19 Blog Nineteen Contracts with Processors

**Whats this about?**

As thoroughly modern GPs operating in the finest health service in the world with up to the moment IT, the jewel in the crown of that NHS IT is GP IT, us, tapping away at our keyboards. Now for most of that keyboard activity the actual processing takes place on machines and equipment that we do not directly manage. NHS GPs operate in a supported environment by virtue of the 2004 nGMS contract. There is almost no processing that occurs on our patients that is not actually managed by a third-party Data Processor. For instance, my core clinical system is Vision, managed by In Practice Systems, Egton Medical Information Systems run the servers for the various EMIS products, The Phoenix Partnership (aka TPP) provide SystemOne and Microtest Ltd supply Open Evolution. In all these circumstances the IT supplier is acting as a Data Processor on behalf of you, the Data Controller. Now under GDPR to be lawful that relationship needs to be reflected in a formal written contract and whats more that contract must have certain items in it. And it ought to be in place by 25th May, 5 days time!

**5 Days!**

Yes 5 days but remember the words of the ICO that she "not going to be looking at perfection, we're going to be looking for commitment".

**But we have loads of Data Processors doing work for us**

True, but the ICO is not expecting you to have sorted out these contracts in the next 5 days, especially when so many people still don’t understand whats happening with GDPR.

**But in fact for NHS GPs hopefully most of the work is done already**

By virtue of the GPSoC arrangements.

**What’s GPSoC?**

GPSoC is the set of arrangements that provided UK GPs with free IT systems under the nGMS contract of 2004. Well, I know, in fact it took us 3-4 years to get Mr Grainger to actually honour his side of the deal, but we got there eventually. GPs have a choice of a wide range of IT systems to help them deliver against their contracts. In England the process is known as the [GP Systems of Choice arrangements](https://digital.nhs.uk/services/gp-systems-of-choice). The devolved nations have their own equivalents.

**How does GPSoC help us with the 5 day deadline?**

Because as it says on the tin, “**GP Systems of Choice is a contractual framework to supply IT systems and services to GP practices and associated organisations in England”**

**GPSoC is a contractual framework**

Its called a “call off contract”. In the days when GPs used to solder their own data leads, swap out hard drives and program .bat files they had a direct relationship with their chosen suppliers. That resulted in our having 16 suppliers pedalling 31 different systems. That was messy for them, us, the NHS and the taxpayer. We already had a central process for accrediting these systems but it had no teeth and suppliers knew how to play that system, they had one good compliant system that they demonstrated to the NHS authorities to get signed off, then put it away in a cupboard and actually sold completely different systems to the likes of you and me.

**From RFA to GPSoC**

That was in the late 1980s. Fast forward from to 2004 and the nGMS contract. GPSoC established a better way of doing this procuring. The best analogy is to imagine the government wanted every GP to have a car. Urban GPs would need a sleek saloon like a Mondeo so they can visit during the day and moonlight for Uber at night. Rural GPs would need a Range Rover to battle through the snowdrifts but at the same time polish up good and proper for the Hunt Ball. Federated GPs would want the self-sacrificial communal cut down one size fits all Citroen DX.

So the government agrees with my team, the professions motoring experts, what a GP car should be able to do, its basic specification. They then ask the chosen manufacturers to quote for supplying these to however many GPs might want them. The cars are all made to meet a certain minimum specification, that way the GP and the Government can be assured that they will do the basics. HMG and we define the spec, they know how many GPs are around, the cars can be tested and accounted for, it’s a managed market, not a free market but a managed one. All the GP has to do is turn up an ask for his car. For each car that’s driven away by a GP the manufacturer bills the government. This is known as a “call off” contract.

**So the contract is with the maufactuers, what about us?**

Indeed, no one’s going to give free cars to 50,000 GPs. No, the contractual framework needs to capture the GPs, we can’t just be left to rush about in these free cars without some responsibility. If we don’t take it in for servicing or thrash it in every gear or leave the fob within easy reach for a scoundrel to open the doors and run of in it, that wouldn’t do.

**So we have a further knot in the blanket of responsibilities**

Each local branch of the NHS has a separate contract with each practice to provide for the day to day running of the car, rather like a service contract or the AA. If it breaks down you need someone to come out and fix it sharpish and that’s best provided locally. On the other hand we need to keep to the speed limit and not smash the wheels against the kerbs.

