What the General Data Protection Regulations mean to Schools and Governors

Tim Care, Partner, Ward Hadaway

SCHOOLS NORTHEAST
The future of our region is in school

A bit of background

SCHOOLS NORTHEAST
The future of our region is in school

- Replaces Data Protection Act 1998
- GDPR – in force **25 May 2018**
- Brexit does not affect introduction
- Regulation with direct applicability
- Data Protection Act 2018
  - Offences relating to personal data
    - Unlawful obtaining of personal data
    - Re-identification of de-identified personal data
    - Alteration of personal data to prevent disclosure

SCHOOLS NORTHEAST
The future of our region is in school

"THE BIGGEST CHANGE TO DATA PROTECTION LAW FOR A GENERATION"

Elizabeth Denham: UK Information Commissioner

What does GDPR do?

SCHOOLS NORTHEAST
The future of our region is in school

- Replaces the Data Protection Act 1998
- Governs how organisations process personal data
- Controllers must be able to demonstrate compliance
- Will affect every organisation as everyone has personal data
  - customer data, employee data, tenant data, supplier data, pupil data
- The key principles – transparency and accountability

Key Definitions (1)

SCHOOLS NORTHEAST
The future of our region is in school

- **"Controller" – GDPR**
  - "*the natural or legal person, public agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purpose and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*"

- **"Processor" – GDPR**
  - "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*"

Key Definitions (2)

SCHOOLS NORTHEAST
The future of our region is in school

- **"Processing" – GDPR**
  - "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*"

- **Examples in a school**
  - payroll services
  - software that profiles pupils
  - preparing spreadsheet with absence records
  - use of own smart phone / laptop to carry out work
  - taking and storing photos
  - disposing of old computer equipment

What Data is Covered?

SCHOOLS NORTHEAST
The future of our region is in school

- Article 4 GDPR – "Personal Data"

  "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"

- Manual filing systems – identified according to specific criteria
  - current narrow definition under DPA changes

- Pseudonymised data covered

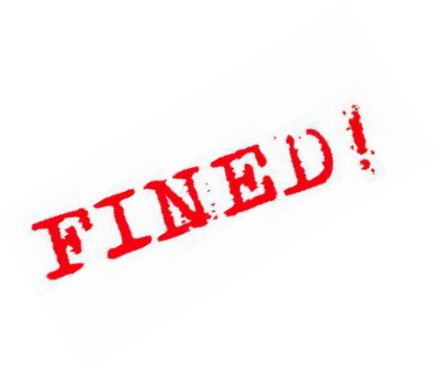
Breaches and Fines

SCHOOLS NORTHEAST
The future of our region is in school

- Breaches
  - notify all breaches to ICO within 72 hours
    - unless unlikely to be a risk to individuals
  - high risk breaches notified to individuals without undue delay

- Fines
  - two levels of fine up to
    - greater of €20m or 4% of group turnover
    - greater of €10m or 2% of group turnover
  - changes the risk profile of data protection

- Other enforcement measures



Special Category Data

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

- Only process if an Article 9 processing condition applies

NB: Not data relating to criminal convictions – this appears to be an individual category of data with special protections in the GDPR

Data Protection Principles

SCHOOLS NORTHEAST
The future of our region is in school

- Lawfulness, fairness & transparency
  - consent and fair processing
- Specific, explicit and legitimate purpose – use for that purpose only
- Adequate, relevant and limited
- Accurate and up to date
  - must take every reasonable step to ensure accuracy
- Keep only as long as necessary
  - keep data in form which identifies individuals no longer than necessary
- Appropriate security

NB: Need to be able to demonstrate compliance with the above – "Accountability Principle"

Lawful Processing – "Normal" Data

SCHOOLS NORTHEAST
The future of our region is in school

- Need to identify which processing conditions you are relying on:
  - consent of the data subject
  - necessary for contract with data subject
    - performance of contract
    - preparation for entering contract
  - necessary for compliance with a legal obligation
  - necessary to protect the vital interests of the data subject or another person
  - necessary for performance of a task carried out in the public interest/ in exercise of official authority
  - necessary to pursue the legitimate interests of controller or third party providing the data subject's rights do not override (***NB**: not applicable to processing by schools and public authorities in the performance of their tasks*)
- Additional requirements for special category data

