How the Council's exceptions degrade Regulation protection well below Directive 95/46/EC (Associated Analysis)

Published in the Hawktalk blog (3 August 2015): http://amberhawk.typepad.com/amberhawk

The blog explains, in detail, how the Council of Minister's text of the Regulation, in particular the exceptions specified in Article 21 and the flexibility granted to Member States to enact variations to the obligations under the Regulation, are very likely to result in a level of data protection below the standard established by Directive 95/46/EC.

For a convenience I am using "The Regulation" to mean "the Council of Minister's text of the Regulation currently under discussion at the Trilog" whilst the "Directive" is shorthand for "Directive 95/46/EC" (see references for links to both if need be).

In order to assist the reader in the comparison between Article 21 (A.21) of the Regulation with the Article 13 of Directive 95/46/EC(A.13). I have to reproduce both Articles. (*I have added an explanation in italics as to the scope of the exception so can you can get the gist if need be*).

Regulation exceptions (Article 21)

> "21(1) Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 20 (*concerning all Data Subject rights*) and Article 32 (*concerning reportable data loss*), as well as Article 5 (*concerning Data Protection Principles*) in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 20, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:
>
> (aa) national security;
>
> (ab) defence;
>
> (a) public security;
>
> (b) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security;
>
> (c) other important objectives of general public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including, monetary, budgetary and taxation matters, public health and social security, the protection of market stability and integrity;
>
> (ca) the protection of judicial independence and judicial proceedings;
>
> (d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (aa), (ab), (a), (b), (c) and (d);

(f) the protection of the data subject or the rights and freedoms of others;

(g) the enforcement of civil law claims".

Directive 95/6/EC exceptions (Article 13)

By contrast, the current Directive 95/46/EC text in Article 13 (A.13) states (plus my brief explanation in *italics*):

"13(1). Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1) (*concerning the Data Protection Principles*), A10 (*Fair processing notice when personal data obtained from data subject*), A11 (1) (*Fair processing notice when personal data obtained from third party*), A12 (*concerning all Data Subject rights)* and A21 (*Publicizing of processing operations*) when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others."

Commentary on the different exceptions

The major differences between the Directive and the Council of Ministers exception Articles can be seen as:

- The Regulation increases number of exceptions. Of particular note is the exception with respect to "*important objectives of general public interests of the … Member State*"; this is a "just in case we have missed something" provision that gives Member States flexibility to introduce additional exceptions at any time in the future.
- This "*general public interest"* objective, by definition, will have **nothing** to do with the other exceptions listed in A.21 (e.g. any general public interest purpose will not be associated with national security; not defence; not public security; not the prevention, investigation, detection

or prosecution of criminal offences; ... and not civil law claims). Can you think of an example of this "*general public interest objective*" that excludes all the others in A.21? Answers on a postcard because I have not got a clue.

- The Regulation extends the exceptions to data loss. This is understandable in the context of policing (e.g. if the police loose some criminal intelligence on criminals, they don't have to notify each criminal about the data loss as that would constitute a tipping off). Whether the text of Article 21 should be so expansive so that data subjects should be kept ignorant about a data loss with respect to "*important objectives of general public interests of the … Member State*" is, of course, a moot point.
- The Directive exceptions in A.13 are linked to the exceptions in Article 8(2) of the European Convention on Human Rights and have to be "*necessary*" in the context of any Article 8(2) exception; A.13 does not contain an "*important objectives* of g*eneral public interests"* exception.
- The Regulation narrows the application of exceptions in Article 5 to the Data Protection Principles but only when they impact on the rights and obligations in Articles 12 to 20; the Directive applies the exception from the Principles in general. As will be seen later, the apparent narrowing of the scope of the A.5 exception is to allow far more wider exceptions to be introduced in the text of A.5 itself!

Does proportionality and necessity safeguard the data subject?

A.21 of the Regulation requires any "*restriction*" to "*constitute a necessary and proportionate measure in a democratic society*". Note that the restrictions of "*necessary*" and "*proportionate*" can only be tested ***after*** legislation that uses any A.21 exception ***has been*** enacted, and **after** interference ***has*** occurred.

