



THE WHY NOT LAB

# The Data Lifecycle at Work - Ensuring Collective Data Rights

A Guide - developed by Dr. Christina J. Colclough, The Why Not Lab

# Negotiating for collective data rights for workers

- 1 Data protection - especially in the GDPR zone - can be helpful for workers. Get to know, and use, the relevant GDPR articles
- 2 Bridge regulatory gaps and management failures by negotiating the Data Life Cycle at Work
- 3 Practice your arguments and prepare for counter arguments. How will you defend your demands?
- 4 Strong data rights is a must to prevent the obscure commodification of workers, and to break the “monopolisation of truth” currently determined by those who hold the data.



**Step 1**

# Use the GDPR

## 1 **GDPR article 5(c) - Principles of Data Processing**

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

## 2 **Art 13: Information to be provided**

The collection of data

How the company plans to use the data

The reason why they are collecting the data

Can the purpose of collecting the data be achieved without collecting the data?

How long will the data be stored to fulfill the purpose?

Is the data periodically reviewed in relation to the above 5 points and deleted if required?

## 3 **Art 15: Rights of Access (incl data subject access request)**

## 4 **Art 35: Data Protection Impact Assessments (DPIA)**

Article 29 Working Party: employers should consult with a "representative sample of employees" when conducting these. Do they?

## 5 **Art 80: Representation**

in effect giving unions the right to represent their members in claiming their GDPR rights.

## 6 **Informed consent not a legal basis for processing data at work**

[Article 29 Working Party Opinion 2/2017 on data processing at work](#)

## 7 **Art 88 Processing in the context of employment**

Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context

## 8 **Art 22. Automated individual decision-making, including profiling**

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

## Art 13: Transparency

If employers followed this article, unions would know what digital technologies are being used.

## Art 35: DPIA

Article 29 Working Party: employers should consult with a “**representative sample of employees**” when conducting these.

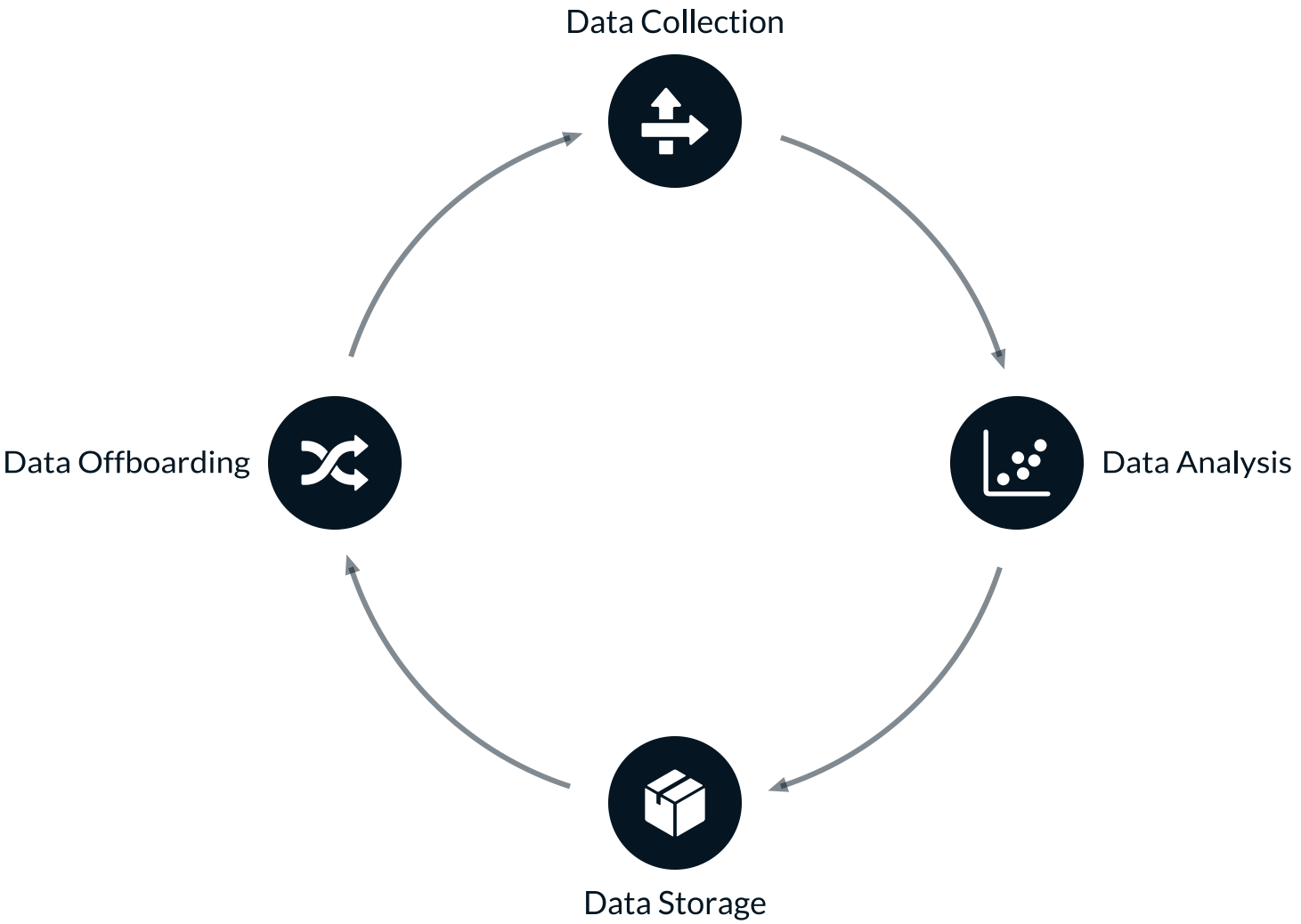
From UK: [ICO](#)

