Privacy Laws & Business
On-boarding and Oversight of Processors

Paul Lavery, McCann FitzGerald

Thursday, 9 May 2019

McCann FitzGerald

On-boarding and Oversight of Processors

- GDPR Requirements – Article 28
- On-boarding – the considerations
- On-going oversight
- The contract/data processing clause - key considerations
- Limitations and exclusions from liability and other issues
- Is the processor located outside the EEA?

Legislative Regime

- General Data Protection Regulation
- Irish Data Protection Act 2018
- Main provisions:
  - Article 28 of the GDPR *(obligations re processors)*
  - Section 144 of the Data Protection Act 2018 *(unauthorised disclosure by processor)*

McCann FitzGerald

Key Data Protection Terminology

- Definitions (Article 4)
- **Personal data** – relates to identified or identifiable living individuals (not anonymised data)
- **Processing** – widely defined – includes any collection, recording, organisation structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, erasure or destruction of data
- **Controller** – entity which determines the purposes and means of processing of personal data
- **Processor** – entity which processes personal data on behalf of controller – e.g. outsource service provider

Service providers

- Service providers may process personal data on behalf of a company
- In such circumstances, the service provider is a “processor”
- If the service provider engages sub-contractors – they will be “sub-processors” if they also process personal data on behalf of the service provider (and ultimately the company)
- Company, as controller, has primary responsibility for ensuring that appropriate care is taken with personal data

  => needs to satisfy itself that service providers, and their sub-contractors, have appropriate controls in place and are compliant with the GDPR

McCann FitzGerald

Engaging Service Providers

- A company may engage a number of service providers, not all of whom may be processors, but who could include the following:
  - Payroll service provider
  - IT maintenance and support service providers
  - Operators of CCTV systems
  - Cleaning contractor
  - Cloud hosting service provider
  - Auditors
  - Legal advisors
- Consider to what extent these service providers may be Processors - are they processing personal data for and on behalf of the company (directly or indirectly) ?

Engaging Service Providers

- Query – will the service provider have any access to your personal data?
- Query – will it process personal data on your behalf?
- If so => Provisions of Article 28 are triggered
- Service providers who are likely to be processors:
  - Support and maintenance provider
  - Payroll processor
  - Cloud hosting service provider
  - Operator of CCTV systems
- Service providers who are more likely to be independent controllers:
  - Legal advisers
  - Auditors

Engaging Service Providers – Article 28 requirements

- Article 28(1) – Only use processors providing sufficient guarantees to comply with the GDPR and ensure the protection of the rights of the data subject
- Article 28(2) - Processor not entitled to engage sub-processor without controller consent
- Article 28(3) - Requirement to have written contract with processor which includes various provisions specified in Article 28 GDPR (more detailed than previously required under previous law)
- Article 28(4) – Engagement by processor of sub-processor requires back to back processing contract
- EU Commission may adopt standard contractual clauses to reflect requirements of Articles 28(3) and 28(4)

On-boarding a new service provider – suggested steps

- Prior to engaging a new provider, the controller should carry out due diligence on provider
- Consider the nature of the data being processed – health data, employee performance review data and financial data (bank account details of individuals etc) carry higher risk
- Provision of data protection questionnaire to processor?
- On-site review if processing is higher risk?

On-boarding of service provider

Due Diligence Questionnaire for potential suppliers

Your organisation		
1.	Data processor name/ Organisation name	
2.	Details of proposed processing/service provided and types of personal data processed	
3.	Has your organisation ever been subject to any regulatory enforcement action concerning privacy or data protection? If so, please provide details.	

McCann FitzGerald

On-boarding of service provider

Due Diligence Questionnaire for potential suppliers

Policies and procedures		
4.	Please list privacy/ data protection /information security policies in force within your organisation.	
5.	Have your organisation's policies been reviewed, and if necessary, amended to take account of the EU General Data Protection Regulation?	
6.	Please detail your data retention periods. What is your policy for deleting data when a services agreement is terminated/expires?	

McCann FitzGerald

On-boarding of service provider

Due Diligence Questionnaire for potential suppliers

Training and security		
7.	What data protection/ information security training is provided? How frequently training is refreshed?	
8.	Does your organisation have any security accreditations or any certification to any relevant standard (e.g. ISO27001)?	
9.	How quickly will your organisation be able to report any data breach to [the Company] and how?	

