Data protection and the firewall

Digital technology use by labour authorities and migrant workers' rights

PICUM

This briefing has been written by PICUM (by Lilana Keith and Rahul Chawla, and edited by Michele LeVoy).

It is based on work commissioned by PICUM and carried out by the Central European Labour Studies Institute (CELSI) in 2023-2024, desk research and inputs from PICUM members. CELSI (S. Brunnerová and M. Kahanec) carried out extensive desk research and semi-structured interviews with labour inspectorate officials in Finland, Czechia, Ireland, Spain, and Belgium. Some content has been adapted from PICUM, 'Data protection and the firewall: advancing safe reporting for people in an irregular situation', 2020.

PICUM would also like to thank Aljosa Ajanovic from EDRi, and Jan-Frederik Keustermans of Cleary Gottlieb Steen & Hamilton LLP for his review and valuable inputs, noting that the views expressed in this publication do not necessarily reflect the position of Cleary Gottlieb.

Cover image: Getty Images

This publication was made possible with the kind support from:

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Union Programme for Employment and Social Innovation "EaSI" (2021-2027). Neither the European Union nor the granting authority can be held responsible for them.

Table of Contents

Introduction

In recent years, the substantial progress and expansion of technology have had impacts across multiple aspects of the world of work, including labour authorities' efforts to tackle undeclared work.

Some uses of digital technologies have the potential to improve employers' compliance with regulations; enhance the work of labour inspectors and their ability to check and verify information; and support migrant workers and associated organisations to claim their rights.

However, if the technologies are used without appropriate data protection safeguards, it raises profound concerns for the rights, security, and wellbeing of migrant workers, who occupy positions of heightened precarity within EU labour markets.

This briefing examines the use of technology and digital tools in labour authorities' monitoring and data management and the potential impacts on migrant workers' rights. It focuses on management of personal data gathered in the context of labour inspections or complaints, and includes some brief reflections on the use of some other digital technologies and tools.

It explains the key legal provisions, including those stemming from privacy and data protection laws such as the General Data Protection Regulation (GDPR), to set out recommendations on how to implement key safeguards while benefitting from technological advancements.

Use of digital technologies by labour inspection authorities

There are important calls to improve cross-government and inter-agency cooperation to tackle undeclared work, both within countries and transnationally (especially to tackle issues related to the posting of workers).[1] A key component of this is increased data exchange across labour, tax and social security databases.

However, data exchange regarding work permits and immigration status needs to be very carefully assessed and managed.

One of the most significant barriers for migrant workers – whether with precarious work permits or undocumented – to exercise their labour rights, is the risk of facing immigration enforcement if they are identified by labour inspection authorities. In most countries, the risk remains even if the worker actively files a complaint with the labour inspection for labour rights violations.[2]

Across the EU, labour inspectors often have to verify or cooperate with law enforcement regarding verification of validity of migrant workers' permits. Often, such cooperation automatically triggers reporting of undocumented workers to the immigration authorities.

Even if labour inspectors independently verify work permits, they often are required by law to report to law enforcement or do so in practice.[3] Even when the purpose is to impose sanctions on employers, data misuse is common, resulting in the sanctioning and targeting of workers.

Consequently, undocumented workers are often unable to engage with inspectorates. This fear reduces the effectiveness of labour enforcement by preventing inspectors from accessing testimonies and evidence necessary to uncover abuse and enforce labour standards and remedies.

Understanding data usage

A core issue is **what** personal data regarding workers is collected during labour inspections or when a complaint is filed, **how** that data is **processed** and **stored**, and whether and how that data is **shared** and/or **accessible** for other government authorities.

The key concern is to ensure that digitalisation of data management and efforts to increase cooperation do not make the use of workers' data for immigration enforcement purposes more frequent or more systematic.

[1] See e.g. Platform on Undeclared Work, 'Tackling Undeclared Work Across Europe: Effective Solutions for Policymakers', 2021.

