TOP 10 PRINCIPLES
FOR WORKERS' DATA PRIVACY AND PROTECTION

About UNI Global Union

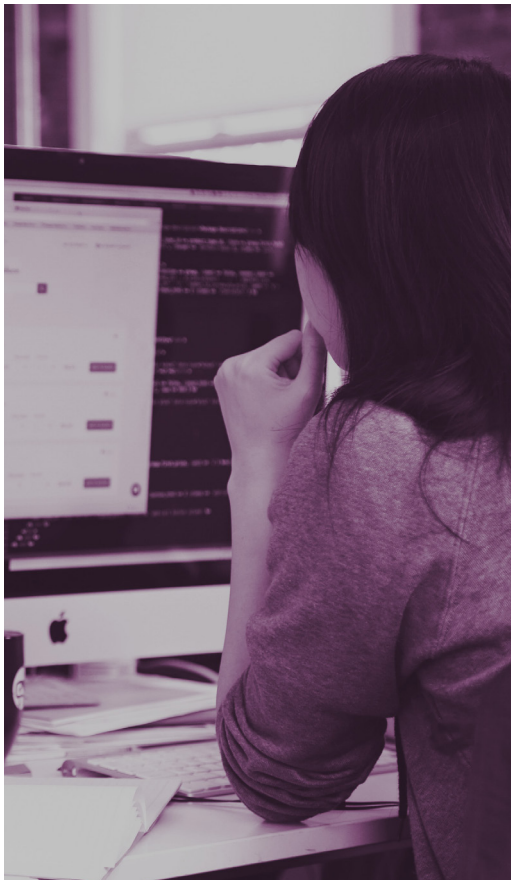
UNI Global Union, based in Nyon, Switzerland, represents more than 20 million workers from over 150 countries in the fastest growing sectors in the world – skills and services. The Future World of Work has been one of UNI Global Union's key priorities in recent years. With a leading voice on the global political and industrial stage, UNI seeks innovative policies and partnerships to ensure an empowering digital future for all. With an urgency of now, UNI calls on all companies and governments to engage with the union movement, to co-create a just transition to a future of decent work. From the design of new technologies, AI and algorithms, to the impact on the end-user, ethical and social considerations must be made that put people and planet first.

UNI Global Union
8-10 Av Reverdil
1260 Nyon
Switzerland

www.uniglobalunion.org
www.thefutureworldofwork.org

TABLE OF CONTENTS

INTRODUCTION



Whilst data, big data and data sets are becoming increasingly used by companies to inform managerial decisions, workers' data protection and privacy rules hardly exist. This document provides 10 operational principles that address this imbalance. By offering concrete demands to corporate data gathering and use, these principles will empower workers and ensure an ethical and sustainable use of data.

There is a definite urgency of now. Action is required to safeguard workers' interests and maintain a healthy balance of power in workplaces. The 10 principles provided in this document are developed by UNI Global Union for this purpose.

Data has been termed the new gold. It is traded, analysed and used in marketing, advertising and human resource management. It is also the building blocks of artificial intelligence and algorithms. By 2030, it is estimated that 15-20% of the world's combined GDP will be based on data flows. It too is the very foundation of the myriad of new businesses and services that are increasingly individualising many aspects of our economy and society, namely the platforms of the so-called gig economy.

As citizens, we daily leave a data trail behind us: from what we search for on Google, to the apps on our mobile phones, from rides we take in taxis, flats we rent, from what we buy, to our loyalty cards, our health records, phone calls to customer services. Not to mention the places we visit, emails we send, Facebook friends we have and tweets we write. Doing all of this provides companies with data – about us and our network of friends. Data is simply the biggest gift we don't realise we are giving away.

We also provide data as workers—our CVs, our biometric data such as our fingerprints or iris scans, and the abundant data mined on us as employers monitor our workflows. Data, or rather sets of data from within and outside of the company, are also used by management in human resource decisions. Who gets hired? Who gets promoted? Should someone be fired

or cautioned? Are the workers productive today and if not, why not? The application and use in companies has even spurred the question whether data is taking the human out of human resources.

But who actually owns the data we provide? And what data exists 'out there' about you and me? These two questions are hard to answer. The CEO of LinkedIn has said that the vast majority of the world's data is ultimately in the hands of Big Tech: Google, Facebook, Amazon, Microsoft and Apple. A recent Twitter feed claimed that for 1000 USD you can get a company to provide you with any and all information possible about a person. We know that certain companies are experts in mining data and selling it on to others so they can manipulate our points of view. By targeting us with particular stories and paying fake Twitter and Facebook accounts to spread opinions, we now know that both the US election and the Brexit vote results were influenced and manipulated using data.

