General Data Protection Regulation Presentation

9 November 2016

General Data Protection Regulation

- Topics Covered:
  - Brexit implications
  - What is "new" within the GDPR?
  - What should you do?
  - Recent events / guidance

General Data Protection Regulation – Brexit Implications

- In force 25 May 2018
- Brexit?
- UK government has confirmed that GDPR will be implemented
- Secretary of State, Karen Bradley MP told the Culture, Media and Sports Select Committee:

"We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public."

- UK ICO, Elizabeth Denham, commented:

"I see this as good news for the UK. The ICO is committed to assisting businesses and public bodies to prepare to meet the requirements of the GDPR ahead of May 2018 and beyond."

General Data Protection Regulation

- What is "new" within the GDPR?
  - Expanded Territorial Reach
  - Accountability / Privacy by Design
  - Data Protection Officer
  - Data Processor Obligations
  - Consent
  - Fair Processing Notices
  - Breach Notification
  - Penalties
  - Notification
  - Data Subjects' Rights

Expanded territorial reach

- Catches all processors and controllers outside the EU
- Offering goods/services/monitoring EU data subjects
- Appoint representative in EU

Accountability / Privacy by Design

- Maintain documentation
- Conduct privacy impact assessments
- Data protection by design and by default – data minimisation

Data Protection Officer

- Public authority
- Core activities (processor or controller) – regular, systemic monitoring of data subjects on a large scale
- Processing of large amounts of sensitive data

Data Processors

- Direct obligations
- Maintain a written record of processing activities carried out for each controller
- Designate a DPO (where required)
- Appoint a representative (if not in EU)
- Notify controller of a breach "without undue delay"

Consent

- Clear consent given – easy to withdraw
- Demonstrate consent was given
- Will existing consents still work?
- Consent and contractual obligations?
- Direct marketing – right to object – explicit consent / attention

Fair processing

- Fair processing notices
  - Transparent information to data subjects
  - At the time the personal data is obtained
  - Review existing arrangements – GDPR more extensive (e.g. right to withdraw; period for which data will be stored)

Breach Notification

- Data breach notification
  - Controllers must notify breaches
  - Without undue delay – within 72 hours
  - Notify data subjects – risk to the rights and freedoms of individuals

Penalties

- Fines
- Two tier system:
- Higher of €20m or 4% global turnover
- Higher of €10m or 2% global turnover

Notification

- Removal of annual notification fee
- Obligation to have appropriate procedures in place
- PIAs for high risk activities
- Consult DPA if PIA indicates "high risk"

Data Subjects Rights

- Understand what data is being processed
- Access to data
- Objection to certain processing
- Right of rectification / right to be forgotten
- Data portability
- Provide a response within a month – no fee

Other points of interest

- European Data Protection Board
- BCRs – controllers and processors
- International transfers

GDPR TO DO LIST

- 1. Are you targeting EU individuals?
- 2. Do you know what personal data your business processes?
- 3. Ensure data protection policies are revised in accordance with the new principles.
- 4. Establish a paper trail to "demonstrate compliance", e.g. privacy impact assessments.

GDPR TO DO LIST (Cont.)

- 5. Does your processing comply with the new lawful processing grounds, e.g. is "consent" being properly obtained?

  - • Not relying on "silence"
  - • Clearly requested / unbundled
  - • Not contingent on consent to processing
  - • Right to withdraw
  - • Simple method to withdraw consent
  - • Indirect collection – notification
  - • Review/update/approval

GDPR TO DO LIST (Cont.)

- 6. Subject access requests
  - • Review procedures and staff training
  - • Template response letters
  - • Technological changes, e.g.
    - formatting issues
    - portability
    - portal access

- 7. Rights to object
  - • Check this is clearly and separately stated at collection
  - • Automated online system
  - • Reviewing marketing suppression lists (internal and external)

GDPR TO DO LIST (Cont.)

- 8.Erasure of data
  - • System to identify and respond to requests
  - • Technological changes – is deletion possible?

- 9. Governance
  - Appoint a Data Protection Officer
  - Compliance programme
    - PIAs
    - Internal policy reviews
    - Training
    - Audits
    - Awareness raising programmes

GDPR TO DO LIST (Cont.)

- 10. Breach notification
  - Breach notification procedure
  - Incident response plan
  - Test/review procedures/plans
  - Technological changes, e.g. "technical and organisational protections" – encryption
  - Check insurance coverage/policies
  - Review existing/template contracts
    - obligations on suppliers/processors
    - limits on liability
    - data breach notification obligations

GDPR TO DO LIST (Cont.)

