General Data Protection Regulation

FSSU Workshops June 2018

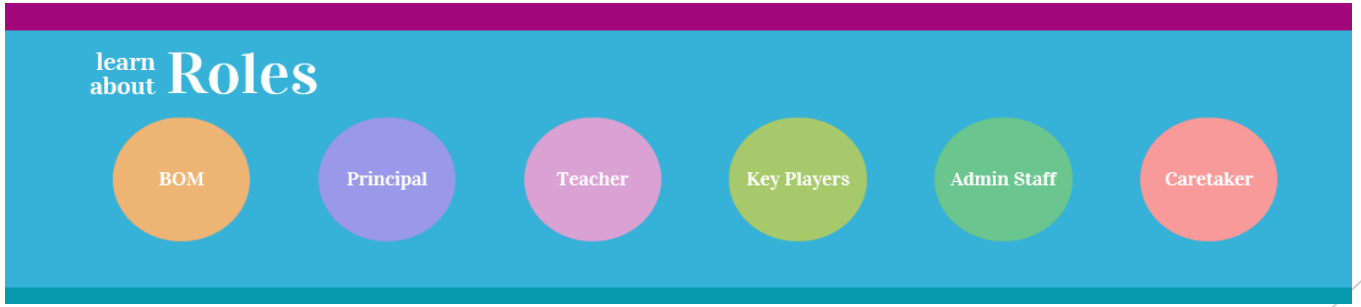
Presented by

Bernadette Kinsella

Assistant General Secretary JMB

New Resource!

www.gdpr4schools.ie



Transparency, security and accountability

- The GDPR emphasises transparency, security and accountability by data controllers and processors, while at the same time standardising and strengthening the right of European citizens to data privacy.

GDPR Principles relating to personal data processing

- lawfulness, fairness and transparency
- specified, explicit and legitimate purpose
- adequate, relevant, and limited to the minimum necessary
- accurate and kept up to date
- data minimisation
- appropriate security of the personal data
- processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of the GDPR Regulation.
  - Article 5 GDPR

Understanding the lawful basis for processing

- Schools are required to explicitly inform data subjects what lawful basis is being relied upon for each data processing operation as part of the transparency requirements.

- The data controller must inform the data subject of "the purposes of the processing for which the personal data are intended as well as the legal basis for the processing".

  - Article 6

Article 6(1)(c): the processing is necessary for compliance with a legal obligation

- For example, where the School is subject to a legal obligation to process certain educational data relating to students pursuant to the Education Act 1998, that legal obligation will constitute the lawful basis for that processing.

- By way of further example, the obligation to inform the Education Welfare Officer (TUSLA) when a student has been absent for 20 school days or more; this is a legal obligation under section 21(4)(b) Education (Welfare) Act 2000.

Article 6(1)(a): the data subject has given consent to the processing

- A school asks parents whether they give consent to their child's photograph being taken at the school sports day and put up on the school website.
- Parents are informed that giving consent is truly optional, and they do not have to give consent if they do not wish to do so, and if the parent declines to give consent their child can still fully participate in every event at sports day.

What is personal data?

- ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’);
  - Article 4 (1)

Who is the Data Controller?

- 'controller' determines the purposes and means of the processing of personal data;
- Board of Management deemed data controller

- Article 4 (7)

What is data processing?

- ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data
- Everyday tasks
  - Collecting
  - Recording
  - Filing
  - Storage
  - Disclosure
  - Retention
  - Destruction

- Article 4 (2)

Data Processor

- ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
  - Article 4 (8)

Third Party

- ‘third party’ means a natural or legal person under the direct authority of the controller or processor, are authorised to process personal data.
  - Article 4 (10)
    - Article 28
    - Article 32

Records of Data Processing Activities

- Each controller shall maintain a record of processing activities under its responsibility.

  - Article 30 (1)

Information to be provided to the Data Subject

- Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with specific information.
- This information is contained in a Privacy Notice.
  - Article 13

- When first collecting personal data, the school must provide the following information to individuals:

- *The name of the data controller*
- *Contact details*
- *Reasons for collecting the data*
- *Uses to which the data will be put*
- *Contractual or statutory requirement*
- *If processing is based on consent, the right to withdraw consent*
- *To whom the data will be disclosed*
- *Whether the data will be transferred outside of the EU*
- *Legal basis for the processing of the data*
- *Right to access, rectification and erasure*
- *Retention period*
- *Right to lodge a complaint*
- *Right to know further processing of data other than that for which it was collected.*
- *Information must be set out in clear, concise and in an easily accessible manner*
  - Article 13 GDPR

Retention

- Data controllers must be clear about the length of time for which personal data will be kept and the reasons why the information is being retained.
- In determining appropriate retention periods, regard must be had for any statutory obligations imposed on a data controller.
- If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner.
- Processing for archiving purposes – Article 89 – is subject to appropriate safeguards.

