals where it affects his or her legal status or rights (including under a contract). Examples given by the guidelines include canceling a contract or denying a social benefit to a person. Decisions that "similarly significantly affect" a person are less clear-cut, as shown by our research (see Section 2.2 below). The EDPB considers that this criterion encompasses decisions that potentially (i) significantly affect the circumstances, behaviour or choices of the individuals concerned, (ii) have a prolonged or permanent impact on the data subject, or (iii) lead to the exclusion or discrimination of individuals.[21] Recital 71 of the GDPR provides useful examples of such decisions: automatically refusing online credit or job applications. The EDPB also includes in its ADM guidelines a nuanced opinion on whether some forms of **online behavioral advertising** may fall within the scope of Article 22, suggesting that this indeed is the case. However, the EDPB stresses that the answer depends on assessing a number of factors

in each specific case (e.g., the intrusiveness of any profiling at stake and whether it uses knowledge about targeted data subjects' vulnerabilities).[22]

1.4 Only legal obligations, contract and consent can justify qualifying ADM

Article 22(2) GDPR lists three exceptions, or permissible uses for qualifying ADM: indent (a) refers to ADM which is necessary for entering into or performing a contract with the data subject; indent (b) covers ADM which is legally authorized; and indent (c) opens up the possibility or relying on data subject consent.

a) As per indent (a), the provision demands that the ADM is **strictly necessary for contractual purposes.**[23] This means that the controller must assess whether there are no other effective and less privacy-intrusive means to achieve the purpose of the processing of personal data underlying the qualifying ADM. According to the EDPB, this requires the controller to "demonstrate how the main subject-matter of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur," also taking into account the data subject's expectations.[24] The United Kingdom's DPA, the Information Commissioner's Office (ICO), offers a more nuanced view, stating that the paragraph's wording allows ADM as a targeted and reasonable way of meeting the controller's contractual obligations.[25]

Case 3: Algorithmic management of gig workers could be justified as contractual necessity

In its July 2021 decision to fine food delivery company Deliveroo for unlawful data practices regarding the algorithmic management of its riders, the Italian DPA (Garante) agreed that it can be argued the "Frank" algorithm was necessary to manage Deliveroo's contractual relationship with the riders.[26] For further details about this case, see our analysis in Chapters 1.5, 1.6.d, and 3.1 below.

Indent (a) may also cover cases where ADM is objectively necessary for the controller to take certain pre-contractual steps. The EDPB guidance mentions the production of a shortlist with job applicants as an example, in cases where the controller has received a very high number of applications.

Guidelines from national DPAs on automated recruiting processes

The DPA from the German State of Baden-Württemberg has taken a more conservative stance in this regard. In its 2020 Annual Report, it stated that using algorithms which automatically analyze job applicants' writing from their CVs and cover letters and thereby decide on whether they continue or are dropped from the process, amounts to ADM that could only be carried out with prior applicants' consent under paragraph (2)(c).[27]

b) The second indent on **legally-mandated or authorized qualifying ADM** states that the authorizing Member State or EU law must lay down "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests." Such measures may include a right for data subjects to obtain human intervention from the controller, to express their points of view and to contest automated decisions.

Member State Law: Estonian Unemployment Insurance Act

For instance, this is the case in Section 23(4) of the **Estonian Unemployment Insurance Act**, which allows the Unemployment Insurance Fund to decide on the attribution or rejection of unemployment benefits to applicants in a solely automated fashion after scanning State-controller databases for relevant information. At that moment, applicants are informed that the decision was automated, that they have a right to be heard and to submit a request for internal review.[28]

However, laws authorizing ADM can go beyond such requirements.

Belgian DPA Opinion: Remote reading of electricity consumption is qualifying ADM

A 2019 opinion from the Belgian DPA (APD) on a draft law proposal regulating the remote reading of electricity consumptions by Belgian citizens through smart-meters stated that the automated authorization or refusal of collective self-consumption operations by the competent energy authority (CWaPE), based on citizens' consumption patterns, would constitute legally-authorized ADM for the purposes of Article 22(2)(b) GDPR. Therefore, the ANP suggested the Wallonian government include certain data subject safeguards in the final text of the law, such as allowing data subjects to demonstrate that a specific consumption pattern was due to a transitory situation.[29]

It is noteworthy that, even where certain ADM or profiling practices do not *prima facie* fall under Article 22(1) GDPR, there may be a need for national legislators to enshrine into law additional safeguards for the protection of data subjects.

Case 4: Automated risk assessments of individuals by Tax Authorities require additional legal protections

On November 10, 2021, the Slovak Constitutional Court delivered its ruling on the legality of an information system managed and used by the Slovakian Tax Authority to detect potential instances of tax fraud (the "e-kasa" system).[30] Under Slovak law, every receipt issued by a seller (or "trader") — including the seller's tax identification number [TIN] and its customers' unique buyer identifier (which could be the latter's TIN or loyalty program participant number) — is sent in real-time to the e-kasa system, which then uses such data to automatically draw risk profiles of all sellers in matters of tax evasion or fraud. Based on the list obtained therefrom, the Authority's employees prioritize their supervisory activities, including individual checks on sellers. The Court found that this constituted an "automated assessment" of traders, who may also be natural persons. According to the Court, "The fact that the system itself does not make a decision on whether to carry out a tax or other control is not relevant," but rather that the "automation refers to the evaluation of a person [i.e., a trader] on the basis of his personal data."[31] In this respect, although the Court notes that the GDPR already includes certain obligations for controllers (such as carrying out a DPIA), **the Slovak Constitution requires that additional measures are introduced by law to protect individuals when automated assessments by State agencies are at stake,** such as: (i) ensuring that the criteria, models or linked databases used in that context are up-to-date, reliable and non-discriminatory; (ii) ensuring that individuals are aware of the existence, scope and impact of his or her automated assessment; (iii) checking the system's quality, including its error rate (both before and while the system is put to use, e.g., through audits, reporting and statistics); and (iv) enshrining redress rights for individuals to effectively defend themselves against the system's errors and imperfections.[32]

c) The third indent mentions "**explicit consent**" as a way to legitimize qualifying ADM. The EDPB has clarified that this entails additional efforts from controllers to obtain, when compared to "regular" consent under Articles 4(11), 6(1)(a) and 7 GDPR. In this context, controllers may want to ask data subjects to submit a signed written statement, file an electronic form or send an email expressing their will to be subject to ADM.[33] Other requirements relating to free, specific, unambiguous and informed consent also apply.

Case 5: Insufficiently informed consent is not valid to allow Article 22 GDPR qualifying ADM

On May 25, 2021, Italy's Supreme Court of Cassation *(Corte Suprema de Cassazione)* ruled that **consent is not valid if the individual is subject to an ADM system that may influence his or her rights when he or she is not adequately informed about the logic behind it.** In the case at hand, individuals voluntarily uploaded documents containing personal data to an online platform managed by the defendant (Associazione Mevaluate Onlus). The IT system would then assign a 'reputational rating,' i.e., alphanumeric indicators capable of measuring the reliability of individuals in the economic and professional fields, with the goal to present the data subjects' "credentials" to the defendant's customers. While the Associazione argued that individuals who adhered to its platform and voluntarily uploaded documents therein were manifesting their consent to the ADM involved, the Court concluded that such adherence does not also imply the acceptance of an automated system that scores the individual who joins it based on his or her personal data, if he or she is not aware of the 'executive scheme' (i.e., the logic involved) and the constitutive elements of the algorithm.[34] This case illustrates the meaningful connection between Article 22 — in particular, paragraph (2)(c) — with the GDPR's transparency obligations.

In addition to the exemptions set out in paragraph (2), paragraph (4) of Article 22 demands controllers that use sensitive data in ADM processes to apply "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests." However, data related to protected characteristics which is covered by Article 9(1) GDPR may only be processed in such a context if data subjects have given their prior explicit consent or there is a "substantial public interest" involved.

1.5 Human intervention, the right to be heard and contestability must be ensured for qualifying ADM

Mirroring the safeguards that laws authorizing qualifying ADM must enshrine in order to lawfully allow for qualifying ADM to take place, paragraph (3) of Article 22 GDPR stipulates that organizations deploying ADM under the contract and consent permissible uses must "implement **suitable measures** to safeguard the data subject's rights and freedoms and legitimate interests." The latter shall include, at least, the rights "to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."

Furthermore, Recital 71 of the GDPR states that, "in any case, data subjects should have a right to obtain an explanation of the decision reached after such assessment" (i.e., after the individual requested human review). The EDPB guidance recommends controllers to adopt a number of additional measures to the minimum required ones, such as regularly checking datasets for bias and introducing procedures to prevent errors, inaccuracies and discrimination.[35]

Cases 3 and 6: qualifying ADM related to gig workers, unlawful due to lack of appropriate safeguards

In its above mentioned decision on Deliveroo, the Italian DPA found that the company had failed to implement Article 22(3) suitable measures to protect its riders' rights, **including systematically verifying the accuracy and correctness of its automated rider-management decisions, as well the relevance of the data to the decision-making process.**[36] The DPA's findings closely resemble the ones that surfaced in an older decision by the *Garante*, targeting another food delivery company, Foodinho. In this case, the DPA ascertained that the company did not implement procedures (like setting up a dedicated communication channel) allowing its riders to exercise the rights listed under Article 22(3) GDPR. It also mandated Foodinho to properly verify the accuracy and relevance of the data it used to assign slots to its riders, with a view to minimize the risk of errors and distortions that could lead to the limitation of the slots assigned to each rider or to their *de facto* exclusion from the platform.[37]

1.6 The rest of the GDPR applies to ADM and qualifying ADM, regardless of Article 22 conditions

It is important to note that both when the qualifying conditions for ADM in Article 22 are met and where they are not met, the rest of the GDPR obligations apply to the processing of personal data underpinning the ADM system. However, there are some specific provisions of the Regulation which are particularly relevant for ADM, including when it falls within the scope of Article 22. These include the definition of "profiling" in Article 4(4), the data processing principles in Article 5, the legal grounds for processing in Article 6 (which are relevant for ADM and profiling that are not covered by Article 22[38]), the rules on processing special categories of data (such as biometric data) under Article 9, specific transparency and access requirements regarding ADM under Articles 13 to 15, the right to object to legitimate interests-based profiling in Article 21, the obligations to ensure data protection by design and by default in Article 25, and the duty to carry out data protection impact assessments in certain cases in Article 35.

This section will outline some examples of cases where courts and DPAs have found touchpoints among these GDPR provisions when deciding on ADM-related breaches or when issuing related guidelines.

a. General data protection principles, including fairness, apply to all ADM

Regardless of whether ADM and profiling practices fall under Article 22 or not, they must comply with the key principles outlined in Article 5 GDPR. These relate to the amount of personal data that may lawfully be processed to attain the intended purpose (data minimization), the accuracy of input and output personal data and the fairness of the data processing at stake, among others.

Case 7: ADM used to grade students allegedly breached the principle of fairness and data protection by design obligations

The Norwegian DPA (*Datatilsynet*) provided some insight into how Article 5 principles, Article 25 on data protection by design obligations and ADM interact, in its intention to order the International Baccalaureate Office (IB) to correct student grades because of unfair profiling, published in August 2020. Given the cancellation of exams during the COVID-19 pandemic, the IB decided to consider students' "school context" and "historical data" in the grading. The DPA established that such consideration was unfair (i.e., it breached the GDPR's **fairness** principle) and led to inaccurate grading (i.e., in breach of the GDPR's **accuracy** principle). Notably, the DPA observed that such grading did not reflect the students' individual academic level, rather potentially leading to discrimination based on the school they attended. The DPA also points to the fairness criteria identified by the EDPB in its data protection by design & by default guidelines, stating that any processing of data — including cases of profiling such as the one at stake — should be non-discriminatory, ethical and transparent, and consider power and information (im) balances.[39] In this regard, the DPA stated that the grading system did not correspond to students' reasonable expectations, who expected their grades to reflect their demonstrable academic achievements, the work they had put in as well as the knowledge and skills they had attained. Furthermore, the DPA noted that the logic behind the grading (profiling) algorithm was not publicly known, and that the IB refused to further explain the model to the DPA and to students. This, according to *Datatilsynet*, translated into a breach of the GDPR's **transparency** principle.[40]

We had the opportunity to follow up with the DPA on the status of the investigation. On that occasion, the DPA's representative clarified that the DPA had forwarded the facts and findings to the ICO, while the UK's Office of Qualifications and Examinations Regulation (Ofqual) was also investigating IB's exam results.[41] Almost in parallel, the ICO had another reckoning with automated student grading, as it dealt with Ofqual's widely-reported A-levels algorithm.[42] Just before the UK government decided to drop the use of the controversial algorithm, the ICO released a statement, underlying the importance of processing students' data in a transparent and fair manner. It also pointed to the fact that "the GDPR places strict restrictions on organizations making solely automated decisions that have a legal or similarly significant effect on individuals."[43]

Finally, the principles of data minimization and fairness also played a significant role in the decision the Dutch DPA took to declare the SyRi algorithm unlawful, in one of the most consequential cases against an automated decision-making system in the EU (we explore it in detail below in Section 2.2 and Case 27).

It is important to note that the principle of fairness in data protection law has been traditionally one of the least explored by literature and case-law, often being conflated with the principles of transparency. This situation is changing as fairness starts to play a role in data protection enforcement, particularly in ADM cases. As the cases in this Report show, fairness is already linked to non-discrimination, but the principle is generous enough to potentially include imbalances of power and other dimensions that will be clarified as case-law evolves.

b. Personal data processing underlying ADM and profiling require a lawful ground for processing

As shown above, ADM which is covered by Article 22(1) GDPR may only be carried out in limited circumstances, which are listed under its paragraph (2). On the other hand, any data processing involved in ADM practices which are not covered by Article 22 — including profiling — must have a lawful ground for processing as required by Article 6(1) and, should the processing include special categories of data, an additional condition stemming from Article 9(2).[44] This is illustrated in several court and DPA decisions we have analyzed.

Case 8: e-screening applications for gun licenses to assess psychological state can be grounded on a legal obligation — Article 6(1)(c) GDPR

The Court of First Instance of The Hague was called upon to solve a dispute between two associations (Royal Dutch Hunters Society and the Royal Dutch Shooting Sports Association) and the Dutch State.[45] The latter required gun license applicants to fill in a special digital questionnaire (e-screener) that assessed their psychological state against ten risk factors (e.g., impulsiveness, lack of empathy, egocentrism, suicidality, narcissistic harm and extremism). Under Article 7(1)(c) of the Dutch Arms and Ammunition Act, a gun license may not be granted by the Dutch State if there is a reason to fear that the applicant cannot be entrusted with possession of a firearm. The plaintiffs claimed that the e-screener breached the GDPR, as it lacked a proper legal basis and countervened the rules on ADM under Article 22. In February 2020, the court decided that the ADM taking place was not covered by Article 22, as decisions regarding gun license attribution were not solely automated (for reasons that we will explore below in Section 2.1), and that the **e-screener data processing was lawfully conducted under Article 6(1)(c) GDPR:** the processing was considered strictly necessary for the controller's compliance with its legal obligation to adequately assess gun license applications.

