BLAKE MORGAN

Data Protection awareness training: GDPR and beyond

Presenter

Mererid McDaid

Associate

Today's Agenda

- What is data protection and why its important
- Tinopolis' responsibilities
- Some definitions: 'personal data & 'processing'
- The data protection principles
- Individual rights
- Data security

Today's Objective

- For you to understand:
  - The what, why and when of GDPR
  - Tinopolis' basic obligations under data protection law;
  - How you can help to ensure that Tinopolis meets those obligations

The Big Picture

The big picture

What is "data protection"?

- The rules that Tinopolis must follow whenever it collects, stores or uses any information about identifiable individuals (staff, contributors, others…)

- For almost 20 years, these rules have been found in the **Data Protection Act 1998**

. . . this is all set to change in 2018

The big picture

What's changing in 2018?

- The **Data Protection Act 1998** has been repealed
- New legislation will apply:
  - The **General Data Protection Regulation**
  - A new **UK Data Protection Act 2018**, which transposed a new **EU Directive** for processing personal data in a criminal context
- A new **ePrivacy Regulation** to replace the existing Privacy and Electronic Communications Regulations due soon

25 May 2018

Key date

Data protection "big bang" on 25 May 2018:

- GDPR applied automatically
- New UK Data Protection Act came into force
- Deadline for new EU Directive to be transposed into UK law
- New ePrivacy Regulation was due to come into force, this has been delayed

What about Brexit?

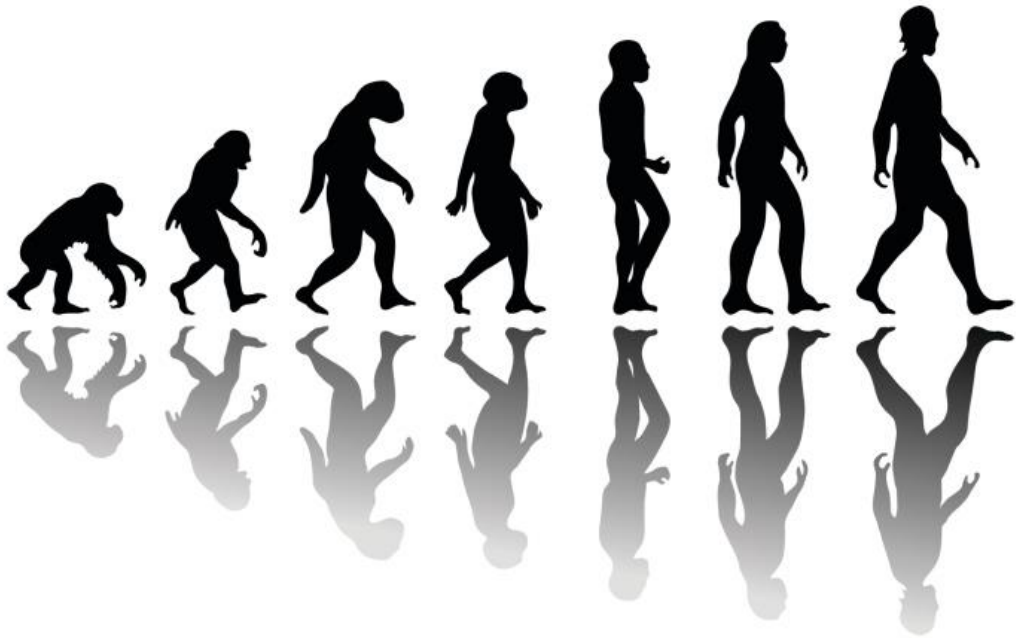
Q: How does the referendum result impact on the data protection reforms?

A: It doesn't

... for now

- Data protection reforms take effect before the UK leaves the EU and UK government intends to implement them in full
- Things may change in the longer term (but probably won't)

“Evolution not revolution”



Why does data protection matter?

Why pay attention?