In Japan the government is preparing to roll out so-called databanks. Public offices that will help citizens decide on what data they want to make available. In Estonia, a country with one of the world's most comprehensive e-government systems and data use, citizens' data is subject to rigorous legal principles empowering the individual to decide what data is available and how it can be used. Yet many countries are lagging behind on providing citizens with a clear and transparent way of knowing what information exists, and not least on providing citizens with a means to control it.

Whilst data protection and privacy laws do exist in various forms in many countries, the data derived from monitoring workers is not specifically covered by these laws. UNI Global Union is cooperating with the global organisation IEEE to create a global standard for transparent employer governance of employee data. It is also vital that trade unions seek to implement, through company and/or sector collective agreements, workers' data rights and protection provisions. Without said provisions, the balance of power in companies will forever be tipped into the hands of data-informed unilateral managerial decisions. Given the relative ease of combining data from many sources, without a say and influence over what data is used, and how, workers will be extremely disadvantaged. Indeed, workers' data rights and protection can be claimed to be the next frontier for unions as the digital economy takes form.

> "Workers and their union representatives must have the right to access, influence, edit and delete data that is collected on them and via their work processes."

Given the importance of workplace data, UNI Global Union demands that workers and their union representatives must have the right to access, influence, edit and delete data that is collected on them and via their work processes.

This document operationalises this key demand and breaks it down into 10 specific action points.

01

WORKERS MUST HAVE ACCESS TO, AND INFLUENCE OVER, DATA COLLECTED ON THEM

Workers must have the right of access to data collected on them, including the right to have data rectified, blocked or erased.

This includes:

A | That consent cannot, and should not, be the legal basis of data processing at work.

B | A worker must be able to obtain, upon request, at reasonable intervals and without excessive delay, confirmation of the processing of personal data relating to him or her. The communication must be in an intelligible form, include all information on the origin of the data, as well as any other information that the controller is required to provide to ensure the transparency of processing.

C | A worker must have the right of data portability, i.e. the right to move rating and ranking systems from one platform to another.

D | In accordance with domestic law and practice, or the terms of collective agreements, personal data may be communicated to the workers' representatives, but only to the extent that such data are necessary to allow them to properly represent the workers' interests or if such data are necessary for the fulfillment and supervision of obligations laid down in collective agreements.

02

IMPLEMENTING SUSTAINABLE DATA PROCESSING SAFEGUARDS

For all forms of data processing, employers must respect the following safeguards. In particular:

A | Inform workers clearly and fully before the introduction of information systems and technologies enabling the monitoring of their activities. The information provided should be kept up to date and must take into account principle 3 below. The information must include

the purpose of the operation, the preservation or back-up period, as well as the existence of the workers' rights of access and rectification and how those rights may be exercised. This safeguard includes any changes to monitoring purposes and systems;

C Take appropriate internal measures relating to the processing of that data and notify workers in advance. This includes running a privacy impact assessment when technologies can lead to high risk for individuals, such as in case of potential profiling or decisions taken by means of automated systems (see principle 5 below).

D Consult workers in circumstances where a possibility of infringement of workers' right to respect for privacy and human dignity is suspected. Respect in said cases the workers' right to call for a veto of said data monitoring until the employer can prove in writing and subsequently receive the workers' approval that the workers' right to respect for privacy and human dignity is fully respected (see principle 5);

03

THE DATA MINIMALIZATION PRINCIPLE MUST BE APPLIED

The principle is that employers may only:

> "Collect data and only the right data for the right purposes and only the right purposes, to be used by the right people and only the right people and for the appropriate amount of time and only the appropriate amount of time."

Employers should develop appropriate measures to ensure that they respect, in practice, the principles and obligations relating to data processing for employment purposes. This includes the principles of proportionality and subsidiarity: that data collection must be limited to what is necessary to achieve the objectives of the collection in question, i.e. that the content and form of the action must be in keeping with the aim pursued.

At the request of the supervisory authority, employers must be able to demonstrate their compliance with such principles and obligations. These measures should be adapted to the volume and nature of the data processed, the type of activities being undertaken, and must also take into account possible implications for fundamental rights and freedoms of workers.

04

DATA PROCESSING MUST BE TRANSPARENT

A | Information concerning personal data held by employers must be made available either to the employee concerned directly or through the intermediary of his or her representatives, or brought to his or her notice through other appropriate means.