Case 4: Automated tax fraud risk assessments require a legal authorisation, as per Article 6(1)(e) GDPR

In the November 2021 ruling from the Slovak Constitutional Court, judges decided that the constitutional interpretation of Slovak law "does not allow the [Tax Authority] to use data from the e-kasa system for automated analytical assessment of entrepreneurs' risk profiles" to detect instances of potential tax fraud committed by traders, on the basis of the receipts that were stored in the e-kasa database.[46] To reach this conclusion, the Court stressed that the Tax Authority's algorithm aided the Tax Authority's employees to decide whether additional investigatory steps should be taken in specific cases. It observed that this form of "automated assessment" by the Tax Authority based on personal data needs to be authorized by Slovak law — as it cannot be implemented in a discretionary manner by the Authority — regardless of the concrete effects they have on data subjects.[47] While it seems clear that the Court does not consider these "automated assessments" to fall under Article 22 GDPR, judges invoke Article 6(1)(e), (2), and (3) GDPR to stress that the Slovak legislator should provide a clear legal basis and additional safeguards — such as the ones mentioned in Chapter 1.4. b) above — given that the issue of automated processing for exercising public authority is not fully harmonized within the EU.[48]

Case 9: Automated assessment of job seekers' chances for employment found unlawful by the DPA, but lawful by the Court in appeal

In a December 2020 ruling, the Austrian Federal Administrative Court (BVwG) decided on an appeal lodged by the Austrian Public Employment Service (AMS) against an Austrian DPA (BSG) decision. The BSG's initial investigation on the AMS's job seekers' potential assessment algorithm (called "AMAS") was triggered by a data subject's complaint. AMAS intends to calculate the probability of registered job seekers finding employment within a certain period in the future, taking into account several factors, notably job seekers' age group, gender, education, health conditions, caring duties, the performance of their regional labor market and how long they have been registered with AMS. Based on the calculated probability, job seekers are assigned into different jobseeker groups: one corresponding to job seekers with high market opportunities, another with medium and a last one with low opportunities. This system seeks to assist the AMS' counselors in assessing job seekers' opportunities and ensuring a more efficient use of resources.

The DSB's August 2020 decision considered that the described data processing was unlawful, under Articles 5(1)(a), 6(1) and 9(2) of the GDPR, and prohibited AMS from processing job seekers' data with the help of the AMAS, with effect from January 1, 2021.

The AMS's appeal against the DPA's decision alleged that data processing through AMAS was justified pursuant to public interest tasks assigned to AMS by law, under paragraphs 25(1), 29 and 31(5) of the Austrian Labor Market Service Act (AMSG). **The court agreed that the processing of job seekers' data by AMS (including sensitive data) was justified by public interest tasks assigned by law, under Articles 6(1)(e) and 9(2)(g) GDPR.** It also noted, disagreeing with the BSG decision in this regard, that profiling (under Article 4(4) GDPR) on the basis of the collected data is covered by what Paragraph 25(1) of the AMSG mandates the AMS to pursue, as such paragraph expressly includes the data types that AMAS processes about jobseekers.[49]

Cases 10, 11, 12 and 13: Processing biometric data for automated identification was found unlawful because it lacked a legal ground for processing (Clearview AI Cases)

The DPA from the German State of Hamburg (HmbBfDI) ruled that **the processing of biometric data collected and made available as a service by Clearview AI was unlawful, given the lack of a valid legal basis for the processing of such data.** It observed that Clearview AI processes data subjects' biometric data (under Article 4(14) GDPR), as it "uses a specially developed mathematical procedure to generate a unique hash value of the data subject which enables identification." The investigation and subsequent decision were triggered by a data subject complaint, which was based on the fact that he had not provided consent for the processing of his biometric data. The DPA determined that Clearview AI, even though it does not have an establishment in the EU, was subject to the GDPR by virtue of the monitoring of data subjects' activity on the web (Article 3(2)(b) GDPR), as it "does not offer a snapshot [of individuals], but evidently also archives sources over a period of time." Therefore, the DPA ordered Clearview AI to delete all of the complainant's personal data.[50]

Cases 10, 11, 12 and 13, continued

In a similar fashion, the ICO has more recently announced its intention to fine Clearview AI for just over £17 million, along with a "provisional notice to stop further processing of the personal data of people in the UK and to delete it," as the company failed "to have a lawful reason for collecting the information," and "to meet the higher data protection standards required for biometric data."[51]

The CNIL has also ordered Clearview AI **to stop collecting facial images of persons in France** from the internet to feed the company's database that trains its facial recognition software, and **to delete the previously collected images,** both within two months. This was due to the unlawful nature of the processing at stake, given that there was no appropriate legal basis under Articles 6(1) and 9(2) of the GDPR for the collection and use of biometric data. In this respect, the CNIL notes that "the company has not obtained the data subjects' consent" and that **the fact that the personal data at hand was publicly accessible does not grant the controller a "general authorisation to re-use and further process" it under the legitimate interests legal basis, given its "strong intrusiveness" and lack of foreseeability and transparency for data subjects.** It is also important to note that, to establish its competence over the processing operations carried out by Clearview AI (which is based in the USA), the CNIL used the same criterion under Article 3(2)(b) GDPR as the HmbBfDI to determine the extraterritorial application of the GDPR, combined with the fact that the controller did not have a lead DPA in the EU as per Article 56(1) GDPR, given its lack of "central administration or establishment with decision-making powers as to its purposes and resources" in the Union.[52]

More recently, the Italian *Garante* reached similar conclusions and imposed similar corrective measures in its decision to fine Clearview AI in a total of 20.000.000 EUR. The DPA grounded its decision on the lack of a proper legal basis — as legitimate interests did not qualify as such — as well as for failure to comply with transparency requirements for biometric data processing and monitoring of persons in the Italian territory. In this regard, the authority notes that: "The possible public nature of the images is not sufficient to suggest that the persons concerned can reasonably expect them to be used for facial recognition purposes, (...)" and "the very circumstance of the public nature of the images does not automatically authorize Clearview to be able to legitimately reuse them in a free way." Furthermore, Clearview AI was found to be in breach of the purpose and storage limitation principles, as it processed such data for purposes which were incompatible with the original ones and did not define a storage period for them. Like the CNIL, the Garante **ordered the company to delete the illegally collected personal data and prohibited it from further collecting and processing** information about Italian residents through web scraping techniques and its facial recognition system. The *Garante* also **ordered the controller to designate a representative in the EU** to be addressed in addition to or instead of the US-based controller, as the company did not have an establishment in the EU but was subject to the GDPR via both Article 3(2) targeting criteria.[53]

c. General transparency requirements apply to ADM and profiling, regardless of whether it is qualifying ADM or not

Articles 5(1)(a), 12, 13, 14 and 15 of the GDPR establish principles of transparency and fairness, as well as rules about notices to be given to individuals, the modalities in which they should be given, as well as rules granting individuals the right to access their own data. These provisions apply to all processing of personal data underlying ADM and profiling, regardless of whether it is qualifying ADM or not,[54] subject to the general exceptions for transparency obligations under the GDPR.

With regard to the obligation of controllers to give notice under Articles 13 and 14, the EDPB Guidelines on Profiling and ADM specify that when the processing of personal data is done for the purposes of either profiling or ADM, "irrespective of whether it is caught by Article 22," this fact "must be made clear to the data subject,"[55] as a consequence of both articles requiring controllers to disclose what are the purposes of processing.[56] The EDPB also recalls that, according to Recital 60 of the GDPR, "giving information about profiling is part of the controller's transparency obligations under Article 5(1)(a)."[57] In practice, some enforcers are applying these rules to cover additional information than the mere existence of profiling and the categories of personal data processed for it, such as details about "how" the profiles were created and the practical consequences of their creation (see Case 16 below).

In addition, there are two specific transparency obligations in Articles 13(2)(f) and 14(2)(g) GDPR requiring controllers to disclose in their notices the fact that qualifying ADM and profiling covered by Article 22 are taking place, both in cases where data is obtained directly from data subjects and where data is obtained from third parties or publicly-available sources. On top of this disclosure, "at least" where qualifying ADM and profiling happen, controllers must also provide "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject." By using this wording ("at least"), the legislators seem to have envisioned situations where, voluntarily, controllers may provide information also about the logic involved in ADM and profiling that do not fall under Article 22.

The EDPB encourages[58] controllers, as "good practice," to provide meaningful information about the logic involved, and explain the significance and envisaged consequences of ADM and profiling **even when these do not meet the Article 22 criteria.** As the EDPB highlights, this is especially because Recital 60 of the GDPR asks that, taking into account the principles of transparency and fairness, controllers should provide "any further information necessary to ensure fair and transparent processing."

The EDPB guidelines interpret the ADM specific transparency requirements for notices as mandating controllers who process data as described in Article 22 to inform data subjects about elements such as "the categories of data that have been or will be used in the profiling or decision-making process; why these categories are considered pertinent; how any profile used in the automated decision-making process is built, including any statistics used in the analysis; why this profile is relevant to the automated decision-making process; and how it is used for a decision concerning the data subject."[59]

In addition to the specific notice requirements under Articles 13(2)(f) and 14(2)(g), the right of access also includes transparency related to "at least" qualifying ADM, according to Article 15(1)(h) GDPR. As such, data subjects making a request to access their own personal data, have the right to obtain information about the existence of qualifying ADM and at least in those cases,

information about the "logic involved" in ADM, "as well as the significance and the envisaged consequences of such processing for the data subject." A February 2022 request for a CJEU preliminary ruling from the Vienna Regional Administrative Court (Austria) invited the CJEU to shed light on the extent of information that controllers who carry out credit scoring through profiling are required to give data subjects about the underlying logic.

Case 14 — Request for a CJEU preliminary ruling: what is "meaningful" information about the logic involved in, the significance and consequences of credit scoring?

An individual in Austria was denied conclusion or extension of a mobile phone contract by a mobile operator. This contract would have led to a monthly payment of only 10 EUR. The operator's refusal was grounded on the fact that the individual had a low credit score. The individual challenged the credit scoring that the company relied on before the Austrian DPA, for not having received meaningful information from the controller about the logic involved in the ADM underpinning the credit score. The Austrian DPA decided in favor of the individual and ordered the company to disclose meaningful information about the logic involved in reaching the credit score. The company challenged the DPA decision in Court.

With the case making its way into the Austrian Court system, the Vienna Regional Administrative Court (Landesverwaltungsgericht Wien) asks the CJEU to clarify whether explaining the "logic involved" to a data subject who has exercised their right of access in relation to credit scoring entails providing information that **enables the person to understand the automated decision taken in the individual case,** including in particular the disclosure of (i) the data subject's processed personal data, (ii) the parts of the algorithm on which profiling is based, and (iii) the relevant information on the profiling process, notably in the form of a list of the most important factors considered in that context.

Furthermore, the referring court seeks to understand **whether the controller can invoke trade secret justifications to avoid the disclosure of essential information** that would allow the data subject to exercise their rights to express their point of view and contest an automated decision. According to the Vienna court, this information includes, among others, the input data used for profiling, the parameters and variables used in the profiling process, the mathematical formula used to calculate the rating, enumeration and explanation of each profile category, and an explanation of why the individual was assigned to a particular profile.

Interestingly, the court also asks **whether the individual (whether directly or through a court or DPA) also has a right to obtain other profiled data subjects' information (even if only in a pseudonymized format) to verify the accuracy** of the controller's profiling process.[60]

The questions for a preliminary ruling specifically refer to the interpretation of Article 15(1)(h) GDPR and they presume that the processing at stake meets the conditions for qualifying ADM under Article 22 GDPR.

Our analysis shows that when applying the GDPR to profiling and ADM, enforcers make a relevant distinction. On the one hand, there are **general transparency obligations** for all processing of personal data, including that underlying profiling and ADM which is not covered by Article 22. On the other, there are **specific transparency obligations** under Articles 13(2)(f), 14(2)(g) and 15(1)(h), only for qualifying ADM subject to Article 22, requiring a more complex set of information to be provided to data subjects ("meaningful information about the logic involved," "the significance and the envisaged consequences on the data subject").

- **In most cases, even where profiling and ADM are not found to meet the Article 22 criteria, data subjects still obtain recourse against unlawful practices or obtain access to their personal data underlying an automated decision, including profiling, under the general transparency provisions.**
- However, there is some **divergence about the level of detail and type of information that needs to be given to data subjects in these cases** under general transparency obligations, varying from only giving access to personal data insofar as they were relied on as the basis for an ADM in such a way that accuracy and lawfulness of the processing can be verified, to *a priori* informing data subjects through the notice about how their profiles were created and about the practical consequences of their creation (i.e., about the decisions which were taken on that basis).
- Applying a strict interpretation of the law, enforcers are reluctant to expand the transparency obligations specific to qualifying ADM — Articles 13(2)(f), 14(2)(g) and 15(1)(h) GDPR — also to profiling or ADM which do not meet the Article 22 criteria. However, one recent case from the Austrian DPA takes this approach, indicating that the enforcement landscape of profiling and ADM transparency could start to vary in a more significant way.
- When enforcing the right of data subjects to obtain transparency about the "logic involved" in qualifying ADM in specific cases, DPAs require individual explanation for each data subject inquiring about it, and a meaningful and high-level explanation of what led the ADM process to reach an impactful decision on the individual. The latter involves listing the specific categories of personal data that were used and considered crucial for the decision, or what circumstances always lead to negative decisions. Mathematical explanations, access to algorithms, or detailed information about computing systems are never considered in these cases.

Case 15: Information about "the logic involved" is due where a bank relies on ADM to decide on credit applications or to detect potential fraud or money laundering

On March 28, 2022, the Swedish DPA (IMY) imposed on Klarna Bank AB a 7.500.000 SEK fine (approximately 750.000 EUR) for several infringements of transparency requirements under the GDPR. Among other findings, the regulator noted that, in a period between March and June 2020, the controller did not provide meaningful information about the rationale, meaning and foreseeable consequences of the qualifying ADM it carried out for the purposes of deciding on credit applications it received from its customers and for detecting potential cases of fraud or money laundering. In this context, the IMY stressed that Klarna's data protection notice "only indicate[d] that certain types of information [were] used in connection with the automated decisions" (like contact, identification and financial information), but it did not explain to customers which circumstances may be decisive for a negative credit concession decision. The IMY considered that "the requirement to provide meaningful information on the logic behind an automated credit decision entails the indication of the **categories of data that are crucial in the context of an internal scoring model and the possible existence of circumstances that always lead to a refusal decision."** As this information was not included in Klarna's notice, the IMY established that the controller breached Articles 13(2)(f) and 14(2)(g) GDPR.[61]

Case 16: Creating commercial profiles of customers may not be qualifying ADM, but still requires detailed information about the profiling involved

In a decision[62] from May 2021, the Spanish DPA (AEPD) fined an energy company (EDP Comercializadora) 1.000.000 EUR for not complying with Article 13 GDPR, finding that, among other issues, **it did not sufficiently inform data subjects about the profiling it engaged in for marketing purposes.** The DPA concluded that the company's customers did not receive adequate information about the processing of their personal data at the point of data collection (e.g., when entering into a contract by phone or electronic means), including about how their commercial profiles were created by the company and about what the practical consequences of such creation were (i.e., about the decisions which are taken on that basis). **Although the DPA found that the company's creation of customer profiles to send personalized marketing communications did not amount to Article 22-covered ADM, it still ruled that controllers that carried out profiling activities are required to be transparent towards data subjects about their profiling practices** and how they can exercise their right to object to such profiling, under Article 21. To reach this conclusion, the DPA referred to the EDPB Profiling and ADM guidelines and relied on Recital 60 and on the obligation to disclose the purposes of processing (under Article 13(1)(c)), including when the purpose is profiling and even if the profiling is not covered by Article 22.[63] In doing so, the DPA rejected the submission of the company that the profiling was in fact associated with the purpose of personalized marketing communications and showed that in the General Terms submitted by the company, profiling was enumerated among the purposes for which personal data is used.[64] On a last note, the AEPD highlighted that it is possible to find, in any given case, a breach of Article 13 GDPR transparency obligations, even where there is no infringement of Article 22 and Article 6, as these such provisions are independent.[65]

Case 17: Ride-hailing drivers have the right to obtain access to their data underlying a decision to terminate their accounts, even if only partly based on ADM

