GDPR Questions Answered from Customers of SIMS

Answering all the questions you have asked us regarding GDPR and Capita's position on compliance

05/05/2018

Contents of the Page

Latest Update

To make locating the latest update easier, we have summarised the update in the list below. You can easily jump to the appropriate section by clicking on the update, or by looking for the yellow highlight on the page.

05/05/2018 - Additional questions answered about SIMS .net

12/04/2018 - Answers to some questions about SIMS .net and terms and conditions.

29/03/2018 - Additional information on when Capita deals with 3rd party

Introduction...

We recognise that our customers will have many questions regarding GDPR and their Capita products. To help you get the answers and the evidence you require, we have put together this GDPR FAQ page. We are being asked the same questions from many customers, so we hope you will review the questions presented here and read though the supporting documents to provide you with the reassurances that Capita are working towards being GDPR compliant.

If after reading the questions or reviewing the additional resources you still have unanswered questions, then please use the link at the bottom of the page to submit your specific question.

In relation to the SIMS Suite of Products and Services...

Dealing with your data when a case gets escalated with the Service Desk
For customers who have a service level agreement with Capita, there will be times when copies of your SIMS Database may be needed for further investigation to aid the resolution of a support incident. The Service desk follow and comply to the ESS policy 'Customer Policy Summary – Data Usage (https://myaccount.capita-cs.co.uk/Search/DownloadDocument?s=ResourceID-1-5985)'
This ensures that customer data is managed and stored by the Service desk according to company data retention guidelines, and are removed after the set retention period of 90 days after the support incident has been closed.

Data is only requested for the continuation of a support incident and is used for troubleshooting or testing purposes, as agreed within your contracts with Capita Education Software Services (ESS). When data is requested for a support incident the Service desk will provide all the required guidance and information by sending a quick reference guide on the original email requesting the required data. Please see the link 'Instructions and Guidance for Uploading Data (https://myaccount.capita-cs.co.uk/Search/DownloadDocument?s=ResourceID-1-5985)' for further information and instructions.

- Instructions and Guidance for Uploading Data (https://myaccount.capita-cs.co.uk/Search/DownloadDocument?s=ResourceID-1-5985)
- Customer Policy Summary - Data Usage (https://myaccount.capita-cs.co.uk/Search/DownloadDocument?s=ResourceID-1-5886)

Dealing with your data when you attend a UAT workshop

The UAT room is a locked down room which only UAT Team Members and some managers have access to. The UAT room is on a separate network locked down from the main capita network.

Before customers send data to SIMS UAT:

1. We must receive an Agreement of Use form from the customer. This form includes information such as how long the data can be held by us, if it can be used for testing and gives us permission to prepare and hold the data for the workshop or other purposes.
2. The school or LA name is added to the dataset library and noted as waiting for data to arrive.
3. Once the agreement of use form arrives the expiry date of the dataset should be added to the dataset library and then the paper copy stored in the agreement of use form [AOU] UAT Folder which is locked in our cupboard.
4. The UAT team must set up a user account for the customer to enable them to upload their data to us securely. This folder will only remain open for a set timeframe of 30 days to ensure that no unsolicited data can be sent via the SFTP. Once this has been created the UAT Analyst must send the log in credentials to the customer in an encrypted email to enable them to upload their data to the correct location securely.

Following Data Upload:

1. Once the customer has confirmed the upload of their data the dataset library must be updated to read data received, in need of preparation for testing.
2. The data must be moved to a secure location until the UAT Analyst is ready to process it. When ready the UAT analyst should contact the customer to obtain the password for their data.
3. The data should then be prepared for download

Processing Customer Data:

Download the zipped and encrypted customer data from the SFTP site to a UAT PC (which is on the separate UAT network) to begin processing. If once extracted, the data is any other format other than the expected it is deleted immediately, as other file formats such as .exe could be or contain malware.

Data Storage. This is the process of recompressing and recording the schools data in a form of a CD or DVD:

1. Encrypt the customer's data. The data is now password protected which only members of the UAT team know and It is compressed into a ZIP file.
2. The zip file is then burnt to disk. Add a disk label with its unique dataset library number to identify the CD. Record on the label, Date of preparation, SQL version of the data, UAT members Initials.
3. Put disk in a sleeve and place in the UAT safe (safe keys are held in our Key lock safe which only UAT team members know the combination.

