Trade Union
Advisory Committee
to the OECD
Commission
syndicale consultative
auprès de l'OCDE

TUAC

The limits of data rights for the workplace

Briefing Paper

Paris, 07 June 2021

Executive summary

This TUAC briefing paper addresses the limitations of current data rights for the workplace by discussing data portability in the data governance and competition policy context. The paper draws on recent TUAC submissions to the OECD's Competition Committee Hearing on Data Portability, Interoperability and Competition and to the OECD Horizontal Project, Going Digital III, on data governance.

It shows that:

- The workplace is typically not at the forefront of data governance and competition debates. This is an omission in terms of resolving data rights, collection, access and sharing issues, but also concerning anti-competitive effects on job mobility and quality.

- A high amount of data is generated on-the-job, both in the public and private sector. Employer's control over recruitment and on-the-job data, limitations to data portability and ownership rights result in an unfair position of workers vis-à-vis their employer in terms of access to data and the sharing of its value. This can lead to adverse practices affecting the livelihoods, health and safety of workers.

- Enforcement of proper data portability rights is particularly important for platform workers. The business model of platform work is based on ratings and reviews that result in an online CV for workers attesting to the quality of their work and allowing them to get more clients. Therefore, if workers are not able to fully access and use their data, they are tied to a unique platform.

1, rue Viala – 75015 Paris
Tél. (33) 01 55 37 37 37 – tuac.org — @tuacoecd

- The accumulation and misuse of workplace data clearly feed into labour market monopsonies. In particular, heightened control, interference with remuneration and the use of data to deter employees from looking for another employer all constitute anti-competitive practices designed to accentuate the asymmetry between employer and employee further. The increasing ability of employers to pay wages below normal market conditions without losing their workforce, while gaining from data-driven productivity, is a source of concern.

- Current standards and approaches are insufficient to cover the workplace and to resolve balance of power, network effect and other lock-in issues, including in the platform economy.

- To operationalise data portability that works for workers, consumers, citizens and firms, data policy makers and regulators need to work hand in hand with competition authorities. They also need to expand the notion and legal base for data portability and devise stand-alone regulation on data access and sharing.

- Competition policies should provide remedies if data access and sharing provisions are not respected. This should especially be the case if one entity accumulates, uses and shares data in a way that brings them in a dominant market position.

Table of contents

The scope of action on data portability for individuals and workers

Data portability is the right given to individuals (citizens, consumers, employees) to have access to and to re-use their personal data collected by an entity upon prior consent. It is included amongst other in Article 12 of the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act 4 ("CCPA") or the UK's Data Protection Act 2018 (DPA). Not all jurisdictions have this right established in legislation. This is of concern in its own. It also of concern when it comes to cross-border data flows, storage systems and online platforms, which can create loopholes for where the right does not exist.

The right to data portability (as in the GDPR) goes together with the rights 'to be forgotten' and of 'access to data'[1]. The right to data portability mostly relates to 'individuals' – a loose term applying to citizens, consumers, and workers alike. The right does not cover collective data – such as those gathered and processed at workplaces. It

[1] The European Consumer Organisation (2021). *EU CONSUMER PROTECTION 2.0 - Structural asymmetries in digital consumer markets*, https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf

only covers personal data that the data controller needs to make available in a re-usable format at the request of the data subject. For consumers, it allows to change service providers (including online platforms) and have 'control' over their personal data. Indeed, "*data portability promises both to ease restrictions on data flows while allowing consumers to control their personal data, and to spur economic growth while protecting consumers' right to privacy*"[2].

A key pillar to operationalise data portability in technical terms is interoperability. For this, there needs to be international agreements on protocols. If put into effect, interoperability can surpass data portability in that it could provide real-time, machine readable and standardised data formats to data subjects (and/ or their representatives).

Data portability as a workplace issue

The workplace is typically not at the forefront of data governance and competition debates. This is an omission:

- A high amount of data is generated on-the-job both in the public and private sector;
- The definition of personal data under current data portability regimes does not cover the full span of data collected at the workplace (see subsection on overall limitations including regarding inferred and observed data, and the understanding of what constitutes personal data); and
- Employer's control over recruitment and on-the-job data results in an unfair position of workers vis-à-vis their employer in terms of access to data and the sharing of its value; it can lead to adverse practices affecting the livelihoods, health and safety of workers.