Often in other Articles, the Member State can introduce variations from the Regulation (i.e. this should be viewed as an exception from the Regulation) subject to "*appropriate safeguards*". In some cases, there are exceptions introduced where the Article is silent on any safeguard at all. There too, the "appropriate safeguards" can only be tested ***after*** legislation ***has been*** enacted, and **after** interference ***has*** occurred.

It would be better if the data protection authorities could test these restriction **prior** to the legislation being enacted and be able to enforce areas where the exception used in a Member State law is neither "*necessary*" nor "*proportionate*". Similarly with respect to "*appropriate safeguards"* and any other exception that is introduced by Member State law.

At the very least, to protect data subjects, the data protection authorities should be given an explicit role that allows them to take Article 8 of the ECHR under their remit in order to make Article 8 accessible to data subjects. (This is an old hobbyhorse of mine; see references). There is not even an obligation on a Member State to consult the data protection authority with respect to "*appropriate safeguards"* or any variation from the Regulation that Member State legislation introduces.

To ensure this point is abundantly clear, consider the following three questions:

- has the UK Government ever enacted legislation (e.g. to create an ID card database, lifelong DNA retention, mass retention of communications data, data sharing) and claimed that the consequential processing of personal data would be "lawful", "necessary" and "proportionate"?
- has a complainant had to argue necessity and proportionality, **not** before a data protection authority, but before a national/European court which has subsequently come to a contrary judgement?
- has there been considerable mass retention of DNA, communications data or data sharing before the Court judgment?

Given three "yesses" to the above, do you now think the "*restrictions"* of *necessity* and *proportionality* as identified in the A.21 exception constitute an effective safeguard? I think the answer is "***NOT REALLY***" for four reasons:

- the interference has commenced (or the appropriate safeguards have been introduced) and the personal data have been processed (probably for years);
- the legislation, once enacted makes the processing of personal data lawful; it can therefore be very difficult for the data protection authority to act. For example, if a law says that dates of birth have to be retained for 5 years for a purpose, then how is a data protection authority going to establish that the processing purpose is unlawful, the collection of dates of birth are excessive for the purpose or even the retention for 5 years is not necessary for the processing purpose?
- the data protection authorities do not have an explicit role in enforcing Article 8 of ECHR;
- as a result, the remedies available to data subjects are remote (data subjects have to possess the resources to take the Government to Court on Article 8 grounds).

Note another implication of the above. Any safeguard identified in the Regulation that is not linked to "*restrictions"* of *necessity* and *proportionality* as identified in Article 21 risks being a lesser safeguard than that offered by Article 13 of Directive 95/46/EC which has an express link to Article 8(2) of the ECHR (i.e. all exceptions in A.13 are linked to concepts of *necessity* and *proportionality*). There are many exceptions in the Regulation that are not explicitly linked to concepts of *necessity* and *proportionality.*

For clarity, I am not saying that I Member States will implement inadequate safeguards; however without the counter-balance of data protection authority involvement the risk is there. Member States have to be viewed as data controllers who can legislate for their own processing objectives.

The "general public interest" is going to be very "flexible"

I have to confess that whenever I read about legislative matters justified in terms of "*important objectives of general public interests of the … Member State*", I get an attack of the heebie-jeebies. The reason? Who knows what "*general public interest*" means?

In the 1980s, I remember the prosecution of Clive Ponting who was facing a considerable period in prison because he disclosed classified information to an MP; Ponting ran a "public interest" defence. In his summing up, the Judge stated "*the public interest is what the government of the day says it is*". (Details of Ponting case in the references).

Well, I think this quote aptly summarises the meaning of "*important objectives of general public interests*". Whenever any Government of the day legislates for anything, it will argue that its legislation is "*important*" and is in the "*general public interest*".

Finally as an exception in the "*important objectives of general public interests*" category does not appear in Directive 95/46/EC; it follows that application of this exception is likely to take the protection afforded to data subjects below that of the standard of protection afforded by the current Directive.