[2] FRA, *Protecting migrants in an irregular situation from labour exploitation —— role of the Employers Sanctions Directive*, 2021; PICUM, *A worker is a worker*, 2020. However, in Belgium, for example, complaints made by undocumented workers outside the context of an inspection are treated confidentially.

[3] Analysis from the EU Fundamental Rights Agency (FRA) found that, of the 25 EU member states under the scope of the EU Employers' Sanctions Directive, 16 require the reporting of undocumented workers identified during inspections to the police or immigration enforcement authorities (though in France this is not always carried out), and in a further four (Italy, Lithuania, Luxembourg and Netherlands) reporting happens in practice. In Austria, Bulgaria, Greece, Spain and Sweden, reporting from the labour inspectorate is not required nor practiced, but in Austria the Financial Police (who carry out control on undeclared work) do report undocumented workers to the authorities. See FRA, *Protecting migrants in an irregular situation from labour exploitation —— role of the Employers Sanctions Directive*, 2021.

- While the use of digital tools is highly varied in different national contexts, labour inspectorates increasingly rely on interconnected data sources when carrying out inspections and related investigations.
- Digitalisation and digital data processing can exacerbate existing risks of immigration enforcement and trust deficits, and raise concerns regarding increased surveillance, data misuse and infringements of privacy.
- Labour inspectors are generally concerned with identification and protection of migrant workers but usually have legal or practical reporting obligations that are inadequately defined from a data protection perspective and can lead to immigration enforcement.
- Even if labour inspectors do not intentionally share information for immigration enforcement purposes, there are risks that, for example:
    - making a query in a data system to verify work permits can trigger an immigration enforcement action.
    - when inspectors access social security records, tax filings, or population registries, undocumented workers may become visible incidentally through their absence from certain databases and datasets.[4]
- Undocumented workers often fear approaching labour inspectors because of uncertainty regarding data flows, consequences of identification, and potential involvement of police or migration authorities. As trust is already weak, digital tools can serve to exacerbate fears. Workers may perceive drones, tablets, or databases as extensions of immigration control, discouraging them from disclosing exploitation or unsafe conditions.
- Inadequate and ineffective mechanisms for migrant workers to lodge complaints and access remedies, including due to risks of immigration enforcement, increase exposure and vulnerability to mistreatment and exploitation, and undermine the ability of authorities to effectively enforce labour standards.
- In cases where labour inspectors do not actively report to immigration authorities, having direct access to data on work permits to verify data without making any request to police or immigration enforcement can reduce the risks of inadvertently triggering immigration enforcement.
- Data protection rules should not be seen as a barrier to supporting people. It is possible to share personal data when in the person's interests and with appropriate safeguards, including that they have freely given specific, informed and unambiguous consent, where required.

[4] The convergence of multiple data streams can result in a form of 'surveillant assemblage', where technologies interlock to produce new knowledge about individuals, even without the intentional targeting of undocumented workers by labour inspectors. David Lyon, *Surveillance Studies: An Overview*, Cambridge: Polity Press, 2007.

Key reflections of other digital tools being explored by labour inspectorates

In addition to ICT systems, electronic databases and cross-database interoperability, some labour inspection authorities are also testing or using technologies including predictive analytics, drone surveillance, social media monitoring, web scraping and data-mining.

While use by labour inspectors is so far quite limited, **drones** have been used for some occupational safety and health or labour inspections of large worksites (e.g. construction sites, roadworks, agricultural fields/ greenhouses), to assist in locating workers, viewing areas that are difficult or dangerous to access, and planning inspection routes.[5]

- However, drone usage raises questions around protection of personal data and rules regarding biometric or identifiable imaging, particularly if a worker who appears in drone footage may be identified or otherwise exposed to immigration enforcement.
- Drone-use also risks deepening mistrust of inspectors by workers, as people tend to feel uncomfortable with drone surveillance in everyday life.

