Coimisiún Cosanta Sonraí
Data Protection Commission

GDPR & Data Protection for Pension Schemes
IAPF Governance Conference

29th November 2018

Garrett O'Neill, Solicitor/ Assistant Commissioner
Head of Private and Financial Sector Consultation

Overview of presentation

- Joint Controllers
- Data Processors
- Review of key problems : - Security / Breaches / Data subject Rights
- Summary of work done to date by Data Controllers to be compliant with GDPR
- Takeaway guidance on good practice.

– Joint Controllers –Art 26

1. 1.Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

– Joint Controllers –Art 26

2.The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
3.Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Key issues – Joint Controllers

1. Define your legal relationship with the Third party.
2. Are they a Joint controller or a Data processor ?

- Examples of Joint controllers are scenarios where the personal data is used for a defined Joint purpose i.e. creation, supervision and provision of a pension.
- Employers / Registered Administrators / Trustees.
- Service Level Agreements should be in place to GDPR standards
- Article 5:- Principles apply such as Purpose limitation ; Data Minimisation ; Accurate; Lawful Fair and Transparent
- Article 6 :- Lawful basis for sharing data :- Contract / Consent / other legal obligation (regulatory compliance)
- Who deals with Customer dispute resolution process?
- Any independent review ? Trustees and /or Pension Authority

– Data Controller OR processor ?

1. Entities that may be a data controller or a data processor include :- Auditors; Actuaries ; Lawyers ; medical advisors ; Investment and scheme advisors.

- Usually, acting under other defined regulatory compliance requirement or dealing with legal issues in dispute then they are a DC.
- Safeguards are :- Job to be done is a statutory requirement (i.e. Audit) and there are statutory rules to the process
- Professional duty of confidentiality and professional bodies to investigate complaints / impose sanctions on misconduct i.e. Law society.

2. Acting as a Data processor may relate to non statutory functions.

Other issues – Data processors

1. "*Processor means a natural or legal person , public authority, agency or other body which processes personal data on behalf of the controller*"

2. Define your Contractual legal relationship with the Third parties DPs.

3. Processor is working strictly on DCs instructions. Cannot go beyond contractual terms or purpose for processing personal data. i.e. cannot use the member data for its own purposes.

- Examples of Data processors are scenarios where the personal data is used for a defined administrative purpose on strict instructions from Data Controller i.e. IT security services / External HR services / External consultants

Mapping of personal data & Data Retention

- Map data retention policy to core timeline events. For example :-
- Start of pension – when member first signed up to scheme.
- Annual update to keep data accurate i.e. Inform member & request any changes to personal data such as a new address.
- Employer notification of employee leaving employment
- Employer notification of death in service
- Employer notification of retirement of member.
- Notification of change in beneficiaries (New spouse)
- Notification by Beneficiaries / Executors of Death of Retiree
- Any Statutory requirement to retain pension data for defined period?
- Delete – destroy. Data

What should you be looking for from Joint Controller?

DPO / Compliance officer Reports on:-

1. Breaches :- How often ? What level of risk has been identified ? Have affected customers been informed

- New threats, what preventive measures to reduce new cyber attack risk

2. Access requests and other rights being exercised. Is there a increase?

- If so, why? Did a media event or incident occur?

3. New Technology i.e. profiling algorithms / Use of A.I. or enhanced monitoring systems. Has the legal basis for processing been risk assessed? Any DPIA done and if so what level of risk has been recorded ? What safeguards or measures have bene considered to reduce the risk?

4. Disclosure to third parties i.e. must be under a defined statutory purpose or legal basis (normally consent / Contract consent).

Security- Breaches. General advice

Who will be responsible for detection / investigation / reporting ?

Make an INCIDENT RESPONSE PLAN now as to how you will deal with it.

Do you get expert outside advice on forensic Investigation or IT?

If so get provisional Contracts in place now with suitable providers.

How will you notify High risk members?

Consider a Call centre for customer complaints and follow up.

What decisions will BoM / CEO/ Units have to make?

Reputational damage or resultant civil claims potential

How will members be informed ?

Loss of production because IT system needs to be investigated
or turned off for repair

Guidance for Good Security practices

- All paper confidential documents sent to Trustees should be securely delivered by Registered post or courier. Vice versa when returning Documents.
- Documents should be held in a secured environment either at home or in office.
  i.e. a locked cabinet
- Electronic messaging should be done on a secured server.
- Sensitive confidential documents should encrypted. Password sent by phone.
- Laptops should have strong security authentication log in and passwords.
- Use a separate email address rather than your own personal email account.
- Alternatively establish a secure Web-Portal that is monitored for security purposes.
- Destroy (duplicate) records that you no longer require.
- Reduce potential risks and human error i.e. lost laptops / cyber hacking.

Key problems – Security Breaches

- Reducing risk of Cyber attack / Ransomware / Human error
- Are there emergency plans in place to deal with a large scale breach ?
- Prevention is better than the cure

Cost of rectifying a major breach (US examples)

1. Compensation fund for Customers
Anthem Insurance $115m / Home Depot $27m / Target €23m / Equifax
Cost of credit monitoring services / Identity restoration services /
Fraud resolution services

2. Settlements with Third party Financial Institutions
Target $39m / Home Depot $25 m

3. Settlements with Visa / mastercard
Target $ 67 m / Home Depot $25m

(Note that none of the above includes a Regulatory Fine of up to, €20m or 4% of annual global turnover)

Cost of rectifying a breach (US examples)

And non monetary relief requires …

Upgrade existing data security systems
Review and amend existing policies and procedures
Triple annual spending on data security for three years
Implement cybersecurity controls and reforms
Follow specific remediation schedules
Do annual IT security & risk assessments (by Independent 3rd party)
Cost of restoring customer confidence.

Consequences of an Individual breach?

Caused by human error i.e. email / letter to wrong person

Potential breach of the duty of confidentiality (Tort law). Potential claim for compensation for material or non material damage.

Case by case basis, as to what harm or detriment could accrue to the individual as a result of the breach . Must Assess harm caused and Rectify damage and Record actions taken. Report High risk breach to DPC

Examples of high risk:- Identity fraud ; Hacking of email accounts ; unauthorised access to company services ; Un-authorised payments. Unauthorised access to special categories of data i.e. Health records Or Financial details.

Good work done by industry data controllers to …

- Mapping of entire data processing operation and business requirements.
- New or updated IT systems to manage and process data more effectively and securely
- Review and amendment of all 3rd party data processing agreements
- Breach detection, investigation, rectification and reporting
- Dealing with exercise of rights under GDPR

Enhancements for …

- In-House data protection teams.
- Updated and new written policies and procedures
- Staff training
- Website policies and Information notices
- Upgraded Customers service and complaints mechanism
- Appointment of DPO

Q & A

Thank you.

www.dataprotection.ie

www.edpb.europa.eu

www.GDPRandYou.ie

@DPCIreland