

## The Data-Protection Toolbox

### ***3x10 recommendations on how to support employment federations and businesses implement data-protection in their organisations***

This World Employment Confederation Toolbox consists out of recommendations for national employment industry federations and their members on the General Data Protection Regulation (GDPR). This new EU Regulation goes into force on the 25<sup>th</sup> of May 2018 and provides the conditions under which personal data can be used by businesses (and others). As the employment industry deals with people it inherently processes a lot of (digital) personal data. The GDPR will therefore impact the industry significantly. This toolbox has been developed by the World Employment Confederation with the support of the internal taskforce of experts (see below).

The toolbox consists out of three sections:

1. **10 Recommendations for board members, CEO's and managing directors of National Federation members of the World Employment Confederation.**
2. **10 Suggestions for services to support members of National Federations understand and implement the GDPR.**
3. **10 recommendations for the members of the National Federation.** (*which can be translated into your own respective language*)

The Toolbox is expressly a guidance for policy. It is in no way a comprehensive technical overview of the GDPR or legal advice, neither is it meant to be. General information about the GDPR is widely available (online), and (as is addressed in this toolbox) it is first and foremost of importance to attract specialist advice on the national and corporate level.

Yet, a quick overview of ***useful links & documents*** about the GDPR is provided beneath:

- The [General Data-Protection Regulation](#) on the website of the European Union
- The [European Commission website on the Protection of personal data](#)
- The [website of the European Data Protection Supervisor](#). Which holds good general information about the background of the GDPR and the supervisory priorities of the EDPS
- The [website of the Article 29 Data Protection Working Party](#) (WP29) which includes the adopted Opinions, Recommendations and Guidelines of the WP29 on the implementation of the GDPR.
- The [WP29 Opinion on Data Processing at Work](#)
- An [overview of all national data-protection supervisory authorities](#)
- The [website of the International Association of Privacy Professionals \(IAPP\)](#) which has a very good news and (paid) database & resources [on the GDPR](#)

#### ***World Employment Confederation Data-Protection Taskforce***

The World Employment Confederation has assembled an expert taskforce on data-protection. This taskforce consists out of the data-protection experts from our corporate and national federations members. The taskforce advises other bodies of the World Employment Confederation, including the Board on issues surrounding data-protection and digitalisation. By participating experts have a unique opportunity to learn and discuss about data-protection in the employment industry. This contributes to their professional development which also benefits the organisations they represent..

Should your data-protection expert wish to join the Data-Protection Taskforce contact Jochem de Boer ([jochem.deboer@wecglobal.org](mailto:jochem.deboer@wecglobal.org)) or Michael Freytag ([michael.freytag@wecglobal.org](mailto:michael.freytag@wecglobal.org)) at the Head Office of the World Employment Confederation.

## **10 Recommendations for board members, CEO's and managing directors of national federations members of the World Employment Confederation**

### **1. Accept reality: the regulatory protection of personal data is here to stay.**

**In fact, most of it has been around quite a while!**

In a world where personal data can move anywhere and be used and abused anywhere, specific regulation should be no surprise. The regulatory protection of personal data is not going away, neither is the GDPR. In fact, chances are that large chunks of its material obligations already applied to you and your constituents under previous national legislation. The best way to deal with personal data-protection regulation is to accept its existence and turn it into a business opportunity and added value for jobseekers, workers and clients.

### **2. Change the narrative**

Personal data is not the 'new' gold in the employment industry. Knowledge and data about workers' and jobseekers' labour market potential have always been the gold. What is relatively new is that the use and analytics of personal data is ever more digitalised. As new data-flows arise and technology become more apparent and data-intensive, the risk of data falling into the wrong hands rises as well. Protection of this data is therefore not a cumbersome red-tape compliance issue, as it is happily framed expensive lawyers and advisors, it's an issue of protection of one's services and business.

More importantly digitalisation of the labour market is the source for future growth of the employment industry. The quality of labour market matching can exponentially be improved through digital tools. As the employment industry inherently deals with people, it inherently deals with personal data in these digital tools. Getting the efficiency and protection of this personal data right within innovative Human Resource Technology, is a crucial competitive advantage. Being smart with personal data is a business opportunity!

Finally, GDPR creates a framework through which to process data. It does not ban the use of personal data: it provides the conditions for use! This means that personal-data one needs for their business, will most probably still be allowed to process! The GDPR merely forces to assess and document whether or not the use is necessary and/or allowed and properly take care of personal data. That question is not just a compliance one, it's a business one as well.

### **3. Create Urgency, Awareness and Tools**

There are numerous ways and tools of supporting your members in improving their compliance with the GDPR. Further suggestions for this are given in Chapter 2 and 3 of this Toolbox.