Social media monitoring and analysis is carried out by labour inspection authorities and civil society organisations, for example, to gather information about exploitative recruitment practices. This information can be used, for example, to provide targeted information to workers who may be at risk, or as evidence in complaints.

- However, processing of publicly available data still requires a lawful basis and must meet standards of necessity and proportionality.
- Serious ethical challenges arise when authorities carry out **online surveillance of migrant communities** that rely on informal digital spaces to exchange information about work opportunities and organise themselves, especially if this information could lead to a labour inspection and without the essential safeguards to protect workers.
- Online monitoring can also lead to disproportionate targeting of migrant-run businesses.
- While **automated web scraping and data mining tools** are not yet systematically deployed to gather large amounts of data from across websites and analyse the large datasets, they represent a potential future risk.

In some cases, the collection or processing of data, for example to carry out risk assessments, relies on **artificial intelligence**.[6]

- This includes risks of 'baking in' existing biases and prejudices from existing law enforcement data, meaning algorithmic management and AI use for labour inspection further targets migrants and racialised people.[7]

[5] EU-OSHA, Unmanned aerial vehicles: implications for occupational safety and health', European Agency for Safety and Health at Work, 11 September 2023.

[6] Under the EU AI Act (Regulation (EU) 2024/1689), AI systems used in employment and law enforcement are typically classified as high-risk. Providers of these systems have extensive obligations, including: implementing comprehensive risk management systems, strict data governance measures to minimise bias, transparency and providing for meaningful human oversight, and establishing quality management systems and monitoring post-market performance. However, migration authorities and law enforcement are exempted from some transparency and oversight safeguards. Deployers of these systems must ensure sufficient human oversight, conduct fundamental rights impact assessments, and offer individuals subject to certain decisions taken using such AI systems a clear and meaningful explanation of the role of the AI system in the decision-making procedure and the main elements of the decision taken.

[7] PICUM, 'A dangerous precedent: how the EU AI Act fails migrants and people on the move', 4 April 2024.

Key legal provisions

A wide range of rights as people, workers and when victims of crime

Migrant workers have a range of individual rights - as people, as workers, and when victims of crime. These rights stem from different legal frameworks at different levels, including several international and EU level instruments.[8]

Rights include, at a minimum and including when undocumented:[9]

- equal treatment regarding pay[10];
- healthy and safe working conditions;
- transparent and predictable working conditions;
- paid holiday leave and parental leave;
- protection from unfair dismissal;
- payment of due wages and salaries, including limited coverage by state guarantee mechanisms in cases of employer insolvency;
- payment of compensation and disability benefits in case of labour accidents;
- non-discrimination in opportunities and conditions at work, at least on grounds of gender, racial or national origin, sexual orientation, religion or belief, age, or disability; and
- privacy and data protection rights.

There are also specific protections and limitations on work for children and specific protections, services and compensation when victims of violence; criminal labour exploitation, forced labour and trafficking in human beings; or other crimes.[11]

Effective complaints mechanisms and labour inspections

For these rights to be meaningful in practice, workers must have access to effective and accessible complaints mechanisms and legal procedures, a right that is also set out explicitly in itself.

In particular, at EU level, the "Single Permit Directive" (recast, Directive (EU) 2024/1233[12]), the "Seasonal Workers Directive" (2014/36/EU), and the "Employers' Sanctions Directive" (Directive 2009/52/EC) all require that governments ensure that there are effective mechanisms and legal procedures for workers to lodge complaints against employers and claim redress. Third parties may engage either on behalf of or in support of migrant workers, with their consent.

[8] For details, see PICUM, Guide to Undocumented Workers' Rights at Work under International and EU Law, PICUM: Brussels, 2022.

[9] Ibid. The 'minimalist' list does not capture the extent of equal treatment provisions for migrant workers with different statuses, under, among others, the Single Permit Directive (recast, Directive (EU) 2024/1233), the Seasonal Workers' Directive (2014/36/EU), the Posted Workers' Directive (Directive (EU) 2018/957).