In a First Instance case brought by several Uber drivers against the ride hailing company before the District Court of Amsterdam for alleged automated termination of their contracts for fraudulent acts, the plaintiffs argued that Uber had failed to comply with its transparency obligations regarding ADM.[66] They had explicitly requested the company to make such information available, pursuant the **specific** transparency requirements for qualifying ADM under Articles 13, 14 and 15. While doing so, they also raised claims under the general transparency obligations of the same Articles. Even if the Court found that Articles 13(2)(f), 14(2)(g) and 15(1)(h) were not applicable **to the case at hand because Uber did not make fully automated decisions, covered by Article 22,** regarding the deactivation of drivers' accounts in the platform (i.e., the termination of the drivers' agreements),[67] **the Court did extend access rights for two of the drivers involved in the case to receive personal data** "insofar as they formed the basis for the decision to deactivate their accounts, in such a way that they are able to verify the accuracy and lawfulness of the processing of their personal data."[68] In doing so, the Court rejected the company's submission that such access would provide the applicants "insight into the fraud detection parameters that can be used to circumvent its anti-fraud system", considering that it was not sufficiently substantiated.[69] The similar data access request of the other drivers involved in the case was rejected by the Court, on the ground that they had already been provided with sufficient information about the deactivation of their accounts through individual messages and other interactions with the company.[70]

Case 18: Access to personal data used to draw up a profile of a ride-hailing driver is not possible when the claim is not "sufficiently specified"

In another case involving ride-hailing drivers and Uber,[71] the District Court of Amsterdam, as the First Instance Court, again made a distinction between transparency rights in relation to qualifying ADM and transparency rights in relation to ADM and profiling which do not fall under Article 22. First, the Court found that there was not enough evidence for qualifying the automated process of matching drivers and clients for a ride as having legal or similarly significant effect, therefore Article 15(1)(h) was not found applicable.[72] Second, the Court noted that, to the extent the applicants wish to have access to their personal data that the company used to draw up a profile in the sense of Article 4(4) GDPR, the applicants "have not sufficiently specified this request."[73] *Per a contrario*, this means that if such a request related to profiling not covered by Article 22 was sufficiently specified, the Court would have considered it. In their submission, the applicants also asked the Court to issue an order against Uber to give them access to "all personal data relating to them that it processes," including personal data used to feed the passenger-drivers matching algorithm.[74] However, the Court rejected it on grounds that the applicants' access request was too general (i.e. not sufficiently concrete on the types of data they wished to access).[75] The court only ordered Uber to grant plaintiffs access to their anonymised individual ratings,[76] and not to other pieces of information, such as each driver's "tags" determined by Uber employees to categorize the driver's behavior.[77] One other request of interest made by the applicants was to have access to their personal data underlying the "upfront pricing" system that the company uses to determine the price of rides. While the Court found that "in general, it can be assumed that **the application of a system of tariff determination involves the processing of personal data if its purpose is to make decisions in respect of one person,"**[78] it was not satisfied with the information provided at the hearing that the applicants want access to these data "in order to verify the accuracy and lawfulness of the processing." Therefore, it rejected this request, but without providing more details about its reasoning or specifically grounding it in one of the restrictions of the right of access under the GDPR.[79]

Case 19: Fraud probability score constitutes profiling, and ride-hailing drivers have a right to access personal data underscoring it even if it is not qualifying ADM

In March 2021, the Amsterdam District Court dealt with another case brought by drivers against a ride hailing company, Ola,[80] in First Instance. The plaintiffs requested Ola to share information about the data it used for driver profiling and ADM purposes, including data on their fraud probability score, earning profile, assigned rides and imposed discounts and fines. Specifically on the fraud probability score, the court held that it constituted profiling under Article 4(4) GDPR, since "the automated processing of personal data of the applicants creates a risk profile that makes a prediction about their behavior and reliability."[81] The Court also noted that it does appear automated decisions have been taken on the basis of this personalized score, therefore this is not ADM covered by Article 22. However, **Ola must provide access to the personal data of the applicants that it used to draw up such a profile,** as well as information about the segments into which the applicants have been classified.[82] The Court was not satisfied that any of the restrictions to the right of access in Article 15(4) were satisfied, arguing that Ola "has not made clear to what extent providing access to the processed personal data offers applicants insight into its working and enforcement policy and the system it uses for this purpose, which would allow applicants to circumvent certain security measures."[83]

Case 20: Qualifying ADM establishing social benefits requires disclosure of information about the logic involved in the decision for every data subject making an access request

In a case where the facts satisfied the criteria of Article 22 for the ADM taking place, the Danish DPA *(Datatilsynet)* observed that *Udbetaling Danmark* — the authority responsible for the collection, disbursement and control of a number of public benefits in Denmark — failed to provide 5 data subjects who requested access to their personal data with mandatory information on the existence of automated decisions on the concession of certain benefits, in accordance with Article 15(1)(h) GDPR.[84] According to the DPA, the templates that *Udbetaling Danmark* used to reply to access requests revealed that the latter could carry out ADM in this context, including by screening information obtained from public registers against information received from data subjects to automatically determine whether the latter were entitled to the requested benefits which were income-based (such as pensions and housing benefits). Therefore, the DPA concluded that *Udbetaling Danmark* should have informed data subjects who exercised their access right about such ADM practices, by providing at least meaningful information on the ADM's logic, as well as the significance and envisaged consequences of such processing for the data subject. *Udbetaling Danmark* eventually committed to changing the wording of its template answers, to ensure that pursuant to each access request received, data subjects are informed about whether automated decisions had been made specifically against them.

Case 21: Meaningful information should be provided about automatically including an individual in a marketing segment, even if it is not covered by Article 22

In a September 2020 decision,[85] the Austrian DPA (BSG) held that the controller must provide the data subject with meaningful information about the **marketing scores** he had been attributed by the former, as a consequence of the fact that it amounts to profiling, even if it may not constitute qualifying ADM. Such scores consisted of alleged likelihoods (expressed in a percentage number) that the subject would belong to certain demographic groups, such as "conservatives," "traditionalists," "hedonists" or "digital individualists." As the data subject wanted to know how his marketing score had been calculated, and as the company refused to provide such information on the ground that it would breach trade secrecy, the individual submitted a complaint to the DPA. The authority held that the marketing scores were considered personal data and that the processing activities leading to the creation of such scores amounted to profiling under Article 4(4) GDPR. Moreover, **according to the DSB, the right under Article 15(1)(h) GDPR is not limited to cases of ADM covered by Article 22 GDPR, but also encompasses other cases, such as the profiling at hand:** the use of the words "at least in those cases" in Article 15(1)(h) points toward a broad scope of application.[86] Therefore, the DSB considered that it is not necessary to ascertain whether the profiling qualifies as ADM under Article 22 or not. While the DPA agreed that the respondent was not required to disclose the algorithm, the source code or compiler code that was used when creating the marketing scores (as those would likely be qualified as trade secrets), it still had to provide the following information in connection with the score calculation: parameters or input variables and how they came about (e.g., using statistical information); their effect on the score; explanation of why the data subject was assigned a particular score; list of possible profile categories; or similar equivalent information that enables the data subject to exercise his or her rights of rectification and erasure and to review the lawfulness of processing.[87]

Thus, the Austrian DPA proposes a broad application of the specific transparency obligation under the right of access tailored to "at least" cover qualifying ADM, to include profiling which does not meet the qualifying ADM criteria. This is consequential, because only the specific transparency obligations in Articles 13(2)(f), 14(2)(g) and 15(1)(h) require disclosure of "meaningful information about the logic involved" in ADM or profiling, "as well as the significance and the envisaged consequences" of such processing on the data subject.

d. DPIAs are always required for qualifying ADM in some EU Member States

Data Protection Impact Assessments (DPIA) are a key accountability measure required by the GDPR whenever a type of processing of personal data is "likely to result in a high risk to the rights and freedoms" of individuals, subject to the conditions detailed in Article 35.[88] This provision specifically refers to a systematic and extensive evaluation of personal aspects based on automated processing, including profiling, on which decisions are based that produce legal or similarly significant effects on the individual, as requiring a DPIA under Article 35(3)(a). However, Article 35(1) allows for additional processing operations underlying ADM and profiling to be covered by the DPIA obligation, depending on whether they are high risk for the rights and freedoms of individuals.

In its profiling guidance, the EDPB stresses that Article 35(3)(a) GDPR "refers to evaluations including profiling and decisions that are 'based' on automated processing, rather than 'solely' automated processing. We take this to mean that Article 35(3)(a) will apply in the case of decision-making including profiling with legal or similarly significant effects that is not wholly automated, as well as solely automated decision-making defined in Article 22(1)."[89]

A number of recent DPA decisions confirm this approach, by finding breaches of the GDPR where controllers carrying out certain forms of profiling or ADM, including qualifying ADM, failed to conduct a DPIA.

Case 3: An algorithm that assigns shifts to platform workers based on certain criteria requires a prior DPIA

In its groundbreaking Deliveroo decision,[90] the *Garante* determined that Deliveroo should have conducted a DPIA on the Frank algorithm, taking into account Article 35(3)(a) GDPR and criteria 1, 2, 3, 4, 5 and 7 of the EDPB/WP29 DPIA Guidelines:[91] the processing used innovative technologies, it was large scale (both in terms of the number of riders — 8.000 — and the types of data used), it related to vulnerable individuals (gig economy workers), and entailed an assessment or scoring of the latter. In this case, the *Garante* found that the ADM at issue was covered by Article 22.

Case 4: Tax Authority must conduct a DPIA before implementing automated tax fraud risk assessments

The Slovak Constitutional Court ruling on the e-kasa system and tax fraud detection algorithm states that "the e-kasa system is a type of processing using new technologies which, given the nature, scope, context and purposes of the processing, is likely to lead to a high risk to the rights and freedoms of natural persons. This finding is all the more true if the [Tax Authority] uses it for automated risk assessment of entrepreneurs and therefore Article 35 GDPR provides one of the guarantees" for the protection of data subjects.[92] It adds that, "As a rule, in the context of an automated assessment, a public authority will be obliged to carry out a [DPIA] pursuant to Article 35 GDPR. However, unlike other processing operations, the impact assessment must focus on the overall human rights impact of automated systems on the individual," as well as on identifying specific risks, (...) [documenting] the scope of human and automated assessment in the different steps of the data processing process, [as well as] how to test the "data-set" and models used."[93] Of note, the Constitutional Court did not make a specific finding related to whether the automated processing at issue falls or not under Article 22 GDPR, since it primarily interpreted and applied the constitutional right to informational self-determination in the Slovak Constitution. It did note tangentially that the automated process used by the Tax Authority does not make a decision *per se* and it only includes an automated risk assessment, but it did not find this of consequence for the application of such constitutional right.[94] In a later paragraph, the Court does refer to Article 22 GDPR under general remarks,[95] without applying it to the facts of the case.

It should be noted that there are some differences resulting from comparing the **ADM covered by Article 22(1) and the ADM that triggers the obligation to perform a DPIA referred to in Article 35(3)(a).** Arguably, certain types of ADM covered by Article 22 are not subject to a prior DPIA, for instance where they are based on an occasional evaluation of a limited number of personal aspects relating to natural persons.

Furthermore, ADM with legal or similar significant effects is only one of nine criteria that controllers should take into account according to the EDPB/WP29 guidance on DPIAs when deciding if a processing is sufficiently high risk to require conducting a DPIA.[96] Other criteria described by the EDPB/WP29 in these Guidelines could also be relevant for identifying high risk processing in other ADM, even if not covered by Article 22 — such as processing that in itself prevents data subjects from exercising a right or using a service, like automated screening of credit applicants, or matching or combining datasets in a way that would exceed the reasonable expectations of the data subjects. According to the Guidelines, if at least two of the nine criteria detailed in the Guidelines are met, controllers should most likely conduct a DPIA. However, the EDPB also recognises that there may be situations where only one criterion suffices for the DPIA to be mandated.[97]

In order to bring more legal certainty about this issue, European DPAs were empowered by the GDPR to clarify what types of profiling and ADM practices they consider to fall under Article 35(1) GDPR, through the approval of specific lists of processing operations which always require a DPIA. Some interesting examples include:

- The Czech DPA's mention of data processing that a data subject cannot influence, which encompasses "processing operations which are performed by the controller (...) as a result of automated decision-making,"[98]
- The Finnish DPA's reference to "Processing of personal data for automated decision-making with legal or similarly significant effects, where the notice exemption under Article 14(5)(b) GDPR applies;"[99] and
- The Greek,[100] Hungarian[101] and Italian[102] DPA lists, all of which deem to clarify that ADM which falls under Article 22(1) always requires a prior DPIA under the Article 35(1) general clause.

2. ASSESSING THE THRESHOLD THAT TRIGGERS ARTICLE 22: CASE-LAW

In order for Article 22 GDPR to be applicable, two conditions must be met at the same time: first, the ADM at stake must involve "solely automated" processing of personal data; and second, the ADM must either produce "legal effects" concerning the data subject, or "similarly significantly" affecting the data subject. If at least one of the two conditions is not met, then the processing does not fall under Article 22 GDPR and its specific requirements.

Courts and DPAs apply an increasingly sophisticated set of criteria when making these assessments. In order for a decision to be considered "solely" automated, enforcers are looking at the entire organizational environment where the processing takes place: organizational structure, reporting lines and chain of approval; effective training of staff; internal policies and procedures. Formal human involvement in making decisions is not considered sufficient, with enforcers paying attention to the quality of human involvement, how it relates to individual and actual decisions (as opposed to setting parameters at the outset for the whole ADM process), and at what time in the decision-making process it occurs.

When assessing if ADM has legal or similarly significant effects, the criteria used are even more complex, layered and considered in relation to one-another. Enforcers pay attention to everything from the categories of personal data on the basis of which the automated decisions are produced and whether they include data points and/or inferences about the behavior of data subjects, to the capacity of a decision resulting from ADM to affect the "conduct and choices" of the persons targeted, and to the more easily quantifiable financial loss or loss of income opportunity.

Our research shows that even in those cases where Courts and DPAs decided that the ADM at issue does not fall under Article 22 GDPR since it does not meet the required criteria, they have still enforced other relevant provisions of the GDPR, such as the principles of transparency, fairness, data minimization, purpose limitation, and other provisions.

2.1 "Solely automated processing" can sometimes include human involvement

The interpretation of the meaning of the "solely automated processing" element of Article 22(1) GDPR is one of the most contentious issues in cases before EU Member-States' courts and one of the biggest focuses of DPA decisions relating to ADM. According to guidance from the EDPB/WP29, not all forms of human involvement in a decision-making process rule out the application of such provision, as **mere token gestures taken by humans are not enough to set aside the ADM prohibition.**[103] The condition that the decision-making must be "solely automated" in order for the prohibition and special conditions in Article 22 to apply has already been assessed in several cases, both by national Courts and DPAs. In the cases we analyzed, the Courts have found that the decision-making is not solely automated primarily when:

- organizational measures are put in place to ensure structured and substantial human involvement, such as when multiple persons analyze automated individual potential fraud flags and have to unanimously agree on whether fraud was committed taking into account additional elements and correlating facts; or when
- internal procedure requires a written assessment made by case officers on the basis of an automated assessment, which then needs to be vetted by the head of the organization; or when
- employees are specifically trained and provided with detailed guidelines on additional elements to take into account in order to make decisions on the basis of automated assessments and recommendations.

As an outlier, a subjective criterion such as employees "using their own judgment" to act upon automated recommendations was also considered in one case (by a DPA) to render the decision-making as not solely automated.

On another hand, the cases where enforcers have found that the ADM at issue was "solely" automated involved outcomes based on an automated process which could not be influenced by humans, or included inconsequential human involvement — as revealed by factors such as lack of training about making decisions based on automated recommendations.