But it starts by creating the awareness and urgency of using these tools. This means turning it into a federation priority and addressing the issue of data-protection and the GDPR in meetings with members. The strategic reason for doing so is threefold:

1. First of all, personal data protection is in its core about trust. Data-breaches or bad press on bad data-protection with one employment agency affects the sector as a whole. If personal data is not properly protected in the sector trust of workers, clients *and* stakeholders (see below) in the sector deteriorates.
2. Secondly, GDPR is a level playing field issue as it is a compliance issue. GDPR Compliance comes at a cost and employment agencies should compete by processing personal data in a compliant way.
3. Finally, building understanding and knowledge of data-protection amongst employment services allows for the recognition as an expert amongst stakeholders and policymakers, but also to recognize regulatory opportunities. Being recognized as expert creates the position to lobby for beneficial national data-protection legislation or GDPR code of conducts (see below) on the national level (which the GDPR apply allows for).

#### **4. Lead from the top and support compliant behaviour**

Getting compliant with the GDPR is no easy task for individual businesses big and small. And it most certainly will change business-models and how individuals have worked in the past. This means that getting compliant requires change-management throughout the organisation. Those people implementing the change need to be able to count on support from senior management and industry's leadership.

Finally, the GDPR does apply to the federation as well. Reserve budget for adjusting. The adjustment might improve understanding of the GDPR as well for the staff working for the federation.

#### **5. Get smart on 'data-minimisation'**

Every piece of personal data concerns risks and costs. It needs to be secured, needs to be kept up to date, could get lost, breached or be used for the wrong purposes, and it always needs to be at the disposal of the person who's data it concerns (the data-subject). To mitigate those risks and costs for employment agencies, stimulate data-minimisation amongst your members.

Data-minimisation means that personal data can only be processed if they're adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (art. 5.1.c GDPR). By assessing which personal data are truly relevant for the business model one can get smart on the use, risks and costs of the processing of personal data.

#### **6. 'Privacy by Design'**

When developing new services and business models, it's better (and cheaper) to take data-protection into account from the start, than to be crippled by it after the launch. To reduce the impact of data-protection regulation for employment agencies stimulate 'privacy by design' amongst your members. Of course, this also contributes to compliant behaviour in general.

## **7. Improve your individual and organisation data-protection maturity and professionalism**

The GDPR is a peculiar regulatory framework which requires a new 'lens' to look at existing processes of labour market intermediation. Where personal data was not seldom perceived as a means to an end in the past, to be dealt with pragmatically and flexible, it's protection has now (even more firmly) become an end in itself. For those specialised in (commercial) labour market intermediation or regulation, adapting to the logic of the GDPR is not so straightforward. Especially when it concerns high costs or changing business-models. To support employment agencies stimulate them and/or provide opportunities to increase understanding, maturity and professionalism on the issue of data-protection .

Data-Protection touches all kinds of topics. It involves most things employment industry associations and their members do. It ranges from collective labour agreements, fiscal issues, research to labour law, stakeholder management and social security. Given the inherent role of personal data use in the employment industry, it is important that (1.) staff of the association are aware of the possible impact of data-protection on their respective portfolio's and (2.) that the issue of data-protection is put on the agenda of board meeting regularly to keeping improving awareness and capacity.

Training and awareness about protection of personal data is just as important to the staff and consultants of the employment industry working in their daily business with jobseekers, (agency-)workers, clients and public employment services. Building their capacity in this field will also reduce collective risks and create smart solutions for data use.

## **8. Engage policymakers and regulators**

As discussed under point 2, the GDPR creates a framework for the use of data. This framework allows for ample national legislation on the use of personal data within EU members states. Maintaining and creating a beneficial regulatory framework is therefore not just a European affair. National policymakers (and social partners when agreeing to a collective agreement) have room to adequately balance labour market functioning and the protection of personal data.

Secondly, the GDPR will change at some point. In fact, it is set to be reviewed by 25 May 2020 and every four years thereafter. *These are lobby windows of opportunities for the employment industry* to get issue across to policy makers! To make use of these windows the industry and their public affairs representatives needs to know what the issues are and how they can be resolved. By better understanding the data-protection framework, solutions can be put forward that benefit the industry and take into account the protection of personal data.

## **9. Data-Protection rules also apply for the federation**

Complying with data-protection rules is as much a federation's issue, as it is an issue of the federation members. This means federations themselves will need to start mapping out the processes within their organisation in which they process personal data and determine they have legal grounds for it. Again, do not be scared by this exercise. Crucial is to start working on it, as

those parties that did not do anything with data-protection rules, are sure to receive no kind of leniency of enforcement bodies.

## **10. Develop a GDPR Code of Conduct (optional)**

The GDPR allows for the creation of a sectoral GDPR Code of Conduct (CoC). These CoC's determine the sectoral data-protection framework under which certain sectoral processes and practises can take place. The CoC has to be validated by the national supervisory authority. The benefit of such a CoC is that it creates a regulatory framework that is tailor-made to the use of personal data for the industry, which improves legal certainty. The downside is that the CoC requires independent self-regulatory certification and enforcement to be validated. Setting this up can be a costly and intensive exercise. Luckily, several National Federation members of The World Employment Confederation-Europe have are in this process and experiences are shared in the Data-Protection Taskforce of the World Employment Confederation.