If the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), you should design a consultation process to seek the views of those particular individuals, or their representatives.



**Step 2**

# Negotiate the Data Lifecycle at Work



## Data Collection:

Sources? Union access to and knowledge of? Rights to refute/block?



## Data Analysis

Used in productivity & Human Resources. What rights do workers have to access these data and the insights/inferences drawn? Can they object to these etc?



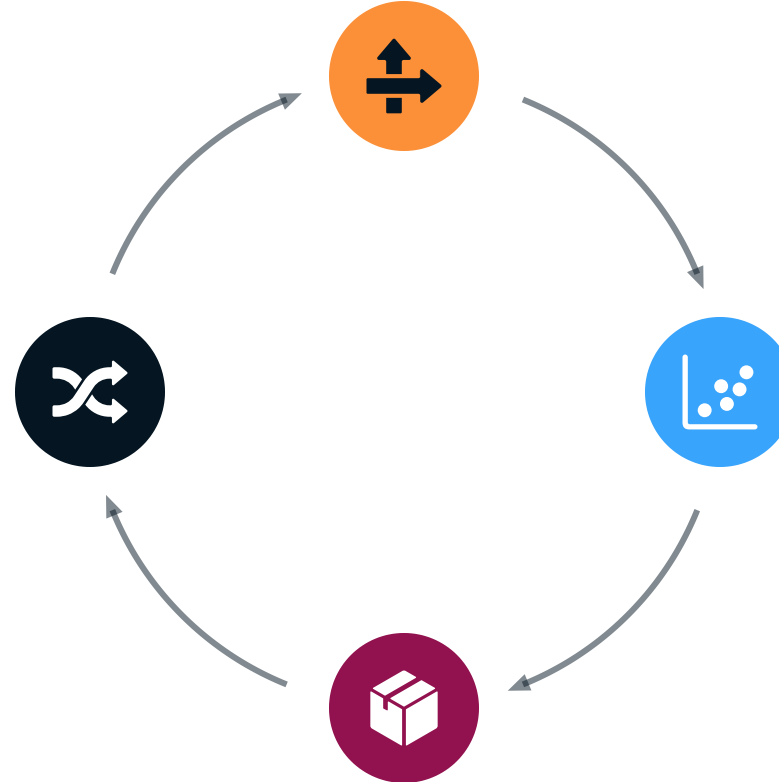
## Data Storage

Servers - where? Who has access?  
Under what jurisdiction?  
Think here WTO/e-commerce discussions



