Using GDPR to improve legal clarity and working conditions on digital labour platforms

Can a code of conduct as provided for by Article 40 of the General Data Protection Regulation (GDPR) help workers and socially responsible platforms?

—

Michael ‘Six’ Silberman and Hannah Johnston

Working Paper 2020.05

etui.

Using GDPR to improve legal clarity and working conditions on digital labour platforms

Can a code of conduct as provided for by Article 40 of the General Data Protection Regulation (GDPR) help workers and socially responsible platforms?

—

Michael 'Six' Silberman and Hannah Johnston

Working Paper 2020.05
european trade union institute

Michael 'Six' Silberman works in the Crowdsourcing Project at IG Metall in Frankfurt, Germany. Contact: michael.silberman@igmetall.de

Hannah Johnston is a geographer at Queen's University in Kingston (Ontario), Canada. Contact: 8hesj@queensu.ca

ETUI publications are published to elicit comment and to encourage debate. The views expressed are those of the author(s) alone and do not necessarily represent the views of the ETUI nor those of the members of its general assembly.

Brussels, 2020
©Publisher: ETUI aisbl, Brussels
All rights reserved
Print: ETUI Printshop, Brussels

D/2020/10.574/16
ISSN: 1994-4446 (print version)
ISSN: 1994-4454 (electronic version)

The ETUI is financially supported by the European Union. The European Union is not responsible for any use made of the information contained in this publication.

Contents

Abstract

This paper examines how the General Data Protection Regulation (GDPR) can be used to address procedural problems faced by platform workers, including opaque rating systems, arbitrary account suspension and nonpayment, and uncommunicative clients and platform operators. GDPR provides workers with a variety of rights with respect to their data, including right of access, right to rectification, and rights regarding automated decision-making. Additionally, Art. 40 of the GDPR establishes the possibility for groups of controllers to develop codes of conduct that clarify the application of GDPR to their particular sectors. This paper details the application of GDPR to labor platforms, provides draft text for an Art. 40 code of conduct for labor platforms, and discusses how such a code could help address procedural problems encountered by platform workers. We hope that this paper can help spark a discussion at European level among trade unions and other stakeholders in platform work about how to use GDPR to address the 'procedural problems' faced by platform workers, regardless of their employment status.

1. Introduction[1]

On 25 May 2018, the General Data Protection Regulation (GDPR) came into force. Long in the making and widely seen as the most comprehensive data protection legislation in the world, GDPR creates a broad array of new rights regarding personal data. Importantly, GDPR creates rights for all natural persons in the EU. Compliance is required of any organisation 'processing' the personal data of persons in the EU, even if the organisation is itself not located in the EU. This paper considers how GDPR can be used to help address problems faced by workers in digital labour platforms.

Many platform workers are self-employed, so it is useful that GDPR applies regardless of employment status. The problems facing many platform workers have been extensively discussed, including low wages, inadequate health and safety protections, lack of paid leave, lack of collective rights, and inadequate integration into national social protection systems (Vandaele *et al.* 2019; Piasna and Drahokoupil 2019; Berg *et al.* 2018; Drahokoupil and Piasna 2019; Vandaele 2018). These problems are often discussed with reference to the self-employed status of platform workers (Risak and Dullinger 2018), and to a lesser extent social protection (Daugareilh *et al.* 2019; Forde *et al.* 2017). Less urgently discussed, however, are what we call 'procedural problems', which typically arise from platform design and operating procedures. These include:

- refusal of payment for completed work without explanation or recourse
- suspension or closure of worker accounts without explanation or recourse
- opaque, error-prone automated systems for rating work and workers and/or allocating work
- uncommunicative clients and/or platform operators.

These procedural problems are experienced by many platform workers, including those who are acknowledged as employees, those who may be falsely self-employed, and those who are probably accurately classified as self-employed (see e.g. Kilhoffer *et al.* 2019). Among the problems faced by platform workers generally, this paper focuses specifically on how GDPR can be used to address these 'procedural problems'. We hope therefore that this paper can support a lively discussion at European level about how to use GDPR to solve at least some of the problems faced by platform workers, regardless of their employment status.

The remainder of the paper has eight parts. Section 2 explores how GDPR can be used to address problems faced by platform workers. Section 3 presents a case study that shows how a platform worker may try (and indeed, did try) to use rights provided by GDPR to resolve procedural problems but how they may also encounter difficulties. The names of the worker and platform are fictionalised but based on real cases. Section 4 discusses some current difficulties with interpretation and enforcement of the rights provided by

[1] Acknowledgements: We thank Bethany Staunton, Jan Drahokoupil and Aída Ponce Del Castillo from the ETUI, as well as Elena Gramano and Antonio Aloisi, for their feedback.

GDPR. Section 5 introduces Articles 40 and 41 of GDPR, which provide for establishment and monitoring of codes of conduct for sector-specific application of GDPR. Section 6 considers GDPR codes of conduct in the context of codes of conduct more generally. Section 7 presents several annotated draft texts for a GDPR code of conduct that would address the most pressing procedural problems faced by platform workers. Section 8 discusses possible concrete next steps toward making an Art. 40 GDPR code of conduct for labour platforms a reality. Section 9 concludes.

2. Using GDPR to address problems faced by platform workers

Platform workers face a variety of procedural problems that negatively affect their working conditions. The first half of this section discusses some of these problems; the second half discusses how the rights established by GDPR could be used to address them.

2.1 Some procedural problems faced by platform workers

Opaque, sometimes error-prone (and often, but not necessarily, automated) systems for rating work and workers and/or allocating work

A platform worker's success frequently relies on their ability to access (or be allocated) tasks, which in turn often depends on various evaluations, ratings, and classifications of their work or of them as a worker. Often, however, the systems and processes platforms use to calculate and assign these evaluations, ratings, and classifications are not transparent (see e.g. Rosenblat and Stark 2016; Woodcock and Graham 2019). For example, workers who have previously qualified for access to jobs may be stripped of their qualifications without explanation. Alternatively, workers may be evaluated according to processes about which they have no knowledge; that is, the existence of an evaluation or even of an entire system of evaluation may be secret. Or, workers may be aware that they are being evaluated, and even know what evaluations or ratings they have been assigned, but be unaware of the exact consequences of those evaluations or ratings. Additionally, these processes — whether automated or executed by humans — are sometimes error-prone, exposing platform workers to the risk that they or their work are *inaccurately* and/or unfairly negatively evaluated, potentially inappropriately limiting their ability to access work in the future (see Wood *et al.* 2018).

Suspension or closure of worker accounts without explanation or recourse

The suspension or closure of worker accounts is one of the most common consequences of poor ratings and evaluations, although it is not the only reason workers' accounts are deactivated. However, in some cases, the platform declines to even provide the worker with a reason for the suspension or closure

(Ravenelle 2019; Rosenblat 2018; Dettmer 2019). Suspension or closure of an account renders a worker unable to access a platform, and thus unable to work. In these cases, they have effectively been 'fired'.

Importantly, such decisions are sometimes made by automated, partially automated, and/or outsourced systems — and such systems may be error-prone.

Refusal of payment for completed work without explanation or recourse

Some platforms have policies that allow customers to refuse to pay for completed work without providing the worker with an explanation (see McInnis *et al.* 2016). In these cases, workers may have spent significant time completing a task for which they are not paid. In some cases, customers managing work from large numbers of workers (especially, for example, on microtask platforms) use automated, partially automated, and/or outsourced systems to make payment decisions. Such systems are quite often error-prone.

Uncommunicative or unresponsive clients and platform operators

In cases of contested decisions (such as non-payment and account suspension or closure), platform workers may try to seek assistance or clarification from the platform about the reason for the decision. In these situations, however, they are often unable to contact a qualified person who is authorised to explain the decision (Irani and Silberman 2013; Brawley and Pury 2016) — and correct it if it was mistaken.