4. Record the Unique Dataset Library number on the Data Agreement of Use form. This will assist when destroying the data after the agreement of use form expires.

Data Destroyal:

When the agreement of use form reaches its expiry date the data is destroyed securely by placing it in the UAT disk friendly shred it bin within the UAT room. The date of destruction is recorded within the dataset library and the customer informed by email that the data has been destroyed. The Data Agreement of Use form is then moved to the expired folder which is locked in our cupboard where it will remain for 3 months.

When a customer wants to take part in a User Acceptance Testing Workshop and use their own data, we ask customers to complete the following form:

- Capita SIMS UAT - Agreement of data use form (https://myaccount.capita-cs.co.uk/Search/DownloadDocument?s=ResourceID-1-5986)

Dealing with your data with any satellite products
Many customers will use additional software and services such as Agora, Parent App or Options Online. We are currently carrying out data protection impact assessments (DPIA) on these products, the outcome of which may result in either a specific Privacy Notice for that product or guidance for schools to write their own. The status of these assessments can be seen below:

- SIMS Student (DPIA in progress)
- SIMS Parent (DPIA in progress)
- SIMS Activities (DPIA in progress)
- SIMS Agora (DPIA in progress)
- SIMS School View (DPIA in progress)
- SIMS Teacher App (DPIA in progress)
- SIMS InTouch (DPIA in progress)
- SIMS Parent Lite App (DPIA in progress)
- SIMS Options Online (DPIA in progress)

How is your Hosted SIMS service made secure and what reassurances can you provide?
As you may understand there is a lot of technical processes in place in delivering our Hosted SIMS Service. The hosting team have put together this comprehensive document that takes you through questions such as:

- Technical overview of our Hosted SIMS
- Guide to our Operating Model
- Our approach to Security
- Our approach to Resilience, Backup and Recoverability
- Connecting local software in your school to Hosted SIMS

- Hosted SIMS Guidance (https://myaccount.capita-cs.co.uk/Search/DownloadDocument?s=ResourceID-1-5057#)

Updates and enhancements to the SIMS Suite of Products
In recent releases of SIMS we have made improvements to help schools with their GDPR compliance, recent improvements have been:

- Introduction of the Person Data Output report to support schools with Subject Access Requests (Autumn 2017 saw this for students, Spring 2018 for Staff and Contacts)
- The Summer 2018 release of SIMS will introduce a bulk delete of data from student's records, this will support data retention policies.

Further information on these changes can be found at here (https://myaccount.capita-cs.co.uk/Notifications/GDPR-Developing-in-SIMS-2018/).

Common questions asked about SIMS Products

Q - Do you have a GDPR contract that schools can sign with you?
A - What do you mean by a GDPR contract? For which product or service? This is rather open to interpretation.

Q - Will all customer terms and conditions be updated in light of the GDPR changes?
A – Yes, new Terms and Conditions for the SIMS Annual Entitlement are in the final stages of review and will be part of the contract renewal packs.

Q - There does seem to be a "good practice" suggestion that the password for the MIS should not only be different to the network password but that we force regular changes. I am in two minds about whether this would be effective but can you let me know if there or will be any functionality in Sims to monitor change of passwords and also set password complexity
A - Schools can choose to enable or not the active directory authentication with SIMS, i.e. to link or not to link network authentication to SIMS or not. More details on the function can be found here (http://simspublications.com/242322/assets/sysman.pdf) on page 8. A schools System Manager can methodically reset users passwords, but this is not currently on our roadmap to automate in any way, nor is to enforce password complexity. A user can re-set their password when they like and they can set it with any complexity they like, for example g~Q6ES.8MEeqx^,z how easy this is to remember without writing down (a risk) is to be decided by the school. Development in this area has been discussed with our SIMS Software Advisory Panel recently and the outcome was that there are more important enhancements we need to achieve to assist schools with their GDPR journey.

Q. Please can you advise us whether Capita considers itself to be a Controller or Processor in relation to our school.
A. In the context of providing Sims to self-hosted schools (sims.net is installed locally on a server within the school), the customer is in control of the system. In this scenario, the school is the data controller and Sims is simply the software provider.

