SIMS helping schools inspire

Supporting GDPR

Best practice Networking Learning

GDPR from a MIS Perspective

Paul Featherstone, Product Manager

Agenda for this session…

- Introduction
- GDPR headlines
- Capita SIMS and GDPR
- Slides will be sent out after the presentation
- Due to the number of people attending the Webinar, questions will be answered and sent out with the slides

Introduction to the General Data Protection Regulation

- The GDPR comes into effect on 25th May 2018
- Although a EU Law, ministers are in the process of transferring this law into the UK in light of Brexit
- GDPR primarily tightens areas already covered by the Data Protection Act with some additional enhancements
- Capita are not GDPR experts!
- www.ico.org.uk is a massively useful website

Owner, Controller, Processor Definitions

Data Owner or Subject

The person who the information is about

Data Controller

The person who makes decisions with the information

Data Processor

Handles the information under instructions of the controller

Responsibilities

SIMS

ON PREMISE

Data Owner or Subject

The person who the information is about

Data Controller

The person who makes decisions with the information

Data Processor

Handles the information under instructions of the controller

SIMS helping schools inspire

ON PREMISE - Where no satellite products are used, e.g. Agora, TeacherApp or InTouch, i.e. no data is sent out from the server to a Capita product

Best practice Networking Learning

Responsibilities

SIMS ON PREMISE

SIMS HOSTED

Data Owner or Subject

The person who the information is about

Data Controller

The person who makes decisions with the information

Data Processor

Handles the information under instructions of the controller

CAPITA

SIMS helping schools inspire

HOSTED - Where Capita processes data in Hosted SIMS or a Capita Satellite product such as Agora

Best practice Networking Learning

Personal information must be fairly and lawfully processed

Lawful Processing

- For processing to be lawful under the GDPR, you need to identify **a lawful basis** before you can process personal data. These are often referred to as the "**conditions for processing**" under the DPA.

Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes

Consent

- There must be some form of clear affirmative action – or in other words, a positive opt-in.
- consent cannot be inferred from silence, pre-ticked boxes or inactivity.
- Consent must also be separate from other terms and conditions, and you will need to provide simple ways for people to withdraw consent.
- Think about 3rd party applications using your MIS data.
- How can SIMS help?

The GDPR contains new provisions intended to enhance the protection of children's personal data.

Children's Personal Data

- Where services are offered directly to a child, you must ensure that your privacy notice is written in a clear, plain way that a child will understand.
- The GDPR states that, if consent is your basis for processing the child's personal data, a child under the age of 16 can't give that consent themselves and instead consent is required from a person holding 'parental responsibility'.
- but note that it does permit member states to provide for a lower age in law, as long as it is not below 13.

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA

Individual Rights

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The right to be informed

- Builds upon the **Lawful Processing** statement earlier.
- The right to be informed encompasses your obligation to provide '**fair processing information**', typically through a **privacy notice**.
- It emphasises the need for transparency over how you use **personal data**.
- Builds upon Principle 1 of the DPA '**Fair and Lawful**'

The right of access

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed
- access to their personal data
- Removal of the €10 charge
- One month to comply
- What about requests for large amounts of personal data?
- How can SIMS help?

The right to rectification

- Individuals are entitled to have personal data **rectified** if it is **inaccurate or incomplete**.
- You must respond within **one month**.
- This can be extended by **two months** where the request for **rectification is complex**.

The right to erasure

- The right to erasure is also known as '**the right to be forgotten**'.
- Where there is no compelling reason for its continued processing.
- The right to erasure **does not** provide an absolute 'right to be forgotten'.
- There are some **specific circumstances** where the right to erasure **does not apply** and you can **refuse** to deal with a request.
- **How will SIMS help?**

The right to restrict processing

- When processing is restricted, you are **permitted to store the personal data**, but **not** further process it.
- Where an individual **contests** the accuracy of the personal data, you should **restrict the processing** until you have **verified the accuracy of the personal data**.

The right to data portability

- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- How will SIMS help?

The right to object

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority.
- Direct marketing.
- Processing for purposes of scientific/historical research and statistics.

Rights in relation to automated decision making and profiling

- The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

You are expected to put into place comprehensive but proportionate governance measures

Accountability and governance

- Ultimately, these measures should minimise the risk of breaches and uphold the **protection of personal data**.
- Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have **good governance measures in place**.

The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority.

Breach notification

- A **personal data breach** means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.
- A notifiable breach has to be reported to the relevant supervisory authority within **72 hours** of the organisation becoming aware of it.

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations

Transfer of data

- Cloud storage or backup solutions
- 3rd party applications using your data

In summary…

- Lots to think about, please discuss with me any concerns or issues you have in relation to a MS.
- The DPA and future GDPR raises a lot of questions, many people say refer to our website for more information, I can vouch for the ICO site, it's really clear and easy to understand.

www.ico.org.uk

Questions and Answers

Q - Is the report available in SIMS Primary?

A - There will be a 'Person Data Output Report' in SIMS Primary in 2018

Q - I don't have the data protection group in my sims yet i am on 7.176

A - 7.176 is the Spring release, the new permission group is available from the Autumn (7.178) release of SIMS

Q - Are there plans to make Parental Consent easier to report on? Currently all consents output to one cell.

A - If you include the Parental Consent Sub-Report and set a filter on the sub report for the first consent, then add the sub report again and filter for the second consent and repeat, you will then get a column for each Parental Consent.

Q - Will the Statement at the end of the CES Data Collection Sheets be amended to reflect DGPR in the next release?

A - That's a good point, we will review this for the Spring 2018 release.

Q - Hi, sorry i was late - is there a recording of this to catch up on please?

A - Yes, the Webinar was recorded and should be made available.

Q - Have you any advice for staff who are accessing SIMS remotely or on school/home computers/mobile devices

A - There are going to be many different ways that schools will achieve this. It's hard for me to advise, but in this case the School will be the Processor and will be responsible. Please seek advise from appropriate security experts.

Q - can a parent of a child aged over 16 request data on that child?

A - If they have the consent of that individual.

Questions and Answers

Q - Will SIMs be fully compliant by May 25th in relation to right to erase?

A - That is what we are investigating and working towards, please see here (https://myaccount.capita-cs.co.uk/Notifications/GDPR-Developing-in-SIMS-2018/)

Q - Under article 30 there is a requirement to record processing activities, if a school uses nothing else other than SIMS, how would you envisage this looking ie. what sort of format should it be in, how much detail would be required.

A - If you are just focusing on SIMS, i.e. SIMS processing the data, then I would state in your privacy notice that you are using SIMS as your schools Management Information System. But I think I can elaborate a little further for the advantage of other scenarios. The ICO have said that in the privacy notice you can state by category how data is processed, i.e. you can state that your school will use a communication 3rd party to send out school emails, now you don't have to name InTouch, SchoolComms etc, as you could be changing providers from time to time. SO mention all your processing by category, Online Payments, Virtual Learning Environments and so on.

Q - Some schools have said that the GDPR will only apply to data collected from the date of the new regulations. Is this correct or does it apply to all data held in SIMS?

A - No, GDPR will apply to all data recorded, no matter when it was recorded.

Keep up-to-date with SIMS...

Be first to hear our news about our latest developments by signing up to our newsletter – **www.capita-sims.co.uk/stayintouch.**

Visit www.capita-sims.co.uk for everything you need to know about SIMS, including our extensive training calendar, webinars and upcoming events and conferences.

@CapitaSIMS