Data Protection changes GDPR

MICHELLE MCLOUGHLIN

27 APRIL 2018

CONTENTS

- Brief overview of the changes
- Consequences of a breach/ litigation impact
- What must we do to comply?
- Lawful basis
- Written contracts – DC and DP
- Subject Access Requests
- Action Plan

The Law

- GDPR – direct effect in Europe 25 May 2018
- Data Protection Bill 2018

- Law Enforcement Directive – law enforcement bodies

- E- Privacy Regulations – still draft

General Data Protection Regulation

- Good resource
- http://gdprandyou.ie/organisations/

- Transparency, security & accountability

Consequences of a breach

General Data Protection Regulation

- Fines: Article 83
- €20 million or 4% global annual turnover.

- Private Claims – sue for compensation

Article 82

- "*Any person who has suffered **material or non-material damage** as a result of an infringement of this Regulation shall have the right to receive compensation from the **controller or processor** for the damage suffered*".

- Circuit court or High court – section 115 – injunction, declaration or compensation.

- Class actions (not for profits orgs) – but no compensation

Article 82

- "*Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller*".

- Exempt – if not in any way responsible

Consequences of breach

- Fines – 28 days to appeal - confirmed by circuit court
- Publication – reputational damage
- High Court application – suspend processing
- Report
- Audit

Amicable resolution – optional - reasonable likelihood of success

Consequences

- Warning
- Reprimand

- Information Notice
- Enforcement Notice

- Suspension to a third country or international organisation

So What

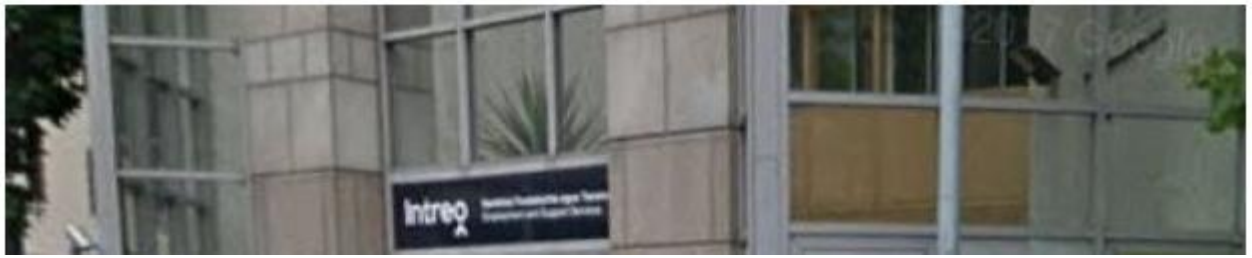
THE IRISH TIMES Wed, Jan 31, 2018

Civil servant jailed for a year for selling social welfare records

Rory Lenihan from Letterkenny received almost €22,000 from private investigators

Fri, Jan 26, 2018, 13:31

Stephen Maguire, Elaine Edwards



Criminal offences – sections 139 - 145

- Selling data
- Attempting to sell
- Unauthorised disclosure by processor
- Disclosure without authority
- Directors liable for company

Criminal - consequences

- Class A - €5,000 – 12 months
- €50,0000 – 5 years
- generally 3 years – 6 months if outside state and return (5 year window)

Case Study

- IT receives a call from Martin.
- He says that he urgently needs to recall an email he had just sent.
- He had thought that he was sending the customer list to John, the accountant, but he was in a hurry and accidently sent it to another John and needs help to sort it.
- **What does the business need to do?**

6 Guiding Principles

Data Processing must be:

- Lawful, Fair and Transparent
- Purpose Limitation (specified purposes)
- Data Minimisation (adequate, relevant and limited)

6 Guiding Principles

Data Processing must be:

- Accurate and Up-to-date processing
- Limitation of storage of identifiable data for no longer than is necessary for the purposes for which it was collected.
- Confidential and Secure – protects integrity and privacy

DATA PROTECTION

- How secure is it, both in terms of encryption and accessibility?

- Do you ever share it with third parties?
- On what basis?

What is personal data?

- a name,
- an identification number – client, mobile, telephone
- address / email
- location data,
- an online identifier (IP address)
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories – sensitive

- **racial** or **ethnic** origin,
- **political opinions**,
- **religious or philosophical beliefs**, or
- **trade union membership**,

Special categories – sensitive

- **genetic data**, **biometric data** for the purpose of uniquely identifying a natural person,
- data concerning **health** or
- data concerning a natural person's **sex life or sexual orientation**

Employment – article 88

- Right to set more specific rules for employment
- Section 43 – sensitive information permitted for employment and social welfare law
- S44 – also permitted to provide or obtain legal advice or for legal rights

General Data Protection Regulation

- Demonstrate & document compliance
- Track third party disclosures

Data Protection Officer

Do you need to appoint one?