[10] The Employers' Sanctions Directive (Directive 2009/52/EC) also reaffirms explicitly undocumented workers' right to be paid at least the minimum wage and to payment of outstanding remuneration, for at least three months unless, a different duration of employment is proved (this presumption of at least three months' employment slightly shifts the burden of proof from workers to employers, at least once an employment relationship has been established).

[11] Ibid.

[12] Directive 2011/98/EU is repealed with effect from 22 May 2026.

Crucially, for labour inspections and labour complaints mechanisms to be "effective" for migrant workers, there must be no risk of facing immigration enforcement.

The ILO Labour Inspection Convention (C81) stipulates in Article 3 that the functions of the system of labour inspection shall be – primarily – to secure the **enforcement of the legal provisions relating to conditions of work and the protection of workers while engaged in their work**, such as provisions relating to hours, wages, safety, health and welfare, the employment of children and young persons, and other connected matters, in so far as such provisions are enforceable by labour inspectors.

Any further duties which may be entrusted to labour inspectors shall not interfere with the effective discharge of their primary duties or to prejudice in any way the authority and impartiality which are necessary to inspectors in their relations with employers and workers.

In addition, although there may be exceptions according to national laws and regulations, labour inspectors 'shall treat as absolutely confidential the source of any complaint bringing to their notice a defect or breach of legal provisions" (Article 15).

The ILO Committee of Experts has underlined that giving labour inspectors duties to enforce immigration law interferes with their primary duties to secure the enforcement of legal provisions relating to conditions of work and the protection of workers, and undermines their relationship with workers.[13]

A '**firewall**' separates immigration enforcement activities from public service provision and systems, such as healthcare, education, social welfare, labour inspection, or justice. Firewalls ensure that individuals can access these services and interact with competent authorities without fear of migration-related repercussions, such as arrest, detention, or deportation.

"Firewalls" are built on the premise that while states have the prerogative to enforce immigration laws, they also have obligations to protect fundamental rights and vital public policy objectives, such as community safety and health, that should not be undermined by political objectives on migration control.

Several other international and regional bodies, guidelines and studies are increasingly recognising this issue and recommending necessary safeguards are put in place.[14]

[13] Every year, the ILO Committee of Experts makes comments and recommendations to governments regarding the implementation of Articles 3(1) of Convention No. 81 and Article 6 (1) of Convention No. 129 and the rights of undocumented workers. In addition to the text of the Conventions, the Committee of Experts refers frequently to the 2006 General Survey on labour inspections. For example, between 2017 and 2022, recommendations were made to Jordan, Montenegro, Mozambique, Poland, Romania, Slovenia, Italy, Saudi Arabia, Hungary, Croatia, and Singapore. For further details of ILO resolutions, reports and recommendations on this issue, see PICUM, *Guide to Undocumented Workers' Rights at Work under International and EU Law*, 2022.

[14] A separation between labour authorities and immigration enforcement has also been strongly recommended by several UN, ILO, OSCE and Council of Europe bodies including, the UN General Assembly in e.g. the Global Compact for Safe, Orderly and Regular Migration, 73/195, 2020; as well as at EU level by the EC Communication on the application of Directive 2009/52/EC (COM (2021) 592 final, 29 September 2021); and the European Parliament resolution of 14 January 2014 on effective labour inspection as a strategy to improve working conditions in Europe (2013/2112(INI)). For further details, see PICUM, *Guide to Undocumented Workers' Rights at Work under International and EU Law*, 2022.