Data Subjects Rights

- Right to complain to supervisory authority.
- Right of access.
- Right to rectification.
- Right to be forgotten.
- Right to restrict processing.
- Right to data portability.
- Right to object and automated decision making/profiling.
  - Articles 12-23

Subject Access Request

(SAR)

Significantly greater rights of access

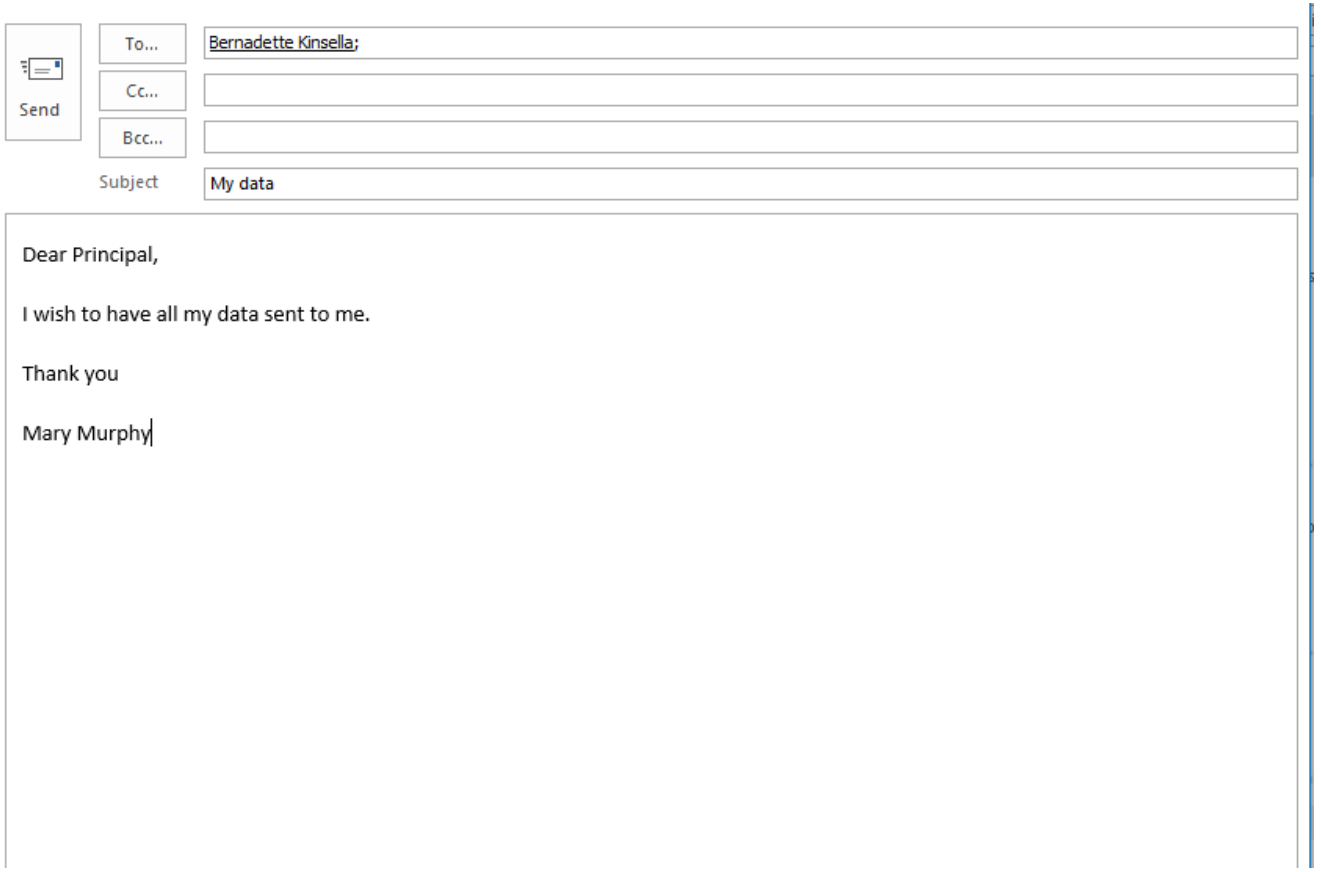
- Right of rectification:
- *"Something is wrong. I want that tweaked."*

- Right of erasure:
- *"I want that removed."*

What does a SAR look like?

- Email request
- Written letter seeking ‘all my stuff’
- Arrive up to the school asking for their data
- Who is responsible for dealing with SARs?

What to do?


