What does GDPR mean for the public sector?	GDPR gives enhanced protection for personal data and puts stricter obligations on those who process personal data. The new rules apply to all organisations, public and private, operating in the EU, as well as those outside the EU that offer services to individuals in the EU.
Who does it apply to?	GDPR affects all organisations (public and private sector) processing personal data. CCS, as the government's procurement policy body, is responsible for advising government departments and other public bodies on those aspects of GDPR that relate to their contracts.
What is CCS doing to ensure that public bodies are compliant with the new rules?	Our Domestic Procurement Policy Team has led a cross-government task and finish group to develop standard generic clauses covering the new provisions of GDPR and detailed guidance notes. A Procurement Policy Note has been developed which contains guidance on how to bring existing and new contracts into line with the requirements of GDPR, for adoption across government. CCS will ensure all relevant existing and new Commercial Agreements will be updated in line with the policy to enable its customers to access GDPR compliant deals.
When will GDPR start?	The new data protection legislation comes into force 25th May 2018.
Will it apply to me as a supplier ?	GDPR requires contracts with data processors to include new clauses.
Will current framework suppliers need to do anything before then ?	Yes, you will need to look out for framework contract changes initiated by Crown Commercial Service which were sent on 28th February 2018 to introduce the new GDPR clauses before 15th May 2018.
What will happen to current customer contracts ?	Existing contracts will need to be updated by customers and suppliers to include new GDPR clauses where personal data is being held or processed.
Can we decline to accept the new clauses ?	No - this is new legislation.
What would happen if we do decline to accept the new clauses ?	In that unfortunate scenario CCS would need to suspend you from the framework.

What are the penalties for not being GDPR compliant by 25 May 2018?	The ICO can issue fines and enforcement orders. The maximum fines available under GDPR are 4% of global annual turnover (for undertakings) or EUR 20m (for organisations that are not undertakings)
What is the timetable ?	The PPN has now been issued and contract variations to CCS framework agreements have been drafted. From 28th February 2018 we have been advising buyers and suppliers to update their respective contracts to include GDPR clauses.
Where can I get more information ?	The source of information is the ICO https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
New FAQ's March 2018	
Could you please clarify if an email address from the buyers organisation, used as a username to login to the back end of an online system (a CMS for example), is classed as personal data and needs to be encrypted.	From our understanding work email addresses can be considered as personal data.
Supplier is trying to limit liabilities to contract value	Suppliers cannot limit liabilities when it comes to infringement as that would negate ICO's penalties enshrined in law.
Please can you tell me what the "Data Protection Act 2018" is and how it differs from the GDPR?	The detail of the application of the GDPR in the UK will be set out in a new Data Protection Act, called Data Protection Act 2018.
As a supplier, can I change the GDPR terms in the call off ?	CCS have to implement a common set of provisions across all suppliers' agreements for a particular framework, as well as complying with the government standard GDPR drafting as promulgated in PPN3/17. We cannot agree supplier-specific revisions or depart from the provisions drafted by GLD for implementation throughout Government.
Do you imply any length or terms that we can hold data for?	This is explained within the schedule of the framework agreement - see the new data processing schedule. All relevant data is to be deleted 7 years after the expiry or termination of the framework agreement unless longer retention is required by law or the terms of any call off
I thought you could only hold data as long	There is a contractual obligation to hold data

as it is required?	for 7 years past the end of the contract - please refer to the audit clauses
So it's up to current customers to be responsible to update a contract to include current GDPR?	Yes it is the customer's responsibility to update their call off agreement to ensure it is GDPR compliant. CCS has engaged with all suppliers who have live call off contracts to ask them to engage with buyers, but please don't rely on suppliers to make the first contact if as a buyer you wish to start working on ensuring your call off is compliant. You can also refer to the framework webpages that host the GDPR compliant call off template currently
My understanding is that the standard position under the framework states that the supplier acts as Data Processor for all Services. Is it possible to amend this position where this is not actually the case, and the Supplier is in fact acting as Data Controller (this is the case for connectivity services for example)?	Under the revised data protection clauses intended to implement compliance with GDPR, it's correct. As standard it says the supplier is the processor and the authority/customer is the controller. This was the case with previous data protection clauses based on DPA. The definition of Controller has not been changed by GDPR and processing of personal data has not changed so we are unsure as to why this has suddenly become an issue. To assess the merits of the argument we need to know exactly why the supplier feels they were acting as the controller, given that the controller is the entity that determines the method and the reason for the processing. Is that really the case for a service that's been commissioned by the customer?
Does CCS regard the names and addresses of their staff as personal data which they are the controllers of? if they do, how can a supplier get consent before signing these clauses?	As the position is not different from previously, CCS don't foresee any change to what we currently do. We could point to a justification that processing is necessary for the performance of a task carried out by a public body as was also the case under the 1998 DPA. This is therefore not really a concern
What guidance have you given customers in relation for asking suppliers to update the call off contracts please?	On the whole we don't necessarily have sight of the customers call offs or when we do it's very limited. so we have answered buyer questions if buyers have contacted us. There is also customer guidance on our website directed at customers telling them what they need to do to get GDPR ready. We have engaged with suppliers to ask them to contact their customers and liaise with them over GDPR compliance.