B | Employers must provide workers with the following information:

> THE CATEGORIES OF PERSONAL DATA TO BE PROCESSED AND A DESCRIPTION OF THE PURPOSES OF THE PROCESSING;
>
> THE RECIPIENTS, OR CATEGORIES OF RECIPIENTS OF THE PERSONAL DATA;
>
> THE MEANS WORKERS HAVE OF EXERCISING THE RIGHTS SET OUT IN PRINCIPLE 1 WITHOUT PREJUDICE TO MORE FAVOURABLE ONES PROVIDED BY DOMESTIC LAW OR IN THEIR LEGAL SYSTEM;
>
> ANY OTHER INFORMATION NECESSARY TO ENSURE FAIR AND LAWFUL PROCESSING.

C | A particularly clear and complete description must be provided of the categories of personal data that can be collected by Information and Communications Technologies (ICTs), including video surveillance and their possible use.

D | The information should be provided in an accessible format and kept up to date. In any event, such information must be provided before an employee carries out the activity or action concerned, and made readily available through the information systems normally used by the employee.

05

PRIVACY LAWS AND FUNDAMENTAL RIGHTS MUST BE RESPECTED THROUGHOUT THE COMPANY

This includes respect for all global and regional conventions on human rights, including;

- THE UN'S UNIVERSAL DECLARATION OF HUMAN RIGHTS
- THE INTERNATIONAL LABOUR OFFICE'S 1997 CODE OF PRACTICE ON THE PROTECTION OF WORKERS' PERSONAL DATA,

The employer must also:

A | Show respect for human dignity, privacy and the protection of personal data should be safeguarded in the processing of personal data for employment purposes, notably to allow for the free development of the employee's personality as well as for possibilities of individual and social relationships in the work place

B | Guarantee that communication is lawful and does not include defamatory or libelous statements,

C | Ensure that enterprise communication facilities are not used as a means of sexually harassing, or spreading offensive comments meant to discriminate.

The employer can require a disclaimer when workers are communicating internally and externally to the effect that the views expressed are those of the author alone and not those of the enterprise.

06

WORKERS MUST HAVE A FULL RIGHT OF EXPLANATION WHEN DATA IS USED

This principle refers to decisions taken by management that include the sourcing of data from within as well as outside the company. For example, in internal and external recruitment processes, workers must have the right to know on what basis a decision has been made. This is to safeguard workers against discriminative decisions based on data predictions not least regarding health.

The employee must be informed when important decisions are taken based on internal as well as external data.

07

BIOMETRIC DATA AND PERSONALLY IDENTIFIABLE INFORMATION (PII) MUST BE EXEMPT

The collection and further processing of biometric data should only be undertaken if there are no other less intrusive means available and only if accompanied by appropriate safeguards, including the additional safeguards provided for in principle 2.

The processing of biometric data and other PII must be based on scientifically recognised methods and should be subject to the requirements of strict security and proportionality.

08

EQUIPMENT REVEALING EMPLOYEES' LOCATION

Equipment revealing workers location can only be introduced if it proves necessary to achieve the legitimate purpose pursued by employers; their use must not lead to continuous monitoring of workers. Notably, monitoring cannot be the purpose, but only an indirect consequence of an action needed to protect production, health and safety or to ensure the efficient running of an organisation. Given the potential to violate the rights and freedoms of persons concerned by the use of these devices, employers must ensure all necessary safeguards for the workers' right to privacy and protection of personal data, including the safeguards provided for in principle 2.

In accordance with principle 3 on data minimalization, employers must pay special attention to the purpose for which such devices are used. Employers must apply appropriate internal

procedures relating to the processing of these data and must notify the persons concerned in advance about them.

09

A MULTI-DISCIPLINARY, INTER-COMPANY DATA GOVERNANCE BODY SHOULD BE ESTABLISHED

A multi-disciplinary inter-company data governance body should be established to govern data formation, storage, handling and security issues. This includes provisions that all representatives on the body, including shop stewards, receive appropriate data training to be equipped to work with companies in upholding and withholding a sustainable data protection policy.

10

ALL OF THE ABOVE SHOULD BE IMPLEMENTED IN A COLLECTIVE AGREEMENT

The above principles should be implemented and enforced through company or sectoral collective bargaining. In the absence of said bargaining, the employer should establish a governance body in accordance with principle 9.

Sources:

This document has drawn inspiration and insights from the following key documents:

GDPR
(http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf)

COE(2015) Recommendation CM/Rec(2015) of the Committee of Ministers to member States on the processing of personal data in the context of employment https://www.apda.ad/system/files/cm-rec-2015-5-en.pdf

(2017): ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 2/2017 on data processing at work http://ec.europa.eu/newsroom/document.cfm?doc_id=45631