Lack of recourse to external mediation

Generally, platform workers have no recourse to external mediation should they wish to dispute a decision taken by a platform or customer. Furthermore, customers and platforms are generally under no obligation to reply to worker inquiries, and often decline to do so.

2.2 GDPR can help

GDPR can help address flaws in rating systems and correct inaccurate, unfair, or otherwise inappropriate ratings

GDPR provides data subjects, in this case platform workers, with the right to fair and transparent processing and the right to ensure that their personal data are accurate. Ratings fall under the definition of personal data as established in Art. 4.1 GDPR. This means that workers have the right to access a copy of their ratings (Art. 15.1, 15.3 GDPR) and can request that they be corrected if they are inaccurate (Art. 16). Additionally, hidden or secret evaluations of which the worker is not informed are illegal, as controllers of personal data are required to inform data subjects when personal data is collected (Art. 15.1-15.4 GDPR). Finally, if a rating system is automated, the worker has the right to 'obtain human intervention' in the decision-making process, to express their point of view and to contest the decision (Art. 22.3).

GDPR requires that processing of personal data be transparent with respect to the data subject (Art. 5.1 lit. a)

Because ratings and evaluations are personal data (as made clear in the European Court of Justice judgment in *Nowak v. Data Protection Commissioner* and in previous guidance from the Article 29 Working Party, especially Opinion 04/2007 'On the concept of personal data'), the processing of ratings and evaluations must be transparent. Therefore, platforms must clearly indicate how workers will be evaluated, classified, and rated. They must also make the consequences of evaluations, classifications, and ratings clear. For example, if an evaluation, classification, or rating may affect payment or access to work, or result in account suspension or closure, the platform is responsible for making these consequences clear as a result of the requirement for transparency.

GDPR provides several ways for workers to contest account suspension or closure

Some platforms' legal terms set out that suspension and closure are only allowed under certain circumstances. In these cases, if a worker's account is suspended or closed and the worker is not offered an explanation for this decision, the worker can use an Art. 15 data access request to receive a copy of all personal data that were used as a basis for the decision. If inaccurate or incomplete personal data led the platform to assume that these circumstances applied, the worker may invoke Art. 16 to request that the data in question be corrected, which could lead to a reversal of the suspension or closure decision.

If, on the other hand, the platform explicitly reserves the right to suspend or close an account for any or no reason, GDPR may not help — unless the decision was automated and produces legal effects concerning the worker or otherwise significantly affects them, in which case Art. 22 applies. The worker may be able to receive a copy of all their personal data being stored by the platform, but this will not necessarily help reverse the suspension or closure.

If, however, Art. 22 applies, the worker has the right to obtain human intervention regarding the decision, to express their point of view and to contest the decision.

GDPR provides several ways for workers to contest non-payment for submitted work

On some platforms, the legal terms set out that non-payment of work is only allowed if the worker has failed to provide satisfactory work. In these cases, the worker may be able to contest non-payment on the grounds that the record of non-payment is an inaccurate reflection of their work performance. This argument is strengthened further if non-payment of work is demonstrably used by the platform as a worker rating or evaluation (i.e. it is interpreted as an indicator of poor worker performance and affects the worker's access to future work).

If the platform’s legal terms set out that a client, or the platform, may refuse payment for any or no reason — and the record of non-payment is not used as a rating or evaluation — GDPR may not help, unless the decision was automated.

If the decision was made by an automated system and produces legal effects concerning the worker or otherwise significantly affects them, Art. 22 applies and the worker has the right to obtain human intervention regarding the decision, to express their point of view and to contest the decision.

GDPR requires data controllers to respond to data protection-related requests within at most three months

In cases where a worker makes an explicit request regarding their personal data rights, the platform’s data protection officer must reply to the request (Arts. 37-39). Additionally, GDPR provides clear timelines for platform response (Art. 12.3-12.4): requests must be replied to within one month. If the request is especially complex, the controller can receive an extension of up to two additional months.

If the platform does not reply, the worker may contact the supervisory authority (Art. 77); if the worker does not believe the outcome meets the requirements of the law, they have access to judicial remedy against the supervisory authority (Art. 78) and/or controller/processor (Art. 79).

3. A case study

The following case study shows some practical problems of using GDPR to promote workers’ rights. The names of the worker and platform are fictionalised, but the text is based on real cases in which the authors have been involved.

Yolanda Marjata is a freelance illustrator based in an (unspecified) EU Member State. Up until 2018, Marjata usually earned 30-60% of her monthly income from royalties on illustrations she had uploaded to Netillo, an art and illustration marketplace. In late 2018, however, Marjata noticed that her income from Netillo royalties fell dramatically – from 1500-3000 euros per month to 500-800 euros per month. The change was not seasonal; it had never happened before.

She investigated by looking into the settings in her Netillo account. There, she noticed that some of her illustrations had been labelled by the platform as ‘inappropriate for promotion’. She found an explanation on the platform’s FAQ page: in order to make the marketplace more welcoming for customers – and especially for potential customers – Netillo had recently introduced a labelling system.

Machine learning (or 'artificial intelligence') systems had been developed to label all the images uploaded to Netillo according to their content. If the machine learning systems indicated that the content of an image included or referred to violence, sexuality, nudity, or other 'adult' or 'potentially controversial' themes – including war or religion – it would not be displayed on the front page of the site or 'recommended' to customers unless they were logged in and had explicitly indicated that they wanted to receive recommendations for this kind of content.

On one hand, the platform was within its rights to do this. On the other, Marjata realised that some of her illustrations were being labelled 'inappropriate for promotion' – and therefore, presumably, labelled with one of the 'adult' or 'controversial' labels – but she could not see anything 'adult' or 'controversial' about these illustrations. For example, one of the illustrations labelled 'inappropriate for promotion' was of a child playing with a puppy in a park. Another illustration, a painting of a centuries-old public statue, could conceivably be argued to have to do with 'violence,' as the statue was of a soldier. But how could this be 'inappropriate for promotion'?

Marjata contacted the platform operator and, two weeks later, received an email saying simply, 'We have looked at the images in question and can confirm that indeed they do not comply with our requirements for promotion on Netillo.' She replied, asking for more information about these requirements. Two weeks later, she received another reply:

> 'If you want to improve the chances of your work being promoted, please make sure it does not include violence, sexuality, nudity, or any other adult or potentially controversial themes, including war, religion, or politics. Unfortunately we cannot provide any further guidance, as this would enable malicious site users to manipulate our systems, to the detriment of customers and conscientious illustrators.'

In the months that followed, Marjata began paying careful attention to which images were labelled 'inappropriate for promotion' and which were not. She also began comparing notes with other illustrators who had previously earned significant income from the platform. Their incomes were all down, and they had all received similar messages from the platform operator. And while there were some unobjectionable cases – clearly violent or sexual illustrations were often labelled 'inappropriate for promotion' – there were many baffling cases, where the images did not seem at all 'inappropriate' or 'controversial.' In a few cases, illustrators wrote to the platform to complain, and the platform operator reversed the decision and apologised, writing that their machine learning systems were still in the process of learning. In other cases, they would reply affirming the original decision. Sometimes it would be months before the platform replied.

After months of unhelpful communication with the platform – and still earning less than 800 euros per month – Marjata had had enough, and she set up an online petition calling on Netillo to change its practices and clarify the rules. She contacted as many illustrators as she could, encouraging them to sign, and spread the petition online widely through social media. It gained attention, and thousands of other illustrators – many of whom had previously earned over 1000 euros per month on Netillo – signed. A few favourable stories were written in the technology media.

Two weeks later, she got an email from an assistant of one of the high-level managers at Netillo, inviting her to an in-person meeting at the Netillo headquarters. Three weeks later, Marjata met with the executive. The executive listened carefully to Marjata's explanation of how frustrating it was to be constantly trying to guess whether an illustration would be judged 'appropriate for promotion' or not. The executive then explained in general terms how the machine learning systems that did the labelling worked. Unfortunately, the executive explained, it would not be possible to give illustrators any more information, as this would make it possible for malicious illustrators to circumvent the labelling system. The executive was attentive and sympathetic, but ultimately could not really help.

