GDPR Issues Committee Responses

Meeting Name:	GDPR Issues Committee Teleconference
Paper Number:	GDPR011_01
Meeting Date:	08 January 2018
Purpose of Paper:	Information
Classification:	Public
Synopsis:	The paper sets out the responses received from GDPR Issues Committee Members, following an urgent request for the Committees input. The paper also provides a general summary of the responses and the issues identified.

RECOMMENDATION:	The Committee is invited to: • **NOTE** the contents of this paper.

Paper Author: Elliot Bird

© MOSL 2017

1. Executive Summary

Following the recommendation of the two Change Proposals agreed by the GDPR Issues Committee to the Panel, Panel Members highlighted issues with the recommended legal drafting. Panel Members highlighted that:

1. **Schedule 13 Section E 1.2a:** This clause requires Trading Parties to *implement appropriate technical and organisational security measures that meet the requirements of Data Protection Laws and are consistent with or equivalent to industry standards, best practices and frameworks.* Panel Members raised that this could be interpreted as being more prescriptive than GDPR legislation, which only requires appropriate measures, and therefore against the light touch approach.
2. **Schedule 13 Section E 2.1:** Similarly, this clause requires Trading Parties to report all breaches to the ICO within 72 hours, which Panel Members highlighted could be interpreted as more prescriptive than GDPR. The GDPR only requires this when there is a significant risk to individuals' rights and privacy, rather than in every instance as this clause suggests.

Following this discussion, the Panel agreed to recommend the Change Proposal, under the condition that the highlighted issues be resolved in a way that was satisfactory to the Panel Members who raised them. The Panel agreed to achieve this by holding a sub-group meeting with Panel Members who raised issues and Members of the GDPR Issues Committee.

The Committee agreed that point 2 could be resolved by including the wording suggested by Panel Members, that doesn't require every breach to be reported to the ICO within 72hours. However, the Sub-group struggled to come to a consensus on how to resolve point 1, The sub-group agreed to consult Members of the Committee urgently for feedback on the issue, in attempt to identify the position of the Committee on the Panel Members suggested wording.

Following the urgent request from the Committee it has been concluded that the majority of Committee Members agree that the text in its current form is necessary and cannot be reduced as suggested by the Panel Members.

Next Steps

The Committee will now need to decide a way forward in resolving issues the Panel have highlighted with Section E 1.2a, and provide a solution to concerns highlight by Panel Members. Panel Members who raised concerns will be consulted following the Committee decision to determine whether they are satisfied with the solution. Once agreement has been reached with Panel Members, the Change Proposal will be provided as a recommendation report to the Authority, based on the Rationale identified by the Panel in the previous Panel meeting.

© MOSL 2017

2. Questions

As part of the urgent request for input from the Committee the following questions were asked:

Question 1

Noting that the inclusion of the second limb of clause E1.2(a) (i.e. *"…and are consistent with or equivalent to industry standards, best practices and frameworks.")* was designed to provide an identifiable context for benchmarking compliance, whilst balancing the light touch approach with the need for mutual assurance in the context of data security, is there a need to retain this (or some equivalent) text?

Question 2(a)

If no, i.e. there is no need to retain this or equivalent text, do you agree that in line with the preferred wording, the amended clause should now read:

1.2 (a) Each Party must implement appropriate technical and organisational security measures, that meet the requirements of Data Protection Laws.

Question 2(b)

If yes, i.e. there is a need to retain a reference to benchmarking standards for technical and organisational security:

do you believe the wording as originally recommended by the Committee to the Panel should be retained?

The GDPR Issues Committee Members responses are provided in the following Section.

3. Responses

2.1 James Gilbert (Wholesaler Committee Member)

Question 1

I saw the second limb of details as a means to clarify expectation, but I can see their perspective. Removing it doesn't change the overall requirement of complying with a nebulous statement of "appropriate technical and organisational security measures." There is no need to retain the statement.

Question 2(a)

I'm comfortable with this.

Question 2(b)

N/A

2.2 Trevor Nelson (Panel Sponsor)

I'm not a voting member of the committee so if it's OK with you I'm not going to go through the formal route of responding to the questions but as the sponsor and Panel member although I saw the advantages of the original wording the new suggestion (i.e. removal of the limb) is acceptable if it helps to break the deadlock we are in.

2.3 Louise Fox (Retailer Committee Member)

Question 1

Yes. Retain this wording. I believe that TPs are looking to MOSL to not only provide guidance on what is expected of them as joint controllers of Market data, but also to set the tone on how they should be achieving it. The ICO does not specify what equates to best practice, and allows a data controller to determine this within their own interpretation and capabilities. As those who will be effectively sharing the data within CMOS, I feel that suggesting industry standards, best practices and frameworks is sufficient without being prescriptive nor heavy handed.