It is interesting to note that in all cases studied, with no exception, the enforcers assessed the last stage of the decision-making process to conclude whether it was "solely" automated or not. Moreover, in one of the cases, the DPA specifically found that the fact human staff manually set out the algorithm's parameters had no consequence on the nature of the decision to be classified as "solely" automated.

Most importantly, even in the cases where Article 22 ADM was not found to be applicable, the DPAs or the Courts applied the other relevant GDPR provisions. Most of the time, breaches of the GDPR were found, such as those related to lawful grounds for processing and those related to general transparency requirements (see, for instance, cases 22 and 23 below, which also resulted in significant million euro fines).

Case 16: Deactivating the account of a ride hailing driver — not "solely" automated when humans make the final decision after considering factors other than the ADM signal

In the Uber case concerning the deactivation of driver accounts, the District Court of Amsterdam was satisfied that Uber had demonstrated it was not carrying out "solely automated" decisions with regards to such deactivation. In that context, Uber showed that its software was used to identify potentially fraudulent activities of its drivers. Such a system merely generated signals for a specialized team of Uber employees (the EMEA Operational Risk team) to initiate investigations of such activities. Uber's protocols required them to analyze these signals and the associated facts and circumstances to confirm or dismiss the existence of fraud. Based on the investigation, two employees from the Risk team needed to unanimously decide to deactivate the driver's account on grounds that there was a consistent pattern of fraud.[104]

Case 8: Granting a gun license is not "solely" automated when the negative result of pre-screening does not automatically lead to rejecting the license application

Likewise, in the gun license applicants case, the District Court of The Hague found that the decisions taken by the Dutch State to grant or refuse such licenses to applicants who filled the legally-vetted e-screener were not solely automated in the meaning of Article 22(1). The court's decision stresses that the weighting of the answers to the e-screener is carried out by a computer program based on validated algorithms, which produces a quick and efficient opinion that would otherwise have to be given by a psychologist or psychiatrist. A negative result in the e-screener does not inevitably lead to a rejection of the gun license application. **The decision whether to grant the license or not is taken by the Dutch Police's chief constable,** based on the opinion formed on the suitability of the person concerned, **weighing all the information assessed. Such information includes the results of the e-screener, but also a background check of the applicant and applicant's own representations.** However, the application is rejected if there are no clear contraindications that put the negative outcome of the e-screener into question.[105]

Case 9: Distributing benefits to jobseekers: not "solely" automated when social security employees are trained and are provided guidance on additional factors to take into account

A similar view was taken by the Austrian BVwG in the already summarized job seekers' potential assessment algorithm case. Therein, the court established that no solely automated decisions under Article 22(1) were taken by AMS in relation to job seekers, as the final decision on labor market potential opportunities — and thus the allocation of funding — rests with the respective AMS counselor. In order to ensure that the result calculated by the AMAS algorithm was not relied upon unquestioned by the counselors, the AMS had published guidelines for action and had carried out training courses, both of which instructed counselors to take AMAS's results only as one of several information sources. **Criteria that cannot be taken into account by AMAS, such as motivation and self-help potential of the jobseeker, addiction, debt, housing situation, etc., are mentioned in the guidelines as decisive** for the final decision of the counselors, which could lead them to diverge from the AMAS results. Counselors ultimately decide, together with each jobseeker, on the optimal support strategy for the latter (e.g., through subsidies and support services).[106]

Cases 22 and 23: Client profiling is not qualifying ADM if employees take the final decision on the best commercial approach in each case, but consent should be informed and specific

In January 2021, the Spanish DPA (AEPD) published a decision in which it found that Caixabank's **client profiling practices did not amount to ADM under Article 22(1), as the individual decisions taken on the basis of the profiling exercise (which included price-tailoring and credit concession decisions) were taken by Caixabank's employees exercising their own judgment.** The AEPD reached this conclusion despite the fact that Caixabank asked its customers to consent to such data processing, and that it told them that they had the right to obtain human intervention, express their point of view and contest the decisions taken by Caixabank on the basis of the profiling, as well as to obtain an explanation of said decisions, all of which are typical of qualifying ADM. **Nonetheless, the AEPD still concluded that the controller breached its transparency duties under Articles 13 and 14 GDPR, and failed to secure a lawful ground for its client profiling activities as per Article 6.** With regards to the former breach, the DPA relies on Recital 60 GDPR and the fact that the controller failed to inform data subjects about the types of profiles it intended to build, their specific uses and consequences, nor about the individuals' right to object. Concerning the latter, the AEPD established that the data subject consent on which Caixabank relied for its client profiling activities was not informed, free nor specific — and hence valid — given the DPA's findings of transparency shortcomings and since the consent was bundled to the contractual terms that clients accepted when opening their accounts. This led the DPA to impose an administrative fine against Caixabank, in a combined total of 6.000.000 EUR.[107]

In a separate case later that year, on September 22, the AEPD issued a 3.000.000 EUR fine against Caixabank, after establishing that the consent on which the company relied to profile prospects and customers for loan default risk analysis (both before and after credit is granted) and personalized promotional activities was not sufficiently informed. Of note, the DPA does not make any findings in relation to the applicability or lack thereof of Article 22 GDPR. The DPA noted that the information provided to data subjects in this regard was generic, as it did not allow data subjects to understand the processing at stake — notably, the profiles' level of detail — and its consequences, such as the determination of an individual loan amount ceiling. Moreover, the DPA found that data subjects were not given the chance to separately consent to each of the profiling purposes, as required under Article 4(11) GDPR, nor to the sharing of data with other Caixabank Group entities.[108]

Case 24: Content moderation algorithm in a dating app is not qualifying ADM if final decision is taken by a human

In the complaint that the NGO Rights International Spain filed against Grindr LLC with the AEPD, there was a claim that the dating app's content moderation algorithm produced prohibited automated decisions that fell under Article 22 GDPR, as it could lead to blocking user accounts where there were indications of illegal activities. Although the controller admitted that it used an automated system to detect possible instances of fraud, spam, or breaches of its Terms & Conditions, it successfully argued that the system merely produced signals that Grindr employees analyzed before deciding whether to remove the content at stake or block the user account. Therefore, in its January 17, 2022 decision, the Spanish DPA found no breach of the GDPR in this regard.[109]

Danish DPA Opinion: Decisions on job offers that are merely supported by automated analyses are not qualifying ADM

The Danish DPA's (*Datatilsynet*) July 2019 response to a parliamentary consultation on the draft law related to active employment efforts presents clear similarities with the AMAS court decision (see Case 9). The DPA's assessment focused on the parts of the bill that dealt with a nationwide digital clarification and dialogue tool that could be used by job centers and unemployment funds. With the tool, a statistically-based analysis could be made of the citizen's risk of becoming long-term unemployed based on information obtained from the citizen himself and information about the citizen collected from the Ministry of Employment's and other public authorities' own records. In this context, the DPA emphasized that **the clarification tool should be used to support the caseworkers' professional assessment in order to improve the chances of offering the right job, but that decisions would not be made solely on the basis of data obtained from the tool.** It was against this background that the DPA considered that the envisaged profiling would not fall within the scope of Article 22 GDPR.[110]

Instances of fully automated decision-making for the purposes of Article 22 GDPR have been found in cases where either human staff had no possibility to influence the outcome of the decision at issue, but also where the human involvement was not considered meaningful and was seen as "rubber-stamping."

Case 25: Automated ranking of students leading to university admissions and placement offers is qualifying ADM

In a pre-GDPR case, the French DPA (CNIL) found that admissions to French universities were determined solely by the use of two computer algorithms: one automatically ranked university applicants on the basis of three criteria (their place of residence, the order of their wishes and their family situation); and another automatically directed an offer of university admission solely on the basis of that ranking. Moreover, if there were several applicants filling the same criteria for admission, exceeding the number of vacancies in universities, the algorithm would randomly select the applicants who would receive the offers. **Human staff at universities had no possibility of influencing the final decision regarding offers of admission delivered to applicants.** The CNIL established that the ADM at stake breached the French national rules transposing Article 15(1) DPD and it ordered universities to put in place an admission procedure which involved meaningful human intervention, thereby allowing them to consider applicants' observations.[111]

Case 6: Assigning income opportunities to platform workers on the basis of their "score" is prohibited under Article 22

The Foodinho case offers another example. In that context, the *Garante* looked into the automated data processing system used by Foodinho to assign riders to certain food and product deliveries, on the basis of the riders' "score." Such score was set considering factors such as customers' and merchants' feedback, as well as riders' service requests history (e.g., how many requests they had accepted and how fast they performed deliveries). **The DPA determined that such a system produced automated decisions covered by Article 21(1) GDPR, which was not affected by the fact that the algorithm's parameters were manually set by Foodinho's employees**.[112]

Even in cases where there is a final decision taken by a human, the ADM process may still be considered "solely" automated when the humans involved in the decision-making process simply "rubber-stamp" an automated decision.

Case 26: Student proctoring software — lack of clear human assessment criteria leads to "rubber-stamping" algorithmic suggestions, thus the decision is "solely" automated

The lack of fully automated decisions was one of the grounds which a Portuguese university that planned to deploy student proctoring software during the Covid-19 pandemic used to try to avoid corrective action from the Portuguese DPA (CNPD), in May 2021. The controller sought to use Respondus Inc's "Monitor" software to analyze students' behavior when taking exams (through the use of the students' computer webcam and video analytics technology, including facial and motion detection). The software would have produced a report with an analysis of each students' "performance," including by attributing a grade to each student corresponding to the likelihood that they had committed a breach of the exams regulations.

In its decision, the CNPD found that the software tool processed the students' "biometric patterns" (by combining their use of mouse and keyboard with their body and facial movements) to build each student's profile through solely automated means, ultimately attributing each of them a fraud likelihood score, which amounted to a breach of the GDPR's minimisation principle. Moreover, the CNPD expressed its views on the university's claims that the system did not produce fully automated decisions, as professors would take the final decision on whether to investigate potential instances of fraud based on the scores produced by the system and ultimately on whether to invalidate exams. It noted that "**the absence of specific guidelines on the interpretation they should give those scores and the lack of guiding criteria for teachers to take coherent and transparent decisions may generate situations of discrimination and lead teachers to validate the systems' decisions as a rule.**" This seems to demonstrate that the CNPD does not believe that human authority and competence on profiling-based decisions are enough to rule out Article 22(1): the human decision-maker also needs to understand why they should follow the automated system's lead or not.[113]

It is important to note that there are also ADM cases that are assessed from the perspective of other branches of law, most often labor law, and not only in the application of data protection law. While such cases are not in the scope of our report, we did identify some of them during our research. In these cases, national courts express reservations toward decisions that impact individuals based on solely automated processes[114] more often than not.

2.2 "Legal or similarly significant effects" require a multi-dimensional, case-by-case analysis

In order for ADM to trigger the protection of Article 22 GDPR, it needs not only be "solely" automated, as explained above, but also to have either a legal effect for the data subject, or a similarly significant effect. Some useful examples can be found under Recital 71 GDPR and the EDPB's guidance (see Section 1.3 above). However, our analysis shows that a multi-dimensional case-by-case analysis is required, with enforcers weighing together a wide variety of criteria, such as:

- the categories of personal data on the basis of which the automated decisions are produced and whether they include data points and/or inferences about the behavior of data subjects;
- the immediate consequence the decisions have on data subjects;
- the temporary or definitive effect of the decisions;
- whether the decisions affect conduct or choices of the data subjects;
- whether the decisions limit opportunity for income or are followed by a quantifiable financial loss for data subjects;
- whether the data subjects are able to demonstrate the impact of decisions on them are not trivial where enforcers do not find the facts of the case sufficient to show a legal or similarly significant effect.

We also note that one of the most consequential adjudicated cases where ADM had broad impactful effects on individuals is the SyRI judgment in the Netherlands (Case 27 below). In this instance, neither the Court nor the DPA decisions relied on Article 22 GDPR to ultimately protect the fundamental rights of individuals. While the Court directly found a breach of Article 8 of the European Convention on Human Rights (the right to respect for private life) when applying GDPR concepts like purpose limitation and data minimization, in a separate case on the same subject matter, the Dutch DPA found a breach of the principles of lawfulness and transparency, as well as a breach of the principle of fairness in the GDPR. Nonetheless, the "significant effects" on individuals of the SyRi algorithm were documented and explored in these cases.

Case 27: Automated fraud signals have a significant effect on the private life of the targeted individual

In February 2020, the District Court of The Hague delivered its seminal ruling on the Dutch governments' controversial System Risk Indication (SyRI) algorithm. SyRI was an algorithmic fraud detection tool targeted at neighborhoods hosting poor or minority groups in the Netherlands. The system built risk profiles of individuals to detect various forms of fraud, including social benefits, allowances, and taxes fraud. The court found that even if "the use of SyRI (...) as such is not aimed at legal effect — neither [under] civil, nor administrative or criminal law — **a risk report does have a significant effect on the private life of the person to whom the report relates.**" This, among other findings (such as the lack of transparency of the system), led the Court to rule that the scheme breached Article 8 of the European Convention on Human Rights (right to respect for private and family life). However, the court left open "the question of whether the precise definition in the GDPR of automated individual decision-making and [whether] (...) one or more of the grounds for exception to its prohibition in the GDPR are met."[115]

More recently, the Dutch DPA (AP) has sanctioned the Dutch Tax and Customs Administration with a 2.750.000 EUR fine for the processing of the dual nationality status of childcare benefits applicants in the SyRi system with a view to detect instances where there was a likelihood of organised fraud, in a manner that the DPA considered to be discriminatory profiling that was unlawful under Article 6(1) GDPR, and in breach of the lawfulness and transparency principles under Article 5(1)(a) GDPR. Specifically, the DPA considered that "dual nationality" status was not necessary to be processed for the performance of a task in the public interest by the Tax Authority, under Article 6(1)(e) GDPR, which also means that the principle of lawfulness under Article 5(1)(a) was not observed. The AP found that Dutch nationality was sufficient to be processed, considering that it was the one triggering the potential benefits. In addition, the AP found that the principle of fairness was not observed either. "In short, such processing can be regarded as discriminatory and for that reason contrary to the principle of fairness within the meaning of Article 5". Significantly, the AP did not make any findings with regard to Article 22 GDPR in this case.[116]

Cases 17 and 18: Ride-hailing drivers did not demonstrate that the effects of ADM impacting them were not trivial

In both Uber cases which we have previously summarized, the Amsterdam District Court did not find that the automated decisions made through algorithms regarding drivers — respectively, the decision to preventively impede drivers from accessing their accounts pursuant to a fraud signal until they reached out to the company, and the decision to favorably match drivers with passengers according to the drivers' location and existing traffic conditions — had the sort of impactful, long term or lasting effects that Article 22(1) would require. In the second case, the court more precisely held that the **plaintiffs were unable to judicially demonstrate that the effects of not being matched with a passenger because of the ADM system were not trivial,** but indeed sufficient to reach the Article 22(1) significance threshold.[117]

Case 19: Automated decisions to impose fines or fare deductions on gig economy workers have the sort of impacts covered by Article 22

In the Ola case, the Amsterdam District Court established that the ride-hailing company's **automated decisions to impose fare deductions and/or fines on its drivers on the basis of the performance data it collects about them "ha[ve] effects that are important enough to deserve attention and that significantly affect the conduct or choices of the person concerned** as referred to in the [EDPB] Guidelines. **Such a decision leads to a penalty which affects the rights of [the applicants] under the agreement with Ola."**[118] It therefore decided that Ola was prohibited from taking such decisions. However, the wording of the decision is not clear as to whether the court finds that Ola's ADM had legal or only similarly significant effects on its drivers (or, indeed, both types of effects).