Marjata digested this experience for several weeks and discussed the situation further with her fellow illustrators. Finally, she decided to file a data subject access request. She sent an email to the email address listed on the Netillo website as the contact email for inquiries relating to data protection issues. The email had the following text:

> 'In the last few months, Netillo has introduced machine learning systems to classify illustrations uploaded by users on the site. The main goal of these systems is to determine which illustrations are "appropriate for promotion". This is determined by a variety of "lower level" labels, such as "violence," "sexuality," "nudity," etc. However, these labels are not shared with illustrators when they are notified that an illustration they posted to the platform is not appropriate for promotion. The only information we are given is that the illustration was deemed not appropriate for promotion – not which "lower level" labels were assigned to my illustrations and led to this decision. However, the "lower level" labels assigned to my illustrations – such as "violence," "sexuality," etc. – are my personal data under the EU General Data Protection Regulation. As such, I have the right to request, and receive, a copy of them. I therefore request a copy of all labels that Netillo has associated with illustrations I have uploaded to the platform.'

One month later, the platform's data protection officer replied, indicating that they needed two more months because of the complexity of the case. Two months after that, the data protection officer replied again, writing simply:

> 'We understand your frustration, but in order to protect users of the site, we cannot disclose the workings of the systems we use to determine which images are not appropriate for promotion, including the labels, or how the labels are applied, as this would make it easier for malicious users to circumvent these systems. This would adversely impact both honest illustrators – such as yourself – and site customers and visitors generally.'

Marjata forwarded a description of the case and her correspondence with Netillo's data protection officer to her national data protection authority, asking them to intervene.

The office of the data protection authority replied within three weeks with the following reply:

> 'The reply from Netillo indicates that the rights and freedoms of others would be adversely affected by the disclosure of the information you requested; therefore, they do not need to disclose it (Art. 15.4 GDPR).'

However, at this point, Marjata was in dialogue with experts in European data protection law, and knew that Recital 63 of GDPR states that:

> '[the right of access to personal data] should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property.... However, the result of those considerations should not be a refusal to provide all information to the data subject.'

But unless she could convince the data protection authority that a more nuanced analysis of her case was needed, she had, at this point, one primary option: litigation. And indeed, at this point the first defendant in litigation was not necessarily Netillo but the data protection authority. Whether she was going to win or lose, it was to be a long and unpleasant journey — and it was certainly not the journey Marjata was hoping for when she first contacted Netillo asking why her illustrations were being labelled 'inappropriate.'

The remainder of the paper discusses how this situation can be avoided in the future by the establishment of data protection codes of conduct, as provided for by Art. 40 GDPR.

4. Difficulties with interpretation and enforcement of the rights provided by GDPR

As partially illustrated by the case in the previous section, there is some ambiguity and confusion around platform operators' obligations under GDPR. For example, it may not be clear to platform operators which data falls under the term 'personal data.' Some platform operators may not realise the breadth of this term, and that ratings, evaluations, and classifications — including the labels of Marjata's illustrations — are personal data. Additionally, ratings may be the personal data of multiple data subjects. For example, if a customer rates a worker, the rating is likely to be the personal data of both the worker and the customer. Disclosing the rating to the worker in compliance with Art. 15 may expose the customer to data protection-related risks. In such a case the controller may not know how to proceed.

Even when they do understand their obligations, platform operators may be resistant to fulfilling them. Platforms may have 'good' business reasons for not wanting to comply with GDPR. However, while good business reasons may allow platform operators to make some use of Art. 15.4 as an ‘exemption clause’, they are not likely to entirely absolve them of their obligation to provide copies of personal data under the regulation. Specifically, Recital 63 establishes that while the right to access a copy of personal data ‘should not adversely affect the rights or freedoms of others… the result of those considerations should not be a refusal to provide all information to the data subject.’

Although GDPR provides many rights that can help address procedural problems faced by platform workers, in some cases it may not help. For example, some platforms explicitly reserve the right, in their legal terms, to carry out adverse decisions (such as non-payment and account suspension or closure) at their sole discretion, without providing any reason. If these decisions are not carried out by automated means, GDPR may not help in such cases.

However, even under these circumstances, we note two important caveats. First, the Article 29 Working Party has made clear that controllers ‘cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing’ (Guidelines on Automated individual decision-making and Profiling, WP251, pp. 20-21).

Second, some of these workers may find they have expanded protections under the EU Regulation 2019/1150 promoting fairness and transparency for business users of online intermediation services (the so-called ‘Platform-to-Business Regulation’), which comes into force on 12 July 2020. Arts. 3-4 of the Platform-to-Business Regulation require platforms to ‘set out the grounds for decisions to suspend or terminate or impose any other kind of restriction upon, in whole or in part, the provision of their online intermediation services to business users’ (Art. 3.1 lit. c). Therefore, under the Platform-to-Business Regulation, the decision to suspend or close an account can only be taken under certain circumstances. These circumstances are made available to platform workers. If the platform reaches the conclusion that the circumstances apply, it may suspend or close a worker’s (‘business user’s’) account. However, if the worker believes that they were suspended based on inaccurate information, they can use GDPR to request the data on which the decision was based. If the data are indeed inaccurate, the worker can invoke Art. 16 GDPR to request the data be corrected — and potentially regain access to the platform. Thus the rights established by GDPR can complement the protections established in the Platform-to-Business Regulation (especially Art. 3).

5. Introducing Arts. 40-41 GDPR

Art. 40 GDPR, titled ‘Codes of conduct,’ establishes the possibility for ‘codes of conduct intended to contribute to the proper application’ of GDPR and the procedures by which such codes can become approved. This is complemented by Art. 41 GDPR, titled ‘Monitoring of approved codes of conduct’, which establishes the relevant monitoring requirements. Art. 40 GDPR codes of conduct can be created by groups of controllers in specific sectors or industries to more concretely specify the application of the Regulation to their sectors. Such codes of conduct can include a variety of topics. Art. 40 GDPR lists some examples of possible topics, including (but not limited to):

- the meaning of 'fair and transparent processing';
- the legitimate interests of controllers;
- appropriate processes for the collection of personal data;
- information to be provided to the public and to data subjects;
- appropriate measures for compliance with Article 24, which places the burden of demonstrating that data processing is taking place in compliance with the Regulation on the controller; and
- out-of-court dispute resolution measures for resolving disputes between data subjects and controllers.

Art. 41 GDPR establishes requirements for the monitoring and enforcement of Art. 40 codes of conduct. These monitoring requirements are discussed in more detail in Section 6 of the paper.

An Art. 40 GDPR code of conduct for, specifically, labour platforms could help resolve the difficulties with interpretation and enforcement of GDPR on labour platforms discussed above in Section 4. For example, such a code could clarify interpretation and application of specific terms and elements in GDPR, such as the term 'personal data,' Art. 15.4, and Art. 22, in the context of labour platforms. It could also help strengthen the rights of platform workers under GDPR, for example, by codifying best practices and reducing legal uncertainty.

6. Considering Arts. 40-41 GDPR in the context of other codes of conduct

Codes of conduct are a voluntary measure, typically part of a firm's corporate social responsibility mandate. Since the 1990s they have become an important tool for regulating private sector working conditions in countries where legal standards are poor or in situations where governments, tasked with enforcing labour standards, are unable or unwilling to do so (Posner and Nolan 2003). For example, they have been widely used by multinational firms and in global supply chains in agriculture and apparel.

They have also been used to promote better working conditions, with varied levels of success. Understanding circumstances under which they have been successful — and less successful — offers lessons for an Art. 40 GDPR code of conduct for platform workers.

