STRONGER TOGETHER
CONGRESS
Irish Congress of Trade Unions

Note on Compliance with General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) became law in April 2016, and will come into force on 25 May 2018, replacing the existing data protection framework under the EU Data Protection Directive (94/46/EC) which has been in force since 1995. The GDPR applies to all organisations of all sizes and all industries, and places an emphasis on transparency, security and accountability by data controllers, while at the same time standardising and strengthening the right of European citizens to data privacy.

Many of the main concepts and principles of GDPR are much the same as those in the current Data Protection Acts 1988 and 2003, so if a company is compliant under current law, the approach should remain valid under GDPR. However, GDPR introduces new elements and significant enhancements which will require detailed consideration by all organisations involved in processing personal data.

The GDPR gives data protection authorities more robust powers to tackle non-compliance, including administrative fines of up to €20m (or 4% of total annual global turnover, whichever is greater) for the most serious infringements. However smaller businesses with fewer resources will be treated proportionately. The new regulations make it considerably easier for individuals to bring private claims against data controllers when their data privacy has been infringed, and allows data subjects who have suffered non-material damage as a result of an infringement to sue for compensation.

The Data Protection Commissioner has issued a 12 step guidelines for organisations to help them to prepare for GDPR. These cover:

1. **Become Aware**
   Key personnel in the organisation must be made aware of the changes in the law, and factor this into future planning. Start to identify potential risk areas which could cause compliance problems under GDPR, and enhance your organisation's risk management processes.

2. **Become Accountable**
   Make an inventory of all personal data held by the organisation and examine it to see:
   a) Why you are holding it?
   b) How did you obtain it?
   c) How was it originally gathered?
   d) How long will you retain it?
   e) How secure is it in terms of encryption and accessibility?
   f) Do you share it with third parties and on what basis might you do so?

   This inventory should enable the organisation to document and demonstrate the ways in which they comply with data protection principles, and to amend incorrect data or track third-party disclosures in the future.

3. **Communicating with Staff and Service Users**
   Under the new GDPR legislation additional information must be communicated to individuals such as the legal basis for processing the data, retention periods, the right of complaint. The

legislation also requires that this is communicated in a concise, easy to understand, and clear language, avoiding pages of terms and conditions.

4. Personal Privacy Rights

Procedures should be reviewed to ensure they cover all rights individuals have, including how you would delete personal data or provide data electronically or in a commonly used format. Under GDPR individual rights include;

i) Subject access
ii) To have inaccuracies corrected
iii) To have information erased
iv) To object to direct marketing
v) To restrict the processing of their information, including automated decision-making
vi) Data portability

5. Access Requests

Procedures should be put in place to handle access requests. Previously access requests had to be handled within 40 days, under GDPR access requests must be concluded within 30 days at the latest. The old charge of €6.35 has been abolished, unless an organisation can prove that the cost of processing an access request will be excessive. Where a request can be proven to be manifestly unfounded or excessive, it can be refused. However, clear refusal policies will have to be put in place with clear criteria for refusal. It is felt that the abolition of the access request fees will result in increased requests from individuals.

6. 'Legal Basis'

Organisations must look at the various types of data processing they carry out and identify the legal basis for carrying it out and document it, particularly where consent is relied upon as the sole legal basis for processing data. Under GDPR individuals will have a stronger right to have their data deleted where consent is the only justification for processing. All organisations need to identify how much personal information they gather, if it needs to be kept in its raw format, and how quickly you can begin the process of anonymisation and pseudonymisation of the data, also the right to be forgotten must be .

7. Consent

If you use customer consent when you record personal data, you should review how you seek, obtain and record that consent, and whether you need to make changes. Consent must be 'freely given, specific, informed and unambiguous'. In essence, customers cannot be forced into consent, or be unaware that they are consenting to, or be in any doubt about what they are consenting to. Obtaining consent requires a positive indication of agreement, it cannot be inferred from pre-ticked boxes or inactivity. Consent must be verifiable, and you must be able to demonstrate that consent was given.

8. Processing Children's Data

If your organisation processes data from underage individuals, you must ensure that you have adequate systems in place to verify individual ages and gather consent from guardians. The GDPR introduces special protections in relation to children's data, particularly in terms of social media and commercial internet services. Consent again must be verifiable and communicated to your underage customer in a language they can understand.

9. Reporting Data Breaches

Organisation must ensure that they have procedures in place to detect, report and investigate a personal data breach. GDPR will bring in mandatory breach notifications to the Data Protection

Commission (DPC), typically within 72 hours, unless the data was anonymised or encrypted. In practise this will mean that most data breaches must be reported to the DPC. Breaches that are likely to bring harm to an individual (identity theft, or breach of confidentiality) must also be reported to the individuals concerned. It's important to note that a failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

10. Data Protection Impact Assessments (DPIA) and Data Protection by Design and Default

A DPIA is the equivalent of a risk assessment of the potential impact that a project or initiative might have on the privacy of individuals. This risk assessment will allow organisations to identify potential privacy issues before they arise, and try to mitigate them. A DPIA may involve conversations with stakeholders and relevant parties.

Best practise is to adopt privacy by design and privacy by default. The GDPR enshrines both of these principles in law. This means that service settings must be automatically privacy friendly, and requires that the development of new services and products takes account of privacy considerations from the outset.

11. Data Protection Officers

The GDPR requires some organisation to assign a Data Protection Officer (DPO), these include public authorities, organisations whose activities involve the regular monitoring of data subjects on a large scale, or organisations who process what is currently known as sensitive personal data on a large scale.

Sensitive personal data is defined in the Data Protection Acts as any personal data that refers to racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs, **or trade union membership of the data subject**, the physical or mental health or sexual life of a data subject, any conviction or alleged conviction of the data subject, and the commission of any offences or any alleged offences that may have been committed by the data subject - the disposal of such proceedings or the sentence of any court in such proceedings.

The Data Protection Acts require additional conditions to be met for the processing of such data to be legitimate. Usually this will be the **explicit** consent of the person about whom the data relates.

12. International Organisation and GDPR

The GDPR includes a 'one stop shop' provision which will assist organisations which operate in many EU member states. Multinational organisation will be entitled to deal with one Data Protection Authority, referred to as the Lead Supervisory Authority (LSA) as their single regulating body in the country where they are mainly established.

Irish Congress of Trade Unions
June 2016