Question 2(a)

N/A – I said Yes to Question 1

Question 2(b)

Yes, I do. As a market with joint liability I do not think that it is unfair to expect anyone sharing that data to achieve a measurable level of security. We should not be compromising on the expected levels of security TPs should have in their respective systems and by including this in the wording MOSL is recognising the importance of this.

2.4 Maureen Wilkinson (Retailer Committee Member)

Question 1

No need to retain or provide equivalent text.

Question 2(a)

Agree with amended clause.

Question 2(b)

Not relevant.

2.5 Caroline Gould (Wholesaler Committee Member)

I think it is easier to discuss this in general with the rationale overall before I consider the questions individually. I have worded this as though I am speaking on behalf of the Panel and I think that my memory and notes are correct – but if anyone in the Panel disagrees please let me know. We have not of course had a chance to discuss this as group so I accept this may only be my view.

I think it is important to set out what the GDPR actually says on this matter:

Article 32 – Security of processing:

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b)the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c)the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d)a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence 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 compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

The Panel narrowed this article down to:

Each Party must implement appropriate technical and organisational security measures, that meet the requirements of Data Protection Laws and are consistent with or equivalent to industry standards, best practices and frameworks.

As you will see from the above the actual GDPR wording is far more detailed than the wording in the proposed Schedule to the MAC. We decided to limit it to the proposed wording as "the requirements of Data Protection Laws" would capture the full text of the GDPR, but that how this is implemented and to what standard would not be captured.

Previously we had a much more detailed security schedule that went into very prescriptive detail as to how we could ensure a consistent approach across the trading parties in relation to the Data sharing being undertaken in the market.

To make it as light touch as possible we took that all out and left it to '*and are consistent with or equivalent to industry standards, best practices and frameworks'*.

We felt that the wording consistent with or equivalent to have as much flexibility as possible as this allowed for trading parties to put completely different measures in place provided it allowed for the same outcome – for example an outcome may be to have the **ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.** There may be a number of industry standards for example in relation to disaster recovery that would apply and provide the same outcome. Industry was not meant to capture the water industry – merely generic terms where things become a usual practice over time.

Best practice in relation to data protection would be the guidance from the ICO. For example there is a guide specifically designed for small businesses to follow published by the ICO in relation to data security. https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf It is already been confirmed that if an organisation had a breach it would be taken into consideration if such guidance was not being followed even though it is not enshrined in law. This is because data protection and security changes over time. What may have been a secure measure to take 5 years ago in the IT world will not be such today. This is why we kept the wording flexible to allow for things to change over time.

In terms of imposing obligations on smaller new entrants we specifically took out the prescriptive security measures for that reason. A small entrant would already be expected to comply with the ICO guidance which is not particularly high tech anyway.

The Panel felt that if there was no minimum security standard set (by way of consistent with etc…) and we had already taken out the prescriptive set of minimum security requirements, then we would not have a secure data sharing arrangement that all parties could sign up to confidential knowing that one party would have no security standards and therefore potentially cause a breach that could affect the whole market..

As this Schedule is essentially the Data Sharing agreement between all the parties as joint data controller, its needs to comply with the ICO Code of Conduct on Data Sharing (which is a statutory requirement) and this specifically mentions in the Code that:

"*When personal data is shared, it is good practice for the organisation disclosing it to make sure that it will continue to be protected with adequate security by any other organisations that will have access to it. The organisation disclosing the information should ensure that the receiving organisation understands the nature and sensitivity of the information. It is good practice to take reasonable steps to ensure that those security measures are in place, particularly by ensuring that an agreed set of security standards has been signed up to by all the parties involved in a data sharing agreement*." https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

The wording we proposed did this as it required parties to be *consistent with or equivalent to industry standards, best practices and frameworks.* This we felt was the lightest touch approach. It also met the mutual assurance point and the Article 26 Joint controllers requirement.

My responses to the questions are therefore:

Question 1

Yes we need to retain the text.

Question 2(a)

N/A

Question 2(b)

Based on the argument above I think this is the lightest touch approach we could take in any event.

2.6 Hugh Laurie (Wholesaler Committee Member)

Question 1

I believe that it is best that we retain the text as approved by the Committee. My rationale for this is as follows.

Whilst its inclusion is not absolutely critical, it adds clarity without adding any additional obligation.