**So we have another contract, between the GP and the local NHS**

In England this is known as the [CCG / Practice agreement](https://www.england.nhs.uk/publication/terms-governing-the-provision-and-receipt-of-gpsoc-services-and-gp-it-services/)

This is an agreement between the practice and the local NHS that defines a variety of conditions on both sides of the agreement to ensure the systems are used properly and kept up to date (well allegedly!)

**So who controls the way the CCG delivers?**

Good question, they need to be tied in because they are the ones who “call off” the provision of each car to their GPs, so they are managed by the government via the [GP IT Operating Model](https://www.england.nhs.uk/digitaltechnology/info-revolution/digital-primary-care/gp-it-operating-model-2016-18/). This is a set of instructions to CCGs from DHSC/NHSE as to what they must do to keep their local fleet of cars on the road.

**So basically…..**

We have all four elements tied together; GPs agreeing the specs with Government, Government controlling the big budget via contracts with the suppliers, delivery at the local level via the CCG and practices and CCGs bound by mutual responsibilities in the CCG / Practice agreement. All of it assured by clearly defined contracts and agreements.

**But it gets better**

So far we’ve only talked about the basic car with its four wheels, what about the flash alloys, the sound system and the sat nav?

**All encompassing GPSoC**

So, the GPSoC arrangements have grown over the years to encompass more than just the core clinical systems and now includes a couple of catalogues of ancillary, often called third party systems, that can be bolted onto, glued or affixed to, installed in or simply carried in the boot, of the NHS supplied car. These are known as the GPSoC “Lots”.

**And there are lots in the lots**

Not a lot of GPs know this, but the number of systems available under the GPSoC is surprisingly extensive. They can be found [here](https://digital.nhs.uk/services/gp-systems-of-choice/gpsoc-services). These have all been assured and underwritten to be safe and do what they claim to do by the GPSoC process. They are not all entitlements, GPs are entitled to the core clinical systems found in Lot 1 and but lot 2 and 3 systems are usually conditionally available, i.e. if there’s enough money.

**So how does this help me with the 5 day deadline?**

Well under the old DPA there was a concern raised by us on your behalf that the manufacturer could still in theory go off and do bad stuff and it would be the GP, the Data Controller, who would be held responsible.

**So we created the Deed of Undertaking**

We couldn’t change the law, the GP remains the DC but we could tie the errant person into the liability. So, we agreed between NHS Digital (when it was called HSCIC) and the suppliers that there would be a thing called the [Deed of Undertaking](http://systems.hscic.gov.uk/infogov/confidentiality/deed/index_html). This is basically a legally approved indemnity from the supplier to NHS Digital saying they will be liable for any naughtiness on their part. The GP would still be sued or fined as the DC, but the supplier would pick up the bill.

**So how does this help me with the 5 day deadline?**

Well we now have a “Call off” contract, a local contract and an indemnifying deed. In short we feel we have every angle covered.

**So how does this help me with the 5 day deadline?**

Well under the DPA this contractual framework was explained to the ICO and they agreed that this was sufficient for their needs to ensure that GPs and everyone else were meeting their responsibilities, under the DPA. The old DPA required there to be “contracts” between DC and DPs but there was no clear definition of what that contract should contain. The ICO felt the overall GPSoC arrangements were sufficient to satisfy those old vague contractual requirements.

**So how does this help me with the 5 day deadline?**

Well because obviously, subject to a few refinements to meet the detail of GDPR, these arrangements would be the obvious candidate to enable GPs to satisfy GDPR in terms of their Data Controller relationship to the various suppliers of their IT systems.

**Sorry what are the “terms of their Data Controller relationship to the various suppliers of their IT systems”.**

So now we’ve come full circle, what is the relationship between we GPs, as data Controllers, and the people, companies and organisations that provide us with systems and or process our data for us. Well that relationship was loosely defined under DPA, but as with everything else it gets a polish and tighten up under GDPR.

**Articles 28 to 36**

Its Articles 28 to 36 in GDPR that are relevant, and for GPs it’s 28 that will have most impact. Basically, this says that where a data processor does stuff for a DC there must be a contract, and that contract must contain certain minimum items. It places very strict constraints on the Data Processor (DP).

**What are those minimum items**

They’re listed at the end verbatim[1](#one) but basically boil down to;

* There must be a contract
* That is binding on the Data Processor
* And defines the
	+ Subject matter to be processed
	+ The duration of the processing
	+ The nature and urpose of the processing
	+ The type of data being processed
	+ The categories of data subjects who data is being processed
	+ The rights and obligations of the Data Controller

The contract must stipulate, in particular and amongst others;

* that the processor processes data only on documented instructions from the controller,
* that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
* takes all measures required pursuant to Article 32,
* recognises its responsibilities to satisfy Article 28(2) and (4)
* where necessary and possible assists the data controller in meeting their obligations under Subject Access rights
* Assists the DC in meeting their Article 32 to 36 obligations
* deletes or returns any data as instructed by the DC

and

* finally confirms compliance with GDPR and allows audits and inspections demanded by the DC.