McCann FitzGerald

On-boarding of service provider

Due Diligence Questionnaire for potential suppliers

Training and security (cont)		
10.	Has your organisation performed any security /penetration testing in the past 12 months?	
11.	What technical measures are taken to restrict access to systems that would hold the personal, confidential or sensitive data of [the Company]?	
12.	How does your organisation enforce your security polices, and who is responsible for ensuring that your security policies are adhered to?	

McCann FitzGerald

Other queries

- Details of proposed sub-contractors/sub-processors
- Location of processing activities or remote access
- Willingness to enter into Article 28 data processing agreement

McCann FitzGerald

Review of questionnaire responses

- Review of answers and identification of concerns
- Potential concerns:
  - Answers suggest lack of knowledge of the GDPR or processor obligations
  - Answers highlight previous or current investigation of processor by Data Protection Commission or previous data protection issues/breaches
  - Answers highlight data security issues or lack of oversight of sub—processors
  - Answers highlight unwillingness to sign up to market standard data processing agreement

On-boarding Queries

McCann FitzGerald

Next Step: Data processing contract

- Ensure contract/data processing clause complies with requirements of Article 28
  - Contract includes details of subject matter and duration of processing, nature and purpose of processing, type of personal data and categories of data subjects;
  - Processing in accordance with instructions;
  - Notification from processor of any legal requirements preventing processing in accordance with instructions;
  - Confidentiality obligations imposed on any persons authorised to process personal data;
  - Compliance with data security obligations;
  - No appointment of sub-processors without consent and/or right to object to sub-processors;
  - Responsibility for acts or omissions of sub-processors

Next Step: Data processing contract

- Ensure contract/data processing clause complies with requirements of Article 28 (cont'd)
  - Rights of audit and inspection;
  - Notification of data security incidents;
  - Assistance to facilitate controller's compliance with data access requests, data security obligations, data protection impact assessment and prior consultation requirements
  - Return or deletion of data on expiry of processing services

Further Consideration

- Is the processor outside the EEA?
- If so, further considerations apply – Chapter V GDPR
- Potential need for standard contractual clauses or other transfer mechanism

The Contract/data processing clause – Issues encountered

- Contract signed before 25 May 2018 – difficulties negotiating required amendments
- Should there be a higher liability cap or no liability cap for data protection breaches?
  - Is there a market standard approach?
  - options
- Processor seeks to charge for assistance on DPIAs or access requests etc.
- Processor seeks to charge for audits
- Processor seeks to limit audits to one per year
- Indemnities?

Contract/data processing clause – issues encountered

McCann FitzGerald

Dealing with Service Providers – On-going oversight

- After service provider is “on-boarded”, controller still needs to carry our periodic review of service provider and its processing activities
- Potential need to review sub-processors also
- Nature of on-going review/oversight will differ depending on nature of data processed by service provider and risk assessment to business.

Dealing with Service Providers – On-going oversight

- Lower risk:
  - desktop/paper based review may be sufficient;
  - Questionnaire to be completed - use questionnaire similar to on-boarding questionnaire and the following queries:
    a) confirmation of any data security incidents;
    b) confirmation re: no DP investigations;
    c) confirmation re: data security measures;
    d) where relevant, confirmation re: business continuity/disaster recovery plans;
    e) confirmation re: no incidents with sub-processors;
    f) confirmation re: contractual arrangements (Article 28 language) with sub-processors; and
    g) has service provider audited/reviewed its sub-processors?

McCann FitzGerald

Dealing with Service Providers (continued)

- Higher risk data or higher risk processing (to business) likely to require more than paper based audit – e.g.:

  a) Attendance on-site to review systems;

  b) Meeting with key personnel in service provider to confirm (i) any data security incidents, (ii) any DPC investigations (iii) any issues with sub-processors and (iv) future plans and spend on data protection compliance;

  c) Review of answers to DP compliance questionnaire

On-going oversight

McCann FitzGerald

Data Protection Act Provisions

- Section 144 – unauthorised disclosure by processor
- Personal data not to be disclosed by processor without prior authority of controller
- Person who knowingly or recklessly breaches this obligation is guilty of criminal offence
- Summary conviction – class A fine and/or imprisonment for up to 12 months
- Conviction on indictment – fine not exceeding €50,000 and/or imprisonment for up to 5 years

Privacy Laws & Business
On-boarding and Oversight of Processors

Paul Lavery, McCann FitzGerald

Thursday, 9 May 2019

McCann FitzGerald