In the Uber (non-existent "Article 22 effects") and Ola (existent "Article 22 effects") cases the same Court reached different conclusions with regard to the effects that the ADM at issue had on data subjects. The various elements the Court took into account, in combination with one another, were:

- the type of personal data on the basis of which the automated decisions were produced (in the Uber cases: factual data as location and traffic, which are not dependent on driver behavior; fraud signals, which are dependent on driver behavior, requiring a further assessment; in the Ola case: broader "performance data" related to the overall and ongoing behavior of an individual as a gig worker);
- the immediate consequence on data subjects (in the Uber cases: matching gigs/rides; suspending access to the gig account until further verification; in the Ola case: imposing fines and penalties);
- the temporary or definitive effect of the decisions (Uber case: the accounts were suspended temporarily before a further decision was reached; Ola case: a sanction was imposed as a fine, which seemed definitive in nature);
- whether the decisions affect conduct or choices of the data subjects (a specific impact highlighted in the Ola case);
- whether the data subjects are able to demonstrate that the impacts of decisions on them are not trivial. However, the burden of proof seems to have been considered as falling on the data subjects only as a second step, once the Court was not satisfied by itself, based on the facts of the case, that the impact on individuals triggered the application of Article 22. In the Ola case, the Court seems to have been satisfied by the facts of the case that the impact of the decisions were covered by Article 22, without mentioning the burden of proof.

Cases 3 and 6: Ranking algorithms have significant effects on workers if they limit their chances of making income

In July 2021, following an Italian court ruling (which is further analyzed below[119]), the *Garante* sanctioned Deliveroo for GDPR breaches related to its rider ranking algorithm. This algorithm automatically ranked and assigned riders to certain delivery slots based on the riders' manifested availability in critical time slots (Friday, Saturday, and Sunday evening) and the riders' reliability regarding their manifested availability (i.e., whether riders actually participate or not in their booked shifts). In its June 2020 defense, Deliveroo claimed that Article 22 GDPR did not apply to its booking system, "given the absence of (even abstract) legal or similarly significant effects on the individuals." However, the DPA concluded that the company carried out profiling and ADM impacting its riders, notably for (i) "reliability" and "willingness" assessments relating to the acceptance of shifts during critical time slots, to exclude riders from shift choices (until November 2, 2020); and for (ii) the assignment of orders within the booked shifts, through an algorithmic system called "Frank." The DPA held that **such ADM produced a significant effect on the riders, consisting of the possibility of allowing (or refusing) access to job opportunities,** in certain pre-established time slots, and therefore offering (or denying) an opportunity for income.[120] The DPA's view on the seriousness of the effects of the ADM system on Deliveroo's riders was equivalent to the one it took in an earlier decision that looked into a similar system set up by Foodinho to manage its riders.[121]

While we have mentioned in Chapter 1.3.c) above that the EDPB took a nuanced view of whether online behavioral advertising may qualify as Article 22-covered ADM, depending on the nature of the advertising and profiling at stake, the Portuguese DPA has offered a specific take on whether targeted political advertising qualifies as such.

Portuguese DPA Guidelines: ADM-powered political advertising is covered by the GDPR's ADM prohibition

The Portuguese DPA (CNPD) adopted political marketing guidelines in March 2019 addressing the issue of tailored political communications. In that context, the CNPD stressed that, where messages (SMS, emails, etc.) by political parties to potential voters are tailored or targeted through profiling or ADM, such activities may be covered by Article 22 GDPR, as they may significantly affect citizens. This means that, according to the DPA, such profiling or ADM requires the recipients' prior explicit consent. Furthermore, the CNPD mentions that the messages sent to potential voters should include information about why they are receiving them.[122]

3. ADM AND THE GDPR CASE-LAW IN SPECIFIC SCENARIOS: WORKPLACE — FACIAL RECOGNITION — CREDIT SCORING

The following sections explore three specific scenarios where individuals tend to challenge ADM systems more often: the workplace (managing employees, contractors, hiring processes); Facial Recognition (automated facial recognition, both in the public interest and for commercial purposes); and credit scoring. The cases summarized show that the GDPR provides for protection of individuals against unlawful practices in these scenarios, even where Article 22 is not applicable. In addition, each section briefly introduces new legislative proposals introduced by the EU to tackle specifically each of these scenarios, creating thus potential overlap which deserves further exploration.

3.1 ADM in the workplace often interacts with labor rights

Courts often assess the lawfulness of profiling and ADM processes through other lenses than data protection law. This is particularly evident in judicial proceedings which involve the use of algorithmic tools by organizations to manage their workforce and individual service providers or contractors. A significant body of case-law is emerging on the issue of ADM in the gig economy, which often includes both GDPR enforcement and labor law considerations. Interestingly, it is precisely the use of ADM systems to manage gig workers which is considered the relevant argument by enforcers to qualify this situation as an employment relationship, and therefore a "labor law" issue (see cases 3 and 29).

Case 28 (related to Case 3): Fairness of automated ranking depends on the factors which are weighed in by the algorithm

In December 2020, the Labor division of the Italian Bologna Court found that Deliveroo's reputational ranking algorithm "Frank," which determined the order in which Deliveroo's riders would be called for a given service, was discriminatory and unlawful, after three riders sued the company. The algorithm took into account riders' absences, without considering the reasons behind absenteeism (e.g., riders or their children could have been sick that day). Riders which were not available for, or canceled a given service would lose "points," thus leading them to a less favorable position to be attributed services in the future, which could eventually result in a quasi-ban from the platform. The Court stressed that **Deliveroo's profiling system could and should have treated riders that did not participate in booked services for trivial reasons differently from riders who did so because of legitimate reasons (like strikes, sick leave, etc.).** The Court did not reach any direct conclusions on whether "Frank" fell under the scope of Article 22 GDPR, as it approached the case from an Italian labour and anti-discrimination law perspective.[123]

Cases 3 and 29: Algorithmic management of gig economy workers leads to qualification of the relationship between platforms and gig workers as "employment"

The Italian DPA devotes a significant part of its Deliveroo decision explaining why the company's rider management algorithm breached Italian labor laws, including a new law that protects gig workers in Italy. The decision states that "**the company carries out the processing of personal data of the riders (...) in the context of an employment relationship** concerning the transport of food or other goods from restaurants or other partner merchants (...), through the use of a digital platform." The Garante reaches this conclusion after assessing several elements of the relationship that exists between Deliveroo and its riders, such as the fact that the company determines the riders' remuneration and supplies them with mandatory working tools (like the Deliveroo app's credentials), garments and work shifts (through the disputed algorithm). Given the "employment" nature of this relationship, the Italian DPA stressed that **Deliveroo is required to comply with Italian labor law rules on the processing of its riders' (i.e. employees) personal data**, regardless of the concrete qualification of such employment relationship, pursuant to Section 114 of the Italian Privacy Law.[124] **This includes the prohibition of excluding workers from digital platforms or reducing their job opportunities on grounds that they refused to accept offered services.**[125] Therefore, and because it established that Deliveroo's rider management algorithm led to the exclusion of certain riders from such opportunities, it found that the controller breached the GDPR's lawfulness principle (Article 5(1)(a)) and its employment-focused provision (Article 88).[126]

A similar view was taken by the Amsterdam District Court — in September 2021 — regarding Uber's drivers, which the Court qualified as the company's employees under Dutch labor laws. Among other grounds, the court found that Uber exercised its employer powers and prerogatives through the algorithmic assignment of rides to drivers (according to Uber-established rules and priorities), as well as the algorithmic determination of the payment they obtain for each ride. The court's decision also mentions the fact that drivers who cancel previously accepted journeys may be automatically excluded (i.e., logged-off) from Uber's platform as an indication of the subordination to which Uber's drivers are subject, which the court notes is typical of employment relationships. Interestingly, the Court notes that Uber's **algorithms have disciplining and instructive effects on drivers, thereby allowing Uber to exercise its "modern employer authority."**[127]

These recent court rulings and DPA decisions may have been one of the factors that inspired the European Commission to propose a **new Directive to improve working conditions in platform work across the EU.**[128] The EC's Proposal states that "Algorithm-based technologies, including automated monitoring and decision-making systems, have enabled the emergence and growth of digital labor platforms", and that "Persons performing platform work subject to algorithmic management often lack information on how the algorithms work, which personal data are being used and how their behavior affects decisions taken by automated systems."[129] Among other groundbreaking rules, the draft text contains provisions on worker status reclassification and the **algorithmic management of platform workers.** The proposal includes provisions on added **transparency** towards workers regarding automated monitoring and decision-making systems (e.g., grounds for decisions to restrict, suspend or terminate the platform worker's account), to a **ban on processing personal data on the emotional or psychological state** of platform workers.[130]

Management of gig workers with the help of ADM is not the only issue that has gained attention of regulators and enforcers. Automated screening of job applications is another point of concern which has generated regulatory action.

Saxon DPA note: An algorithm which automatically filters job applicants that are selected for interviews counts as qualifying ADM

In its 2019 Annual Report, the DPA from the German Free State of Saxony elaborated on a job application assessment tool that the Saxon State Chancellery wished to deploy. Applicants would be automatically assessed and ranked by a software according to predetermined criteria (with differing and predetermined degrees of importance). The types of personal data used for the assessment were the applicants' names, addresses, contact details, gender, severe disabilities (if any), certificates and work assessments. **The evaluation made by the tool would ultimately serve as the sole basis for deciding which applicants would be invited to interviews.** Taking the above into account, the DPA concluded that there was profiling and qualifying ADM involved, as the **decisions taken lacked meaningful human intervention and were liable to significantly affect applicants' rights.** Moreover, the DPA took the view that the system did not seem to comply with Article 22 requirements with regards to the use of an exception to the ADM prohibition, under paragraph (2).[131]

3.2 Facial Recognition is broadly regulated by the GDPR, beyond Article 22

There is a large trove of cases decided by EU courts and DPAs in the application of the GDPR, involving either building Facial Recognition (FR) products, or the use of live FR technologies in contexts as varied as recording attendance in schools and keeping former convicts from entering a supermarket. Thus, it is not only the **providers** of FR technologies that have been subject to GDPR enforcement (see Cases 10, 11, 12 and 13 above) for the way they processed personal data to build FR systems, but also the **users** of such technologies.

These cases mainly focus on the issue of lawfulness under the GDPR (Articles 6 and 9), as well as on principles, such as accuracy and data minimisation (Article 5). Only some of them refer specifically to Article 22.

Our research shows that the GDPR offers individuals meaningful safeguards against some uses of FR, notably via its rules on lawfulness of processing personal data in conjunction with the rules on processing sensitive data (such as biometrics), profiling and ADM. For instance, these provisions have protected students in France, Sweden and Bulgaria from being subjected to attendance checks or access permission on school grounds through automated FR.

One notable common feature of the cases we identified is the fact that enforcers considered explicit consent as being the only lawful ground that can justify the use of live FR in most cases. In all cases where controllers argued they relied on the consent of data subjects for the use of live FR, enforcers found that the consent was invalid, primarily because it was not freely given. In one case, where public interest was argued to justify the use of live FR, the Court rejected this submission and required that any public interest that may justify the processing at issue must be grounded on a specific law to be considered as a valid lawful ground (cases 32 and 33).

In the one case identified where live FR was considered to be lawfully based on substantial public interests, and thus not requiring explicit consent, the DPA requested specific safeguards to be in place in order to consider the processing lawful: refraining to store images that fail to generate a match with the database used, posting clear signage that automated FR checks are being carried out, and deploying cutting-edge encryption (Case 34).

Cases 30 and 31: Automated FR to monitor school attendance and control access requires explicit and free consent under Article 9(2) GDPR

A February 2020 ruling by the Marseille Administrative Court annulled a decision from the Provence-Alpes-Côte d'Azur (PACA) region of France to conduct two FR pilots at the entrance of schools located in Nice and Marseille. **The system would allow the schools' staff to either grant or refuse students access to the schools' premises, depending on whether a match in the student facial images database was detected or not.** While the case — which was brought by two NGOs and a parents association — was pending, the CNIL expressed concerns about the implementation of such a system, given the target audience (children) and the sensitivity of the biometric data at stake.[132] The Court's decision to annul the pilots was taken on grounds that **the consent collected from high school students was not given in a free, specific, informed and univocal way** (in line with Article 9(2)(a) GDPR), and that **less intrusive means were available to schools to control their students' access to their premises** (e.g., badge/ID card checks, coupled with CCTV).[133]

Likewise, in June 2021, the Stockholm Administrative Court upheld the decision of the Swedish DPA (IMY) to impose a 200.000 SEK (roughly, 20.000 EUR) on the Upper Secondary School of Skelleftea for unlawful use of automated FR to record students' attendance at a test.[134] Aligning with the IMY, and amongst other findings, the Court stressed that **there was an imbalance of power between the school and data subjects (i.e., the pupils), which meant that the latter's consent to the processing of their biometric data could not be considered free and, hence, valid.** The court also held that the school had the right to monitor students' attendance, but not by collecting biometric data, given its sensitive nature under Article 9 GDPR.[135]

Bulgarian DPA Opinion: The decision to prevent students from entering school premises on the basis of automated FR and temperature checks amounts to prohibited ADM

The Bulgarian DPA (CPDP) took a similar position to its Swedish counterpart in an opinion issued in 2020 upon a school's request. The controller in this case wished to install an FR and temperature measurement system at the school's doorway and to deny entrance to its premises to students and teachers who rejected being subject to such monitoring. Besides noting that the only suitable legal basis for processing special categories of data (such as biometric and health data) in this context would be consent, the DPA stressed that consent in such a scenario would not be free. However, the CPDP went beyond the IMY, by holding that **decisions to impede data subjects from entering a school's premises by using these systems would not comply with Article 22 GDPR, and that access control therein should be conducted without the processing of special categories of data.**[136]

Cases 32 and 33: Using FR to keep convicted individuals away from a shop is unlawful

In a different context, the Court of Appeal of Barcelona ruled, in February 2021, that the use of an automated FR system to prevent the entry of judicially banned persons into a supermarket chain's premises was unlawful. The background of the decision was the following: two persons were sentenced to prison by the Criminal Court of Barcelona for violent robbery in a Mercadona supermarket. They were also prohibited from entering the supermarket for two years. Mercadona asked the court to allow it to use an automated FR system to monitor their entrance to the supermarket and to stop them from accessing. They added that relying on traditional means (i.e., instructing the security personnel to perform the control) would be virtually impossible. In order to justify this, Mercadona invoked a legitimate interest to ensure compliance with the judgment of the criminal court and a public interest based on the Spanish Private Security Act.[137] The criminal court rejected the petition, a decision which Mercadona contested before the Court of Appeal. The latter, however, dismissed the appellant's arguments, as it concluded that the use of such FR systems in the field of private security would imply the processing of biometric data aimed at uniquely identifying a natural person, which is, in principle, prohibited under Article 9 GDPR. The Court of Appeal added that **any public interest justifying the processing of special categories of data would have to be grounded on a specific law, which currently does not exist in Spain.** Alternatively, the controller would have to rely on the data subjects' consent for the intended data processing which, in the given case, would not be free (since it would always be made a precondition to enter the supermarket's premises).[138]

Since then, on July 27, 2021, the Spanish DPA has imposed a 2.500.000 EUR fine against Mercadona for its automated FR pilot in 48 of its supermarkets to detect the two banned persons. In a preliminary opinion of early July, on whether controllers could rely on automated FR technologies to comply with the Anti-Money-Laundering regime, the DPA had stated that controllers cannot make consenting to the processing of biometric data a condition for data subjects to access their services, and that there was no legal provision in the Spanish legal order that otherwise allowed such processing.[139] Later, in its decision to fine Mercadona, the AEPD confirmed that Mercadona:

- could not rely on the Article 9(2)(f) and (g) GDPR derogations for processing shoppers' biometric data through the automated FR system, as such processing served Mercadona's private interests only. In that respect, the DPA underlines that the criminal court sentence did not specify the electronic means (e.g., live FR) that Mercadona could use to ensure the convicted persons complied with the ruling;
- did not adequately inform data subjects about the processing, notably about the underlying logic of the automated FR system, thereby effectively barring data subjects from exercising their rights;
- failed to carry out a DPIA and to consult with the DPA prior to the processing;
- did not implement appropriate measures to ensure data protection by design and by default, which allowed Mercadona to collect its customers' biometric data in a remote, massive and indiscriminate fashion.[140]

Case 34: Monitoring attendance on a football stadium through automated FR technology is allowed for substantial public interest reasons, as long as adequate safeguards are implemented

A position which seems to **directly conflict** with the Mercadona court ruling and DPA decision was taken by the Danish DPA (*Datatilsynet*), in May 2019. Back then, the regulator allowed the Brondby I.F. football club to install an automated FR system in its stadium to prevent the entrance of (about 50) banned spectators.[141] The DPA took the view that **the processing of match attendants' personal data through the automated FR system would be allowed under Article 9(2)(g) GDPR, as it would be necessary and proportionate to attain objectives of substantial public interest, notably to ensure the spectators' security.** Nonetheless, the DPA establishes certain conditions that the controller needed to observe before deploying the automated FR system, including not storing images that fail to generate a match with the banned spectators' database, posting clear signage that automated FR checks are being carried out and deploying cutting-edge encryption.[142]

DPAs across the EU have expressed serious reservations about the use of live FR systems in the law enforcement context.