Codes of conduct are an effective way for firms who want to engage in self-regulation to do so. For example, firms sometimes establish codes of conduct to make them more appealing to consumers, or to highlight their commitment to ethical procurement and processing (Toffel *et al.* 2015). However, there are some challenges and concerns relating to codes of conduct broadly:

- Historically, there have not been general legal standards for codes of conduct. At times, this has resulted in codes of conduct that have not had much substantive content (Posner and Nolan 2003).

- Codes of conduct are sometimes developed without input from workers; under such circumstances, codes of conduct risk being poorly aligned with workers' main concerns (Compa 2001).

- Codes of conduct have often been difficult to enforce legally. Because of this, stakeholders often raise concerns about effectively monitoring and enforcing them. Initially, these concerns were based primarily on the fact that many codes of conduct were monitored by the very businesses that they purported to govern. More recently, however, efforts have been made to create more effective enforcement and monitoring mechanisms. These have been particularly effective when they have involved workers and state regulators (Ponce Del Castillo 2020; Fine 2014; Fine and Bartley 2019; Dias-Abey 2018).

- Finally, codes of conduct risk undermining the political will to create state regulation (which may be more enforceable). While critics have expressed concern about codes of conduct supplanting public regulation, it is now generally believed that voluntary private regulation, including codes of conduct, can usefully complement state regulation (Bartley 2005; Klein 2009; Weil 2014).

Helpfully, the requirements established by Arts. 40-41 GDPR address some of these limitations and concerns. First, unlike purely voluntary codes of conduct that were criticised for having little or no enforcement or oversight, Art. 40 GDPR codes of conduct can be described as 'self-regulation on a legal basis'. Art. 40 codes of conduct must be approved by a supervisory authority or by the European Data Protection Board, and cannot undermine the protections and rights afforded by GDPR. This ensures that Art. 40 GDPR codes of conduct cannot be 'content free', like some entirely voluntary codes of conduct in other sectors have been. Indeed, Art. 40 codes must describe in detail all the obligations of the controllers. Additionally, while platforms can voluntarily adopt an Art. 40 code of conduct, they are legally bound by its terms once they have adopted it. If a signatory to such a code is shown to have violated the code's terms, the signatory may be suspended or excluded from the code. Monitoring and enforcement provisions also exist: creators of Art. 40 codes of conduct are required to identify an oversight body for the purpose of monitoring compliance of signatories to the code; the oversight bodies are accredited by the supervisory authorities (Art. 41).

An additional argument for using codes of conduct in the context of digital labour platforms is that codes of conduct have previously and successfully been used to improve working conditions in transnational work arrangements (Weil 2009; Klein 2009; Anner *et al.* 2013). Many digital labour platforms are transnational, and these transnational operations are difficult to regulate (Cherry 2019). While GDPR applies extraterritorially, enforcement and compliance pose some challenges in practice (Sirur *et al.* 2018). Creating an Article 40 code of conduct for platforms may help address these challenges by clarifying interpretations, establishing sectoral best practices, and reducing the enforcement burden on supervisory authorities.

Nonetheless, for a code of conduct to successfully promote workers’ rights, firms must have a stake in upholding the terms and conditions included. Merely excluding a signatory from an Art. 40 GDPR code may not be an adequate incentive for compliance. Art. 42 GDPR, however, establishes the possibility for GDPR certifications that could provide additional incentives, for example, by improving market access for certified platforms.

Certifications can be (and have been) effectively used for marketing and public relations purposes; a certification as provided for by Art. 42 GDPR could incorporate compliance with an Art. 40 GDPR code of conduct. Because of the potential use of certifications for improved market access (for example, large clients or associations could require certifications in their procurement policies), such a combination could create significant economic incentives for platforms to participate in an Art. 40 code of conduct.

7. Annotated draft text for an Art. 40 GDPR code of conduct for labour platforms

This section presents a draft text for an Art. 40 GDPR code of conduct for labour platforms. The text presented here is intended to address only the problems discussed above (i.e. the ‘procedural problems’), not all problems relating to GDPR compliance on labour platforms.

We suggest that the code be structured in two parts. Part 1 should be dedicated to an interpretation of GDPR for the purpose of providing clarity in the context of labour platforms. We view these as non-negotiable legal realities to which platforms must conform to be in compliance with already existing European regulation. Part 2 of the code should include language that provides platform workers with additional rights that exceed those explicitly afforded by GDPR. Recognising that GDPR does not address all issues relating to personal data processing that platform workers may experience, Art. 40 codes could include language establishing additional rights. For example, an Art. 40 code could provide workers with a general right to an explanation for decisions made based on personal data.

Various parts of the draft text are presented below, each followed by a brief explanation of the reasoning behind the text. We begin with text that would be included in Part 1 (‘Application of GDPR to labour platforms’) of an Art. 40 code of conduct. This is followed by select recommendations that could be included in Part 2 ('Additional data rights and guidance for platform operators').

7.1 Part 1: Application of GDPR to labour platforms

Definition of 'labour platform'

The code should define 'labour platform.' The definition does not need to be as precise as such a definition would need to be if it were part of legislation, as it only needs to signal what kinds of platforms the code is designed to be relevant for.

Draft text

A labour platform is any digital information system (or interconnected collection of such systems) that connects, or acts an intermediary between, on one hand, parties providing work or the products of work ('workers' or 'providers'), and, on the other, parties seeking work or the products of work ('customers').

Generally, labour platforms make parties to a labour transaction aware of one another and facilitate transactions in ways other than only processing payment (for example, by allowing potential customers to search for workers qualified to perform a particular task, or allowing workers to submit offers for work).

Even if payment is not involved in the transactions on a platform, a platform may be considered a labour platform.

If payment is involved, the platform in question may or may not process the payments. There may be multiple parties to labour platform transactions in addition to the platform, workers, and customers.

Digital platforms that act only as payment processors are unlikely to be seen as labour platforms under this definition.

Remarks:

This definition intentionally does not require transactions on a platform to involve money for the platform to be potentially considered a labour platform.

If money does change hands, the definition is agnostic to the platform's technical role in processing these payments.

Some platforms only process payment but provide no means for potential parties to a transaction to 'discover' one another and no other features that facilitate the transaction. While it cannot be entirely ruled out that this code may be useful or relevant to such platforms, we suspect it is not especially likely.

Such platforms are probably better described as 'payment processors' than as 'labour platforms'.

The definition intentionally includes more complex relationships than the classical 'triangular' labour platform relationship of 'platform, worker, customer'. For example, on content marketplaces, there are (at least) four parties: the platform, the content creator, the advertiser (the paying customer), and viewers (who may or may not pay).

The definition intentionally includes platforms where payment is involved and platforms where it is not; on some types of platforms, like contest-based platforms, workers commonly compete to win money in the form of a contest. Under these types of platforms it is common for many participants to submit work they have done and to receive no remuneration. (In some cases, even winners may only receive 'exposure' rather than payment.)

Clarification of the term 'personal data' in the context of labour platforms

Because it has been a topic of confusion, the code should clarify the meaning of the term 'personal data' with regard to various categories of information that are common in labour platforms.

Draft text

The definition of 'personal data' from Art. 4.1 GDPR applies.

The phrase 'relating to' in this definition is to be understood as set forth in C-434/16 *Nowak v. Data Protection Commissioner* in the case law of the ECJ, paragraphs 34-35; namely, information is personal data in the sense concerning GDPR 'where the information, by reason of its content, purpose or effect, is linked to a particular person'.

The terms 'content,' 'purpose,' and 'effect' are elaborated further in pp. 9-12 Opinion 4/2007 of the Article 29 Working Party 'On the concept of personal data' (where the term 'result' is used in place of 'effect'); these elaborations shall be interpreted as binding on signatories to this Code.

These definitions and elaborations make clear that the following categories of information that often appear in labour platforms are generally to be understood as 'personal data':

- Ratings
- Work approval and rejection rates (even when not used as evaluations)
- Work acceptance and refusal rates (that is, the rates with which a worker has accepted or refused offered tasks/jobs)
- Rankings of workers, and any data used to create such a ranking

Generally, such data are only **not** personal data if they are completely anonymised.