The pandemic opened up new data sources to employers: health data and data gathered due to the increased use of telework. They add to the data gathered during recruitment processes and at work (via communication tools, human-machine interfaces, movement-capturing sensors, etc.). Employers collect an array of data pertaining to the worker from which they can create value (either by enhancing productivity or by sharing the data with third parties); they should normally share profits in the forms of higher wages or reductions in working time. However, this increased capture of information on workers' performance and state of being (also via surveillance technology) leads to heightened control.

Reliance on prior consent can be problematic for prospective employees. Workers who enter into a recruitment process, start a new job or are asked to agree to new data protection processes at their current job (if they are indeed informed of those), it is almost impossible not to consent. Unless trade unions are able to negotiate collective agreements on data, most workers have to handle their data on their own.

Furthermore, if workers do not know or cannot access all the data that is being collected about them and hence, then they cannot effectively bargain over their working conditions. The balance of power tilts towards the employer – who with more information at hand can modify the variable elements of the remuneration, or make firing

[2] Fed. Trade Comm'n, Data to Go: An FTC Workshop on Data Portability (Sept. 22, 2020), https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability.

decisions based on data driven performance criteria. This is why, more effective data portability at work matters. It can allow workers and their representatives (unions) to claim access to data sets and by doing so, obtain some insight on what data has been collected. It can also help workers to address any issues they might have with algorithmic management and any decisions made based on the data sets. This of course is only useful if this can happen on a regular basis, on broader data sets, and via trade unions.

All of these components point to broader data governance challenges at the workplace. If workers are not in the loop and control over the processing, use and sharing of data that can be linked to them, it results in a lesser bargaining power. If trade unions and worker representatives are not sufficiently informed and consulted over such data use, and cannot negotiate collective terms, it affects employment security (hiring and firing, promotions based on HR and other performance data), wages (since the data value is not disclosed or shared) and, importantly, the ability to switch jobs – if data portability is only limited to one-off personal data transfers.

Under the GDPR or the UK's Data Protection Act 2018 (DPA), the data subject – here the worker – has the right to access personal data. This includes the right 'to be informed' about data processing and 'to be forgotten'. Personal data relates to someone who is identifiable, directly or indirectly, by an 'identifier' such as their name, or an identification number, or by location. This is limiting, as inferred and observed data do not fall under this definition. Yet, they form a big part of what firms might collect at the workplace.

The French data protection regulator CNIL has provided a standard (referential) on human resource data[3]. It only concerns personal data used for management purposes. It gives a good overview on the legal bases – including retention periods. It also provides a categorisation of ways employers collect and process data including: (1) recruitment (excluding some tools, e.g., psychometrics); (2) employee administration; (3) compensation management and administrative formalities; (4) provision of professional tools; (5) work organization; (6) career and mobility management; (7) training; (8) compulsory records and management of relations with employee representatives; (9) internal communications; (10) social benefits; and (11) auditing and (pre)litigation management. Falling out of the referential due to adjacent regulations and indeed the scope of data protection regulation are:

- access control with biometrics;
- operation of a whistleblowing hotline;
- CCTV; and
- recordings.

Governance is also blurry when it comes to 'sensitive data' that includes a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual orientation and genetic or biometric data. Normally, to process this data – the data subject has to give consent. However, as discussed, very high transparency parameters over data access and sharing goals and mechanisms should be in place and one-off consent could be insufficient when there is no follow-up on e.g. third party

[3] CNIL, référentiel relatif à la gestion des ressources humaines (2019) : https://www.cnil.fr/sites/default/files/atoms/files/referentiel_grh_novembre_2019_0.pdf

involvement. Employers can use such data in the realms of the employment contract and for their legitimate interests – which allows for more room for manoeuvring. As for data portability, it means that it is too narrow to capture all the data flows linked to workers. There needs to be regulatory guidance and oversight on the workplace dimension. This would allow setting criteria to see if competitive distortions are taking place.

In summary, the current system is limited to certain types of data, provides one-off consent as a legal basis and is not adapted to workplace challenges. It thus limits data portability for workers in terms of both data content but also recourse and control over data processing and sharing. The legitimate interests of employers can be widely interpreted and easily refer to intellectual property rights and other confidentiality clauses, meanwhile their control over data results in a more subordinate position for workers. This results in less bargaining power over wages and working conditions, limits to job mobility (if data portability is limited) which, overall feed into labour market monopsonies.