I do not feel the wording goes beyond what is prescribed by the GDPR and the ICO Code of Conduct on Data Sharing, as described so clearly by Caroline. Hence it would appear to be incorrect to delete the words on the grounds that it exceeds GDPR requirements or creates an unnecessary barrier to new entrants. Solutions for GDPR compliance for companies with a small customer base could well be simpler, perhaps partly manual, from that required by retailers with many customers, but the requirements are the same.

It is clear that this is the start of our GDPR journey and that best practices are yet to evolve. The industry needs to work together to share experiences, agree and spread good practice.

Question 2(a)

N/A

Question 2(b)

Yes, I believe that the wording as previously recommended by the Committee should be retained.

2.7 Nick Rutherford (Wholesaler Committee Member)

Question 1

Yes

Question 2(b)

Yes we should retain the original wording.

I think the wording gives enough to feel satisfied that mutual assurance will be achieved, not too prescriptive yet still set setting an expectation. There are many standards for consideration to comply with the obligations and I think the wording is effective to allow a 3rd party to check the level of technical standards/security that has been applied by an organisation. There is plenty of guidance out there from Water UK for Wholesale organisations to be considering and there are plenty of other security standards that companies can align against. There is also IASME for smaller organisation (& government departments) to consider which is not as broad as full ISO27001 so something like this may be suitable for smaller Retailers etc.

So I think it's fair to set an expectation that organisations "are consistent with or equivalent to industry standards, best practices and frameworks". The challenge may be more about how this is demonstrated via audit etc and how the Market Operator will judge sufficient controls/standards/measures are in place and trading parties are sufficiently compliant.

2.8 Gillian Hill (Retailer Committee Member)

My thoughts are:

Whilst I understand the desire to include additional wording on account of the shared risks in relation to personal data, I do think it could be successfully argued that the wording "and are consistent with or equivalent to industry standards, best practices and frameworks" goes further than the GDPR requirements. If you look at Article 32 it says the controller and processor have to implement appropriate technical and organisation measures to ensure an appropriate level of security "taking into account the state of the art, the costs of implementation….persons". Obliging all parties, whether large or small, including new entrants, to implement security measures that are consistent with or equivalent to industry standards, best practices and frameworks does not seem to me to meet the subjective standard in the GDPR.

I did take the reference to "industry standards" as meaning standards in the water industry and I suspect some other people reading this and trying to work out what they need to do may take the same view. "Industry standard" is taken as meaning generally accepted requirements followed by the members of an industry. On a simple reading of this, our industry in this case is water.

I do think the phrase "best practices" imposes a high burden. It is generally taken to mean the best or most efficient way to do something. Again, that does not take into account the subjective nature of the wording of Article 32. I appreciate Caroline's comment that best practice here would be guidance from the ICO but in relation to other discussions about guidance from the ICO we agreed we would only have to comply with mandatory guidance.

It's interesting to note that the current wording elicits different responses from us as to what it obliges us to comply with.

I agree with Nick that it will be a challenge to audit compliance with this wording. Who is going to decide whether a party has implemented appropriate technical and organisational security measures?

Question 1

Whilst I would prefer the amended clause proposed by the 2 members of the Panel, I understand the requirement to have some additional wording.

Question 2(b)

I think we should amend the wording originally recommended by the Committee to delete the reference to best practices and agree what we mean by industry standards or find some alternative way of describing it.

2.9 Sally Marshall (Retailer Member)

Question 1

No. I think the text within GDPR covers the requirement and how individuals go about this should not be made overly prescriptive. What might be useful would be a link to codes of practice produced by the ICO to which we know they refer in terms of investigation of a breach etc., but this is to be helpful rather than rigid. Also, what I believe we should take into account is the need for recognition of the fact that all parties will be required to prepare for the new data protection law

and will be doing so with recognition of their own policies/procedures and/or technical expertise which could be compromising and conflicting.

Question 2(a)

No. The amended clause should now read: *1.2 (a) Each Party must implement appropriate technical and organisational security measures, that meet the requirements of Data Protection Laws.* The wording that refers to data protection law is sufficient to meet the requirements and give scope for individuals attainment of those regulations. I appreciate that there is further information contained within the legislation but this is not prescriptive to a standard. Also until the Bill is passed, I would withhold the mention of standards/frameworks etc as this could be subject to change or a more prescriptive context in guidance from the ICO, which would require a rewrite.

Question 2(b)

N/A

4. Recommendation

The Panel is invited to:

- **NOTE** the contents of this paper.

Elliot Bird

Market Analyst