The definition of Art. 4.1 GDPR applies regardless of the source of the data. In the context of labour platforms, this means, for example, that:

- If a rating is collected from a customer about a worker, the rating is personal data. It may be the personal data of both parties.
- If a record about a worker or customer is created algorithmically, 'internally' to the platform, that is the worker's or customer's personal data.

Remarks:

Worker ratings (and other evaluations, qualifications, and classifications of workers and their work), approval and rejection rates, and a worker's acceptance and refusal rates of work offered to them are frequently important determinants influencing access to work — and therefore worker income. The relevant case law of the European Court of Justice, especially *Nowak v. Data Protection Commissioner*, makes clear that they are 'personal data' under EU data protection law. However, because of confusion regarding the meaning of the phrase 'relates to' in the definition of 'personal data' in Art. 4.1 GDPR, some platform operators have not understood this. By clarifying this potential point of conflict 'in advance', the Code can avoid protracted debates (and potentially litigation) between platforms and data subjects.

Clarification regarding information to be provided

Some platforms maintain 'hidden' or 'secret' ratings of workers and/or customers. This is not compatible with the requirements set forth in Art. 14 GDPR and should therefore be clarified by the code.

Draft text

Art. 14 GDPR applies to all personal data, regardless of the source. Data subjects must be informed in a manner consistent with the requirements set forth by Art. 14 GDPR whenever data relating to them has been collected or created.

Signatories to this Code will not create or maintain secret or hidden ratings about data subjects, unless required to do so to comply with applicable European or national law or with legal obligations established by public authorities.

Remarks:

As discussed previously, some platforms have secret ratings about workers. These can be based on information that is collected, or created, about data subjects unknowingly. For example, secret ratings may rely on ratings from customers or algorithmic assessments of work about which workers are unaware. Such secret ratings are unlawful under Article 14 GDPR unless required by specific circumstances, such as compliance with European or national law or legal obligations established by public bodies. Clear language in a code of conduct affirming the obligation of platform operators to inform data subjects of the collection or creation of all personal data relating to them serves as an important reminder, and can avoid confusion and improve legal certainty.

Clarification of the interpretation and application of Art. 15.4 GDPR

Art. 15.4 GDPR has been interpreted by some controllers as an 'escape clause' which they can use to decline to provide access to personal data they have business reasons for wishing to withhold, or about which their legal obligations may be unclear (for example, when a piece of information is the personal data of multiple data subjects with potentially conflicting interests). As indicated by Recital 63, however, it cannot be used this way. The code should clarify what platform operators should do in such difficult cases, and clarify the meaning and proper application of Art. 15.4.

Draft text

Where personal data relates to multiple data subjects:

In situations where a piece of information is the personal data of multiple data subjects, signatories to this Code will endeavour to provide procedurally and economically relevant information to data subjects without infringing on other data subjects' right to privacy.

Specifically, ratings and evaluations left by customers of workers and work performed (and vice versa) are likely to be the personal data of both workers and customers. To ensure both the right of access and the right to privacy, signatories to this Code will provide rated parties with the content of such ratings, but not the personally identifying information of the persons leaving the ratings.

Exceptional circumstances and appropriate procedures for such circumstances may be elaborated by the signatories in cooperation with the monitoring body of the Code. Examples of such circumstances may include:

- When the content of a rating or evaluation (potentially in connection with other data) is likely to reveal the identity of the person who left the rating, for example because the content of the rating includes a date and time, and the rated party is likely to have timestamped records about their interactions with other parties on the platform.
- When one or both parties may be at risk of harassment from the other.

Remarks:

Platforms may find themselves in situations where personal data relate to multiple data subjects. For example, if a customer rates a worker, the rating is the personal data of both the customer and the worker (unless the platform anonymises the record in such a way that it can no longer be linked to one or the other party). If a worker makes a data subject access request under Art. 15 GDPR and asks for a copy of their ratings by customers, the platform's data protection officer may wonder if the platform is, in one extreme case, obligated to include the rating customer's personally identifying information (for example, their name) in the response to the worker — or, in the other extreme, to decline to provide any data relating to the rating to the worker at all. In fact, neither response is appropriate; the worker has the right to know what the rating was, but the customer's right to privacy implies that the worker does not have the right to personally identifying information about the customer who left it.

Additionally, platforms may cite trade secrets or intellectual property as a reason that they do not have to comply with data subject access requests. Art. 15.4 provides that the right of the data subject to obtain a copy of their personal data from a controller 'shall not adversely affect the rights and freedoms of others'. Recital 63 elaborates that these rights and freedoms may include trade secrets and intellectual property. Recital 63 also provides, however, that 'the result of those considerations should not be a refusal to provide all information to the data subject'. While a controller may be tempted to argue that the entirety of their data-processing operations are a trade secret, such considerations cannot entirely take precedence over the rights provided by GDPR to data subjects. An Art. 40 GDPR code should clarify the circumstances under which Art. 15.4 GDPR may be invoked. Specifically, it should clarify the extent to which the 'trade secret exemption' can be used to decline data subject access requests. We have not been able to formulate draft text to address this situation; the matter is complex enough to require the expertise of a lawyer conversant with the interaction of trade secrets and data protection law.

Clarification of the interpretation and application of Art. 22

Art. 22 GDPR provides that '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'.

Draft text

Signatories to the Code are advised of, and will adopt, the Guidelines on Automated Individual Decision-Making and Profiling set forth by the Article 29 Working Party.

Specifically, signatories are advised that controllers 'cannot avoid the Article 22 provisions by fabricating human involvement' (p. 21).

Remarks:

The adjective 'solely' has created some confusion among data subjects and controllers; specifically, some platforms may have incorrectly assumed that by minimally involving humans in data processing, even if such involvement does not meaningfully change the nature of automatic processing, that they are exempt from their obligations under GDPR. The Article 29 Working Party has pointedly clarified the definition of automated processing in the Guidelines on Automated Individual Decision-Making and Profiling.

Recourse to a supervisory authority remains available

Given the historic concerns that codes of conduct could undermine public or legal regulation, it is important to ensure that any Article 40 code of conduct affirms the data subject's right to lodge a complaint with the supervisory authority.

Draft text

Nothing in this Code, including the data subject's use of external mediation procedures provided for in this Code, is to be construed as abridging the data subject's right to lodge a complaint with a supervisory authority as established by Art. 77 GDPR.

Recourse to judicial remedy remains available

Similarly, it is important to ensure that the code affirms the data subject's right to seek judicial remedy.

Draft text

Nothing in this Code, including the data subject's use of external mediation procedures provided for in this Code, is to be construed as abridging the data subject's rights to judicial remedy as established by Arts. 78-79 GDPR.

7.2 Part 2: Additional data rights and guidance for platform operators

Guidance on ensuring the transparency, accuracy and fairness of rating, evaluation, and classification systems

Algorithms, systems, and processes for allocating tasks to workers (or otherwise determining which workers get which work), ranking and rating or otherwise evaluating workers and work should be transparent, accurate, fair, and fit for purpose. When used to describe a rating system, 'fit for purpose' means that they should elicit evaluations that indicate, as clearly, objectively, and verifiably as possible the extent to which submitted work met or failed to meet the specific requirements set forth in the task assignment.

Draft text

Workers are entitled to see all information stored about them by the platform, including work evaluations, metrics, qualifications, and other information pertaining to their fitness for performing certain tasks or types of tasks.

Workers have a right to receive clear, pertinent written explanations about how information stored by the platform affects them, such as how they are assigned tasks.

Neither work quality evaluation nor payment decisions shall rely on automatic systems that determine the most common response submitted for a given task to be correct.

Evaluation and task assignment/worker qualification processes shall not be designed in a way that assumes that if a client refuses payment for submitted work, or provides a poor evaluation of work, this indicates that the work did not meet the requirements. Accordingly, client payment or non-payment rates, or evaluations, shall not be used as indicators of worker quality, and shall not be the basis for determining access to work.

