20/03/2018

# GDPR and Shared Services

Shared Services Conference

# Presentation Contents

Part one: Getting to Grips with GDPR

Part two: Research Data and Shared Services

# GDPR Definition of 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, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

# GDPR Definition: Special Category Data

Special Category data

"**Processing of personal data** revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation **shall be prohibited**."

# Data Protection Key Changes with GDPR

Focus on 4 key changes:

1. Accountability

- Jisc processes personal data belonging to Staff and Members
- We are required to document what personal data we hold, where it came from and who we share it with – Information Audit
- Document personal data flows and processing activities
- Data Processors are now accountable for the personal data that it processes

# Data Protection Key Changes with GDPR

## 2. Privacy by Design

- Inclusion of data protection compliance from the outset of systems and process design including research and development and pilot projects and services
- Data Protection Impact assessments where appropriate

## 3. Consent

- Conditions of consent tightened – clear and concise terms and conditions
- Most of Jisc's processing is likely to need other justifications (fair and legal processing will no longer apply) – process and privacy changes

# Data Protection Key Changes with GDPR

## 4. Reputational Damage and Penalties

- Reputational damage of a Member data breach would do Jisc serious harm
- Add to this GDPR maximum fine from £500,000 to 20 million euros or 4% of annual global turnover
- Important change – Rules apply to data processors – we are increasingly processing and giving insight on Member data

## Other changes include:

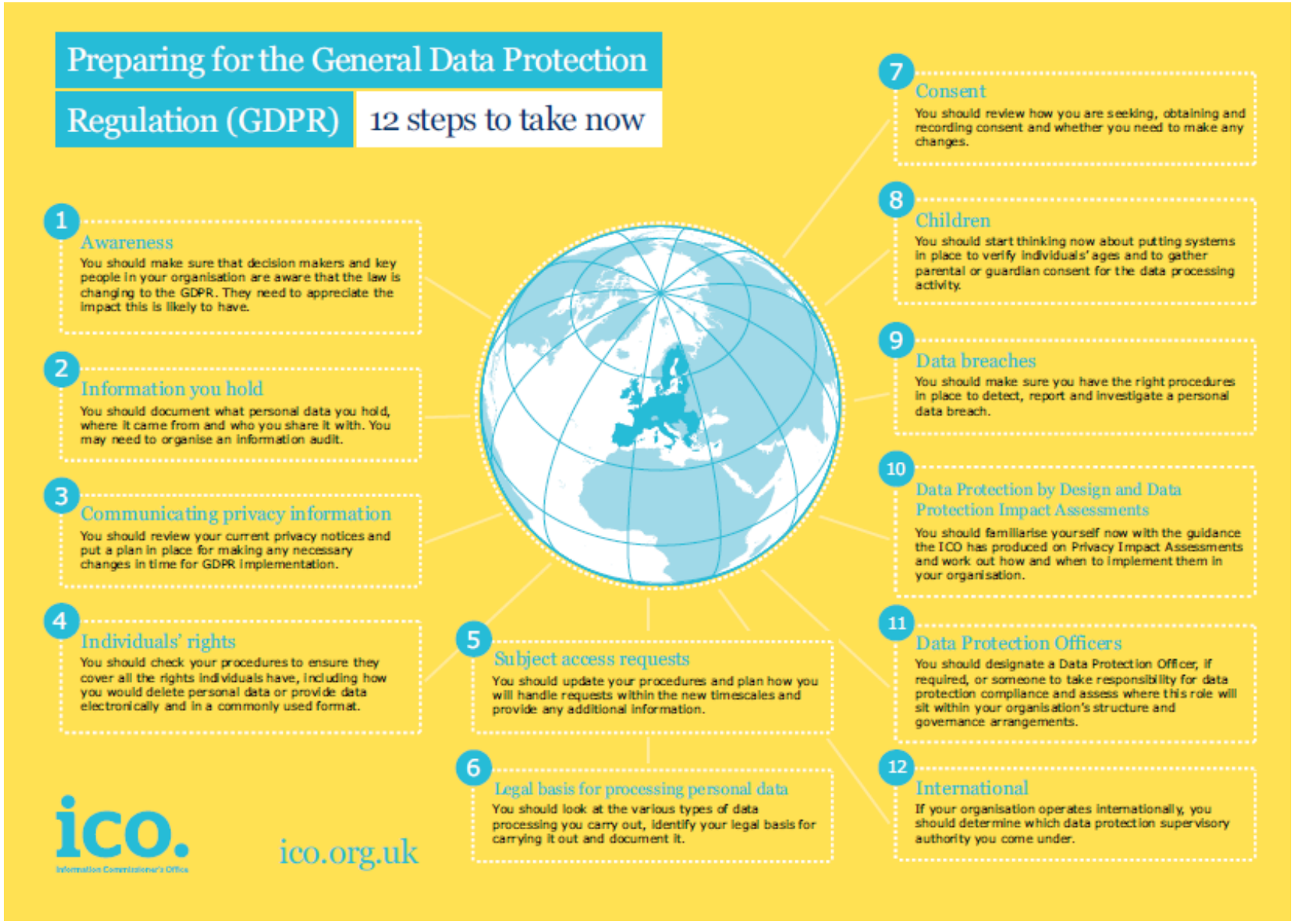
- Breach Notifications
  - Breach notification is mandatory
  - Notifications will need to be reported within 72 hours of first detection, data processors will be required to notify their customers and controllers "without due delay" after becoming aware of the breach
- Additional Rights
  - The GDPR also grants data subjects a number of rights over their information (eg access, erasure, portability) – waiting for final ICO guidance