Clause 25.5.4.4 states that when personal data is transferred outside of the EEA, we must ensure rights and effective legal remedies... does this mean for example, if data was transferred to Africa, we would need to ensure they have legal rights over in that country?	Yes we would need to ensure that they have legal rights.
Most companies have a email/contacts system (e.g. MS Outlook) that contains personal information for clients, associates, subcontractors, former colleagues. This data set is non-specific to any individual contract - Are companies expected to establish extra measures for these systems under GDPR?	They must ensure that their handling of that personal data is compliant with GDPR - this doesn't have any bearing on updating your framework agreement
How do suppliers get consent to transfer data outside the EEA before these clauses are signed?	Suppliers should get consent from the framework manager at framework level and from the buyer at call off level
If the Supplier is using personal data but working under the client's management and control and the data is remaining on the Clien's systems and the processes around it are the Client's, then is the Supplier a Data Processor if they are only using the data as directed to by the Client?	Yes they are a processor - they are using / processing the data that belongs to the customer (the controller) and will be a processor in this instance
DOS 2 only	
DOS 2 only: I am not legally authorized by my company to accept the GDPR variation, but I am the only one who has access to the link. Is there a word document available where I can print out and get our company's authorised contact to sign the form? **Can the pdf version of the contract variation (once available for DOS2) be signed and returned to us which can then be marked by GDS as signed on the supplier's DM account? Or is there another way like creating a user account for their authorised signatory?**	The supplier has misunderstood how the acceptance works. It is a tick box exercise and the supplier simply needs to log on to their DMp account, review and accept the contract variation by ticking the box and clicking save and continue to accept the revised clauses. No signature is required. If the person with the link to the DMp within the supplier organisation wants to send a link to the pdf of the contract variation to the person legally authorised to accept it so they can review the variation, then they can do so using this: https://www.gov.uk/government/publications/digital-outcomes-and-specialists-2-framework-agreement The contract variation MUST be accepted on the Digital Marketplace however. Alternatively the supplier can add the legally authorised person as another contributor to their account and thereby they can accept the variation.

Technology Products 2 only	
The Call Off Contract on the CCS Portal for RM3733 doesn't appear to have been updated?	All GDPR compliant call off contracts across all frameworks within the Technology pillar have been uploaded to the relevant framework webpages - we will check to see if the request to edit has been actioned and chase through approval. This may take up to 3 days
G-Cloud specific	
We (supplier) can't agree to GDPR terms because we act as a data controller.	The revised G9 call-off includes a schedule where the exact controller / processor relationships can be entered. Clearly you are acting as a controller for the data you collate and the call-off refers to any buyer personal data that could be involved in the contract. We cannot have individual terms for suppliers - we need one set for all suppliers. Or In circumstances such as this the buyer would set out the exact relationship to controllers & processors in the GDPR schedule as part of the contract.
I have not seen my variation notice.	The variation notification went out to the latest email address we had for each supplier. Suppliers need to logon on to their Digital Marketplace account to see the variation notice. If you cannot access your account or need a contributor account to be set up, then please email enquiries@digitalmarketplace.service.gov.uk
I am not legally authorized by my company to accept the GDPR variation, but I am the only one who has access to the link. Is there a word document available where I can print out and get our company's authorised contact to sign the form? **Can the pdf version of the contract variation (once available for G-Cloud 9) be signed and returned to us which can then be marked by GDS as signed on the**	The supplier has misunderstood how the acceptance works. It is a tick box exercise and the supplier simply needs to log on to their DMp account, review and accept the contract variation by ticking the box and clicking save and continue to accept the revised clauses. No signature is required. If the person with the link to the DMp within the supplier organisation wants to send a link to the pdf of the contract variation to the person legally authorised to accept it so they