- Because the GDPR requires Tinopolis to examine its systems and processes in detail and inform individuals of their new rights.
- Increased risks if get it wrong:
  - Higher fines (up to £17m or 4% global turnover)
  - Greater risk of individual claims and group actions
  - Breach of mutual trust and confidence
  - Reputational damage

Key Definitions

Tinopolis' responsibility under GDPR

- GDPR applies to Tinopolis' processing of personal data, regardless of whether acting as a controller or a processor
- What does this mean?

Tinopolis as a controller

- Tinopolis is the 'controller' of staff, freelancers, contributors, talent and others' data
  - i.e. Tinopolis determines the manner and purpose for which it will be processing personal data
- Tinopolis is therefore legally responsible for complying with GDPR
  - But, staff are responsible for handling data in accordance with Tinopolis' obligations
  - Criminal offence for staff to 'obtain or disclose or retain' personal data without Tinopolis' consent

Obligations of a processor

- A processor is responsible for processing personal data on behalf of a controller
- If Tinopolis is a processor, the GDPR places specific legal obligations e.g:
  - required to maintain records of personal data and processing activities
  - will have legal liability if Tinopolis is responsible for a breach

What is Personal Data?

- Means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier
  - Note: relates only to living individuals
- Wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people, including:
  - name
  - identification number
  - location data or online identifier

Special category personal data

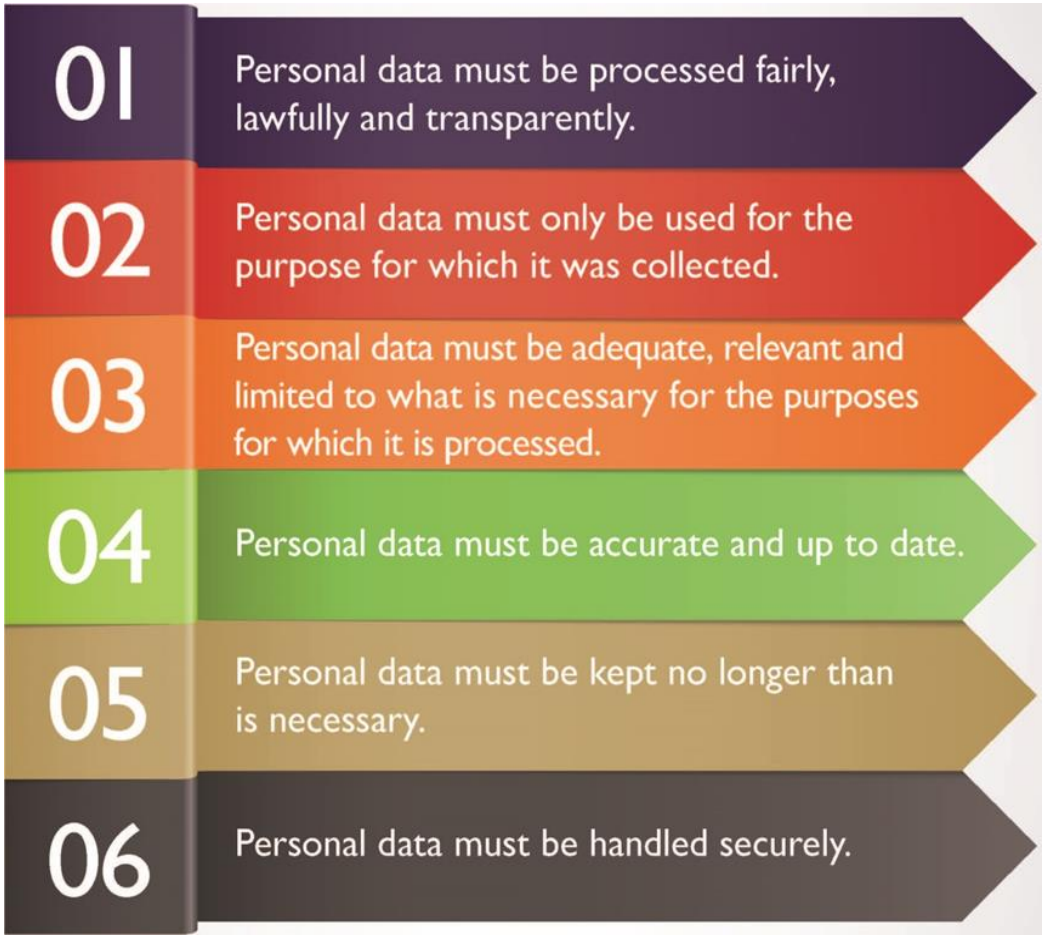
- Personal data revealing:
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade union membership
  - *Genetic data*
  - *Biometric data for the purposes of uniquely identifying a person*
  - Data concerning health
  - A person's sex life or sexual orientation
- Note: no longer includes criminal offences committed or alleged or any convictions, but safeguards in place