- 11. Transfers of data
  - Assess if this is relevant to your business
  - If relevant, check transfer is compliant, e.g. model clauses

General Data Protection Regulation – Recent Events / Guidance

- Breaches:
  - Unsolicited Marketing Communications (Company Directors) Bill
  - From Spring 2017, company directors can each be fined up to £500,000 by the ICO should they breach the Privacy and Electronic Communications Regulations
  - UK ICO, Elizabeth Denham, supported the move: "making directors responsible will stop them ducking away from fines by putting their company into liquidation. It will stop them leaving by the back door as the regulator comes through the front door."
  - Make sure direct marketing consents are in place / adequate

General Data Protection Regulation – Recent Events / Guidance

- ICO – breaches

  "Data security incidents (breaches of the seventh data protection principle and personal data breaches reported under the Privacy and Electronic Communications Regulations) are a major concern for those affected and a key area of action for the ICO."

General Data Protection Regulation – Recent Events / Guidance

- ICO action:
  - Q2 2016 (April to June):

  - Four monetary penalties:
    - Chief Constable of Kent Police - £80,000
    - Blackpool Teaching Hospitals NHS Foundation Trust - £185,000
    - Chelsea & Westminster Hospital NHS Foundation Trust - £180,000
    - Chief Constable of Dyfed Powys Police - £150,000

  - Two undertakings:
    - Health and Social Care Information Centre (HSCIC)
    - Wolverhampton City Council

General Data Protection Regulation – Recent Events / Guidance

- Types of breach by sector:
  - General Business:
    - Data being posted or faxed to an incorrect recipient – 15% of incidents
    - Data being sent by email to an incorrect recipient – 13% of incidents
    - Cyber incidents – 13% of incidents
- Finance, insurance & credit:
    - Data being posted or faxed to an incorrect recipient – 38% of incidents
    - Cyber incidents – 15% of incidents
- Charitable & voluntary:
- Cyber incidents – 31% of incidents
- Loss or theft of paperwork – 21% of incidents

General Data Protection Regulation – Recent Events / Guidance

- TalkTalk
- Record £400,000 fine for failing to prevent October 2015 attack
- Security failings that allowed a cyber attacker to access customer data "with ease"
- ICO's in-depth investigation found that the attack could have been prevented if TalkTalk had taken basic steps to protect customers' information
- Technical weaknesses in TalkTalk's systems
- The attacker accessed the personal data of 156,959 customers including their names, addresses, dates of birth, phone numbers and email addresses
- In 15,656 cases, the attacker also had access to bank account details and sort codes

General Data Protection Regulation – Recent Events / Guidance

- Data was taken from an underlying customer database that was part of TalkTalk's acquisition of Tiscali's UK operations in 2009
- Data was accessed through an attack on three vulnerable webpages within the inherited infrastructure
- TalkTalk failed to properly scan this infrastructure for possible threats and so was unaware the vulnerable pages existed or that they enabled access to a database that held customer information
- TalkTalk was not aware that the installed version of the database software was outdated and no longer supported by the provider – had the bug been fixed, the attack would not have been possible
- Two early warnings – TalkTalk unaware

- UK ICO, Elizabeth Denham:

"TalkTalk's failure to implement the most basic cyber security measures allowed hackers to penetrate TalkTalk's systems with ease

Yes hacking is wrong, but that is not an excuse for companies to abdicate their security obligations. TalkTalk should and could have done more to safeguard its customer information. It did not and we have taken action

In spite of its **expertise** and **resources**, when it came to the basic principles of cyber-security, TalkTalk was found wanting

Today's record fine acts as a warning to others that cyber security is not an IT issue, it is a **boardroom issue**. Companies must be diligent and vigilant. They must do this not only because they have a duty under law, but because they have a duty to their customers"

General Data Protection Regulation – Recent Events / Guidance

- Concentrix
  - Independent contractor used by the government to cut tax credit payments
  - Data protection breach - 100 claimants were incorrectly sent information such as bank statements, self-assessment details and National Insurance numbers belonging to others
  - Investigation on-going - HMRC has already said that the firm will not have its contract renewed

General Data Protection Regulation – Recent Events / Guidance

- Employee prosecuted for taking data
- Former waste disposal employee who left his job
- Took information about previous clients with him
- E-mailed the details of 957 clients to his personal email address as he was leaving to start a new role at a rival company
- Prosecuted and fined
- Steve Eckersley, Head of Enforcement at the ICO:

"Employees need to be aware that documents containing personal data they have produced or worked on belong to their employer and are not theirs to take with them when they leave. Don't risk a day in court by being ignorant of the law"

General Data Protection Regulation – Recent Events / Guidance

- Privacy Notices
- "Transparency, innovation and building a culture of data confidence and trust"
- ICO asked 1,200 people to list the social issues they were most concerned about
  - Personal data appeared among 15% of people's top three concerns
  - Survey found that only 1 in 4 adults trust businesses with their personal information
- "Personal data trust is key"
- "An organisation that uses transparent methods when it comes to personal information naturally strengthens its reputation and builds the trust of its customers"

General Data Protection Regulation – Recent Events / Guidance

- Organisations need to do more to explain to consumers what they're doing with their information and why
- Reputation can be easily lost when people discover you haven't been completely honest about how you are using their information
- A clear and effective privacy notice is one way to do it
- "It's your job to embed transparency and invest in innovative ways of telling people what you're doing with their data"
- What to cover in a Privacy Notice – see the Code of Practice

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

PCI Compliance & DPA

- What is PCI DSS?
- PCI DSS - Payment Card Industry Data Security Standard
- Worldwide standard that was set up to help businesses process card payments securely and reduce card fraud
- Achieved through tight controls surrounding the storage, transmission and processing of cardholder data that businesses handle

PCI Compliance & DPA

- 12 high level requirements – 6 categories:

- Build and Maintain a Secure Network
- 1. Install and maintain a firewall configuration to protect data
- 2. Do not use vendor-supplied defaults for system passwords and other security parameters

- Protect Cardholder Data
- 3. Protect stored data (use encryption)
- 4. Encrypt transmission of cardholder data and sensitive information across public networks

PCI Compliance & DPA

- Maintain a Vulnerability Management Program
- 5. Use and regularly update anti-virus software
- 6. Develop and maintain secure systems and applications

- Implement Strong Access Control Measures
- 7. Restrict access to data by business need-to-know
- 8. Assign a unique ID to each person with computer access
- 9. Restrict physical access to cardholder data

PCI Compliance & DPA

- Regularly Monitor and Test Networks
- 10. Track and monitor all access to network resources and cardholder data
- 11. Regularly test security systems and processes

- Maintain an Information Security Policy
- 12. Maintain a policy that addresses Information Security

PCI Compliance & DPA

- Why is PCI DSS Compliance Important?
- Compliance = you are doing your very best to keep your customers' valuable information safe and secure
- Not holding on to data reduces the risk that your customers will be affected by fraud - don’t hold on to data that you don’t need to
- If you lose card data (suffer a data breach and you are not PCI DSS compliant) =
  - Card Scheme fines for the loss of this data
  - Liable for the fraud losses incurred against the cards
  - Liable for operational costs associated with replacing the accounts
  - Loss of customers / third party contracts
- You are responsible for looking after your customers' card data, regardless of who processes the data on your behalf

PCI Compliance & DPA

- What do I need to do to be compliant and where do I begin?
- Understand how card payments are processed in your organisation
- Outsource your card data to a Payment Service Provider – "fully hosted solution"

PCI Compliance & DPA

- If you are using a fully hosted solution:
  - Document the payment transaction journey illustrating all systems, applications and environments that card data touches
  - List the various service providers who provide the hosting environment, shopping cart, and payment application
  - Verify that you are not unknowingly storing or transmitting any card data making you non-compliant
  - Conduct regular checks of your website to ensure that new or unknown web pages or files have not been added
  - Regularly check the IP address that redirects customers to the third party hosted payment page to ensure that the IP address has not been changed and redirecting the card data to another site before the data is received by the hosted payment page

PCI Compliance & DPA

- When you utilise a web hosting provider or a third party payment provider that stores, processes and/or transmits cardholder data the third party is classed as a third party service provider and particular rules apply, e.g.
  - The contract must require the supplier to handle card data securely and must maintain on-going compliance to PCI DSS and evidence the compliance with the standard to you on an annual basis

PCI Compliance & DPA

- Compliance Checklist
  - Assessed annually
  - Train staff on requirements
  - Strong passwords – regularly changed
  - Watch for suspicious activity, e.g. unauthorised access to your systems, failed log-in attempts or out of hours activity
  - Remove user accounts that are no longer being used, e.g. on employee leaving

- Breach of PCI DSS = breach of DPA

Gareth Yates, Partner

Email: gareth.yates@wardhadaway.com

Tel: 0789 451 3195