Data protection and privacy rights

The EU General Data Protection Regulation (GDPR) provides additional standards that reinforce the rights of undocumented workers. It sets out clear rules on the processing of personal data, with the aim of fostering greater transparency and accountability in the use of personal data.[15]

The GDPR:

- Imposes strict rules on the use of personal data by public authorities and private actors who are active within the European Union and/or monitor behaviour of individuals in the European Union.
- Strengthens and implements fundamental human rights to privacy and data protection, and protects individuals' rights without distinction based on nationality, place of residence, or residence status.
- Is grounded in rights already well-established under the EU Charter of Fundamental Rights (Articles 7 and 8) and the European Convention on Human Rights (Article 8), born out of atrocities committed during WWII and privacy right infringements during the Cold War.
- Responds to concerns about advancements in technology, the ease with which personal data can be collected and transmitted today, and the potential encroachment of big data on those rights.
- In most cases, forbids the sharing, transfer or exchange of personal data between service providers and immigration authorities for enforcement purposes as contrary to the bedrock principles of privacy and data protection.

See also PICUM's factsheets (2020):

Data protection and the firewall: Advancing safe reporting for people in an irregular situation

Data protection and the firewall: Advancing the right to health for people in an irregular situation

The GDPR establishes several key principles for the lawful processing of data.

Purpose limitation. The GDPR sets strict limits on the reasons for which data can be processed.

The principle of "purpose limitation" is a cornerstone of the GDPR,[16] and of data protection rights under the European Convention on Human Rights. It requires that personal data be collected for a specified, explicit and legitimate purpose, and not be further processed in a way incompatible with this purpose.

- If information is originally collected by labour inspectors or law enforcement authorities during a labour inspection, it should be for the purpose of enforcing standards relating to conditions of work and the protection of workers while engaged in their work.
- However, if this data is then processed to initiate immigration enforcement against the worker, it will be incompatible with the initial purposes for the processing – particularly given the private nature of the data and the potential far-reaching negative impact on an already vulnerable population of data subjects.
- This may constitute a GDPR violation, unless the processing is based on a clear, proportionate, and necessary legal derogation and, even in such circumstances, the affected individual must be notified of the subsequent incompatible processing in advance and be given an opportunity to exercise their data protection rights.

[15] Much on the content of this section has been adapted from PICUM, 'Data protection and the firewall: advancing safe reporting for people in an irregular situation', 2020.

[16] In particular Article 5, GDPR.

Data minimization. The GDPR prohibits processing of personal data beyond what is needed to achieve the purpose for which the data was collected.

The principle of "data minimization"[17] requires that personal data gathered must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected.

- Processing information about an individual's immigration or residence status will generally not be necessary for the purpose of enforcing standards regarding conditions of work, or following up on a complaint that has been lodged.
- Where it might be needed, for instance because of reporting requirements linked to imposing sanctions on employers, or implementing/making referrals into specific protections for undocumented workers or groups like possible victims of trafficking, the purpose limitation must be respected.

Data protection by design and by default. The GDPR requires that systems used to process personal data are designed to embed data protection rights and, by default, not process more personal data than what is necessary.

GDPR requires public authorities and private actors using automated systems to process personal data to:

- Put in place appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed, and all data processed is kept confidential and secure ("privacy by default").
- Design their systems to implement and embed therein the core data protection rights and principles ("privacy by design"), such as purpose limitation and data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the fundamental rights of individuals.

Sensitive data. The GDPR provides enhanced protection for sensitive data. This includes data revealing racial or ethnic origin, or, in certain circumstances, immigration or residence status.

Sensitive data[18] also includes personal data concerning trade union membership or health, and, in some cases, biometric or genetic data. Processing of sensitive data is prohibited unless a specific exception is available under the GDPR. It should generally only be processed with the explicit consent of the person, or in specific circumstances that are generally in the person's interests, with appropriate limitations and safeguards. This includes processing that is necessary in the context of employment, social security and social protection rights and obligations as per law and/or collective agreements or for the provision of health or social care or treatment.

Sensitive data can also be processed in specific circumstances when necessary for reasons of substantial public interest under national or EU law, but any such processing must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the individual.

- Information regarding the validity of work permits and immigration or residence status may qualify as sensitive data.
- In any event, the processing of such data gives rise to significant risks associated with disclosure or a data breach, and should therefore be subject to enhanced protection.