What is ‘processing’

- GDPR set out how Tinopolis should process personal data, but what is “processing”?
- Any data handling, whether done electronically or not, including:
  - Collecting, recording, organising
  - Structuring, storing, adapting or altering
  - Retrieving, consulting, using, disclosing
  - Disseminating or otherwise making available
  - Aligning or combining, restricting,
  - Erasing or destroying

The principles

The data protection principles



- New requirement under GDPR is that Tinopolis must not only *comply* with the principles, but must also *demonstrate* such compliance
- i.e. the 'accountability principle'

‘Fair, lawful and transparent’

- Fair handling is about being clear with individuals and managing their expectations:
  - What do individuals think you are doing with their data?
  - Have they been provided with a “fair processing notice”/ data protection statement?
  - Are you using their data in a way that would come as a surprise to them?
- What are the expectations around confidentiality and the further use of data for other purposes?

‘Fair, lawful and transparent’

- Processing personal data lawfully means Tinopolis has to have a ‘lawful basis for processing’
- Do you always need consent to process personal data?
  - No, common misconception!
- If processing ‘personal data’, you only need a general lawful basis for processing
- If processing ‘special category data’ or criminal data, you also need to have an additional lawful basis for processing

Lawful basis for processing

- Individual has given **consent**
- Necessary for the purposes of a **contract** with the data subject
- Necessary for compliance with a **legal obligation**
- Necessary in order to protect **vital interests** of an individual
- Necessary for the performance of a **task carried out in the public interest** or official authority
- Necessary for the performance of the **legitimate interest** of Tinopolis or a third party where such interests are not overridden by rights of the individual

Lawful basis for special category data

- Individual has given **explicit consent**
- Necessary for the purposes of carrying out **obligations under employment** or social security law
- Necessary to protect the **vital interests** of an individual where DS cannot give consent
- Personal data has been **made manifestly public** by DS
- Necessary to establish, exercise or defend **legal claims**
- Necessary for reasons of **substantial public interest**
- Necessary for **assessment of working capacity** of an employee

A quick quiz – True or False

True & False?

Information about someone who is deceased can never be personal data.

Tinopolis must always get consent to process personal data.

Financial information is a type of special category data.

True & False?

If Tinopolis breaches the GDPR, it could be fined up to £2 million.

Processing personal data “fairly” means making sure that people are aware of how their personal data will be used.

Shredding old applicant information is a type of processing of personal data.