The special case of platform workers

Online platforms, which rely on on-demand or cloud workers, provide limited options to exercise the right to data portability. For these workers, switching platforms is important to profit from different pricing/ fees, working conditions and to build their reputational portfolio. As the OECD writes: "*personal ratings are usually lost when switching platforms (ILO, 2018[18]). Given that platforms de facto favour workers with good ratings, the loss of individual ratings represents a strong barrier to worker mobility, and may limit competition for workers across online platforms. Governments could therefore consider further interventions to enhance worker mobility across platforms such as regulating moneyless payments and facilitating data portability.*"[4]

If platforms are market-makers and service providers as they claim – not direct employers (in which case the previous section would apply) – workers should be able to control their online reputation (work history) and make use of data portability rights on an instant and regular (if not continuous basis). Let us not forget that such platforms are capturing working hours and sometimes moves (GPS tracking) of workers. Their business model is based on ratings and reviews that result in an online CV for workers attesting to the quality of their work and allowing them to get more clients. Therefore, if they are not able to fully access and use their data, it should be considered an anti-competitive non-poaching practice.

In the absence of enforcement of data portability rights and overall more transparency over the data collected by online platforms, workers are locked-in on specific platforms, as they have to choose between building reputational credit over possibly better working conditions or higher pay. Not many can work on multiple platforms with disparate (non-portable) profiles simultaneously and compete with those workers, who stay on the same platform. Hence, there is a lock-in effect. Balance of power is clearly tilting towards the platform that can impose fees, hours and working conditions on workers. All while refusing to assume employer responsibilities.

[4] Lane, M. (2020), "Regulating platform work in the digital age", Going Digital Toolkit Policy Note, No. 1, https://goingdigital.oecd.org/toolkitnotes/regulating-platform-work-in-thedigital-age.pdf

Enforcement of proper data portability rights is hence important. Indeed, some existing legislation – such as the GDPR – covers casual workers, agency workers and other independent contractors under the same rights as all data subjects. So, there is a legal basis to go from. If not enacted by companies, competition authorities should step in.

Otherwise, this has wider economic consequences since hours worked on online platforms might become an important data source for social protection, pension and training rights in the future. In a unionised context fees and pay, including of over-time work, can be negotiated and blockages (quotas) from attaining minimum wage hour ceilings set by platforms could be contested under better data transparency and portability systems.

Overall limitations of the current systems with regard to individuals

Data portability on its own and in regard to achieving greater competition faces a set of limitations also beyond the specific challenges raised by workplace data. As the European Consumer Organisation rightly points out: "*There are a number of notable differences between the way in which data portability operates as a right under data protection law, and its application as a remedy for competitive harms. The right to data portability only applies when particular legal basis in the GDPR are relied upon (contract and consent); it only provides to data 'provided' by the data subject (to the exclusion of inferred data and possibly observed data); the right only extends to personal data and may not apply where there is an interference with the rights and interests of others.*"[5] Especially, the fact that inferred and observed data (e.g. health data from movement trackers) is excluded, is problematic in the workplace context. Current rules also only foresee 'one-off' transfers and not provisions allowing for transfers on an on-going basis.

Another issue under the current system is that it is up to individuals to understand and use their rights – importantly, from the beginning when they provide 'consent'. From an individual perspective, it is already difficult to understand all settings and read all elements of terms and conditions. Not to agree means not being able to use services. To take (legal) action or contest shortcomings in the way data was provided is even more difficult. Not many individuals have exercised their data portability rights since the GDPR is in place. This is explainable with transaction costs that are quite high.

Many data controllers are not clear about their obligations either when it comes to data that relates to a group of people or when their intellectual property rights are at play[6]. Irrespectively, the reality is that many businesses will put "legitimate interests" as the legal basis for data collection. This allows for much wider data collection from the start and it can limit the scope of data portability.

Further, current provisions concern only data collection – not data processing, including of metadata, and uses of (aggregated) data sets including by third parties. Thus, the protections for data subjects are too limited to be truly meaningful in terms of data control and ownership.

---

[5] Idem, https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf
[6] Idem, https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability

These limitations significantly limit control over one's personally identifiable information. A lot of agency and self-determination is taken away from individuals and groups of people (workers) represented by the data in question.