Send
To...
Bernadette Kinsella;
Cc...
Bcc...
Subject
My data
Dear Principal,
I wish to have all my data sent to me.
Thank you
Mary Murphy

Responding to a Subject Access Request

- Calendar month
- Protocol for responding
- Data mapping/data audit trail
- Redaction
- Complex and time consuming
- Sanctions and fines

Data Breach

Integrity and Confidentiality

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
  - Article 5(1)f)

Incident breach management

- Recommend a simulation exercise
- In real time assess how you are going to respond
- Can happen at any time on any day in the year
- Remember, the clock starts ticking from the time of the breach
- Data vulnerability v data breach?

Data Breach Notification

- Type of Breach
- How serious?
- Risk to affected individuals?
- Data Breach Notification Form
- https://www.dataprotection.ie/documents/gdpr_forms/National_Breach_Notification_Form.pdf

Cyber attack

Plan for when not if!

DO

- Update your software regularly
- Use anti-virus software
- Browse and download software only from trusted websites
- Regularly back up the data stored on your computer
- Report it!
- Consult your anti-virus provider on how to unlock and remove the infection from the device

DON'T

- Click on attachments, banners and links without knowing their true origin
- Install mobile apps from unknown providers/sources.
- Take anything for granted.
- Install or run non-trusted or unknown software.
- Do not pay out any money

Awareness

Log your data activities

- What kind of data do I process?
- What kind of data is on the files?
- Where is it stored?
- What type of software system is it on ?
- Who has access to it?
- What levels of security are in place?
- How long do I keep it for?

What can I do in my role?

- Engage in a data protection compliance audit
- Encryption/Passwords
- USB
- Turning off computer screens
- Note-taking
- Telephone messages
- Emails
- Government Departments - communications

Responsibilities

- Adherence to high standards of ethics and professionalism in all data entries
- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data.
- Assisting the Principal with access requests

Responsibilities

- Ensure that any handwritten notes in any notebook/school diary are transferred to the school administrative system as soon as possible (to ensure availability of data, allowing appropriate back-ups to be made, accountability, transparency, keeping data safe and secure, etc).

Best-practice

- Ensure personal data (particularly sensitive personal data) is processed in a safe and secure environment
- Never brought off-site unless appropriate steps are taken to protect the data in motion

Consideration!

- Never signing the School up to any apps or software relating to school business, or requiring students to engage with apps/software without the prior written approval of the Principal.
- Never storing data relating to school business on unapproved devices or systems (eg. personal smartphones, tablets, cloud storage accounts etc).
- Never sharing work-related data on unapproved systems (eg. talking about a student or teachers on a WhatsApp group).

Don't

- Use information for a different purpose than that for which it was collected
- Disclose data to other staff (unless it is required as part of their work)
- Take personal data out of the school unless strictly necessary

Routine

- Adherence to the school's data policy which requires all staff to store work-related materials on the approved school system.

- This is to ensure that there is adequate transparency, accountability, oversight, and that appropriate back-ups are made.

It's the little things!

- IT Security
- Physical and environmental security
- Taking work home
- Trickery and Impersonation
- Cyber attack

IT Security

- Consideration should be given to:
- the level of IT security
- logging and audit trail capability on software
- access permission levels
- fire-wall software
- encryption software
- physical and boundary security for offices and file storage areas and
- the safe and secure destruction of data and data-storage devices

Physical and Environmental Security

- It is important not to forget issues like doors, locks, filing cabinets, alarms, security lighting
- Physical and boundary security for offices and file storage areas (including CCTV systems), and
- Where hardware has become outdated and is being replaced (e.g. servers and personal computers), due consideration needs to be given as to how the personal data stored on those units can be securely destroyed.

Taking work home?

- Need to ensure that personnel are fully aware as to how to use USB devices securely.
- Where personnel take work home or off-site in the form of manual files, (which is more vulnerable to loss) consideration needs to be given as to whether manual data should be converted to electronic data to avoid the need to take manual data off-site.
- Encryption
- Strong passwords

Trickery and Impersonation

- Front-line staff are the individuals most susceptible to blagging and phishing attempts (i.e. obtaining personal information about third parties without that party's knowledge and without their consent, through the use of impersonation, trickery, or deception).

- Establish simple procedures that personnel can understand and follow easily. For example, front-line staff should be trained to seek proof of identity so that they can verify the identity of the person with whom they are dealing before they release information to that person.

Protocols

- Do not provide information unless you are certain of the person's identity and can show proof that you have taken steps to verify that identity.
- Always take steps to ensure that the person to whom you are providing the information has a valid, legal entitlement to receive that information. If in doubt, ask them to furnish their request in writing.
- The normal rigours should not be relaxed just because the person making the request for information works for a Government Department, or is a State official (e.g. the Department of Education and Skills, An Garda Síochaná).

Questions

www.gdpr4schools.ie