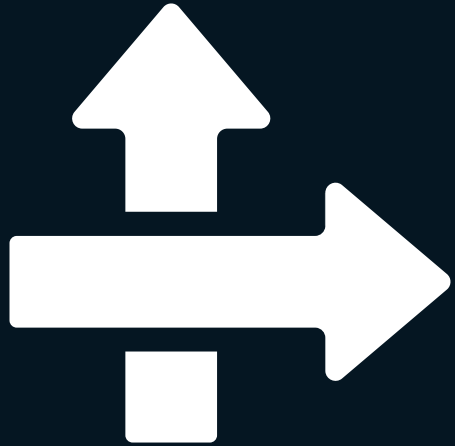
## Data Offboarding

Is data sold? To whom? Deleted? Can workers deny/block who it is sold to? This includes data sets, statistics, inferences.





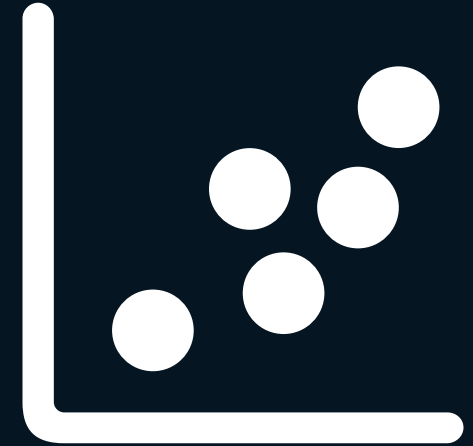
# 1. Data Collection Phase



- The data-collection phase asks what are the internal and external collection tools, the sources of the data, whether shop stewards and workers have been informed about the intended tools and whether they have the right to rebut or reject them?
- Much data extraction is hidden from the worker (or citizen) and management must be held accountable.

## 2. Data Analysis Phase

- In this phase unions must ask how the data is used and for what purposes? What rights do workers have to access these data and the insights/inferences drawn? Can they object to these etc?
- Unions should set redlines for what the data can be used for and what not





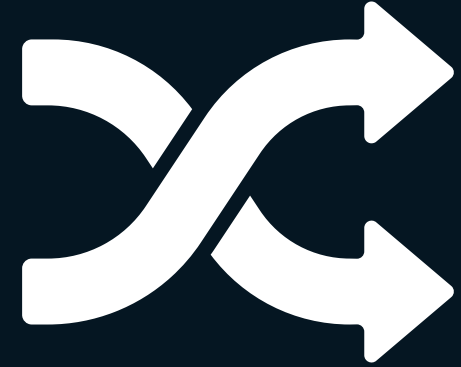
**Read more about  
E-commerce  
negotiations, also  
know as Digital  
Trade negotiations  
[here](#)**

### 3. Data Storage Phase

- Workers should know under which jurisdiction their data is stored.
- Especially relevant if e-commerce negotiations within, and on the fringes of, the World Trade Organization, are actualised. This would entail data being moved across borders to what we can expect would be areas of least privacy protection. They would then be used, sold, rebundled and sold again in whatever way corporations saw fit.

## 4. Data Offboarding

- 1 Here workers should ask, what happens to the data after it is used?
- 2 Is it deleted?
- 3 Or are data sets and inferences sold or transferred to third parties?
- 4 Unions should negotiate much better rights to know what is being off-boarded and to whom, with scope to object to or even block the process.




### TIP

**FSU Ireland has negotiated an agreement that forbids management to sell data sets that include workers' personal data**




# Dr. Christina Colclough

Expert Future of Work & Politics of Technology

 [christina@thewhynotlab.com](mailto:christina@thewhynotlab.com)

 [@cjcolclough](https://twitter.com/cjcolclough)

 [www.thewhynotlab.com](http://www.thewhynotlab.com)