# Established GDPR working group:

- Head of information strategy (Jisc Data protection officer)
- Records Manager
- Legal team
- Chief Regulatory Advisor
- Head of information security
- Membership and sales subject specialist (technology and the law)
- Digital Resources specialist

Remit to deliver GDPR to Jisc and give guidance and support to the FE HE and skills sector

# Implementing GDPR at Jisc



# Links to Jisc blogs

## Step 1: Awareness

Communications Plan and presentations to Senior Board; Risk Register; Intranet presence; Data Protection awareness training for all staff (current and any subsequent new staff); work with key teams handling personal information; Updates through Communication channels

GDPR: Alumni Process

Data Protection Bill and Public Authorities

## Step 2: Information we hold

You should document what personal data you hold, where it came from, who you share it with and how long you need to keep it for. You may need to organise an information audit, across the organisation, or within particular business areas.  Then need to map your personal data flows and record  of processing

GDPR: Information Lifecycle Registers

Service Categories

## Step 3: Communication Privacy Information

Review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation. There are changes to the legislation that will require you to give additional information to people

ICO Guidance to privacy notices

# Links to Jisc blogs

## Step 4: Individual rights

Check your procedures to ensure they cover all the rights individuals have (access, erasure, direct marketing and portability)

Portability Rights and Data Protection Challenges

GDPR: Backups, Archives and the Right to Erasure

## Step 5: Subject Access Requests

You should update your procedures and plan how you will handle requests within the new timescales (1 month from 40 days) and provide any additional information

# Step 6 and 7: Legal basis for processing personal data including consent

There are 6 legal basis for processing personal data and at least one must be applied :

- ***Contract****:* the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
- ***Legal obligation****:* the processing is necessary for you to comply with the law (not including contractual obligations).
- ***Vital interests****:* the processing is necessary to protect someone's life
- ***Public task****:* the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- ***Legitimate interests****:* the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
- ***Consent:*** has to be a positive indication of agreement to personal data being processed – it cannot be inferred from silence, pre-ticked boxes or inactivity

What's Your Justification ? Web forms and consent GDPR: Student Unions Service categories GDPR: A New Kind of Consent

ICO draft guidance: GDPR Consent Guidance

# Links to Jisc blogs

## Step 9: Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach. The GDPR will bring in a breach notification duty across the board

Incident Response and GDPR

## Step 10: Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments (PIAs) and work out how to implement them in your organisation.  Look at embedding mandatory data protection requirements in all procurements. Lok to embed retention and disposal periods into core systems holding and processing personal data

Article 29 Working Group Draft Guidance: See Data Protection Impact Assessment Draft Guidance

Jisc Guidance GDPR: Data Protection Impact Assessment

## Step 11: Data Protection Officer

- Required by public authorities and organisations dealing with sensitive personal data on a large-scale
- Expert, independent oversight of data processing and compliance, report to the Senior management

ICO: data protection officer guidance

## Research and the GDPR

- Research occupies a privileged position within GDPR
- Organisation that process personal data for research purposes may avoid restrictions on secondary processing and processing sensitive categories if data (Art 6 (4); recital 50)
- **As long as they** implement appropriate safeguards may also override data subject rights to object to processing and to seek the erasure of personal data
- GDPR **may** permit organisations to process personal data for research purposes without the data subject's consent (Art 6 (1)(f); recitals 47, 157)

# Research data shared service and GDPR

- **Research as a basis for processing**
- Research doesn't have a designated lawful basis of processing so will be one of the above. Does allow for re-purposing collected for research without the data subject's consent – produce record of processing

1. **Research and Consent as a legal basis**

- Under the GDPR, consent must be "unambiguous" and specific to the processing operation. This poses a challenge for research because

  > "[i]t is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of collection" (Recital 33).
  >
  > To address this challenge, Article 6(4) allows for subsequent processing operations that are "compatible." Recital 50 specifies that further processing for research purposes "should be considered to be compatible."

- Exemption: Article 5(1)(b) states, "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes." Article 89 sets out the safeguards that controllers must implement in order to further process personal data for research.

# Research data shared service and GDPR

## Research as a basis for processing

### 2. Research as a legitimate basis for processing?

- Possible that in some circumstances legitimate interest can be used legitimate interest balancing test needs to apply … rights of the individual.
- "processing for research purposes (including marketing research)" could constitute a legitimate interest, provided the controller implemented sufficient safeguards

Anonymised data is not personal data so data protection doesn't apply!!

# Shared service and GDPR

**Issues to deal with:**

1. Are you dealing with personal or anonymised data?
2. Where is data being stored? Within EEA or outside. If outside where and what provisions in place for sharing personal data? Privacy Shield v EU Model Clauses
3. Clear digital strategy around the technical and legal complexities strategy for the adoption of cloud services
4. Arduous nature of data management
   - Look carefully at any data sharing agreements:
     - Ensure they meet new transparency requirements – fairness ad transparency. Research and GDPR
     - Have a legal basis for sharing the personal data
   - Carry out appropriate due diligence on service providers
   - Check the GDPR clauses in any contract/agreement
5. Long term preservation/digital continuity

**Jisc RDSS platform is designed as an attractive and cost effective solution that focuses on these issues for you**

# Where to go for help

Information Commissioner's Office: https://ico.org.uk/

Article 29 Working Group: https://edps.europa.eu/

Legal changes: Number of free sites including: Bird and Bird guide to the GDPR

Sector guidance and advice: www.jisc.ac.uk/gdpr

Jisc Research Data Shared Service: Jisc Research Data Shared Service