Work shall not be evaluated by automated systems known or demonstrated to erroneously judge work as not meeting requirements, especially machine learning-based systems.

Workers have a right to contest evaluations, to have contested cases reviewed by a qualified human platform employee, and, if necessary, further reviewed by a qualified neutral third party empowered to issue a final and binding decision.

Evaluation systems which assign a numerical rating or evaluation of a worker or of completed work (from the client, from a platform employee, or from any other source) will provide clear criteria to the evaluator to promote an objective evaluation of the worker and of the work completed. The evaluation criteria will also be made available to the worker.

Remarks:

GDPR requires that personal data be accurate, and that processing be fair and transparent. This is particularly important within the context of rating, evaluation, and classification systems, because of the direct impact it can have on workers’ access to the platform and to future work opportunities. Regarding transparency, workers should have a right to see all information stored about them by the platform, including work evaluations, metrics, qualifications, and other information pertaining to their fitness for performing certain tasks or types of tasks. (Ideally, this should be made available by the platform proactively — meaning that a worker should be able to access this information easily, for example through an online dashboard, as discussed below.) Workers should also have a right to receive clear, pertinent written explanations about how information stored by the platform affects them. This pertains to task eligibility, task assignment (including ranking in search results, if clients can search for workers according to criteria related to a worker’s history and performance), evaluation and subsequently payment.

Platforms commonly use automated systems that deem the most common answer to be correct, with potentially adverse impacts on the accuracy of such systems and the data that they generate. This practice is frequently used on micro-tasking platforms, where multiple workers are asked to do the same task. Workers who have submitted the most common answer are paid and the remainder of workers are not, even if their answer is in fact, correct. The draft code includes language that prohibits this decision procedure. Relatedly, sometimes clients make mistakes, use faulty algorithmic processes to evaluate work, delegate the evaluation to unqualified workers or third parties, or have biases. For this reason, client payment or non-payment rates, or evaluations, should not be used as indicators of worker quality, and should not be the basis for determining access to work. Finally, work should not be evaluated by automated systems known or demonstrated to erroneously judge work as not meeting requirements, especially machine learning-based systems. Systems that are known to be faulty are neither fair nor accurate for workers.

Evaluation systems must also be fit for purpose. As mentioned above, this means they should elicit evaluations that indicate, as clearly, objectively, and verifiably as possible the extent to which submitted work met or failed to meet the specific requirements set forth in the task assignment. This will help ensure evaluations are fair. To this effect, generic, potentially ambiguous, and/or subjective systems such as those which elicit a numerical rating from the client without explaining clearly the criteria according to which workers should be evaluated, or the meanings and consequences of the numerical ratings, should be avoided.

Finally, ensuring fairness in ratings, evaluation and classification systems means that workers should be able to contest evaluations, to have contested cases reviewed by a qualified human platform employee, and, if necessary, further reviewed by a qualified neutral third party empowered to issue a final and binding decision.

Guidance for when a platform customer is the controller

In some cases, a customer of a platform may also be a controller of a worker's personal data. This can occur, for example, if a platform customer refers a worker to a private site to perform a task, or uses an information system that they have developed independently to assess submitted work for the purpose of deciding which workers will be paid.

Draft text

If a customer on a platform which is a signatory to this Code acts as a controller, the platform shall inform the customer of their legal obligations as a controller of personal data under GDPR, and ensure that data subjects whose personal data are processed by the customer in question are informed of the identity and contact details of the customer (and/or their representative).

Optional additional draft text

Signatories to this Code shall require that customers acting as data controllers agree to the procedural obligations the Code establishes for platforms, for example, by including these obligations in the terms of service accepted by customers.

Remarks:

A customer may recruit workers via a labour platform but require them to complete work on a separate system controlled by the customer. In such a case, the customer may be a controller of some personal data relating to workers. Alternatively, or additionally, a customer may maintain a filing system separate from the platform which contains workers' personal data, including but not limited to evaluation of work or of the workers themselves. In such cases the customer is also a controller of workers' personal data. Customers are not themselves signatories to this code, but data subjects must know how to appropriately direct their requests under GDPR. Therefore the code should at least require that signatories inform customers acting as controllers of workers' personal data of their obligations under GDPR, and ensure that workers whose personal data are processed by customers are provided with the identity and contact details of those customers (or their representatives, for data protection compliance purposes). The code could additionally require that signatories require customers to meet similar obligations to those laid out for the signatories themselves with respect to data protection rights, and lay out those requirements in draft text to be included in the platform's legal terms.

If the optional additional draft text were to be included in the code, the monitoring body could be tasked with developing appropriate language for platform terms of service.

Best practices for improving ease of access to data subjects' personal data

On some platforms, the process through which data subjects submit requests is rudimentary and cumbersome.

Draft text

Signatories of this Code will provide data subjects secure access to an online interface where their personal data can be viewed and downloaded.

Remarks:

On some platforms, the process through which data subjects submit requests can be inconvenient, difficult to navigate, or time consuming. Platforms should thus create systems to make personal data easily available to the relevant data subjects. This will reduce friction in platforms' systems for processing data subjects' access requests. It will also promote transparency, accuracy, and fairness by proactively providing data subjects with access to their personal data.

Mediation/external dispute resolution procedures

With the aim of improving compliance and enforcement while reducing the burden on supervisory authorities, this code proposes to establish an 'intermediate' dispute resolution procedure to which data subjects may have recourse if they do not believe that the outcome of an interaction with a signatory to the code was not compliant with the rights and obligations set forth by GDPR, or by the code.

Draft text

Should a data subject be unsatisfied with the outcome of a data subject access request or other interaction with the data protection officer or office of a signatory to this Code, the data subject may submit a complaint to the monitoring body.

The monitoring body shall operate a multilateral dispute resolution procedure for handling complaints submitted in this fashion.

The procedure shall include qualified representatives of at least the following groups: platform operators, platform workers, and platform customers. The representatives shall be selected independently and transparently from among the respective groups.

The monitoring body shall further specify the dispute resolution procedure and the respective roles of the stakeholder representatives.

Remarks:

Not only would an external dispute resolution process alleviate some of the administrative burden on supervisory authorities, it would also create an opportunity to incorporate workers into the monitoring process for the Art. 40 GDPR code of conduct. Generally, codes of conduct have more effectively promoted workers' rights when monitoring and compliance protocols have included the involvement of workers.

Additional considerations

Part 2 of an Art. 40 code might also establish further rights relating to personal data processing on labour platforms, such as:

- a general right to explanations for individual decisions made using personal data (the so-called 'right to an explanation') (Wachter *et al.* 2017)
- a general right to 'reasonable inferences' (Wachter and Mittelstadt 2019)
- a right to recourse (for example, a right to object and a follow-on right to independent mediation) for platform workers who are adversely affected by decisions that do not result from automated processing

While we do not provide specific draft text on these rights, we view them as important features that should be considered by parties interested in drafting an Art. 40 code for labour platforms.

8. Possible next steps

Developing an Art. 40 GDPR code of conduct is an opportunity to foster dialogue among many (well-intentioned) actors and stakeholders in the platform economy. Historically, codes of conduct have proven most effective at improving workers' rights and working conditions when they have promoted involvement, in creation and monitoring, of multiple stakeholders (Fine and Bartley 2019; Fine 2014; Dias-Abey 2018). Additionally, dialogue is important to ensuring that the interests of all parties are adequately reflected in the outcomes achieved.

Trade unions could initiate and facilitate this process. The following steps might be useful:

1. Internal review and further development of the present proposal, including consultation with legal experts.

2. Consultation and dialogue with platform workers, trade unionists, and relevant civil society actors.

3. Dialogue with platform clients and platform operators, especially those already engaged in voluntary dialogue, and collaboration with trade unions, civil society actors and regulators in efforts to improve platform working conditions.

4. Selection or establishment of a monitoring body. The monitoring body should have representatives from at least workers and platforms, and possibly other stakeholders (for example, platform clients or civil society).