Purpose limitation

- PD shall be collected for specified, explicit and legitimate purposes
- PD can't be further used in a manner which is incompatible with those purposes
- However the following further processing is permitted:
  - archiving purposes in the public interest or
  - scientific or historical research purposes or
  - Statistical purposes
  - provided have 'appropriate safeguards' in place
- *New* processing using *existing* data is potentially in conflict with the purpose limitation principle

Compatible purposes

- To determine whether the processing is compatible with the original purpose consider:
  - Link between the original and new purpose
  - The context PD was collected for e.g. reasonable expectations of the DS as to further use
  - The nature of the PD, e.g. special categories of data or criminal data
  - Consequences of the new processing for the data subjects
  - What safeguards will be in place?
- Can use data for incompatible purposes where can be specifically justified, e.g. formal disciplinary investigation, assist with police enquiries

Data minimisation

- PD must be adequate, relevant and limited to what is necessary
- Personal data should not be collected or retained on a ‘just in case’ basis
- When considering what personal data you need, ask:
  - What is the purpose?
  - Is the personal data relevant and necessary for purpose?
  - Can I achieve the purpose by collecting less/no personal data?

Accuracy

- PD must be accurate and, where necessary, kept up to date
- Every reasonable step must be taken to ensure that PD that are inaccurate are erased or rectified without undue delay
- Therefore, it's essential to
  - take every opportunity to check records are accurate and up to date
  - respond to any report from system users regarding the accuracy of their data
- When designing or procuring IT systems that will be used to process personal data, ensure that there is a facility to update/correct/annotate inaccurate data

Storage limitation

- Tinopolis has an obligation to hold personal data for **no longer than necessary** for the purposes it was processed
  - How long do you retain records for?
- Personal data that is no longer required is a liability (not an asset) and should be disposed of
  - If in doubt check Tinopolis' Data Retention Policy or seek advice
- Remember: disposing of personal data is a form of data processing!

Integrity and confidentiality

- PD must be processed in a manner that ensures appropriate security of personal data including protection against:
  - unauthorised processing
  - unlawful processing
  - accidental loss
  - destruction
  - damage
- This was a major source of DPA 1998 related risk

Security of processing

- Tinopolis must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk taking into account:
  - the state of art, the cost of implementing, the nature, scope and purpose of processing; and
  - The likelihood and severity of harm suffered by an individual

Appropriate measures

- Such measures may include:
  - Pseudonymisation and encryption
  - Ability to provide ongoing confidentiality, integrity, availability and resilience
  - Ability to restore availability in the event of a physical or technical incident
  - Process for regularly testing effectiveness of measures

The Risks

- Any loss or accidental disclosure of personal data could result in:
  - a voluntary undertaking
  - enforcement action in the form of an enforcement notice; or
- Loss or accidental disclosure likely to cause significant damage or distress could, additionally, result in a financial penalty