Exceptions within the Article 21 exception

You can see from the A.21 extract at the beginning of the analysis (which applies exemptions to Articles 12-20 of the Regulation) that it can apply to Article 14; this latter Article deals with the provision of a Fair Processing Notice (FPN) to the data subject. As a reminder A.21 allows any Member State to legislate an exception from providing a FPN for any of the purposes identified in A.21, even for a purpose associated with "*important objectives of general public interests".*

Now consider A.14(a)(c) of the Council of Minister's text; this also provides an additional exception; there is an exception from providing a FPN when "*obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests*".

So what does the exception in A.14(a)(c) have that the exception in A.21 does not have? What are the "*appropriate measures to protect the data subject's legitimate interests"* other than those in specified in A.21?

As we have to apply some logic to deduce this, I suggest a pause for a caffeine infusion!

If A.21 allows Member States law to apply an exception, for example, in the "*important objectives of general public interests of the … Member State*" then it follows that the Member State law intended in A.14(a)(c) applies when there is **no such** "*important objectives of general public interests of the … Member State*" arise.

In general, therefore, there is no need for a Member State to legislate an A.14(a)(c) exception if one of the many exceptions in A.21 can be applied. It follows that Member States **only** a need to legislate for an A.14(a)(c) exception if **all** the exceptions in A.21 **do not apply** (i.e. the exception in A.14(a)(c) has nothing to do with national security; nor defence; nor public security; nor crime…. etc etc… the whole list in A21 – and not even in the "*general public interest*").

In addition, the requirement in A.14(a)(c) to take "*appropriate measures to protect the data subject's legitimate interests"* are delinked from Article 21's requirement that any "*restriction constitutes a necessary and proportionate measure in a democratic society*". In other words, Member States are legislating for an exception (e.g. not even in the "*general public interest*") where the "*appropriate measures*" that safeguard the data subject's position are not linked to the thresholds of "*necessity*" and "*proportionality*".

Similarly, A.14(a)(e) provides an exception to the provision of a Fair Processing Notice to each data subject when the personal data "*must remain confidential in accordance with Union or Member State law*". Following the logic as per A.14(a)(c), this Member State law in A.14(a)(e) is also providing for **additional** exceptions to those authorised by A.21.

In other words, the need for "confidentiality" exception in A.14(a)(e) does not relate to crime, nor national security, nor defence…. nor even any "*important objectives of general public interests of the … Member State*". There again, the A.14(a)(e) exception is **only** needed when **none** of the extensive A.21 exceptions apply. However, in this case, there is the added "bonus" of no explicit provisions to safeguard the data subject.

What are the circumstances that require *confidentiality* and an absence of data subject safeguards in circumstances that are not identified in A.21? Your guess is as good as mine.

I now turn to the Article 17(3)(b) "right to erasure"; this right does not apply if the exception is necessary "*for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*" (i.e. the fact that the processing is by a public body is sufficient).

As A.21 provides an exception from the "*right to erasure*" for a host of reasons (including "*general public interest*"), the A. 17(3)(b) exception is therefore linked to a different kind of "*public interest*" or a public function task that is wholly unconnected with a purpose described in A.21. Note a unspecific "*public interest"* in A. 17(3)(b) is well below the level of "*important objectives of general public interest"* in A.21.

In summary, as we have already established that the use of the "*important objectives of general public interests*" category lowers the protection afforded to data subjects below that of the Directive, then it follows that application of the A.14 and A.17 exceptions identified above will do likewise.

Be prepared; it does not gets better!

I will now explain why the Council of Ministers have narrowed the application of A.21 exception in A.5 which contains several familiar Data Protection Principles; the reason is so that the Council text can introduce "exceptions" that avoid the safeguards of the A.21 exception. These A.5 "*exemptions*" can take the level of protection below that afforded by the Directive.

Article 5(b) defines the important Finality Principle which states that personal data have to be "*collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*". However the Council of Minister's text adds that "*further processing of personal data for archiving purposes in the public interest or scientific, statistical or historical purposes shall in accordance with Article 83 not be considered incompatible with the initial purposes*". (Note: I address Article 83 later!).