For customers who use the Hosted Sims Services, the customer remains the data controller however Sims is primarily the data processor here. This is because although control over what the data is used for, how long it is kept for etc. remains with the school, the data is held on our systems and can be accessed by our employees where required.
In certain scenarios, within some of our products and services, Sims takes on data controller responsibilities. This is outlined in relevant Privacy Notices/Privacy Notice Guidance.

Q. The headteacher of one of the schools that we support has suggested that the absence of an audit trail within SIMS 7 - to identify edits/changes along with dates/times and the author of these changes - means that the database does not conform to the requirements of GDPR. Please could you comment on this?
A. An audit of data is held for certain modules within SIMS, one of those areas is Dinner Money, here financial transactions are taking place. We do recognise that our current SIMS system does not have a full and in-depth auditing facility, for this to be in place for every module, process and action, would have needed to have been implemented at the beginning of SIMS development several decades ago. To fit in full auditing into SIMS .net would be a huge technical undertaking, one which would cause issues with not only SIMS, but our and partner products. We are currently completing Data Protection Impact Assessments for all our products, any outcomes that we can share with our customers in the form of updated Privacy Notices will be made available in this notification.

Q. Please advise how historical staff records can be deleted, as this has been an issue in the past where records are linked to timetables/permission/assessment/user accounts, and cannot be deleted, just renamed and personal details just blanked out.
A. Once we have completed the work on supporting data retention policies for students, we are reviewing the

current delete staff routine. We understand that where you had a future member of staff all ready and set up in SIMS prior to their start date, but they declined the job last minute, it's difficult to delete their record, this is what we hope to improve. Where a member of staff has been at the schools for many years, because of the numerous and detailed links to all things in SIMS from attendance registers, classes, detentions, cover, medical events, achievements, behaviour, SEN and many more, deleting staff is really hard. We must ensure that when we do, the SIMS database remains in tack and continues to function. Another area we hope to introduce in the future is anonymisation for staff and students. It may well be safer to anonymise the record rather than delete it.

Q. Staff Personal Data: Staff names and contracts passed to solicitors for contractual queries or any other business is effectively sharing personal data; should we have an agreement signed or will this come under public task as employers? Is a contract "sensitive" data?
A. If you are sharing personal data with solicitors or any other third party, then you need to ensure that they are compliant with GDPR. It's the data controller at the school who needs to ensure they have checked with all third parties their GDPR readiness. Capita cannot judge or advise if that agreement you have with the solicitors can be performed under a pubic task. The anecdotal piece of advice I would give is to make sure that none of the individuals on whom you share their data cannot turn around to you and say "I didn't know you were do that with my data…"

Q. Do Capita check that partner organisations are GDPR compliant?
A. Partners are requested to liaise with the Partner Development Support team for all products that require Accreditation. The team will ask for the details on the following areas:

- Data Protection Statement (Public URL Please)
- Privacy Statement (Public URL Please)
- Public Information about the Product (Public URL Please) *
- Public Information about the Company (Public URL Please)
- Technical Contact details

In relation to personal data we hold on you…

What policies and procedures do you have in place to protect personal data?
ESS is required to be compliant to Capita Group Policies and Standards. Our Cyber and Information Security Policy is available upon request, however the accompanying standards are confidential internal documents.

The Group Policies and Standards include (but are not limited to):

- Cyber and information Security Policy
- IT Standard
- Data usage Standard
- Acceptable Use Standard
- Physical Security standard

ESS also has local security policies which all employees must be compliant to, these include (but are not limited to):

- Vetting and rechecking
- Supplier Security
- Clear desk
- Building security policy
- Change management policy
- Information Security incident reporting
- Data Usage Policy

What technical and organizational security measures do you have in place to protect personal data?
Technical and organisational controls protecting personal data include (but are not limited to):

- Employee training and awareness
- Access control measures across ESS systems involving authorisation, approval and review
- Threat assessments
- Risk assessment and treatment
- Change management
- Encryption
- Masking of data
- Appropriate removable media handling
- Back up processes
- Disaster recovery procedures
- Data Protection Impact Assessments (DPIAs)
- Penetration testing
- CCTV

- We hold a current ISO27001 certification (https://myaccount.capita-cs.co.uk/Search/DownloadDocument?s=ResourceID-1-5988)

What data does your organisation hold in relation to our school?
As a customer of Capita and to enable us to provide software and services to you, we hold information such as school name, address and primary contact information, details which would have been provided to us by you when signing a contract. In addition to this information, customers at the school can sign up for services to access support and on-line help, this information is linked to the schools main record to enable us to track service level agreements, software licence and maintenance contracts. We use Microsoft Dynamics 365 to securely manage your personal contact information, account information and service desk case history. Dynamics 365 is a highly encrypted system hosted in Azure, with our data centres being in Dublin UK. You can find out more about Microsoft's commitment to data security in the Microsoft Trust Centre (https://www.microsoft.com/en-us/trustcenter).