## **10 Suggestions for services to support members of national federations to understand and implement the GDPR.**

Beneath are 10 tools for national federations of the employment industry to support the implementation of the GDPR amongst their members and create added value by providing services. Some of these services have already been created by National Federations. Should you seek support in further developing one or more of these tools, do not hesitate to contact the Head Office. They can refer you to other members who have relevant experience with particular tools.

### **1. Dedicated information meetings**

Use the general meetings with members (such as the general assembly) to address the GDPR and its technicalities, consequences ad/or policy initiatives.

### **2. Training courses for internal employees**

Develop and organise seminars, workshops, etc. on the GDPR for the people working in the employment industry. As an option identify the various roles within recruitment and employment agencies and tailor specific courses for each role.

### **3. Internal data-protection taskforce**

Assemble a sectoral data-protection taskforce or committee out of the specialists of members to advice the national federation on technicalities and policy and provide a platform for capacity building.

### **4. Helpdesk**

Create a telephone and/or online helpdesk for your members to contact about data-protection regulation.

## **5. Resource Website**

Create a website for members to find information about the GDPR and answers to Frequently Asked Questions in the sector.

## **6. Collective external advisor**

Contract or recruit a dedicated GDPR advisor who is available for tailor made advise to individual members at reduced costs.

## **7. Template agreements**

Develop and provide templates and models for particular agreements as the 'processor agreement' or an agreement on the use of data with clients.

## **8. Template provisions**

Develop and provide templates or model provisions for agreements with workers and/or clients on the use and protection of data.

## **9. Self-scan**

Develop a self-assessment scan for individual members to check to what extent they comply with the GDPR.

## **10. Certification schemes**

GDPR provisions can be introduced through existing or new self-regulatory certification systems. These certification can concern the company as a whole but also concern specific sectoral training certificates for employees working in the industry.

## 10 Recommendations for members of national federations

1. The GDPR is a framework of principles and no strict list of do's and don'ts. This means that businesses have to assess their individual use of personal data in their own particular situation and circumstances, and determine whether the processing complies or not. The business is responsible for compliance. Read the GDPR yourself, or at least read about the legal conditions of personal data use (or processing) to improve your understanding.

Good information can in general be found on the website of the [national data-protection authority of your country](#). Finally, take into account [the Opinions, Guidelines of the WP29](#) on how the European supervising authorities interpret and explain the GDPR.

2. ***Not all the answers are available.*** Over time, court-cases and national legislation will further shape the more concrete interpretation of the law. ***This inherently means uncertainty*** which individual business will have to deal with. To deal and with the impact of data-protection rules and (future) developments in your business, improve your own maturity and professionalism on data-protection rules.

Moreover, the better understanding of data-protection rules you have, the less you'll have to spend on expensive advisors as you better understand what you really need them for.

3. The GDPR only covers data that can be directly or indirectly retraced to a person: personal data. All other data is not covered by the GDPR. If you do not know what kinds of personal data you process in your business, start mapping it out.
4. There are six grounds for the of personal data (see article 6 of the GDPR). Consent is just one of them. In fact, as a rule of thumb in the employment relationship Consent for the use of personal data can only be used very scarcely and under very strict conditions. Therefore looking past 'Consent' alone, might prove beneficial.

5. Provide a Privacy Notice and be transparent on the personal data you process. Furthermore, If you wouldn't want others to process a particular piece of data about you, chances are others wouldn't want you to process that particular piece of data about them. When in doubt: ask the respective data-subjects how they feel about it and always be sure to communicate in full in your Privacy Notice.

Personal data about race, ethnicity, religion, political beliefs, biometrics, genetics, trade union membership, health, and sexual orientation may not be processed unless the law expressly allows or obligates you to. Processing these types of personal data aren't just attached to strict conditions, processing them significantly increase risks and costs of compliance.

Be ready for jobseekers and workers asking for an overview of all data you process on them. You are obligated to provide such an overview.

6. If you do not expressly know or cannot explain why you process, collect or use a particular piece of personal data, stop collecting, using, or processing that particular piece of personal data. If there is a way to process a particular piece of personal data without collecting other pieces of personal data, you must do so. For examples of this 'proportionality-principle' see [the guidelines on data-processing at work](#).
7. Data-Protection is not just an issue between employment & recruitment agencies and jobseekers and workers. The client or user-company can also be involved in the processing of workers' and jobseekers' data. Therefore always set up good agreements on who is the data-controller and who is the data-processor.
8. If you contract others (a 'data-processor') to process personal data on your behalf include provisions on data-protection in your bilateral agreement.
9. Secure personal data properly, including limiting access to it to those employees who actually need it.
10. If you have a data breach, report it to the competent supervisory authority within 72 hours!