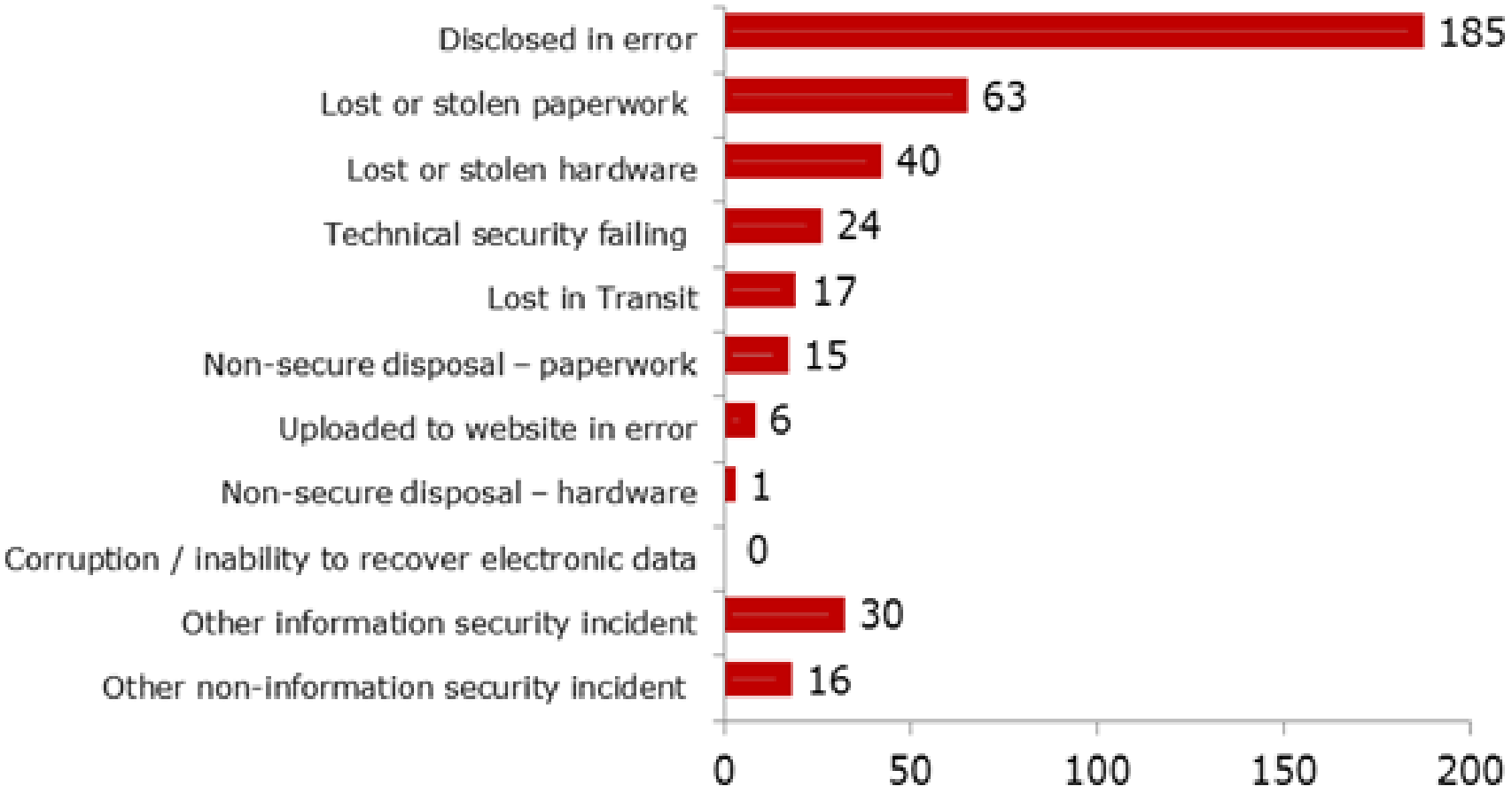
Data Breach

- Data breach reporting
  - Tinopolis must report a breach to the ICO unless the data breach is unlikely to result in a risk to the rights and freedoms of the individual
  - Within 72 hours of becoming aware of the breach, where feasible
- Reporting breaches to data subjects
  - Tinopolis must also inform those individuals without undue delay if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms
- Risk based approach
  - Be familiar with the breach reporting process to ensure that swift action can be taken

What is a data protection breach

- A personal data breach is a security incident that has affected the confidentiality, integrity or availability of personal data
- There will be a personal data breach whenever:
  - any personal data is lost, destroyed, corrupted or disclosed;
  - if someone accesses the data or passes it on without proper authorisation;
  - if the data is made unavailable and this unavailability has a significant negative effect on individuals.
- This includes breaches that are the result of both accidental and deliberate causes

Incident Types (typical quarter)



Accountability

- Article 5(2) requires Tinopolis to demonstrate that comply with the principles
- Explicit and implied obligations
- Good practice tools that the ICO has championed for a long time are now legally required in certain circumstances;
  - Data Protection Impact Assessments
  - Privacy by design
- Practically, this is likely to mean more policies and procedures for Tinopolis

How to demonstrate compliance

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply e.g.
  - internal data protection policies
  - staff training,
  - internal audits of processing activities,
  - reviews of internal HR policies
- Maintain relevant documentation on processing activities
- Appoint a data protection manager