Why data portability matters to competition

Data carries significant economic value for the one who controls and holds it – hence, without proper data portability and ownership rights, the data subject is at the short end of the stick. Portability could "*reduce the "lock in" effect that can inhibit competition*"[7] between firms and mitigate anti-competitive effects on workers' job mobility and working conditions. Data portability remedies could be used to fight on dominant market behaviour of data holders/ collectors/ third parties. However, "*especially the privacy law-based data portability of Art. 20 GDPR proves insufficient for solving competition and innovation problems caused by data access problems, due to a too narrow definition of the scope of portable data and the need for additional complementary regulations for making data portability effective. Therefore data portability rights outside of privacy laws, e.g., based upon the consumer data rights approach or in competition policy, can offer more flexible and effective solutions for fostering competition and innovation.*"[8]

More specifically on workplace data, the capture of information on employees' performance strengthens employers' unilateral control over working conditions. The trade union movement has serious concerns about the increasing ability of employers to pay wages below normal market conditions without losing their workforce. In previous submissions, the TUAC has repeatedly called on competition authorities to address labour market monopsonies resulting from either industry concentration and related market power, or deep asymmetries in employer / employee bargaining power[9].

The accumulation and misuse of workplace data clearly feed into labour market monopsonies. In particular, heightened control, interference with remuneration and the use of data to deter employees from looking for another employer all constitute anti-competitive practices designed to accentuate the asymmetry between employer and employee further.

Excessively unbalanced labour relations contribute to wage stagnation and artificially low levels of permanent employment. This harms the economy, the consumer and ultimately social welfare. There is an obvious need for policy discussions.

---

[7] Idem, https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability .
[8] Gill, Daniel and Kerber, Wolfgang, Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data (October 11, 2020), http://dx.doi.org/10.2139/ssrn.3715357
[9] Competition issues in labour markets – TUAC proposals to enhance protection against labour market monopsonies

Main points for policy making

Competition policies should provide remedies if data access and sharing provisions are not respected. This should especially be the case if one entity accumulates, uses and shares data in a way that brings them in a dominant market position – by locking data for their own profit, by creating systems for its storage and sharing or by making it uneasy available through complex consent mechanisms or non-standardised sharing formats. For now, there is a lack of regulation on data access and sharing, and difficulties to measure data value and to detect data capture.

Competition policies can do something else. It could start enforcing data access and sharing obligations, engage on the separation of data sets and similarly limit data use, if it goes against workers', citizen and consumer interests[10].

This means tackling excessive economic power of online platforms, who belong to the most prolific data holders, when it comes to personal, industrial and workers' data. Regulation of digital platforms that considers data access and sharing rights of data subjects, and limits data capture would help competition goals.
Data portability may be a distraction in the competition debate[11] and should not prevent broader (and likely more effective) actions by competition authorities against excessive market power (concerning data capture and network effects on online platforms) and by policy makers on data access and sharing regulations.

It is evident that there needs to be regulatory guidance and oversight on the workplace dimension. This would allow setting criteria to see if competitive distortions are taking place including excessively unbalanced employment relationships, and non-poaching/ non-compete practices. Trade unions have to have the right to bargain over 'collective data' and to benefit from comprehensive information and consultation rights on data collected, used and shared in the workplace context. Workplace data needs to be developed further as category in revisions of privacy laws and the development of data access and sharing regulations.

Current data portability rights limit control over one's personally identifiable information. A lot of agency and self-determination is taken away from individuals and groups of people (workers) represented by the data in question. Effective regulations in the data governance space tied to a specific group (consumers, workers) and/ or sectors that allow for a greater scope to portability, both in regards to the data concerned (not only personable data, but different data types including observed and inferred data) and to the way it is provided (e.g. on a continuous basis), could help.

What needs to be done, is expand the scope of data portability beyond personal data and resolve some legal and technical issues including:

[10] Idem, D. Gill & W. Kerber, http://dx.doi.org/10.2139/ssrn.3715357

[11] See amongst other, https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition

- Create industry standards for data transfers (including their formats), followed by an obligation for data holders to ensure that they are met (for now, they can refuse a request if it is not technically possible);
- Lower transaction costs for data subjects by allowing for collective data rights (intermediaries claiming access), more lean standards on transparency and on simplicity of consent mechanisms, and a move towards trustworthy data management systems.

There also need to be institutional frameworks underpinning it such as data trusts, ways to claim data collectively (e.g. trade unions for workers) and interoperable platforms. With international agreements on protocols, interoperability could help providing real-time, machine readable and standardised data formats to data subjects (and/ or their representatives).

In conclusion, without a more effective and broad regime on data exchanges, competition goals cannot be met on the current data portability rights alone. Without regulation on data access and sharing, and difficulties to measure data value, a competition approach against market concentration in the digital economy and non-poaching/ non-compete practices and labour monopsony practices in labour markets cannot be effectively dealt with either.