Case 35 and Italian DPA Opinion: Using live FR systems for law enforcement purposes lacks an appropriate legal basis

In February 2021, the Swedish (IMY) DPA found that Clearview AI had been used by the local police on a number of occasions. The DPA held that the Police had unlawfully processed biometric data for facial recognition and failed to conduct a legally-mandatory DPIA. Therefore, the DPA imposed an administrative fine of 2.500.000 SEK (approximately 250.000 EUR) on the Police Authority.[143]

Likewise, in March 2021, upon a request for an opinion by the Ministry of Interior, the Italian DPA took the view that the mobile real-time automated FR system (Sari) that the Ministry intended to roll-out for security purposes would be unlawful. Such a system would compare recorded subjects with a predefined "watch-list" of 10.000 faces. The Garante noted that the biometric data processing at stake would lack an appropriate legal basis and that the system would lead to mass surveillance.[144]

Finally, it is of note that live Facial Recognition technologies are a focus of the AI Regulation Proposal presented in April 2021 by the EC. Such systems would generally be qualified as "remote biometric identification systems" under the Proposal, either leading (or intending to lead) to real-time or post-identification of data subjects.[145] Thus, it is essential to understand how the relevant GDPR provisions and the AI Act provisions will overlap, in order to effectively protect the fundamental rights of individuals and their communities.

3.3. Credit Scoring is justified on "contractual necessity" only if it relies on relevant information

Courts and DPAs in Europe have been active in assessing the lawfulness of automated credit scoring practices under the data protection framework. This is illustrated by the questions referred by the Vienna Regional Administrative Court to the CJEU that we outlined in the introduction to Chapter 1.6.c, by the fine imposed by the Swedish DPA against Klarna for transparency shortcomings (analyzed in the same Chapter as Case 14), and by the Spanish DPA decisions against Caixabank in 2021 (Cases 22 and 23 above). Below we outline other examples of rulings which provide insight into creditworthiness assessments that may be considered profiling or qualifying ADM under the GDPR.

The key question in most of the cases analyzed is whether the credit scoring or the decisions to provide credit that financial institutions make are qualifying ADM. There is no unitary practice, with the CJEU currently considering questions for a preliminary ruling to clarify under what conditions credit scoring is the type of ADM that falls under Article 22 GDPR.

Existing case-law indicates that relying on certain criteria, such as age, to automatically exclude a credit application from being analyzed, is qualifying ADM and needs to comply with the prohibition in Article 22 GDPR and its exceptions. Interestingly, in one case, the DPA decided that for the contractual necessity exemption to be applicable, the personal data on the basis of which the ADM process reaches a conclusion about the individual has to be relevant for the purpose pursued (e.g. age should not be taken into account, but the applicant's financial situation should; see Case 37).

Case 36: Automated credit scoring is not qualifying ADM if a human ultimately decides whether to grant a loan or not

In anearly pre-GDPR ruling from 2014, the German Federal Court of Justice (*Bundesgerichtsoft*) stated that "credit-scoring only amounts to an automated individual decision where the responsible body takes a decision with a legal consequence for the person concerned or a decision that has a significant impact on the person concerned, solely on the basis of a score result without further examination of the content. **That is not the case where the knowledge gained through automated data processing is only the basis for a final decision still to be made by a human being.**"[146] The court's remarks are similar to the ones made by the Spanish DPA in the Caixabank case, which we have covered above as Case 22.[147]

Case 37: The use of certain factors in automated creditworthiness assessments leading to the exclusion of credit applicants is prohibited ADM

The Finnish DPA (Data Protection Ombudsman) assumed a different view in April 2019, when it ordered a financial credit company (Svea Ekonomi) to correct its data processing practices related to creditworthiness assessments. In its decision, the DPA stated that **the use of an upper age limit as an automatically excluding factor from having a credit application further analyzed was not acceptable,** as "the mere age of the credit applicant does not describe their solvency, willingness to pay or ability to deal with their commitments." Such an automated decision would, according to the DPA, fall under Article 22(1) GDPR. The Ombudsman added that, for such a decision to be justified under paragraph (2)(a) — the contractual necessity exception — it would need to consider the applicant's financial position as well. Lastly, the DPA ordered the controller to provide credit applicants with information on the logic involved in the ADM, its role in making the decision as well as the automated decision's consequences for the data subjects.[148]

Case 38: Credit scoring amounts — at least — to profiling that requires an explanation to data subjects

A September 2020 decision from the Icelandic DPA (*Persónuvernd*) stresses that **data processing in connection with the preparation of individual credit scores must be considered to involve profiling under Article 4(4) GDPR,** as it relies on data subjects' financial information to evaluate or predict their economic situation by attributing certain creditworthiness ratings to them. The decision was triggered by a data subject complaint against financial information agency Creditinfo Credit Ltd. (Creditinfo), where the complainant claimed that Creditinfo failed to explain how his credit score had been calculated pursuant to a data subject access request.

On the complainant's access request, the DPA noted that the data subject had received relevant information by email from Creditinfo on how it carried out creditworthiness assessments, including an **explanation of the factors that had downgraded the complainant's credit rating** — e.g., his recent entries in the default register and his ownership relationship with a company which was on the default register, and directing the complainant to Creditinfo's website to obtain further information. Thus, it concluded that Creditinfo **complied with Article 15 GDPR when it provided the data subject with information on how it prepared his credit score.**[149]

More recently, a set of questions sent — and later withdrawn — by the Administrative Court of Wiesbaden (Germany) to the CJEU reveals that the lower German courts may be willing to diverge from the *Bundesgerichtsoft*'s earlier take on the lawfulness of automated credit scoring practices (see Case 36). The questions could have also provided an opportunity to the CJEU to clarify the meaning behind many of the concepts laid down in Article 22(1) GDPR, but the case has been removed from the Court's register, as the referring court withdrew its request for a preliminary ruling.[150] Even if this case has been withdrawn by the referring Court, there are still three ongoing preliminary ruling procedure cases referring to SCHUFA, including one specifically on the interpretation of Article 22 GDPR.[151]

Case 39: Request for a CJEU preliminary ruling — Can an automated credit score created by a credit reference agency which is later shared with third parties be qualifying ADM?

In this case, the Wiesbaden Court is called upon to assess the business model of German credit reference agency SCHUFA — which is providing its clients (e.g. banks) with information on the creditworthiness of consumers through so-called score values — against GDPR provisions. The Court seems to take the **preliminary view that the upstream credit scoring automated process itself** — and not merely the downstream decisions taken on basis of such score (e.g., to automatically reject a loan application) — **goes beyond mere profiling, as it decisively influences subsequent decisions that significantly affect data subjects.** Through the way it drafted the questions, it seemed that the referring Court intended to obtain confirmation from the CJEU on whether credit scoring can amount to an automated decision which is prohibited under Article 22 GDPR.

Policymakers are taking stock of the increasing use of AI systems to inform or take decisions on credit concessions. In June 2021, the EC proposed an overhaul of its 2008 Consumer Credit Directive, to equip the EU's legal framework with tools to tackle new phenomena in the financial sector, such as fully digital consumer creditworthiness assessments and personalized offers powered by ADM and "non-traditional data." The Proposal's explanatory memorandum clarifies that the new Directive "aims to address the concerns identified in the processing of personal data that are specific to practices observed in the consumer credit market," notably the ones relating to data minimisation and lack of transparency.[152]

The EDPS has recently delivered an opinion on the EC's Proposal, in which it makes several recommendations to ensure a good alignment of its text with the GDPR's general principles, profiling and ADM provisions. It suggests the EU co-legislators exhaustively list the types of personal data that may be used in consumer lending, which means going beyond merely prohibiting the use of certain types (e.g. social media or health data). It also notes that **Article 18(6) of the Proposal essentially mimics Article 22(3) GDPR, by granting consumers the rights to an explanation, obtain human intervention, express their point of view and contest automated creditworthiness assessments.** Finally, the Supervisor looks at how Article 13 would force controllers to inform data subjects when they are presented with a personalized offer that is based on profiling or ADM. In this respect, the EDPS worries that the provision "might be seen as implicitly legitimating personalized processing in ways that exacerbate existing information and power asymmetries between consumers and providers," and recommends that the final text requires the provision of "clear, meaningful and uniform information [to consumers] about the logic and the parameters used to determine the price."[153]

CONCLUSION

In a decision issued in February 2022 and published the same week we were finalizing this Report, the Hungarian DPA sanctioned a bank for unlawfully processing personal data resulting from voice recordings through an AI system that promised emotion detection and measurement for customers calling the bank, and prioritization of those cataloged as the most upset and impatient customers for callbacks.[154]

The DPA found multiple breaches of the GDPR: the principles of lawfulness, transparency and purpose limitation; notice obligations; the right to object; controller accountability obligations; and data protection by design and by default. The case resulted in a fine of over 650.000 EUR and an order to bring the processing of personal data into compliance within 60 days. The DPA did not pursue an assessment under Article 22 GDPR, since it concluded early on in the decision that "no direct decision-making is made" using the AI system. The outcome of the processing at issue merely served as a basis for further actions by the bank or its employees. However, this did not prevent the DPA from finding that the processing significantly breached the GDPR.

This case, involving a truly novel proposition of automated processing of personal data resulting in emotion recognition and classification, confirms the main conclusion of our study based on more than 70 decisions, opinions and guiding documents issued by Courts and DPAs: the provisions of the GDPR cover ADM processes and systems in a comprehensive manner, beyond the specific safeguards offered by Article 22 for processing of personal data resulting in decisions solely based on automated processing and that have legal or similarly significant effects on individuals. This is valid for AI systems involving the processing of personal data even when they are not qualifying ADM, live Facial Recognition systems, algorithms that distribute gigs in the sharing economy, automated tax fraud flags or automated assessments for issuing gun licenses — only to give some examples.

Even if the threshold for automated processing to be classified as qualifying ADM is high, Courts and DPAs have found multiple instances where Article 22 GDPR is applicable. In doing so, they have been developing sophisticated criteria to assess the degree of human involvement in ADM and to establish whether the impact of solely ADM on individuals is significant enough to trigger the protection of Article 22. Without going into detail (see Sections 2.1. and 2.2.), we note elements such as the broad organizational context in which an automated decision is being made, existence of training for the staff involved in the ADM process, influencing of choices and behavior of concerned individuals, the categories of personal data on the basis of which the ADM is being made and whether they draw on monitoring of behavior, or affecting opportunities of making income.

One of the most significant elements of the lawfulness of ADM, be it qualifying ADM or not, remains the existence of an appropriate lawful ground for processing. For instance, the use of live FR in schools was declared unlawful in several cases primarily because it did not have a valid lawful ground for processing in place — consent was considered to be the only ground that could justify the use of this technology to process personal data of students, and consent was not considered to be freely given in any of the cases analyzed that related to students and schools. On the contrary, relying on live FR to ensure safety on a football stadium was considered lawful by a DPA even if it was not based on consent, but on substantial public interest, and provided that a set of safeguards was also ensured. In other cases, the mere fact that consent was not sufficiently informed made the qualifying ADM unlawful (see Case 5).

Transparency obligations are very often invoked and applied in relation to ADM cases. Generally, enforcers make a distinction between general transparency obligations for all processing of personal data, including that underlying profiling and ADM which is not covered by Article 22, and specific transparency obligations under Articles 13(2)(f), 14(2)(g) and 15(1)(h) GDPR, only for qualifying ADM subject to Article 22, requiring a more complex set of information to be provided to data subjects ("meaningful information about the logic involved," "the significance and the envisaged consequences on the data subject"). In this sense, a point of divergence is emerging in practice, with some enforcers (mainly DPAs) starting to push for a recognition of the right to obtain information about the logic involved in ADM not only in cases of qualifying ADM, but in any profiling or other ADM instances.

It is clear that since 2018 Courts and DPAs have started to ramp up enforcement of data protection law in ever more complex cases involving ADM and similar technologies. On top of issuing fines, the DPAs are making full use of their powers to issue corrective measures, such as ordering erasure of personal data or stopping certain processing activities.

A particular need emerging from analyzing these cases is for a concerted effort to better understand how data protection law is applicable to ADM and technologies like AI, ML, FR that rely on or result in ("process") personal data. This would ensure that new legislative intervention — such as the proposed AI Act, the Platform Workers' Directive, the Consumer Credit Directive — does not create an inflation of legal uncertainty, but only occurs where there are clear lacunae.

ANNEX 1 — LIST OF CASES

Audiencia Provincial de Barcelona, Sección 9ª, Auto 72/2021, Rec. 840/2021, ECLI: ES:APB:2021:1448A, February 15, 2021, available at https://diariolaley.laleynext.es/content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1CjUwMDCzNDUwtzRVK0stKs7Mz7Mty0xPzStJBfEz0ypd8pNDKgtSbdMSc4pT1RKTivNzSktSQ4sybUOKSIMBe81L1EUAAAA=WKE.

AEPD, Gabinete Jurídico, N/REF: 0047/2021, 2021, available at https://www.aepd.es/es/documento/2021-0047.pdf.

AEPD, Procedimiento Nº: PS/00120/2021, July 27, 2021, available at https://www.aepd.es/es/documento/ps-00120-2021.pdf.

AEPD, Procedimiento Nº: PS/00477/2019, available at https://www.aepd.es/es/documento/ps-00477-2019.pdf.

AEPD, Procedimiento Nº: PS/00500/2020, available at https://www.aepd.es/es/documento/ps-00500-2020.pdf.

AEPD, Procedimiento Nº: E/03624/2021, available at https://www.aepd.es/es/documento/e-03624-2021.pdf.

AEPD, Procedimiento Nº: PS/00037/2020, 2021, available at https://www.aepd.es/es/documento/ps-00037-2020.pdf.

AP, *Boete Belastingdienst voor discriminerende en onrechtmatige werkwijze*, December 7, 2021, available at https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-belastingdienst-voor-discriminerende-en-onrechtmatige-werkwijze.

Bundesverwaltungsgericht, Case W256 2235360-1/5E, ECLI:AT:BVWG:2020:W256.2235360.1.00, December 18, 2020, available at https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=504bdea3-1859-475c-9106-ad839576d5e5&Position=1&SkipToDocumentPage=True&Abfrage=Bvwg&Entscheidungsart=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=&BisDatum=&Norm=DSGVO&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=BVWGT_20201218_W256_2235360_1_00.