Consent

SCHOOLS NORTHEAST
The future of our region is in school

- Need a processing condition to process personal data
- Consent is a freely given, specific, informed and unambiguous expression of wishes
- Implied consent (opt-out) no longer sufficient
- Need opt-in or clear affirmative action
- Can you rely on a pupil's consent?
- Need to keep record of how consent obtained
- No consent if significant imbalance in relationship
  - e.g. employer / employee
- Consent notice must be clear and not bundled up into a larger document
- Examples:-
  - use of photographs
  - transfer of data to education app providers
  - providing parent information to online payment systems

Data Subject Rights

- Right of access
- Right to be informed (fair processing notices)
- Right of rectification
- Right to be forgotten (erasure)
  - right to request deletion or removal of personal data
  - right only arises in specific circumstances
  - no need to comply in certain circumstances
- Right to restrict processing

Data Subject Rights continued

- Data portability
  - obligation to provide data in a structured, commonly used and machine readable format on request
  - applies in limited circumstances only:-
    - individual has provided data + is processed automatically; and
      - processing based on consent or for performance of a contract
- Right to object to processing
- Right to object to profiling and rights re automatic decision making

Accountability

- Obligation to demonstrate compliance with the data protection principles including:-
  - data protection officers
  - data protection impact assessments and privacy by design
  - documentation
    - processing record (250+ employees)
      - record processing condition relied on
    - privacy policies
    - fair processing notices
    - data breach log
    - data protection policy

Security

SCHOOLS NORTHEAST
The future of our region is in school

- Requirement to ensure appropriate security when processing personal data
- What is appropriate security?
- Balance state of technology with costs and impact and likelihood of risk
- Consider:-
  - pseudonymisation and encryption
  - ability to assure confidentiality, integrity, availability and resilience
  - ability to restore access in the event of an incident
  - process for regular testing, assessing and evaluating security
- Take into account particular risks of the processing when assess appropriate security

Data Protection Officer (1)

- GDPR requires organisations to appoint a DPO where:-
  - processing carried out by a public authority or body;
  - core activities of controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or
  - core activities of controller or processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

- Must be designated on the basis of professional qualities and expert knowledge of data protection law.

- Can be a staff member or fulfil duties on the basis of a service contract.

Data Protection Officer (2)

SCHOOLS NORTHEAST
The future of our region is in school

- Must report directly to highest management level.
- May fulfil other tasks and duties but must ensure that such tasks / duties do not create conflicts of interest.
- Tasks of a DPO are set out in Article 39 and include:-
  - inform and advise controller / processor and its employees who carry out processing;
  - to monitor compliance with the GDPR and with policies of the controller / processor;
  - to provide advice with regard to DPIAs; and
  - to cooperate with the ICO.

Privacy Notices (1)

SCHOOLS NORTHEAST
The future of our region is in school

- GDPR sets out what information you must provide to a data subject if you obtain personal data from the data subject (Article 13). This includes:-
  - identity and contact details of the controller;
  - contact details of the Data Protection Officer;
  - purposes of the processing and the legal basis;
  - if based on legitimate interests, what those legitimate interests are;
  - recipients / categories of recipients of personal data;
  - retention periods (or criteria used to determine such periods); and
  - existence of data subject rights.

- Information must be provided to a data subject **at the time the personal data is obtained**.

Privacy Notices (2)