Now as an aside and before we continue there’s an important principle in there, that first bullet point; “that the processor processes data only on documented instructions from the controller.”

**I repeat**

“that the processor processes data only on documented instructions from the controller.“

that’s an important message and statement, note the reference because you may want to quote it in the future when the next bod pitches up wanting data from your system for some ‘strat or other, attempting to tell you, as a Data Controller, what to do.

***GDPR, page 47, Article 28, section 3, paragraph 1, last sentence and continuing to sub paragraph (a). the processor processes data only on documented instructions from the controller.***

So now back to the story on contracts with our suppliers

**Err OK that’s beginning to look a bit complex**

Are we really expecting 10,000 Data Controller NHS practices to start drawing up GDPR compliant contracts with the dozens of GPSoC suppliers?

**No.**

**Because we also have Article 28(5)**

As mentioned elsewhere one of the themes running through GDPR is consistency, not only of data flow but also of process, so how data is protected in one country should look like the next. The way data is protected by one GP surgery ought to be pretty like the next. And thus, we have throughout GDPR the concept of “Codes of Conduct”.

**Article 28 allows in para 5;**

“5.   Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.”

**And what is GPSoC?**

An approved certification mechanism, exactly what GDPR is calling for.

**And there’s more, paragraph 8**

“8.   A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.”

So by now it should all be falling into place, there’s no point in re-writing the GPSoC contractual framework. There’s every point in upgrading the GPSoC framework to make it GDPR compliant and the whole concept fits very neatly into the GDPR concept of consistency and continuity.

**So what has GPC done**

Well I’ve, as you might imagine, asked the various parties to agree this approach. I’ve not heard anything yet but that because we are have quite a lot of GDPR stuff on our respective plates but I cannot really conceive of anyone wanting to disagree.

**So what do we have to do for 5 days time**

In terms of your GPSoC supplied systems, nothing. You do not have to exchange GDPR complaint contracts with any of the suppliers listed in the GPSoC catalogues.

**Do they know that?**

No idea, I don’t have time to track each and every suppliers activities but I do know several of the major suppliers have been in touch with NHSE/NHSD to make the same request. I hope if the others stumble across this blog they may take up the same approach.

**What about other non GPSoC software or systems we use?**

Well if those systems process data on your behalf, they are going to need to have a GDPR compliant contract put in place, asap.

**What? in 5 days time.**

If possible yes, but as I began the ICO is taking a reasonable approach and considering the number of companies and organisations who simply do not understand GDPR we are unlikely to be high on the list of priorities.

**What should we do?**

As they supply systems to you I’d suggest its in their best interests to ensure that their arrangements are GDPR compliant. Contact them and ask them what they are proposing to do to offer you a GDPR compliant contract.

**That could be a lot of contacting!**

Indeed, so make sure you are only contacting people who process personal data on your behalf. You don’t need to ask the local plumber who has your contact details for a GDPR compliant contract.

Use your Practice Processing Register [(Blog 15)](https://www.dropbox.com/s/tngpyum7iscm502/15%20Blog%20Fifteen%20Documentation.doc?dl=0) to help identify who you ought to have Controller / Processor contracts with.

# Dr Paul Cundy

# GPC IT Policy Lead

# GMC 2582641

# 20th May 2018

**1) Article 28 in full**

*Article 28*

**Processor**

1.   Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2.   The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3.   Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

|  |  |
| --- | --- |
| (a) | processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; |

|  |  |
| --- | --- |
| (b) | ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; |

|  |  |
| --- | --- |
| (c) | takes all measures required pursuant to Article 32; |

|  |  |
| --- | --- |
| (d) | respects the conditions referred to in paragraphs 2 and 4 for engaging another processor; |

|  |  |
| --- | --- |
| (e) | taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III; |

|  |  |
| --- | --- |
| (f) | assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor; |

|  |  |
| --- | --- |
| (g) | at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; |

|  |  |
| --- | --- |
| (h) | makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. |

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4.   Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5.   Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6.   Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7.   The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8.   A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9.   The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10.   Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

<https://digital.nhs.uk/services/gp-systems-of-choice/gpsoc-services>