Bundesgerichtsoft, VI ZR 156/13, January 28, 2014, available at https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=66910&pos=0&anz=1.

Commission nationale de l'informatique et des libertés, *Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI*, available at https://www.cnil.fr/sites/default/files/atoms/files/decision_ndeg_med_2021-134.pdf.

Commission nationale de l'informatique et des libertés, *Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position*, October 29, 2019, available athttps://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position.

Commission nationale de l'informatique et des libertés, Décision 2017-053 du 30 août 2017, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000035647959/.

Corte Suprema de Cassazione, Ordinanza sul ricorso 3599-20189, November 8, 2021, available at https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/QUOTIDIANI_VERTICALI/Online/_Oggetti_Embedded/Documenti/2021/11/09/32411.pdf.

Corte Suprema de Cassazione, Civile Ord. Sez. 1 Num. 14381, May 25, 2021, available at http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snciv&id=./20210525/snciv@s10@a2021@n14381@tO.clean.pdf.

Cour de Cassation — Chambre criminelle, September 28, 1998, available at https://www.doctrine.fr/search?q=Cass.%20crim.,%2024%20sept.%201998,%20n%C2%B0%2097-81.748.

Court of Appeal (Civil Division), EWCA Civ 1058, Case No: C1/2019/2670, August 11, 2020, available at https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

CNPD, *Diretriz/2019/1 relativa ao tratamento de dados pessoais no contexto de campanhas eleitorais e marketing político*, March 25, 2019, available at https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121820.

CNPD, Deliberação n.º 2021/622, May 11, 2021, available at https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121887.

CPDP, Становище на КЗЛД относно монтиране на система за достъпа в училище с лицево разпознаване и измерване на телесна температура, 2020, available at https://www.cpdp.bg/?p=element_view&aid=2261.

Datatilsynet, *Tilsyn med Udbetaling Danmarks behandling af personoplysninger*, February 26, 2020, available at https://www.datatilsynet.dk/afgoerelser/afgoerelser/2020/feb/tilsyn-med-udbetaling-danmarks-behandling-af-personoplysninger.

Datatilsynet, *Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion*, May 24, 2019, available at https://www.datatilsynet.dk/afgoerelser/tilladelser/2019/maj/tilladelse-til-behandling-af-biometriske-data-ved-brug-af-automatisk-ansigtsgenkendelse-ved-indgange-paa-broendby-stadion.

Datatilsynet, *Advance notification of order to rectify unfairly processed and incorrect personal data — International Baccalaureate Organization*, August 7, 2020, available at https://www.datatilsynet.no/contentassets/04df776f85f64562945f1d261b4add1b/advance-notification-of-order-to-rectify-unfairly-processed-and-incorrect-personal-data.pdf.

Datatilsynet, *Supplerende høringssvar over forslag til lov om en aktiv beskæftigelsesindsats og forslag om ændring af lov om organisering og understøttelse af beskæftigelsesindsatsen mv., lov om aktiv socialpolitik, lov om sygedagpenge, integrationsloven og forskellige andre love (konsekvenslovforslag)*, July 5, 2019., available at https://www.datatilsynet.dk/media/7758/fornyet-udtalelse-til-star.pdf, p. 3, 6 and 7.

Datenschutzbehörde, Case DSB-D124.909, ECLI:AT:DSB:2020:2020.0.436.002, September 8, 2020, available at https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=-f2a9b55f-02bc-446d-a8fa-4fd931cb1b57&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20200908_2020_0_436_002_00.

Garante, Ordinanza ingiunzione nei confronti di C.S. GROUP S.p.a. — 18 gennaio 2018 [8341304], available at https://gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/8341304.

Garante, Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. — 22 luglio 2021 [9685994], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994.

Garante, Ordinanza ingiunzione nei confronti di Clearview AI — 10 febbraio 2022 [9751362], available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751362.

Garante, Ordinanza ingiunzione nei confronti di Foodinho s.r.l. — 10 giugno 2021, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9675440.

Garante, Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano — 16 settembre 2021 [9703988], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9703988#,

Garante, *Parere sul sistema Sari Real Time* [9575877], March 25, 2021, available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575877.

HmbBfDI, Az.: 545/2020; 32.02-102, January 27, 2021, available at https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF.

Hungarian National Authority for Data Protection and Freedom of Information, Case No. NAIH-85-3/2022 *Budapest Bank*, issued February 8, 2022.

IMY, DI-2019-2221, August 20, 2019, available at https://www.imy.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf.

IMY, *IMY får rätt om ansiktsigenkänning*, June 24, 2021, available at https://www.imy.se/nyheter/imy-far-ratt-om-ansiktsigenkanning/.

IMY, *Beslut efter tillsyn enligt brottsdatalagen – Polismyndighetens användning av Clearview AI*, DI-2020-2719, A126.614/2020, February 10, 2021, available at https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-polismyndigheten-cvai.pdf.

IMY, DI-2019-4062, March 28, 2022, available at https://www.imy.se/globalassets/dokument/beslut/2022/beslut-tillsyn-klarna.pdf.

Information Commissioner's Office, *ICO issues provisional view to fine Clearview AI Inc over £17 million*, November 29, 2021, available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/11/ico-issues-provisional-view-to-fine-clearview-ai-inc-over-17-million/.

Landesverwaltungsgericht Wien, VGW-101/042/791/2020-44, February 11, 2022, available at https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=91aad282-0e8f-4ef0-85f7-bc-2b3e9ef8a6&Position=1&Abfrage=Lvwg&Entscheidungsart=Undefined&Bundesland=Unde-fined&AenderungenSeit=Undefined&SucheNachRechtssatz=True&SucheNachText=True&G-Z=&VonDatum=01.01.2014&BisDatum=&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRis-Seit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=LVWGT_WI_20220211_VGW_101_042_791_2020_44_00.

Office of the Data Protection Ombudsman, *Poliisille huomautus henkilötietojen lainvastaisesta käsittelystä kasvojentunnistusohjelmalla*, September 28, 2021, available at https://tietosuoja.fi/-/poliisille-huomautus-henkilotietojen-lainvastaisesta-kasittelysta-kasvojentunnistusohjelmalla.

Office of the Data Protection Ombudsman, *The Data Protection Ombudsman ordered Svea Ekonomi to correct its practices in the processing of personal data*, April 1, 2019, available at https://tietosuoja.fi/en/-/tietosuojavaltuutettu-maarasi-svea-ekonomin-korjaamaan-kaytantojaan-henkilotietojen-kasittelyssa.

Persónuvernd, *Vinnsla Creditinfo Lánstrausts hf. á persónuupplýsingum í tengslum við gerð lánshæfismats og aðgangs- og upplýsingaréttur vegna gerðar skýrslna um lánshæfismat, Mál nr.* 2020010592, September 22, 2020, available at https://www.personuvernd.is/urlausnir/vinnsla-creditinfo-lanstrausts-hf.-a-personuupplysingum-i-tengslum-vid-gerd-lanshaefismats-og-adgangs-og-upplysingarettur.

Rechtbank Amsterdam, Case C/13/692003 / HA RK 20-302, ECLI:NL:RBAMS:2021:1018, March 11, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1018.

Rechtbank Amsterdam, Case C/13/687315 / HA RK 20-207, ECLI:NL:RBAMS:2021:1020, March 11, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1020.

Rechtbank Amsterdam, Case C/13/689705 / HA RK 20-258, ECLI:NL:RBAMS:2021:1019, March 11, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1019, para 4.44-46.

Rechtbank Den Haag, Case C-09-550982-HA ZA 18-388, ECLI:NL:RBDHA:2020:865, February 5, 2020, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865,

Rechtbank Amsterdam, Case 8937120 CV EXPL 20-22882, ECLI:NL:RBAMS:2021:5029, September 13, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:5029

Rechtbank Den Haag, Case C-09-585239-KG ZA 19-1221, ECLI:NL:RBDHA:2020:1013, February 11, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1013&showbutton=true&keyword=avg.

Sächsischen Datenschutzbeauftragten, *Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten 2019*, available at https://www.saechsdsb.de/images/stories/sdb_inhalt/oeb/taetigkeitsberichte/Ttigkeitsbericht_2019_final.pdf,

Tribunal Administratif de Marseille — 9ème chambre, N° 1901249, available at https://forum.technopolice.fr/assets/uploads/files/1582802422930-1090394890_1901249.pdf.

Tribunale Ordinario di Bologna — Sezione Lavoro, N. R.G. 2949/2019, December 31, 2021, available at http://studiolegalemeiffret.it/wp-content/uploads/2021/03/Trib.-Bologna-ord.-31-dicembre-2020.pdf.

Ústavného súdu Slovenskej republiky, Case 492/2021 Z. z., November 10, 2021, available at https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2021/492/20211217.

ENDNOTES

1 By virtue of the very broad material scope of application of the GDPR. See the definitions of "personal data" and that of "processing" in Article 4 of the GDPR.

2 For a tentative definition of AI and ML and associated concepts, see Brenda LEONG and Sara JORDAN, *The Spectrum of Artificial Intelligence*, The Future of Privacy Forum, August 2021, available at FPF-AIEcosystem-Report-FINAL-Digital.pdf.

3 Article 6 GDPR.

4 Article 5(1) GDPR.

5 Article 32 GDPR.

6 Article 25 GDPR.

7 Under Chapter III of the GDPR. The "data subject" is the person whose personal data is being processed.

8 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Article 2 from the initial version of the law stated that "*Aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé. Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé.*"

9 Article 3 added that "*Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés.*"

10 "1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

"(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests."

11 Cour de Cassation — Chambre criminelle, September 28, 1998, available at https://www.doctrine.fr/search?q=-Cass.%20crim.,%2024%20sept.%201998,%20n%C2%B0%2097-81.748.

12 Garante, Ordinanza ingiunzione nei confronti di C.S. GROUP S.p.a. — 18 gennaio 2018 [8341304], available at https://gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/8341304.

13 Corte Suprema de Cassazione, Ordinanza sul ricorso 3599-20189, November 8, 2021, available at https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/QUOTIDIANI_VERTICALI/Online/_Oggetti_Embedded/Documenti/2021/11/09/32411.pdf.

14 See L A BYGRAVE, *The EU General Data Protection Regulation (GDPR) – A Commentary*, 1st edn, Oxford University Press, 2020, p. 530-532.

15 The latter was apparently the position taken by the Greek DPA (HDPA) in its November 19, 2021 decision following a complaint filed by a data subject. In this case, the complainant argued that his bank's nuisance calls related to debts from his consumer loan qualified as Article 22-covered ADM. Although the DPA found that the individual failed to substantiate his claims, it held that, should the processing fall under Article 22, the complainant should first exercise his right to object with the controller under said provision. See Αρχή Προστασίας Δεδομένων, Decision 51/2021, available at https://www.dpa.gr/sites/default/files/2021-12/51_2021anonym.pdf.

16 EDPB/WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP251rev.01), as last Revised and Adopted on 6th February 2018, p. 19 (endorsed by the EDPB).

17 L A BYGRAVE, note 14. See also Michael VEALE and Lilian EDWARDS, *Clarity, Surprises and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling*, 34(2) CLSR, 2018, p. 398.

18 EDPB/WP29, note 16, p. 20.

19 EDPB/WP29, note 16, p. 20-21.

20 The Netherlands Scientific Council for Government Policy has warned about risks to individuals resulting from semi-automated decision-making (*semi-automatische besluitvorming*). See De WetenschappelijkeRaad voor het Regeringsbeleid (WRR), *Big Data in Een Vrije En Veilige Samenleving*, Amsterdam University Press, 2016. There are borderline cases, such as those of "triage" automated systems that ultimately limit the scope of choices that the final human decision-maker can make, to which Article 22(1) may not apply. For further analysis of such borderline situations, see Reuben BINNS and Michael VEALE, *Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR*, International Data Privacy Law, 2021.

21 EDPB/WP29, note 16, p. 21.

22 EDPB/WP29, note 16, p. 22.

23 EDPB/WP29, note 16, p. 23.

24 EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, 2019, p. 9-10.

25 ICO, *Guide to the General Data Protection Regulation (GDPR) — Automated Decision-Making and Profiling*, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/.

26 Garante, Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. — 22 luglio 2021 [9685994], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994.

27 Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, *Tätigkeitsbericht Datenschutz 2020*, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/02/LfDI-BW_36_Ta%CC%88tigkeitsbericht_2020_WEB.pdf, p. 106.

28 Eesti Töötukassa, *Millal teeb töötukassa Teie suhtes automaatse otsuse*, 2019, available at https://www.tootukassa.ee/content/tootukassast/millal-teeb-tootukassa-teie-suhtes-automaatse-otsuse.

29 APD, Avis n° 44/2019 du 6 février 2019, available at https://www.autoriteprotectiondonnees.be/publications/avis-n-44-2019.pdf.

30 Ústavného súdu Slovenskej republiky, Case 492/2021 Z. z., November 10, 2021, available at https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2021/492/20211217.

31 Idem, para. 130.

32 Idem, paras. 132 to 135, 137 and 138.

33 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, 2020, p. 20-21.

34 Corte Suprema de Cassazione, Civile Ord. Sez. 1 Num. 14381, May 25, 2021, available at http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snciv&id=./20210525/snciv@s10@a2021@n14381@tO.clean.pdf.

35 EDPB/WP29, note 16, p. 28.

36 Garante, note 26.

37 The details used by Foodinho in that context included riders' communications with Foodinho's customers, their real-time geolocation during each delivery, estimated and actual delivery times, details on the management of previous and ongoing orders, feedback from customers and partners, remaining battery level of the device, the percentage of orders each rider accepted and how long it took them to accept each order. See Garante, Ordinanza ingiunzione nei confronti di Foodinho s.r.l. — 10 giugno 2021, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9675440.

38 EDPB/WP29, note 16, p. 12.

39 EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2020*, p. 18.

40 Datatilsynet, *Advance notification of order to rectify unfairly processed and incorrect personal data — International Baccalaureate Organization*, August 7, 2020, available at https://www.datatilsynet.no/contentassets/04df776f85f64562945f1d261b4add1b/advance-notification-of-order-to-rectify-unfairly-processed-and-incorrect-personal-data.pdf.

41 The Telegraph, *Ofqual steps in as thousands of students miss out on expected IB Diploma grades*, July 12, 2020, available at https://www.telegraph.co.uk/news/2020/07/12/ofqual-steps-thousands-students-miss-expected-ib-diploma-grades/.

42 Wired, *Everything that went wrong with the botched A-Levels algorithm*, August 19, 2020, available at https://www.wired.co.uk/article/alevel-exam-algorithm.

43 Information Commissioner's Office, *Statement in response to exam results*, August 14, 2020, available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/08/statement-in-response-to-exam-results/.

44 EDPB/WP29, note 16, p. 12 and 15.

45 Rechtbank Den Haag, Case C-09-585239-KG ZA 19-1221, ECLI:NL:RBDHA:2020:1013, February 11, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1013&showbutton=true&keyword=avg.

46 Ústavného súdu Slovenskej republiky, note 30, para. 147.

47 Idem, para. 120 to 123.

48 Idem, para. 141.

49 Bundesverwaltungsgericht, Case W256 2235360-1/5E, ECLI:AT:BVWG:2020:W256.2235360.1.00, December 18, 2020, available at https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=504bdea3-1859-475c-9106-ad839576d5e5&Position=1&SkipToDocumentPage=True&Abfrage=Bvwg&Entscheidungsart=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=&BisDatum=&Norm=DSGVO&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=BVWGT_20201218_W256_2235360_1_00.

50 HmbBfDI, Az.: 545/2020; 32.02-102, January 27, 2021, available at https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF.