- a public authority or body;
- core activities - consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or
- core activities - consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Must have a lawful basis 1of 6 grounds

Processing is only **lawful** if:

- Data Subject has given **consent**
- Necessary for the performance of a **contract** or to take steps prior to entering into a contract
- Necessary for compliance with **legal obligation** to which the controller is subject

Must have a lawful basis

Processing is only **lawful** if:

- In order to protect **vital interests** of a person
- Necessary for **public interest or official authority**
- For the **legitimate interests** of data controller/3rd party

Data Processor – article 28

- Process information for the data controller

- Need written contract
  - Conditions to process
  - Security conditions
  - Delete/return on completion
  - Ensure compliance

Data Processor

- Information
- Assistance – security breach, pseudonynimsation, encryption
- Audit assistance

Records of processing activities – article 30

DC & DP Keep detailed records

(unless less than 250 employees)

Must keep records of Special Category of personal data processed.

(profilers/regular monitoring must comply)

Data Protection Impact Assessment

DPIA

Taking into account

- the nature,
- scope,
- context and
- purposes of the processing,

is likely to result in a **high risk** to the rights and freedoms of an individual

Valid Consent

- **Unambiguous**
- **Freely given** – must take into account whether or not the service is conditional on consent
- **Specific**
- **Informed** – notices must be intelligible language

GDPR - Consent

- Know giving consent – can withdraw it
- Positive indication of agreement - proof
- Cannot infer from silence, pre-ticked boxes or inactivity

Privacy Statement – article 13

- Identity & contact details of Data Controller
- Contact details of DPO (if you have one)
- Purposes of processing & legal basis
- What is the legitimate interest?
- Recipients or categories who receive PD
- Transfers abroad of Personal Data

Privacy Statement

- Retention period or criteria to determine the period
- Right of access
- Right to data rectification
- Right to be forgotten/right of erasure
- Right to restrict processing
- Right to object to processing

Privacy Statement

- Data Portability
- Right to withdraw consent if processing is based on consent
- Right to lodge a complaint

Privacy Statement

- Provision - a statutory or contractual requirement or necessary to enter a contract – any obligation to provide & consequences of failure

Breach

A breach of security leading to the **accidental** or **unlawful**

- destruction,
- loss,
- alteration,
- unauthorised disclosure of, or access to,

personal data transmitted, stored or otherwise processed.

Scenario

- Amanda was in a hurry back to work.
- In her haste she forgot her coat and carrier bag. She rang the cafe the minute she got to the office. The café searched the area she was sitting in and located her coat but could not locate her bag. The carrier bag contained a work laptop and some work papers.

- **What should Amanda do?**

GDPR – Reporting a breach

- Mandatory notification to regulator
- 72 hours unless no risk
- Failure – fine up to €10 million or 2% global annual turnover

Notify individuals of a breach

- If the breach is likely to result in high risk to affected data subjects- then controller must inform the data subjects without undue delay

- Clear & plain language

Subject Access Request – article 15

- No cost
- One month
- Need procedure with refusal policy & Justify

Legal privilege exclusion – section 158

- Seeking, giving or receiving legal advice
- Course of legal proceedings - including client & legal adviser or between advisers
- To do so be contempt of court

Privileged legal material – section 149

- Refusal
- 28 days or extended period
- High Court determination

- Preserve information

- Appoint person to review

GDPR by Default and by Design

Transfers Abroad

- Where are the servers
- Who will be processing data for you?
- Where are their servers?
- Whitelist, privacy shield, model clauses, consent?

Action Plan

1. Check current procedures;
2. Check consents – not part of terms & conditions
3. Check & update privacy statements
4. Check security systems – encryption

Action Plan

5. Check existing contracts:
   I. Contracts of employment & handbook
   II. Contracts with data processors – need an addendum – liability clause

6. Update Subject Access Request procedures

7. Create reporting policies and procedures

Action Plan

8. Draft mandatory report template documents
9. Consider certification
10. Follow Guidance of Regulator & Article 29 working group
11. Follow any codes of conduct

Action Plan

12. Do you need a DPO?
13. Do you need to do DPIA? – policy?
14. Data Storage Policy
15. Data Retention Policy

Action Plan

16. Incidents log/breach register

17. Template SARs Response with extra information ready.

18. Be clear on the go to persons within the organisation

Action Plan

19. Staff training

20. Ensure ongoing monitoring – state of the art, costs of compliance

THANK YOU

Michelle McLoughlin - Train With Us
Crossboy, Ballintogher, Co. Sligo.
info@mmcloughlinsolicitors.com
info@trainwithus.ie
087 6674534