5. Preparation and submission of the draft code to a competent supervisory authority.

9. Conclusion

We hope that this paper can help initiate a discussion at European level among trade unions and other stakeholders in platform work about how to use GDPR to address the 'procedural problems' faced by platform workers, regardless of their employment status. GDPR is a strong and promising piece of legislation, but questions of interpretation, application, and enforcement remain. The proposals advanced in this paper have been developed from a 'ground level' or 'practitioner' perspective, and would benefit from further discussion with legal experts as well as with platform workers and other trade unionists with different experiences with platform work and European data protection law. We look forward to this discussion, and perhaps to the creation of an Art. 40 GDPR code of conduct for labour platforms. The final measure of the exercise, of course, will be whether it leads to concrete improvements in working conditions for platform workers.

References

Anner M., Bair J. and Blasi J. (2013) Toward joint liability in global supply chains: addressing the root causes of labor violations in international subcontracting networks, Comparative Labor Law and Policy Journal, 35 (1), 1-43.

Article 29 Data Protection Working Party (2007) Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, 20 June 2007. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Article 29 Data Protection Working Party (2018) Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679, WP251rev01. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Bartley T. (2005) Corporate accountability and the privatization of labor standards: struggles over codes of conduct in the apparel industry, Research in Political Sociology, 14, 211-244.

Berg J., Furrer M., Harmon E., Rani U. and Silberman M. S. (2018) Digital labour platforms and the future of work. Towards decent work in the online world, Geneva, ILO.

Brawley A. M. and Pury C. L. S. (2016) Work experiences on MTurk: job satisfaction, turnover, and information sharing, Computers in Human Behavior, 54, 531-546.

Cherry M. A. (2019) A global system of work, a global system of regulation? Crowdwork and conflicts of law, Tulan Law Review, 94 (2), 183-246.

Compa L. (2001) Wary Allies, The American Prospect, 19 December 2001. https://prospect.org/api/content/bb94c786-7a5a-5f6d-aa74-bf46dbb9f7a5/

Daugareilh I., Degryse C. and Pochet P. (eds.) (2019) The platform economy and social law: key issues in comparative perspective, Working Paper 2019.10, Brussels, ETUI.

Dettmer M. (2019) Sind Crowdworker selbstständig oder angestellt?, Der Spiegel, 26 July 2019. https://www.spiegel.de/politik/sind-crowdworker-selbststaendige-oder-angestellte-a-00000000-0002-0001-0000-000165100976

Dias-Abey M. (2018) Justice on our fields: can ‘alt-labor’ organizations improve migrant farm workers’ conditions?, Harvard Civil Rights-Civil Liberties Law Review 53 (1), 167-211.

Drahokoupil J. and Piasna A. (2019) Work in the platform economy: Deliveroo riders in Belgium and the SMart arrangement, Working Paper 2019.01, Brussels, ETUI.

Fine J. (2014) Strengthening labor standards compliance through co-production of enforcement, New Labor Forum, 23 (2), 76-83.

Fine J. and Bartley T. (2019) Raising the floor: new directions in public and private enforcement of labor standards in the United States, Journal of Industrial Relations, 61 (2), 252-276.

Forde C. *et al.* (2017) The social protection of workers in the platform economy, Brussels, European Parliament, 128.

Irani L. C. and Silberman M. S. (2013) Turkopticon: interrupting worker invisibility in Amazon mechanical turk, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 611-620. https://doi.org/10.1145/2470654.2470742

Kilhoffer Z. *et al.* (2019) Study to gather evidence on the working conditions of platform workers VT/2018/032, Final Report, 13 December 2019, Luxembourg, Publications Office of the European Union.

Klein N. (2009) No logo, Toronto, Vintage Canada.

McInnis B. J., Cosle D., Nam C. and Leshed G. (2016) Taking a HIT: designing around rejection, mistrust, risk, and workers’ experiences in Amazon mechanical turk, Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 2271-2282. https://doi.org/10.1145/2858036.2858539

Piasna A. and Drahokoupil J. (2019) Digital labour in central and eastern Europe: evidence from the ETUI Internet and Platform Work Survey, Working Paper 2019.12, Brussels, ETUI.

Ponce Del Castillo A. (2020) Labour in the age of AI: why regulation is needed to protect workers, Foresight Brief #08, Brussels, ETUI.

Posner M. and Nolan J. (2003) Can codes of conduct play a role in promoting workers’ rights?, in Flanagan R.J. and Gould IV W.B. (eds.) International labor standards: globalization, trade and public policy, Stanford, Stanford University Press, 207-226.

Ravenelle A. J. (2019) Hustle and gig: struggling and surviving in the sharing economy, Oakland, University of California Press.

Risak M. and Dullinger T. (2018) The concept of ‘worker’ in EU law: status quo and potential for change, Report 140, Brussels, ETUI.

Rosenblat A. (2018) Uberland: how algorithms are rewriting the rules of work, Oakland, University of California Press.

Rosenblat A. and Stark L. (2016) Algorithmic labor and information asymmetries: a case study of Uber’s drivers, International Journal of Communication, 10, 3758-3784.

Sirur S., Nurse J. R. C. and Webb H. (2018) Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR), in MPS '18: Proceedings of the 2nd International Workshop on Multimedia Privacy and Security, Toronto, October 2018, 88-95. https://doi.org/10.1145/3267357.3267368

Toffel M. W., Short J. L. and Ouellet M. (2015) Codes in context: how states, markets, and civil society shape adherence to global labor standards, Regulation & Governance, 9 (3), 205-223.

Vandaele K. (2018) Will trade unions survive in the platform economy? Emerging patterns of platform workers’ collective voice and representation in Europe, Working Paper 2018.05, Brussels, ETUI.

Vandaele K., Piasna A. and Drahokoupil J. (2019) ‘Algorithm breakers’ are not a different ‘species’: attitudes towards trade unions of Deliveroo riders in Belgium, Working Paper 2019.06, Brussels, ETUI.

Wachter S. and Mittelstadt B. (2019) A right to reasonable inferences: re-thinking data protection law in the age of big data and AI, Columbia Business Law Review, 2019 (2), 494-620.

Wachter S., Mittelstadt B. and Floridi L. (2017) Why a right to explanation of automated decision-making does not exist in the general data protection regulation, International Data Privacy Law, 7 (2), 76-99.

Weil D. (2009) Rethinking the regulation of vulnerable work in the USA: A sector-based approach, Journal of Industrial Relations, 51 (3), 411-430.

Weil D. (2014) The fissured workplace. Why work became so bad for so many and what can be done to improve it, Cambridge Mass., Harvard University Press.

Wood A. J., Graham M., Lehdonvirta V. and Hjorth I. (2018) Good gig, bad gig: autonomy and algorithmic control in the global gig economy, Work, Employment and Society, 33 (1), 56-75.

Woodcock J. and Graham G. (2019) The gig economy: a critical introduction, Cambridge, Polity Press.

All links were checked on 19 May 2020.

Annex

Note of the authors

This annex presents in a single block the draft text discussed with comments in Section 7 of the paper. Note that this draft text is not intended to be a complete Art. 40 GDPR code of conduct for labour platforms, but only draft text addressing the issues discussed in the paper. For further context, please consult the paper, especially Section 7.

Part 1 Application of GDPR to labour platforms

Definition of 'labour platform'

A labour platform is any digital information system (or interconnected collection of such systems) that connects, or acts an intermediary between, on one hand, parties providing work or the products of work ('workers' or 'providers'), and, on the other, parties seeking work or the products of work ('customers').

Generally, labour platforms make parties to a labour transaction aware of one another and facilitate transactions in ways other than only processing payment (for example, by allowing potential customers to search for workers qualified to perform a particular task, or allowing workers to submit offers for work).

Even if payment is not involved in the transactions on a platform, a platform may be considered a labour platform.