[17] In particular Article 5, GDPR.

[18] Article 9 GDPR.

Exceptions to the GDPR are narrow, recognising that data protection and privacy rights are fundamental rights.

- The GDPR allows for more specific rules to ensure protection of rights and freedoms in respect of the processing of employees' personal data in the employment context, as long as those rules include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights.[19]
- Governments can only deviate from the GDPR based on clear EU or national legislation that:
    - respects the fundamental rights and freedoms of individuals who would be affected by the exception;
    - safeguards a specific and pressing social need (such as national security, the prevention, investigation, detection or prosecution of criminal offences or other important objectives of general public interest);
    - is sufficiently clear and precise to be foreseeable to affected individuals; and
    - is necessary and proportionate in a democratic society.
- **Immigration enforcement that interferes with the enjoyment of fundamental rights at work is unlikely to meet this high threshold to deviate from the GDPR principles.**

[19] Article 88, GDPR.

Final remarks

With the EU increasingly focused on deregulation as a means to be competitive in global markets, essential legal frameworks to protect people and planet where the EU had previously stepped out as a leader are at risk.

It will be crucial to protect the 2018 General Data Protection Regulation (GDPR), which remains all the more relevant as the use of technologies and Big Data, including artificial intelligence (AI), continue to evolve and penetrate all aspects of our lives.

It is not red tape; the GDPR remains a powerful legislative framework that reinforces everyone's right to the protection of their personal data by improving transparency and accountability in the processing of personal data and strengthening individuals' control over how their data is used.

The GDPR has particular relevance for migrants' rights given the growing large-scale use of data processing to enhance migration control and policing.[20]

Appropriate safeguards to protect undocumented migrant workers during a labour inspection or complaint are essential to promote effective multi-stakeholder cooperation and enforcement of labour standards and rights for all workers.

[20] Statewatch, Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status, 2019.

Recommendations

1. **Develop data management, sharing and confidentiality protocols to make data protection measures and GDPR compliance robust and applicable in practice for labour inspectors, in their collection and processing of workers' personal data and use of digital tools.**

   Such protocols should:

   - Stipulate which personal information can be shared, with which enforcement agencies and other entities, and **for which purpose** (e.g. application of employment law, detection and investigation of labour violations).
   - Clearly delimit the access and use of the data by other enforcement agencies, including police.
   - Ensure that personal data collected in the context of a labour complaint or inspection is strictly protected under the principle of **purpose limitation**, such that it cannot legally or technically be used for immigration enforcement purposes.
   - Address data sharing both within the country and transnationally among EU member states.[21]
   - Include provisions for individuals to exercise their **data subject rights**, including the rights to request, verify, correct and, where appropriate, delete their personal data.
   - Include processes for sharing information when in the interest of workers and with their informed consent, to facilitate effective support, referral and enforcement of rights and obligations.
   - Mandate adequate and auditable prior **data protection impact assessments** and, where artificial intelligence is used, fundamental rights impact assessments, as required under GDPR and the AI Act.
   - Provide an even higher level of protection for **highly private or sensitive data**, including data on ethnicity, immigration or residence status, and work permit data.
   - Ensure these rules and guardrails are operationally and technically embedded in the systems and software used by authorities, ensuring compliance with the **privacy by design** principle.
   - Be supported by mandatory training.

2. **Strengthen collaboration between labour inspectorates, trade unions and non-governmental organisations and associations working with migrant workers to facilitate access to complaints mechanisms and redress with due safeguards.**

3. **As labour authorities increasingly experiment with and integrate digital technologies and tactics into their work, conduct in each case fundamental rights impact assessments.**

[21] If any data sharing outside the European Union were to be allowed, it would need to be subject to further specific restrictions.

PICUM

For undocumented migrants,
for social justice.

Rue du Congres 37,
1000 Brussels, Belgium
+32 2 883 68 12
info@picum.org
www.picum.org