How to demonstrate compliance

- Implement measures that meet the principles of data protection by design and default e.g.:
  - data minimisation;
  - pseudonymisation;
  - transparency;
  - Allow DSs to monitor processing; and
  - creating and improving security features on an ongoing basis
- Use DPIAs where appropriate
- Adhere to approved codes of conduct and/or certification schemes

International transfers

- The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations
- Transfers can occur by email or over the phone, or when using cloud based IT solutions
- Some transfers are permitted e.g.
  - with consent (but very limited application)
  - to permitted countries i.e. Jersey, Guernsey, Argentina, Canada, Switzerland, Israel, Isle of Man, Andorra, Faroe Islands, New Zealand
  - using approved contracts
  - specifically authorised arrangements

International transfers

- Seek advice if you are:
  - involved in transferring personal data to countries outside EEA (unless you are doing so at the request of data subjects)
  - using cloud-based solutions from providers using servers based outside EEA (beware providers' standard terms!)

New and extended rights for individuals

Privacy notice	Right to information in a detailed processing notices in concise, **transparent,** intelligible and easily accessible form
Subject access	Request and receive details of personal data held, and processing activities and safeguards No fee and responses within one month
Data portability	To receive personal data in a “structured, commonly-used and machine-readable format” where the processing has been based on consent or a contract with the data subject and has been processed by automated means.
Erasure/right to be forgotten	Controller to erase data following a request where retention of data no longer necessary; consent is withdrawn or unlawful processing
Rectification	Controller to correct (and ensure that Processors correct) data where identified as inaccurate or incomplete

Subject access requests

- In practice, the most commonly exercised right is the right to request a copy of one's personal data
- Some information may be exempt e.g. where compliance would involve the unfair disclosure of information about other people or would tip someone off about a live investigation

Can you withhold information?

- Often little scope for withholding information that has been requested so it is essential that all Tinopolis staff members appreciate that emails, reports, statements, minutes, references that they write about other individuals are potentially disclosable.
  - Avoid subjective and careless comments
  - Always assume that records could be accessed by the individuals concerned
  - Markers such as “confidential” or “private” have very limited legal status

Tinopolis' GDPR compliance project

The Audit

1. **Carried out a data audit**

- What we hold, where does it come from, where do we hold it and why?
- Do we still need it?
- Could you be doing things differently?

Documentation

2. **What information we are giving to individuals?**

- Reviewed your:
  - Privacy notices / application forms
  - Internal policies and procedures / employment contracts
  - Consent wording
- For each production, ensure that the GDPR questionnaire is completed and production specific privacy statement is completed before PD collected

Governance

3. Tinopolis' internal governance:

- Data protection manager appointed
- Reviewed internal systems / policies / procedures to ensure fit for purpose
- Remember: it's not good enough to merely comply. We need to demonstrate compliance
  - Notify Data Protection Manager:
    - if new companies that will process PD are incorporated so that can register with ICO
    - New processing activities are undertaken so record of processing can be updated
  - Carry out DPIAs of new activities which could be high risk

Individual Rights

4. **Get ready for the new rights for individuals:**

- Audit of internal systems to ensure that they meet the additional requirements
- Put in place policies and procedures to ensure compliance (remember the tighter deadline and no more fees)
  - Notify Head of HR if SAR from employee
  - Notify Data Protection Manager if SAR from someone else
  - See Individual Rights Policy for more details

Contracts

5. **Checked that contracts are fully compliant:**

- Ensure all key contracts with clients and suppliers and all contracts with talent, contributors, freelancers and release forms etc include relevant GDPR clauses
- Existing key client / supplier contracts which are continuing beyond 25 May 2018 should have the new GDPR clauses added via a data processing addendum
- Additional checks need to be put in place if data is being transferred outside the EEA
- Legal and Business Affairs team can assist with this

Questions?

BLAKE MORGAN