IRISH CONGRESS TRADE UNIONS
SUBMISSION ON THE
EUROPEAN COMMISSION'S PROPOSAL FOR A NEW
DATA PROTECTION REGULATION

MARCH 2012

Introduction

1. The Irish Congress Trade Unions is the national representative body for workers and their unions on the island of Ireland. There are 48 unions representing almost 820,000 workers across all sectors and industries in both the private and public sectors.

2. Congress welcomes the opportunity to contribute our views on the European Commission's proposal for a new Data Protection Regulation. We are pleased that the EU Commission recognises the need to improve the coherence of the legal framework in Europe for the purpose of protecting the fundamental right to privacy, as expressed both in the European Convention of Human Rights, and the EU Charter of Fundamental Rights.

3. Privacy is a human right, and we believe that it must be discussed, promoted, protected, and continuously enhanced. The right to protection of personal data is established by Article 16 TFEU and in Article 8 of the ECHR. Data protection rights are also relevant to the practice and enjoyment of other fundamental human rights[1]

4. Trade unions have been strong supporters of the EU Data Protection Directive and the Data Protection Act 2003. The Data Protection Directive (95/46/EC) and the Irish legislation have on the whole worked well and it is essential that when moving to the proposed EU Regulation, the existing protections for data subjects are not in any way eroded but enhanced.

5. Effective data protection rights are of fundamental importance to decent working conditions. The ILO has specific guidelines in relation to data protection in the employment relationship and the ICTU believes that the new Regulation should aim to improve the working conditions in Europe (Art. 151 TFEU) by enhancing workers data protection rights.

6. **An overarching principle that must be secured in the Regulation is that the collection, processing and use of data must not have the purpose or effect to unlawfully discriminate against workers or trade unions, including the right to organise and collective bargaining.**

7. The new Regulation needs to take account of the inclusion of the EU Charter and ECHR in the European Treaties, (TEFU). Practices such as 'blacklisting' and the use of surveillance technologies to interfere in workers right to organise or the

---

[1] Data protection is closely linked to respect for private and family life (Article 7 of the EU Charter):Freedom of expression (Article 11 of the Charter); freedom to conduct a business (Article 16 EU Charter); the right to property and in particular the protection of intellectual property (Article 17(2) EU Charter); the prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21 EU Charter); the rights of the child (Article 24 EU Charter); the right to a high level of human health care (Article 35 EU Charter); the right of access to documents (Article 42 EU Charter); the right to an effective remedy and a fair trial (Article 47 EU Charter).

right to strike must, in light of the new status of the Charter and the rulings of the European Court of Human Rights, be prohibited.

8. Trade unions, should be explicitly recognised as having the right to lodge a complaint with the relevant supervisory authority, on behalf of the union, or on behalf of one or more workers, if it considers that the right to organise, collectively bargain or strike, or other rights have been infringed as a result of the collection, processing or use of personal data.

Protecting the Principle of 'Freely Given' Consent in the Employment Relationship

9. The importance of ensuring that consent is 'freely given' is of the utmost importance. In the past, 'consent' requirements have been interpreted in ways which do not benefit workers, and have often served to legitimise inherently objectionable practices, such as requiring consent as a condition of employment. For these workers their 'consent' to hand over data to employers is far from voluntary as workers fear that they will not be recruited unless they 'consent' to all the tests and background checks and agree to all terms in the contract, even those that require them to waive their privacy and data protection rights.

10. Against the backdrop of downsizing and increasing job security the unequal power in the employment relationship means that workers, on their own, without the protection of their union are unlikely to be able to mount an effective defence of their individual data protection rights when faced with employers' demands to introduce new monitoring and surveillance methods. In the context of the employment relationship 'consent' should not provide a legal basis for the collection, processing or use of data as there is the danger of a significant imbalance between the position of the data subject (i.e. the worker) and the controller (i.e. the employer or employment agency).

11. The new EU Regulation must reinforce the principle that consent is freely given before data is collected, processed or used. Special measures are needed to protect valid consent in the context of the employment relationship and Congress is calling for the Regulation to:

    - Prohibit employers (and employment agencies) from relying solely on the worker's consent as a means to legitimise, by itself, the collection, processing and use of his/her personal data;

- Set out obligations on employers to reach a collective agreement before the introduction or modification of a) automated systems permitting the processing of workers' personal data, b) any technical devices that can be used for monitoring/surveillance of workers at the workplace and c) questionnaires or tests of any form including medical, genetic, personality tests used at the stage of recruitment or during employment.
- Give workers (similar to health and safety) the right to establish a workplace committee and elect a data-protection representative equipped with adequate skills and rights to allow proper interventions in the field of data-protection on all levels, including cross-border circumstances in Multinational companies.
- Set out rights for information, consultation and involvement of workers' and their trade union representatives as regards regular evaluation concerning the operation of data protection systems in the workplace;
- Restrict employment agencies from making privacy invasive requests to job seekers;
- Employment agencies and employers should not be permitted to request that job applicants or workers use their right of access to their records (e.g. health, criminal records) in order to supply these to them;
- Employers and agencies should not be permitted to request that job applicants use their right of access to supply records of leave from their last employment (e.g. parental leave)
- Personal data should in principle be collected from the individual worker to whom they relate. If it is necessary to collect personal data from third parties, including transfer of data to third countries, the worker should be informed in advance and give his/her valid consent;
- In all circumstances employers and employment agencies must be required to objectively justify the data processing using reasons for legitimacy mentioned in Article 7 of Directive 95/46/EC, while respecting, in any case, the other general data protection principles such as the relevance, necessity and proportionality of the request

Ensure that the definition of data covers all information related to a worker

1. One of the main objectives of the Regulation is to harmonise definitions of data across the EU. Congress is calling for the Regulation to ensure that the definition is drawn in such a way that it anticipates future technological developments. The EMI Records & Ors -v- Eircom Ltd provides an example of the urgent need to bring legal certainty across the EU. In this case the court ultimately ruled that IP address data collected for the purpose of identifying persons was not personal data, because it was not directly identifiable by the collector of the data. This ruling makes no sense in the employment relationship as the worker is almost certainly clearly identifiable from the IP address and when read in conjunction with recital 12 of the directive, which states that, to determine whether a person is identifiable, account should be taken of "'all the means likely reasonably to be used either by the controller or by any other person to identify said person."