51 Information Commissioner's Office, *ICO issues provisional view to fine Clearview AI Inc over £17 million*, November 29, 2021, available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/11/ico-issues-provisional-view-to-fine-clearview-ai-inc-over-17-million/.

52 Commission nationale de l'informatique et des libertés, *Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI*, available at https://www.cnil.fr/sites/default/files/atoms/files/decision_ndeg_med_2021-134.pdf.

53 Garante, Ordinanza ingiunzione nei confronti di Clearview AI — 10 febbraio 2022 [9751362], available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751362.

54 EDPB/WP29 Guidelines on Transparency under Regulation 2016/679, 11 April 2018, para. 41, p. 22.

55 EDPB/WP29, note 16, p. 16.

56 Article 13(1)(c) and Article 14(1)(c) GDPR.

57 EDPB/WP29, note 16, p. 16.

58 EDPB/WP29, note 16, p. 25.

59 EDPB/WP29, note 16, p. 31.

60 Landesverwaltungsgericht Wien, VGW-101/042/791/2020-44, February 11, 2022, available at https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=91aad282-0e8f-4ef0-85f7-bc2b3e9ef8a6&Position=1&Abfrage=Lvwg&Entscheidungsart=Undefined&Bundesland=Undefined&AenderungenSeit=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.2014&BisDatum=&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=LVWGT_WI_20220211_VGW_101_042_791_2020_44_00.

61 IMY, DI-2019-4062, March 28, 2022, available at https://www.imy.se/globalassets/dokument/beslut/2022/beslut-tillsyn-klarna.pdf.

62 AEPD, Procedimiento Nº: PS/00037/2020, 2021, available at https://www.aepd.es/es/documento/ps-00037-2020.pdf.

63 Idem, p. 128, 129.

64 Idem, p. 129.

65 Idem, p. 115, 116.

66 Rechtbank Amsterdam, Case C/13/692003 / HA RK 20-302, ECLI:NL:RBAMS:2021:1018, March 11, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1018.

67 Idem, para 4.24 and 4.26.

68 Idem, para 4.29.

69 Idem, para 4.30.

70 Idem, para 4.28.

71 Rechtbank Amsterdam, Case C/13/687315 / HA RK 20-207, ECLI:NL:RBAMS:2021:1020, March 11, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1020.

72 Idem, para 4.67.

73 Idem, para. 4.68.

74 Idem, para 3.1.1.

75 Idem, para 4.35.

76 Idem, para 4.52.

77 Idem, para 4.42 to 4.44.

78 Idem, para 4.59.

79 Idem, para 4.59.

80 Rechtbank Amsterdam, Case C/13/689705 / HA RK 20-258, ECLI:NL:RBAMS:2021:1019, March 11, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1019, para 4.44-46.

81 Idem, para 4.45.

82 Idem, para 4.45.

83 Idem, para 4.46.

84 Datatilsynet, *Tilsyn med Udbetaling Danmarks behandling af personoplysninger*, February 26, 2020, available at https://www.datatilsynet.dk/afgoerelser/afgoerelser/2020/feb/tilsyn-med-udbetaling-danmarks-behandling-af-personoplysninger.

85 Datenschutzbehörde, Case DSB-D124.909, ECLI:AT:DSB:2020:2020.0.436.002, September 8, 2020, available at https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=f2a9b55f-02bc-446d-a8fa-4fd-931cb1b57&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNach-Rechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20200908_2020_0_436_002_00.

86 Idem, para D.1.h.

87 Idem, para D.1.i. and D.2.a.

88 Article 35, Data protection impact assessment: "1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. (...) 3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (...) 4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1."

89 WP29, note 16, p. 29.

90 Garante, note 26.

91 WP29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, 2017, p. 9-11.

92 Ústavného súdu Slovenskej republiky, note 30, para. 98.

93 Idem, para. 134.

94 Idem, para. 130.

95 Idem, para. 140.

96 EDPB/WP29, note 91, p. 9-11.

97 Idem, p. 11.

98 Úřad pro ochranu osobních údajů, *List of processing operations subject to data protection impact assessment*, available at https://iapp.org/media/pdf/resource_center/czech_blacklist.pdf.

99 Office of the Data Protection Ombudsman, *List compiled by the Office of the Data Protection Ombudsman of processing operations which require data protection impact assessment (DPIA)*, available at https://tietosuoja.fi/en/list-of-processing-operations-which-require-dpia.

100 Αρχή Προστασίας Δεδομένων, *List of the kind of processing operations which are subject to the requirement for a data protection impact assessment according to article 35 par. 4 of GDPR*, available at https://iapp.org/media/pdf/resource_center/hellenic_blacklist.pdf, p. 2.

101 NAIH, *List of Processing Operations Subject to DPIA GDPR 35 (4)*, available at https://www.naih.hu/data-protection/gdpr-35-4-mandatory-dpia-list, para. 13.

102 Garante, *Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto*, available at https://www.garanteprivacy.it/documents/10160/0/ALLEGATO+1+Elenco+delle+tipologie+di+trattamenti+soggetti+al+meccanismo+di+coerenza+da+sottoporre+a+valutazione+di+impatto, para. 2.

103 EDPB/WP29, note 16, p. 21.

104 Rechtbank Amsterdam, note 66, para. 4.19 and 4.26.

105 Rechtbank Den Haag, note 45, in particular the conclusion at para. 4.26.

106 Bundesverwaltungsgericht, note 49. It is noteworthy that, in its prior decision on the case, the Austrian DPA (BSG) had held that the counsellors' intervention tended to rely solely on the AMAS's results. It further noted that actual consultation time between counsellors and job seekers — during which they were supposed to discuss the latter's wishes/expectations, their previous CV and the causes of their unemployment — was normally very short (around 10 minutes). This meant that, according to the BSG, counsellors were merely rubber-stamping AMAS's conclusions and that their intervention was not meaningful enough for the decision-making to escape Article 22 GDPR.

107 AEPD, Procedimiento Nº: PS/00477/2019, available at https://www.aepd.es/es/documento/ps-00477-2019.pdf.

108 AEPD, Procedimiento Nº: PS/00500/2020, available at https://www.aepd.es/es/documento/ps-00500-2020.pdf.

109 AEPD, Procedimiento Nº: E/03624/2021, available at https://www.aepd.es/es/documento/e-03624-2021.pdf.

110 Datatilsynet, *Supplerende høringssvar over forslag til lov om en aktiv beskæftigelsesindsats og forslag om* ændring *af lov om organisering og understøttelse af beskæftigelsesindsatsen mv., lov om aktiv socialpolitik, lov om sygedagpenge, integrationsloven og forskellige andre love (konsekvenslovforslag)*, July 5, 2019., available at https://www.datatilsynet.dk/media/7758/fornyet-udtalelse-til-star.pdf, p. 3, 6 and 7.

111 Commission nationale de l'informatique et des libertés, Décision 2017-053 du 30 août 2017, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000035647959/.

112 Garante, note 37.

113 CNPD, Deliberação n.º 2021/622, May 11, 2021, available at https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121887. The Italian DPA has more recently sanctioned the Bocconi University of Milan for an unlawful use of the same software, notably for a lack of an appropriate legal basis for the processing of students' biometric attributes. See Garante, Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano — 16 settembre 2021 [9703988], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9703988#, Section 3.4.

114 See the teacher mobility algorithm Buona Scuola cases, decided by two Italian instances (the Consiglio di Stato and the TAR Lazio) in 2019, as reported by Algorithm Watch in its "Automating Society Report 2020", available at https://automatingsociety.algorithmwatch.org/report2020/italy/.

115 Rechtbank Den Haag, Case C-09-550982-HA ZA 18-388, ECLI:NL:RBDHA:2020:865, February 5, 2020, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865, para 6.59-60 and 6.91.

116 AP, *Boete Belastingdienst voor discriminerende en onrechtmatige werkwijze*, December 7, 2021, available at https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-belastingdienst-voor-discriminerende-en-onrechtmatige-werkwijze.

117 Rechtbank Amsterdam, note 66, para. 4.26; and Rechtbank Amsterdam, note 71, para. 4.66-67.

118 Rechtbank Amsterdam, note 80, para 4.51.

119 See Case 28, in Chapter 3.1.

120 Garante, note 26.

121 Garante, note 37.

122 CNPD, *Diretriz/2019/1 relativa ao tratamento de dados pessoais no contexto de campanhas eleitorais e marketing político*, March 25, 2019, available at https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121820.

123 Tribunale Ordinario di Bologna — Sezione Lavoro, N. R.G. 2949/2019, December 31, 2021, available at http://studiolegalemeiffret.it/wp-content/uploads/2021/03/Trib.-Bologna-ord.-31-dicembre-2020.pdf.

124 DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" (in S.O n. 123 alla G.U. 29 luglio 2003, n. 174), integrato con le modifiche introdotte dal DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei

dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205).

125 Article 47(5) of Legislative Decree no. 81/2015, in force since 3.11.2019, provides that "1. The anti-discrimination rules and the protections to the dignity and freedom applicable to employees are also applicable to workers mentioned in Article 47-bis, including rules on access to the platform. 2. The exclusion from the platform and the reductions in job opportunities attributable to non-performance of the contract with the platform are prohibited."

126 Garante, note 26.

127 Rechtbank Amsterdam, Case 8937120 CV EXPL 20-22882, ECLI:NL:RBAMS:2021:5029, September 13, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:5029, para 23, 28, 31, 33.

128 European Commission, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on improving working conditions in platform work, COM(2021) 762 final.

129 Idem, Recitals (4) and (8).

130 Idem, Article 6.

131 Sächsischen Datenschutzbeauftragten, *Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten 2019*, available at https://www.saechsdsb.de/images/stories/sdb_inhalt/oeb/taetigkeitsberichte/Ttigkeitsbericht_2019_final.pdf, p. 99-104.

132 Commission nationale de l'informatique et des libertés, *Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position*, October 29, 2019, available at

https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position.

133 Tribunal Administratif de Marseille — 9ème chambre, N° 1901249, available at https://forum.technopolice.fr/assets/uploads/files/1582802422930-1090394890_1901249.pdf.

134 IMY, DI-2019-2221, August 20, 2019, available at https://www.imy.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf.

135 IMY, *IMY får rätt om ansiktsigenkänning*, June 24, 2021, available at https://www.imy.se/nyheter/imy-far-ratt-om-ansiktsigenkanning/.

136 CPDP, Становище на КЗЛД относно монтиране на система за достъпа *в* училище *с* лицево разпознаване *и* измерване на телесна температура, 2020, available at https://www.cpdp.bg/?p=element_view&aid=2261.

137 Ley 5/2014, de 4 de abril, de Seguridad Privada.

138 Audiencia Provincial de Barcelona, Sección 9ª, Auto 72/2021, Rec. 840/2021, ECLI: ES:APB:2021:1448A, February 15, 2021, available at https://diariolaley.laleynext.es/content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbH1CjUwMDCzNDUwtzRVK0stKs7Mz7Mty0xPzStJBfEz0ypd8pNDKgtSbdMSc4pT1RKTivNzSktSQ4sybUOKSIMBe81L1EUAAAA=WKE.

139 AEPD, Gabinete Jurídico, N/REF: 0047/2021, 2021, available at https://www.aepd.es/es/documento/2021-0047.pdf.

140 AEPD, Procedimiento Nº: PS/00120/2021, July 27, 2021, available at https://www.aepd.es/es/documento/ps-00120-2021.pdf.

141 According to the European Digital Rights (EDRi) NGO, the DPA authorisation procedure is specific to Denmark. Under the Danish Data Protection Act, whenever private sector controllers wish to use the substantial public interest Article 9(2) GDPR derogation to process special categories of data, they are required to seek a permit from the DPA. See EDRi, *Danish DPA approves Automated Facial Recognition*, June 19, 2019, available at https://edri.org/our-work/danish-dpa-approves-automated-facial-recognition/.

142 Datatilsynet, *Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion*, May 24, 2019, available at https://www.datatilsynet.dk/afgoerelser/tilladelser/2019/maj/tilladelse-til-behandling-af-biometriske-data-ved-brug-af-automatisk-ansigtsgenkendelse-ved-indgange-paa-broendby-stadion.

143 IMY, *Beslut efter tillsyn enligt brottsdatalagen – Polismyndighetens användning av Clearview AI*, DI-2020-2719, A126.614/2020, February 10, 2021, available at https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-polismyndigheten-cvai.pdf. Later this year, the Finish DPA announced that it had also found that the Finish National Police Board has also unlawfully processed biometric data of potential victims of child sexual abuse through a trial use of Clearview AI's automated FR technology. Therefore, the DPA ordered the National Police Board to notify a data breach to data subjects whose identity was known, and to request Clearview AI to remove police-transmitted data from its systems. See Office of the Data Protection Ombudsman, *Poliisille huomautus henkilötietojen lainvastaisesta käsittelystä kasvojentunnistusohjelmalla*, September 28, 2021, available at https://tietosuoja.fi/-/poliisille-huomautus-henkilotietojen-lainvastaisesta-kasittelysta-kasvojentunnistusohjelmalla.

144 Garante, *Parere sul sistema Sari Real Time* [9575877], March 25, 2021, available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575877. See also the UK's Court of Appeal ruling, where the court decided that the use of automated FR by the South Wales Police breached Article 8 of the European Convention on Human Rights (right to respect for private and family life) and the GDPR's DPIA requirements. Court of Appeal (Civil Division), EWCA Civ 1058, Case No: C1/2019/2670, August 11, 2020, available at https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

145 European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, COM(2021) 206 final, Article 3(36), (37) and (38). See also the proposed ban on the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement — subject to exceptions — under Article 5(1)(d) of the Proposal.

146 Bundesgerichtsoft, VI ZR 156/13, January 28, 2014, available at https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=66910&pos=0&anz=1.

147 AEPD, note 107.

148 Office of the Data Protection Ombudsman, *The Data Protection Ombudsman ordered Svea Ekonomi to correct its practices in the processing of personal data*, April 1, 2019, available at https://tietosuoja.fi/en/-/tietosuojavaltuutettu-maarasi-svea-ekonomin-korjaamaan-kaytantojaan-henkilotietojen-kasittelyssa.

149 Persónuvernd, *Vinnsla Creditinfo Lánstrausts hf. á persónuupplýsingum í tengslum við gerð lánshæfismats og aðgangs- og upplýsingaréttur vegna gerðar skýrslna um lánshæfismat, Mál nr.* 2020010592, September 22, 2020, available at https://www.personuvernd.is/urlausnir/vinnsla-creditinfo-lanstrausts-hf.-a-personuupplysingum-i-tengslum-vid-gerd-lanshaefismats-og-adgangs-og-upplysingarettur.

150 CJEU, Order of the President of the Court of Justice "Deletion" in Case C-552/21, January 25, 2022, ECLI:EU:C:2022:105.

151 Verwaltungsgericht Wiesbaden, Request for a preliminary ruling in Case C-634/21, October 1, 2021, available at https://curia.europa.eu/juris/showPdf.jsf?text=&docid=250522&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1368545.

152 European Commission, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on consumer credits, COM/2021/347 final.

153 EDPS, *Opinion 11/2021 on the Proposal for a Directive on consumer credits*, August 26, 2021. For an analysis of the available GDPR legal bases for conducting price personalisation, see Sebastião BARROS VALE, *The Omnibus directive and online price personalization: a mere duty to inform?*, Issue 2020/2, European Journal of Privacy Laws and Technologies, 2020, available at http://www.ejplt.tatodpr.eu/Article/Archive/index_html?ida=213&idn=7&idi=-1&idu=-1.

154 Hungarian National Authority for Data Protection and Freedom of Information, Case No. NAIH-85-3/2022 *Budapest Bank*, issued February 8, 2022.

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005 FPF.ORG | info@fpf.org