Using GDPR to reinforce trust

Practical steps for Financial Planners

Society of Financial Planners of Ireland
22 May 2018

John Holohan is a partner at KingramRed Consulting with over 25 years' experience in information management, business transformation, strategy development and global project delivery with IBM and HP, two of the world's leading technology companies.

He is a Certified Information Privacy Practitioner (CIPP/E) with extensive experience of the implementation of data privacy protection programs to organisations in construction, property management, public administration, healthcare and finance.

David Gunning is also a partner at KingramRed and is a recognised business leader with more than 20 years' senior leadership experience at a number of blue chip organisations including Coillte (as CEO), Tellabs, Inc. (Nasdaq: TLAB), Massachusetts-based start-up Integral Access, Inc. (acquired by Telco Systems (LSE: BVC) and Hewlett Packard (HPQ: NYSE). He also has extensive experience in the field of compliance having served on the Commission for Communications Regulation (COMREG).

Consumer attitudes to privacy

Consumer attitudes about privacy vary depending on the type of data at issue, but privacy concerns are highest for online companies, financial companies, and governments.

Boston Consulting Group 2018

Agenda

- GDPR overview – Apologies, it's unavoidable
- Scenarios - Examining some scenarios that are relevant to your industry
  - Customer scenarios
  - Employee scenarios
  - Breach Examples
- Practical Steps towards Privacy as a Positive Advantage for your Business
- Q&A time

What is the GDPR?

The EU General Data Protection Regulation - GDPR

Due to be enforced from 25th May 2018.

The regulation will require organisations that control or process personal data to implement processes and technical changes to uphold the rights of data subjects and meet their own obligations as controllers or processors.

It will be necessary for organisations to demonstrate that they are compliant.

Organisations will be responsible and accountable for the entire eco-system (both internally and externally) that they employ to manage personal data.

What is aim of the GDPR?

- GDPR is fundamentally a rights-based regime
- It applies to all organisations who control personal data of data subjects in EU no matter where the organisation is located.
- The aim is to ensure that personal data is:
  - Lawfully and transparently controlled
  - Collected for specified, explicit and legitimate purposes
  - Adequate, relevant and limited to what is necessary
  - Accurate and Up-to-Date
  - Stored for no longer than necessary
  - Secured
  - Demonstrably so

Personal Data

‘personal data’ means

- any information relating to an identified or identifiable natural person (‘data subject’);
- an identifiable natural person is one who can be identified, directly or indirectly, ….

Special Category Data

Processing of personal data revealing

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- data concerning health
- data concerning sex life or sexual orientation

Definitions

‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data…

‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

What does Lawful look like?

There are specific lawful grounds for controlling personal data:

- CONTRACTUAL
- LEGAL OBLIGATION
- VITAL INTEREST OF SUBJECT
- PUBLIC INTEREST
- LEGITIMATE INTEREST *
- CONSENT *

* Explicit conditions apply where children are concerned

Data Subject Rights

- Transparency
- Information
- Access & Rectification
- Erasure
- Restriction & Notification
- Portability
- Right to Object
- Auto Decision Making

KINGRAMRED

GDPR Myths

- The biggest danger is massive fines FALSE
- I need to bring in the lawyers FALSE
- You must have consent to process personal data FALSE
- Everyone needs a data protection officer FALSE
- GDPR compliance is just like Y2K FALSE
- Breaches are all about hacking FALSE
- The IT guys will handle it FALSE
- GDPR is for the big companies. FALSE

KINGRAMRED

Scenarios

Client Scenarios

A client is concerned that she is being contacted by people who seem to know lots about her. She wants to know with whom you are sharing their data.

A client wishes to see everything that you have concerning him. He then wants to rectify or erase information.

A prospect or former client now objects to you contacting them with marketing materials.

Client Scenarios

As part of your normal processes, you collect personal information on clients through notes and forms. Is the client or prospect informed of their rights at this time?

Your website has a privacy statement already. How does this statement stack up regarding GDPR rules?

Insurance company have said that they are the controllers of data for a particular type of investment. Are you now off the hook? Are you a processor?

Employee Scenarios

A former employee wants to see all her personal data.

She requests that you delete particular records.

An unhappy employee wishes to see all performance-related information held.

Data Breach Scenarios

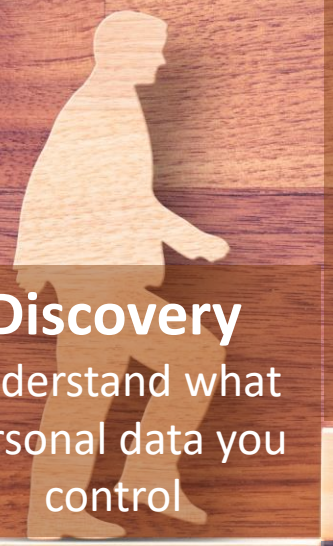
'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'

Loss or theft of documents or un-encrypted equipment.

Inappropriate access controls allowing unauthorised use.

An external attack on electronic data assets resulting in loss or exposure of data.

Steps to Compliance



STEPS

Discovery
Understand what personal data you control

Processes
- Create Rights Processes
- Build a Privacy Policy
- Amend Contracts

Obligations
- Security
- Prepare for Breaches
- Transparency

Report
- Keep Records
- Manage 3rd Parties
- Show Compliance

TRUST

OUTCOME

- **A Detailed Inventory of Personal Data**
- **Documented Privacy Playbook**
- **Amended Contracts**
- **Validated Security**
- **Breach Readiness**
- **Privacy Notices**
- **Demonstrable Compliance**
- **Eco-system confidence**

KINGRAMRED

GDPR Program Development