Similalry Article 5(e) outlines the Retention Principle which requires the keeping of personal data for no longer than is necessary; the Council of Ministers' text then adds that "*personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, or scientific, statistical, or historical purposes in accordance with Article 83*".

It can be seen that the above italic quotes are in effect is an exemption from the Finality Principle and the Retention Principles; for instance it is not a breach of the Finality Principle if the further processing is for an "*archiving purpose in the public interest*" or any *"scientific, statistical or historical purposes".* Similalrly there is no breach of the Retention Principle if the purpose of retention relates to these purposes.

Note that the use of these two exceptions therefore does not need an "*important objectives of general public interests*" and both are delinked from A.21 safeguard that any "*restriction constitutes a necessary and proportionate measure in a democratic society*".

The Regulation introduces a general "*archiving purpose in the public interest*" when archiving is not a purpose in itself; organisations create "archives" for a specific purpose (e.g. in order to prove that payments have been made, because legislation requires retention for a purpose such as money-laundering). The notion of "*archiving purpose in the public interest"* needs additional clarification as to the purpose of archiving and the nature of the "*public interest*"; note that the "*public interest"* associated with the archiving purpose is much lower that the test of "*important objectives of general public interests"* specified in A.21.

It could be that Member States have archiving for a scientific, statistical or historical research purposes in mind with respect to the exception described above; however, the use of the word "*purpose*" in A.5 is not qualified by the word "*research*". Thus in the attempt to facilitate research, the Regulation may have constructed an exception that is far too broad which takes the level of protection below that of Directive 95/46/EC. For example, if you look at the text of A.17(3)(d) (as well as A.83 above) the word "*research*" in the Council of Ministers text has deliberately been removed.

Far from making it easier for researchers, this exception could undermine trust in researchers who need data subjects to embrace the research.

A purpose that has no need to have a "general public interest"

I will now show that Article 83 has been changed by the Council of Ministers because Member States do not want data subjects to challenge on the grounds that "*a scientific, statistical or historical*

purpose" is not of "*general public interest*". Note that these purposes are broadly defined; for example a "*scientific purpose*" includes a "*scientific research purpose*" but is not limited to research.

> *A.83: "Where personal data are processed for scientific, statistical or historical purposes Union or Member State law may, subject to appropriate safeguards for the rights and freedoms of the data subject, provide for derogations from Articles 14a(1) and (2), 15, 16, 17, 17a, 17b, 18 and 19, insofar as such derogation is necessary for the fulfilment of the specific purposes".*

Note that the derogation list (Articles 14a(1) and (2), 15, 16, 17, 17a, 17b, 18 and 19) are all contained in the Articles 12-20 identified as qualifying for the A. 21 exception. It follows that the derogations could fall within A.21 if the purpose of the processing was included in the list of exception purposes in A.21 (e.g. crime, national security, defence etc). The same goes for the "right to erasure" in A.17(3)(d); this does not apply "*for archiving purposes in the public interest or for scientific, statistical or historical purposes*".

It follows that the "*scientific, statistical or historical purpose*" is not even guaranteed to fall within the requirement that the purpose is of "*general public interest*"; indeed, the way Article 83 works is that there has to be no "*public interest*" in the "*scientific, statistical or historical*" purpose at all.

Now clearly, Member States have the research purpose in mind and arranging things so that any research can occur without too much interference from data protection. However, the purpose goes far wider than the research purpose and by removing the word "research", the Council of Ministers have constructed an exception that is far too broad which is likely to take the level of protection below that of Directive 95/46/EC.

Finally, note that it is the Member State that defines the protection and not the data protection authority; this fact alone could undermine trust in researchers who need data subjects to embrace the research. Don't believe me; just look at the problems that the attempts to get wider use of medical records has encountered (https://medconfidential.org/).

"Member state law" equates to further exemptions

I have already mentioned in a previous blog that Member State law can change the impact of the Regulation in the following Articles: A1(2a), A3(3), A4(5), A5, A6(3b), A8(1), A9(2a), A9(2b), A9(2g), A9(2h), A9(2hb), A9(2i), A9(4), A9(5), A9a, A14a(4c), A14a(4e), A17(3b), A20(1a), A21(1), A21(1c), A24(1), A24(3), A26(2), A26(2)(a), A26(2)(g), A26(2a), A30(2b), A32, A33(5), A34(7a), A35(1), A35(7), A44(1)(g), A44(5), A44(5a), A55, A56, A74, A76, A79(3)(b), A79b, A80, A80a, A80aa, A80b, A82, A82(3), A83, and A84.