If payment is involved, the platform in question may or may not process the payments.
There may be multiple parties to labour platform transactions in addition to the platform, workers, and customers.

Digital platforms that act only as payment processors are unlikely to be seen as labour platforms under this definition.

Clarification of the term 'personal data' in the context of labour platforms

The definition of 'personal data' from Art. 4.1 GDPR applies.

The phrase 'relating to' in this definition is to be understood as set forth in C-434/16 Nowak v. Data Protection Commissioner in the case law of the ECJ, paragraphs 34-35; namely, information is personal data in the sense concerning GDPR 'where the information, by reason of its content, purpose or effect, is linked to a particular person'.

The terms 'content,' 'purpose,' and 'effect' are elaborated further in pp. 9-12 Opinion 4/2007 of the Article 29 Working Party 'On the concept of personal data' (where the term 'result' is used in place of 'effect'); these elaborations shall be interpreted as binding on signatories to this Code.

These definitions and elaborations make clear that the following categories of information that often appear in labour platforms are generally to be understood as 'personal data':

— Ratings
— Work approval and rejection rates (even when not used as evaluations)
— Work acceptance and refusal rates (that is, the rates with which a worker has accepted or refused offered tasks/jobs)
— Rankings of workers, and any data used to create such a ranking

Generally, such data are only **not** personal data if they are completely anonymised.

The definition of Art. 4.1 GDPR applies regardless of the source of the data. In the context of labour platforms, this means, for example, that:

— If a rating is collected from a customer about a worker, the rating is personal data. It may be the personal data of both parties.
— If a record about a worker or customer is created algorithmically, 'internally' to the platform, that is the worker's or customer's personal data.

Clarification regarding information to be provided

Art. 14 GDPR applies to all personal data, regardless of the source. Data subjects must be informed in a manner consistent with the requirements set forth by Art. 14 GDPR whenever data relating to them has been collected or created.

Signatories to this Code will not create or maintain secret or hidden ratings about data subjects, unless required to do so to comply with applicable European or national law or with legal obligations established by public authorities.

Clarification of the interpretation and application of Art. 15.4 GDPR

Where personal data relates to multiple data subjects:

In situations where a piece of information is the personal data of multiple data subjects, signatories to this Code will endeavour to provide procedurally and economically relevant information to data subjects without infringing on other data subjects' right to privacy.

Specifically, ratings and evaluations left by customers of workers and work performed (and vice versa) are likely to be the personal data of both workers and customers. To ensure both the right of access and the right to privacy, signatories to this Code will provide rated parties with the content of such ratings, but not the personally identifying information of the persons leaving the ratings.

Exceptional circumstances and appropriate procedures for such circumstances may be elaborated by the signatories in cooperation with the monitoring body of the Code. Examples of such circumstances may include:

- When the content of a rating or evaluation (potentially in connection with other data) is likely to reveal the identity of the person who left the rating, for example because the content of the rating includes a date and time, and the rated party is likely to have timestamped records about their interactions with other parties on the platform.
- When one or both parties may be at risk of harassment from the other.

Clarification of the interpretation and application of Art. 22

Signatories to the Code are advised of, and will adopt, the Guidelines on Automated Individual Decision-Making and Profiling set forth by the Article 29 Working Party.

Specifically, signatories are advised that controllers 'cannot avoid the Article 22 provisions by fabricating human involvement' (p. 21).

Recourse to a supervisory authority remains available

Nothing in this Code, including the data subject's use of external mediation procedures provided for in this Code, is to be construed as abridging the data subject's right to lodge a complaint with a supervisory authority as established by Art. 77 GDPR.

Recourse to judicial remedy remains available

Nothing in this Code, including the data subject's use of external mediation procedures provided for in this Code, is to be construed as abridging the data subject's rights to judicial remedy as established by Arts. 78-79 GDPR.

Part 2 Additional data rights and guidance for platform operators

Guidance on ensuring the transparency, accuracy and fairness of rating, evaluation, and classification systems

Workers are entitled to see all information stored about them by the platform, including work evaluations, metrics, qualifications, and other information pertaining to their fitness for performing certain tasks or types of tasks.

Workers have a right to receive clear, pertinent written explanations about how information stored by the platform affects them, such as how they are assigned tasks.

Neither work quality evaluation nor payment decisions shall rely on automatic systems that determine the most common response submitted for a given task to be correct.

Evaluation and task assignment/worker qualification processes shall not be designed in a way that assumes that if a client refuses payment for submitted work, or provides a poor evaluation of work, this indicates that the work did not meet the requirements. Accordingly, client payment or non-payment rates, or evaluations, shall not be used as indicators of worker quality, and shall not be the basis for determining access to work.

Work shall not be evaluated by automated systems known or demonstrated to erroneously judge work as not meeting requirements, especially machine learning-based systems.

Workers have a right to contest evaluations, to have contested cases reviewed by a qualified human platform employee, and, if necessary, further reviewed by a qualified neutral third party empowered to issue a final and binding decision.

Evaluation systems which assign a numerical rating or evaluation of a worker or of completed work (from the client, from a platform employee, or from any other source) will provide clear criteria to the evaluator to promote an objective evaluation of the worker and of the work completed. The evaluation criteria will also be made available to the worker.

Guidance for when a platform customer is the controller

If a customer on a platform which is a signatory to this Code acts as a controller, the platform shall inform the customer of their legal obligations as a controller of personal data under GDPR, and ensure that data subjects whose personal data are processed by the customer in question are informed of the identity and contact details of the customer (and/or their representative).

Optional additional draft text

Signatories to this Code shall require that customers acting as data controllers agree to the procedural obligations the Code establishes for platforms, for example, by including these obligations in the terms of service accepted by customers.

Best practices for improving ease of access to data subjects' personal data

Signatories of this Code will provide data subjects secure access to an online interface where their personal data can be viewed and downloaded.

Mediation/external dispute resolution procedures

Should a data subject be unsatisfied with the outcome of a data subject access request or other interaction with the data protection officer or office of a signatory to this Code, the data subject may submit a complaint to the monitoring body.

The monitoring body shall operate a multilateral dispute resolution procedure for handling complaints submitted in this fashion.

The procedure shall include qualified representatives of at least the following groups: platform operators, platform workers, and platform customers. The representatives shall be selected independently and transparently from among the respective groups.

The monitoring body shall further specify the dispute resolution procedure and the respective roles of the stakeholder representatives.

ETUI Working Papers

« One in, one out » dans le système juridique de l'Union européenne : une réforme en trompe l'oeil ?
Working Paper 2020.04
Éric Van den Abeele

European multinational companies and trade unions in eastern and east-central Europe
Working Paper 2020.03
Martin Myant

EWC Confidential
Confidentiality in European Works Councils and how representatives deal with it: case study and survey insights
Working Paper 2020.02
Lise Meylemans and Stan De Spiegelaere

Pushing the limits: the European Central Bank's role in restoring sustainable growth
Working Paper 2020.01
Jörg Bibow

Towards a progressive EMU fiscal governance
Working Paper 2019.13
Nacho Álvarez, *et al.*

Digital labour in central and eastern Europe: evidence from the ETUI Internet and Platform Work Survey
Working Paper 2019.12
Agnieszka Piasna and Jan Drahokoupil

She works hard for the money: tackling low pay in sectors dominated by women – evidence from health and social care
Working Paper 2019.11
Torsten Müller

The platform economy and social law: key issues in comparative perspective
Working Paper 2019.10 (EN, FR)
Isabelle Daugareilh, Christophe Degryse and Philippe Pochet

Legislative implementation of European social partner agreements: challenges and debates
Working Paper 2019.09 (EN, FR)
Jean-Paul Tricart

These publications can be downloaded free of charge from our website.
Please visit: www.etui.org/publications

European
Trade Union Institute
Bd du Roi Albert II, 5
1210 Brussels
Belgium
+32 (0)2 224 04 70
etui@etui.org
www.etui.org

D/2020/10.574/16
ISSN: 1994-4446

etui.