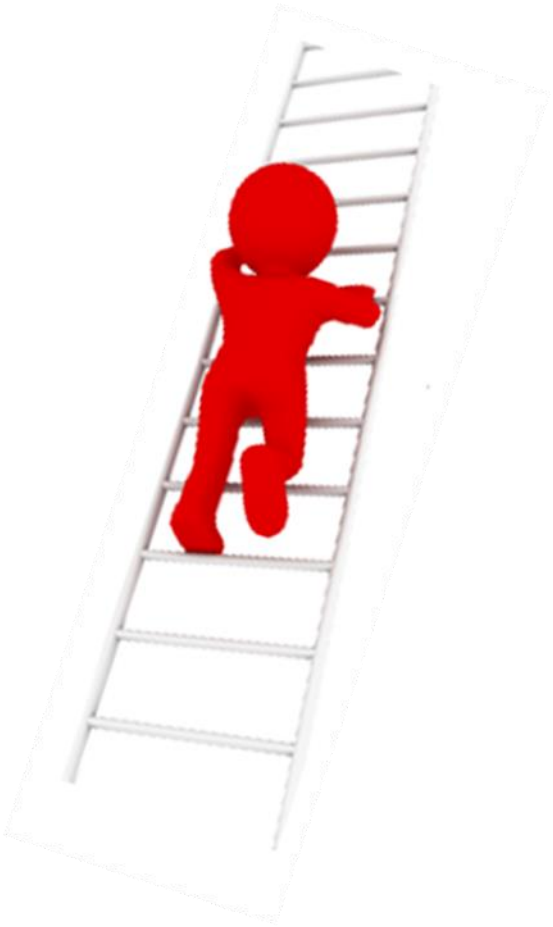
- GDPR sets out what information you must provide to a data subject if you obtain personal data from somewhere other than the data subject (Article 14). Includes most of the requirements in Article 13 but you also need to specify:-
  - the categories of personal data collected; and
  - the source of the personal data and whether it was obtained from publicly accessible sources.
- No need to inform data subject whether the provision of the personal data is part of a statutory or contractual requirement / obligation and the possible consequences of not providing the personal data.
- Information must be provided to a data subject:
  - within a reasonable period, but at the latest within one month; or
  - if used to communicate with data subject, at time of first communication; or
  - if disclosed to a third party, at the latest when the personal data is disclosed.

What should you do now?

Practical Steps

SCHOOLS NORTHEAST
The future of our region is in school

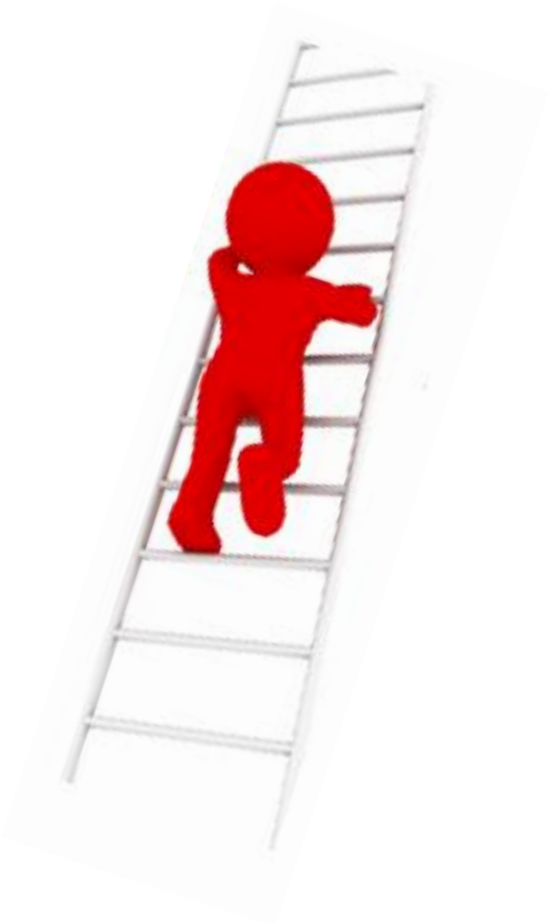
- Understand what data you hold
  - Pupil Data:-
    - address, family data, etc.
    - medical
    - disciplinary
    - academic
  - Employee Data:-
    - payroll
    - pensions
    - disciplinary file
- Understand what you do with it:-
  - cloud services
  - data retention
- Assess how GDPR will apply to that data use
  - accountability



Practical Steps

SCHOOLS NORTHEAST
The future of our region is in school

- Draw up new documentation
  - Processing record
  - Data Processing Notice
  - Data Protection Policy
  - Breach Log
- Consider
  - Data protection officer
  - Privacy by Design
  - DPIA
- Train relevant staff
- Amend existing contracts
  - Payroll
  - Outsourcing (CCTV)



Any Questions?

SCHOOLS NORTHEAST
The future of our region is in school

Tim Care

Partner | Public Sector

E: tim.care@wardhadaway.com

T: 0191 204 4224