2. The definition must include all personal data – that is any information related to a 'worker' including sound and image data. Biometric data, such as fingerprints, hands, eyes, or body, genetic data.

3. On the question of definitions of 'sensitive data'. Congress is of the view that any data can become sensitive in certain circumstances and/or if linked to other available data. All personal information should have strong protection. However, it is recognised that some distinctions (with associated higher penalties for breaches) are useful and we would urge the addition of the following categories of personal information to the list: psychological, genetic, biometric, family history. We underline that trade union membership must be retained in the definition of sensitive data.

4. The definition must be drawn in such a way that it include existing and future technologies, including the large scale monitoring of workers and through the use of devices which allow employers to eavesdrop on telephone conversations, software that allows an employer to see what is on the employees computer monitor, e-mail monitoring systems, surveillance cameras which track behaviour and movements, sound devices, tracking tools on mobile telephones and other communication equipment, location (GPS)including ID cards with imbedded microchips, swipe cards, or devices attached to vehicles, emerging methods of establishing identity, (biometrics) and any other method of surveillance.

5. The definition of data must also include all manual processing, including the automated data which do not form part of the filing system.

6. In the case of biometric data it is essential that the information is stored and processed in such a way that the data cannot be reconstructed by the data controller.

Restricting the use of workers data to protect privacy, the right to family life, health and safety and dignity at work

7. It is essential that the Regulation ensures in practice – that the data on workers is used only for the purpose for which it was originally agreed to be collected. In addition the Regulation must ensure that the use of personal data on workers must be processed for purposes only directly relevant and necessary to the employment of the worker – meeting an objective and reasonably required standard.

8. **Workers should be provided with a right to know**. In particular, where employment agencies have passed a worker's information along to prospective employees, workers must be informed of what employers and what information.

9. Constant surveillance in the employment context has serious privacy and health and safety implications. Take for example, smart cards, introduced as a means for buildings security, these can also track workers' movements, monitor rest breaks, and hold personnel and occupational health records. The card records whether they are in the lavatory, another workstation, the canteen area and the like. Although the surveillance may be intended to capture only security related matters, constant surveillance has the potential to record very personal information; every private activity even scratching a body part is captured and capable of being replayed. Giving rise to concerns about workers' dignity, matters inherent in the concept of privacy.

10. Increasingly the line between work and private and family life is being blurred. Employer surveillance should not be permitted to extend into what employees consider to be private space e.g. from the place of employment into their homes. (e.g. where GPS is fitted to a vehicle provided by the employer- the employee must be enabled to switch it off during private life).

11. Workplace CCTV footage has made its way into TV programmes (usually with workers faces disguised) or on line, for example utube. This is a very worrying development and the Regulation should ensure against the use of workers data, for entertainment or 'info-tainment' purposes. An exemption to the prohibition is the use of footage to catch criminals e.g. CRIMECALL.

12. The use of video surveillance to discipline workers is fraught with difficulty, especially where the worker is unaware of the surveillance or where it happens outside the workplace. Recently employers have even tried to dismiss workers according to comments made on their personal Facebook or other social media sites. Congress view is that, with exception of criminal activity, the general rule should apply that unless the worker has freely consented (see earlier section) the material cannot be used in their discipline or dismissal.

13. Employers should look to fit the job to the worker, but frequently do the opposite. There is every danger that genetic tests and screening for "hyper susceptible" workers will present a new data protection threat in the future.

14. Other areas of concern relate to drug testing (including blood, hair and urine samples). Depending on the test used can disclose, off work and legal use of a range of medications and drugs, sometimes going back over a number of months, give rise to involuntary disclosure because the test shows medication taken for illnesses or pregnancy.

15. Congress supports the right to be forgotten, this should include a limitation on the amount of time that employers and employment agencies can retain data after the worker has left employment.

Problems with the use of automated data in profiling for employment

16. The Regulation seems to allow a broad use of automated processing of personal data for profiling purposes. This raises particular concerns in the employment context. The draft regulation states' *'where a person consents they can be subject to automated profiling based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.'*

17. Congress rejects this proposal. Workers should not be subjected to such measures in the course of the entering into, or performance of, an employment contract. The principle of the right to obtain human intervention should be retained along with a requirement to have in place robust measures to prevent unauthorised persons' interference especially as regards sensitive data.

Finally we strongly caution against the proposals for self-regulation, implied in the removal of the requirement to register with the data protection commissioner. The history of 'self-regulation in most sectors is one of dismal failure, with workers and consumers invariably losing out to powerful commercial interests. The data protection rights being addressed in the Regulation are fundamental human rights questions. At root, the issue is one of human dignity. The aim of reducing regulation on business is an important one but it does not hold the same importance as respect for human rights and should not be presented as holding equal importance as an objective for the Regulation.

Esther Lynch
Legislation and Legal Affairs
Irish Congress Trade Unions, 31/32 Parnell Square