supplier's DM account? Or is there another way like creating a user account for their authorised signatory?	can review the variation, then they can do so using this: https://www.gov.uk/government/publications/g-cloud-9-framework-agreement The contract variation MUST be accepted on the Digital Marketplace however. Alternatively the supplier can add the legally authorised person as another contributor to their account and thereby they can accept the variation.
C**an you please advise on how to submit the 'Accept the contract variation for G-Cloud 9'. Due to the 'legal authority' statement – I will need to have this authorised by the company (Scan Optics) CEO.Need advice on how to proceed – electronically or through paper channel**	You have 2 options here: 1) You can request an additional Digital Marketplace contributor account for your boss so that he can be the one to log on and accept the contract variation - you would need to email enquiries@digitalmarketplace.service.gov.uk 2) You could share the link to pdf of the contract variation: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/684958/G-Cloud_9-proposed-contract-variation.pdf with the company CEO and get it in writing from him by email when you send him the link to the pdf of the contract variation that he is happy for you to accept it and then you can log on to your Digital Marketplace account and accept the contract variation In any case the contract variation must be accepted by you. You will need to log on to the Digital Marketplace, review it and tick the box and click save and continue to accept the revised clauses.
Will CCS be updating the G-Cloud 7 framework agreement for GDPR ?	We will not be updating expired G-Cloud framework agreements. If required you can undertake a variation of your live G7 contract with the supplier. The GDPR version of the G9 call-off contract can be found on both our website and the Digital Marketplace. You can extract the relevant clauses from this, alternatively you can use your own.
On the back of recent communications from CCS re varying G-Cloud call-offs to incorporate GDPR, we have had a very few approaches (3 out of 100+) customers approach us (we are in the process of writing out to them proactively as I don't want to be under a deluge in May). **Part of what is required is to complete a**	The template should really be completed by the data controller, in most instances the buyer, as it would involve any personal data they are passing to you as a processor. I suspect as it's so new many are having issues. It might be easier for you to part populate the

data processing template, which I'm assuming (but happy to be corrected) is the legal basis for processing data. Those that have approached us are asking us to complete this. The challenge is that as an IaaS provider, we don't see or access the data, so this could only ever be our best guess. I'm pushing back and asking for their help to complete this. Just wanted to sense check who CCS thinks should be completing this?	varied call-off contract template which includes schedule 7 and send this to your other customers to complete. You can't fill much of it in however as it's primarily for them to do.
Our legal team has reviewed the changes made to the G-Cloud 9 (G9) framework agreement and call-off contract to comply with the new General Data Protection Regulation (GDPR) and have asked me to forward the following request to you."Section 33.7 would obligate us to "immediately" notify the buyer of data loss events or certain communications from third parties. The GDPR regulation would give us 72 hours for such notices. If possible, we'd like G Cloud to revise this section to allow 72 hours as per the regulation." Would this be an acceptable amendment?	CCS have to implement a common set of provisions across all suppliers' agreements for a particular framework, as well as complying with the government standard GDPR drafting as promulgated in PPN3/17. We cannot agree supplier-specific revisions or depart from the provisions drafted by GLD for implementation throughout Government. On that basis, we can't accommodate your request.
It appears that the changes to 8.57 of the Framework Agreement limit the processing of personal information to processing strictly necessary for the management.administration of the Framework Agreement AND is limited to personal data related to CCS and Buyer personnel. Our services process personal date (ip address, geography etc) of of third party visitors to websites owned by Buyers (who are Controllers of such personal data) which pursuant to 33.4 of the Call Off Agreement are permissible. How do we go about revising 8.57 to be consistent with Section 33.4 of the Call Off Contract?	The scenario outlined is not part of the CCS / Supplier framework agreement. i.e. as part of the framework agreement between CCS and yourselves there is no website monitoring or IP address processing etc. There may well be as part of their normal business processing but this is not CCS personal data.
Section 33.3 of the Framework Agreement appears to require Buyers to "review and approve as appropriate" the security measures of used by Supplier? Who determines whether the Buyer must review and review and	This is purely a matter between CCS & the supplier. If we deem it necessary to review, the framework manager at CCS would initiate.