If Member State law can change the impact of the Regulation then this can be seen as implementing an exception by the Member State from the effect of the Regulation. "Member State law" is therefore a euphemism for "Member State exception".

As most of these Articles that allow Member States to go their own way are not specified by reference to the requirements in A.21 then any exception that the Member State law introduces is not required to be "*a necessary and proportionate measure in a democratic society*". Indeed there is no need for the Member State exception to possess any "*important objectives of general public interests of the … Member State".*

As with A.83 (see above) it is easy to see how each Member States can construct wide exceptions to protect its national specialist interests from the obligations of the Regulation. That is why, if the Council of Ministers text prevails, the level of privacy protection established under Directive 95/46/EC cannot be guaranteed.

If that is the result of the Trilog, then the Regulation will offer a lowering of the protection afforded to data subjects below that of Directive 95/46/EC.

What needs to be done?

If there are going to be a large number of exceptions from the provisions of the Regulation available for Member States to enact, then ….:

(1) There needs to be an Article in the Regulation that explicitly states that the use of any exception or modification to the Regulation introduced by Member State law does not take the level of data subject protection below that of Directive 95/46/EC.

(2) Data protection authorities must have to have a role in advising Member States whenever any exception introduced by virtue of Member State legislation is being considered.

(3) All exceptions in the Regulation including those introduced by Member State law have to be brought within the compass of A.8 of the ECHR (i.e. subject to a test of "necessity" and "proportionality").

(4) The data protection authorities have to have a role in enforcing A.8 of the ECHR where any enforcement can be appealed through the judicial system.

(5) Groups representing data subject interests or data controller interests can raise issues of data protection importance with a data protection authority (and/or the Courts).

(6) Data subjects are not charged a fee to instigate review or appeal proceedings with respect to a breach of the Regulation (given recent moves in the UK re charging and FOI requests this is essential).

References:

(1) The Trilog Regulation set of documents (520 pages); I have provided the EDPS version as it is useful to see his compromise solution in his "Comparative table of GDPR texts with EDPS recommendations Comparative table of GDPR texts with EDPS recommendations**"**. https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package

(2) Data Protection Directive 95/46/EC: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

(3) A recent blog explained how the Council's text removes the data subject protections established by recent ECJ Judgements http://amberhawk.typepad.com/amberhawk/2015/07/council-of-ministers-regulation-text-negates-ecj-rulings-in-lindqvist-and-ryne%C5%A1.html

(4) More detail on the list of Articles where Member States can go their own way: http://amberhawk.typepad.com/amberhawk/2015/06/harmony-what-harmony-disharmony-extends-to-one-third-of-the-data-protection-regulation.html

(5) **History**: the infamous Clive Ponting prosecution in 1985 was under the Official Secrets Act. It concerned a Civil Servant who disclosed classified documents to Tam Dalyell MP which allowed him to asked precise Parliamentary Questions about the location and direction of travel of the "General Belgrano", the World War II cruiser, when it was torpedoed at the start of the Falklands War. The judge's summing up in the Ponting case: https://www.documentcloud.org/documents/1386622-ponting-summing-up-as-sent-by-lslo-to-pm.html

(6) More on data protection authorities acting as Human Rights Commissioner for Article 8: http://amberhawk.typepad.com/amberhawk/2010/04/information-commissioner-should-enforce-article-8-privacy-rights.html

And

http://amberhawk.typepad.com/amberhawk/2012/11/information-commissioners-enforcement-proceedings-links-article-8-to-unlawful-processing.html

(7) We are discussing the Data Protection Regulation at our half day workshop on Sept 28 (**http://www.amberhawk.com/bookevents3.asp)** or Update session on Oct 19 **(http://www.amberhawk.com/bookevents.asp**