20 Blog Twenty Things to do, letter for CCG

**Where were you on GDPR Day?**

Well GDPR Day has come and gone and we’re all still here. The dreaded data destruction has proven as harmless as the millennium bug and the ICO has not raided every GP in the land handing out 20 million Euro fines.

**Life goes on.**

But in keeping with the theme of my blogs, whilst no one, least alone the ICO, expects excellence from everyone from day one she does expect commitment.

And that commitment can begin by practices getting a tighter grip on whats happening to their patients’ data.

There are of course many extractions that we all know about but probably an equal number that we may not, and I’m particularly struck by how many practices I speak to who don’t really understand who’s doing what with their data.

One area specifically is so called “local processing”, a bit of a misnomer because local can mean anything up to county wide. Whilst most of us will know about QUOF and the national DESs there are multitudes of local data extractions that go on to support local priorities, my practice has them for access, Frailty, Ambulatory Blood Pressures amongst others. These all rely upon data processing and they almost invariably involve data extraction commissioned by your CCG.

**So the CCG is the place to start.**

In my last blog[, Blog 19](https://www.dropbox.com/s/k20kxnczrm8fzmu/19%20Blog%20Nineteen%20Contracts%20with%20Processors.docx?dl=0), I spoke about the need for data processors to be acting only under direct instruction from you, the Data Controllers. That whole process of DC and DP needs to be tightened up and GDPR is the perfect vehicle for doing so.

No practice should have data being extracted from them without their knowing about it. (Dr Paul Cundy, 29th May 2018)

**And remember**

And remember under GDPR it is possible for even pseudonomised data to be considered to be identifiable and thus personal data.

**So even pseudonomised medical records can fall under the protections of GDPR?**

Yes

Even pseudonomised medical records can be considered to be identifiable and thus would count as Article 9 Special Category Data.

**Really?**

Yes, see Recital 26, “*Personal data which have undergone pseudonomisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.”*

Whilst there are caveats and mitigations the principle is established, GDPR raises the threshold for what is personal identifiable data.

As I have often stated, pseudonomisation is a weasel way of saying not truly anonymised. Anonymisation means complete removal of any potential for re-identification. Pseudonomisation means you’ve made it more difficult, but not impossible. GDPR recognises that not impossible means it remains potentially possible, thus pseudononomised data is considered to be identifiable.

And thus Recital 75 says even the process of reversal of pseudonomisation is in itself a risk to the rights and freedoms of individuals and Recital 85 identifies it as a formal Data Breach, so even if you do nothing other than simply identify a person from their pseudonomised data that act is itself a punishable breach.

**So the CCG are the “Processor” for these schemes?**

Usually, although not often directly, they are most likely to be sub-contracting (aka “commissioning”) the actual processing to a 3rd party company. The point is that you are the Data Controller and unless you have agreed to act a Joint Data Controllers with the CCG, the CCG will be acting as your primary data processor and the 3rd party company their subcontracted processor, lets call them the secondary processor.

Essentially GDPR allows for processing to be “daisy chained” but each link in the chain, primary to secondary, secondary to tertiary, is subject to the same controls, that of the DC to the DP.

Therefore, there must be a [GDPR Article 28](#one) compliant contract, or some other lawful mechanism, between the you and the CCG and subsequently between the CCG and any daisy chained processor(s).

**So could a previous LIS scheme specification or data sharing agreement be used as a base for the GDPR compliant Controller Processor contract?**

Yes.

**So, what do we do next?**

Well I’d recommend you start and demonstrate your commitment by opening up a discussion between yourself and the CCG about what exactly they are doing with your data.

This week.

**But they are the CCG, what notice are they going to take of this lonely little practice?**

Little and lonely you may be but you have the might of GDPR behind you. That’s a potential 20 million Euro fine heading their way. As from last Friday it’s the law. They can’t ignore you. There has to be a contract or another legal Act under which this data processing is being done, and even if it is being done under a justifiable legal Act then the specifics still need to be understood.

Because not only must there be the contract, but you need to understand whats happening to your data, which is what the [Practice Data Processing Registe](https://www.dropbox.com/s/088oqp9fmtxifzz/Template%20Practice%20Processing%20and%20Breach%20Register%20REVISED%2030th%20April.xlsx?dl=0)r is all about.

To remind you, you need to get information about the processing the CCG is doing for you to fulfil your obligations under [Article 30, which is covered in Blog 15](https://www.dropbox.com/s/tngpyum7iscm502/15%20Blog%20Fifteen%20Documentation.doc?dl=0) and where [my comment above comes in.](#statement)

**So how do we start?**

Well you send the CCG the letter that follows.

**Could the LMC do this on our behalf?**

Yes, indeed that may be a more convenient approach for all concerned, although do bear in mind as the Data Controller it is your practice itself that is ultimately liable. The LMC can gather the data for you, but you must take any necessary actions that arise.

**So here’s the letter**

You’ll see its from your DPO to their DPO asking for details of any plans to make any data sharing / extraction / processing that they may do on your behalf GDPR compliant.

Please cut copy and paste to your hearts delight.

[Your letterhead]

Data Protection Officer

[insert your CCG name address]

[Date]

Dear Data Protection Officer,

**Article 28 data processing on our behalf**

I am writing to you as the Data Protection Officer for [insert surgery name]. As a fellow Data Protection Officer you will be aware of the requirements of Article 28 of GDPR[1](#one). Where a Data Processor carries out functions for a Data Controller there needs to be a contract and a clear understanding of the responsibilities on both parties. We have identified that you process data on our behalf [insert name(s) of examples if you know them, i.e a Hospital admission risk stratification LIS]. Such processing is subject to Article 28 and therefore the arrangements will need to be made GDPR compliant. As the original arrangements and specifications were drawn up by yourselves I am writing to enquire what your proposals are to have these updated so that they are Article 28 compliant and in what timeframe?

In addition, and as a supplement to this I would be grateful if you could complete the attached table so that we both can have a full picture of the processing being carried out by yourselves on our behalf. This information should be readily available under your Data Processing Register compiled under Article 30 of GDPR.

Finally, whilst existing processing is carried out under these prior arrangements I should remind you that as from 25th May Article 28, section 3, paragraph (a) applies and that in future data can only be processed on our behalf after receipt of our “documented instructions”.

I look forward to hearing from you and receiving the requested information.

Yours sincerely

Dr / Mr / Mrs / Ms [name]

Data Protection Officer

[GMC number]

[surgery name]

Table of Processing carried out by [insert CCG name] on behalf of [insert practice name]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Processing arrangement’s name or identifier, for example “Frailty LIS”** | **Duration of processing** | **Nature and purpose of the processing. Article 28(3)** | **Data subject identifiers being used. Article 28(3)** | **Type of data being processed\* please attach a separate list of coded items if applicable. Article 28(3)** | **Categories of data subjects whose data is being processed. Article 28(3)** | **Name or identity of any data processor carrying out the processing on your behalf. Article 28 (2) & (4)** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1) Article 28 GDPR

*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.