approve?	
With respect to Section 8.60 of the Framework Agreement and 33.5 of the Call-Off Agreement, how does a Supplier obtain CCS's written consent to transfer Personal Data outside of the European Economic Area? Personal data from the EU is always stored in the EU but we need the ability to have it viewed or access from locations outside the EU on occasion. Our form of data processing agreement provides that we can make such transfers so long as we ensure appropriate safeguards to protect the data in accordance with the requirements of the GDPR. Can the Framework Agreement be amended to permit that?	Written consent would be gained by contacting the CCS Framework manager for the Framework Agreement, and buyer contact for the Call-Off Agreement.
I don't believe this means we are obliged to host our customers data within the EU. Please can you point me to the part of GDPR that states this is a requirement?	To answer your question, GDPR prohibits transfer of personal data of EU citizens outside the EU unless adequate privacy safeguards are provided - see Chapter V of the Regulation, Article 44 onwards (copy attached).The G-Cloud clause 8.60 says that the supplier must not transfer personal data outside the EEA (EU plus Norway, Iceland and Liechtenstein) without our consent. In deciding whether such a transfer would meet the requirements for adequate protection of data subjects' rights we'd be guided by Articles 45 and 46 of the Regulation. You refer to processing in the US under the Privacy Shield scheme, which as I understand it has been approved by the European Commission under Article 45 as providing adequate safeguards. The decision for Call-Off Customers, is whether they are therefore happy to give approval to such US processing on this basis or whether they want further assurances.
The change to 9.32.2 states we may only process data belonging to CCS and buyer personnel, which sounds fine, except that we host websites which may, in some cases, contain personal information of people who interact with the Buyer's services, and we are contract bound to back up that data, which I believe counts as "processing" under the new regulation. So in other words, 9.32.2 would preclude us from carrying out contractual obligations to	For the G-Cloud 9 Framework Agreement, it is very unlikely CCS would have any CCS personal data with them that would need backing up (none that I could think of). The only backups would be their own regular ones - nothing additional required. For Call Off Agreements it would be as per their service description

back up personal data of those using the Buyer's services. What is the official line on backups as regards processing and this G-Cloud update? Are we to inform Buyers we are no longer permitted to back up user data, or does CCS consider backups to be an exception? If the latter, we could do with some formal clarification, as I have read all changes and I cannot see any exception pertaining to backups of data. If the former, we'd prefer CCS break this news to the customer Buyers than us, as it could be quite awkward!	
My concern is not the CCS, but the *Buyer*. It is entirely possible that a Buyer's website would contain personal data beyond that of their personnel. To give you a concrete example, hosting a communication system for public housing tenants to communicate issues to housing managers on behalf of a Buyer who is a local government customer necessarily means the personal data of the tenants is stored by the system, thus backed up by the Supplier. That would place us in breach of the terms above. Perhaps I am misunderstanding the context, but that is the reason for my question.	The appropriate provision for such processing would need to be made in Schedule 7 of the new GDPR compliant call off agreement on an individual basis and to be agreed with the individual buyer.
In the new text of the framework agreement clause 8.59(b), it states that 'The Supplier will ensure that the Supplier Staff only process Personal Data in accordance with this Framework Agreement..', without being specific as to whether this processing is related to CCS or Buyer personal data. Does this not conflict with clause 12.1 of the Call-off contract, which states that 'The Supplier must: comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data'? Will this not also override any elements of the Supplier Terms in relation to the processing of personal data, even those which do not conflict with the framework agreement or call-off contract? As I understand it, these contract variations cover the CCS and Buyer personal data being held by the Supplier. How do you propose to	Clause 8.59b governs processing of Personal Data in relation to performance of the Supplier's obligations under the Framework Agreement ie in respect of the contractual relationship between the Supplier and CCS. Clause 12.1 of the Call-Off Contract governs processing of Personal Data under individual Call-Off contracts. There is no conflict The Supplier terms do not apply at the Framework level ie to the obligations between the Supplier and CCS so the question of "overwriting" does not arise. At the Call-Off Level an obligation to process Personal Data only in accordance with the Buyer's instructions should not cause a conflict/"over-write" as this is a legal obligation under article 28 of the GDPR. CCS and the Buyer would be acting as both Controller and Processor in respect of such

cover Supplier personal data being processed by CCS and the Buyer in these revised agreements, or would you expect this to be included in the Supplier Terms?	data and hence there is no requirement for contractual provisions to provide full assurance the Processor will enable the Controller to meet its obligations under the Data Protection Legislation. We will of course comply with those legal obligations