Does your organisation provide training to staff on data protection or management?
Yes, all Capita staff are required to take regular training on:

- Information Security Awareness
- Data Protection Awareness and GDPR
- Financial crime

Are you registered with the Information Commissioners Office?
Yes we are registered and details can be found on the ICO's Data Protection Public Register (https://ico.org.uk/ESDWebPages/Entry/Z6674638).

Does your organisation have differentiated access to data depending on the sensitivity level?
Yes, we have strict procedures and access arrangements for all our systems when dealing with personal data. Please see the information under the headings when dealing with your data.

Who is the person responsible for data management / protection in your organisation?

- Name: Jenny Coombs
- Position: Group Data Privacy Officer
- E-Mail: privacy@capita.co.uk

Does your insurance cover the costs related to data breaches?
GDPR sanctions exist as a deterrent against non-compliance. Our understanding at the moment, is that if financial penalties are indemnified by another, this would defeat the purpose of the fines and would therefore not be permitted. For this reason, ESS is not insured to cover the costs related to data breaches.

Other GDPR related activities

What action are you taking to prepare for the GDPR?
This is a question asked a lot and is very broad, the following may help to answer the underlying questions:

- Internal Security and GDPR Forum to monitor GDPR readiness, reports monthly to the Board
- Capita GDPR Training/Data Protection Mandatory Training
- GDPR blogs, videos and webinars for staff and customers on GDPR
- Internal GDPR lunchtime workshops

How secure are your systems?
As well as our ISO certification, employees undergo frequent and mandatory training on all matters relating to GDPR and security. Customer data is processed in a variety ways and as part of our GDPR readiness have undergone assessments with providers such as Microsoft Azure to seek reassurance that they too are GDPR ready and their systems are secure.

When dealing with third party suppliers...
Before acquiring services from a third party supplier, ESS completes due diligence if access to systems and or sensitive information is required to be given or if the third party is to hold sensitive information for us on their systems. Often, this is done at least partially through a quality, security and business continuity questionnaire.

ESS policy is to complete regular checks with our third parties to ensure no changes are made that may affect the security of our commercial/client information and our compliance to Data Protection Legislation.

Where appropriate, data sharing agreements are in place with our third party suppliers. These are commercially sensitive and therefore would not be made available to our customers

Further Resources

MyAccount

- GDPR Hot Topic (https://myaccount.capita-cs.co.uk/hot-topics/sims-gdpr/) from here there are lots of links to Notifications all relating to GDPR and SIMS, customers should be encouraged to Watch the notification so they are alerted to any updates

Capita SIMS Website

- Getting ready for GDPR (https://www.capita-sims.co.uk/gdpr)
- GDPR Blog on getting ready for GDPR (https://www.capita-sims.co.uk/resources/blog/helping-you-gear-up-for-gdpr)
- GDPR Blog on what schools need to know (https://www.capita-sims.co.uk/resources/blog/gdpr-what-schools-need-to-know-2018)
- GDPR Video on How SIMS can help with GDPR (https://www.capita-sims.co.uk/resources/videos/how-sims-can-help-your-school-comply-gdpr)

Other useful links

- ICO Website (https://ico.org.uk)

- DfE GDPR Blog (https://teaching.blog.gov.uk/2017/10/24/general-data-protection-regulation-evolution-or-revolution-for-schools/)
- DfE YouTube Video on GDPR (https://youtu.be/y09IHXv6u6M)

Please Note…

- Where the term 'Capita' is used, these FAQs are in relation to Capita ESS for the products and services we provide around the SIMS Suite of software.
- We will not be replying directly to questions or questionnaires sent to us, any un-answered questions submitted will be added to this notification as a direct FAQ or a new linked resource