GDPR Issues Committee – Summary of Industry Consultation Responses

Meeting Name:	GDPR Issues Committee
Paper Number:	GDPR08_01
Meeting Date:	10th November 2017
Purpose of Paper:	For Information
Classification:	Public
Synopsis:	This paper provides a summary of the responses received for the industry consultation issued on behalf of the GDPR Issues Committee. It also sets out many issues raised by respondents for the Committee to consider, and provides recommendations on how to resolve these issues.

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

Paper Author: Elliot Bird

1. Executive Summary

Following the industry consultation on the proposed additions for compliance with GDPR we had a total of 17 respondents, 6 were Retailers, 10 were Wholesalers and we received 1 response from CCWater. Most of responses were positive and commended the thorough investigation and light touch approach, but there were some respondents that would have liked the provisions to be lighter touch than the proposed.

Most of the disagreements focus around the revisions made to the drafting following legal advice which don't seem to follow the light touch approach the Committee was aiming for. Several respondents did not agree with the requirement to restrict the use of data to compliance with the codes, both for its effect on the competitiveness of the industry and with operating the market. There were issues with both marketing and pricing if market data could not be used for any purpose other than compliance with the codes, as it is currently being used for both things which are not in the codes. The market structure and definitions which describe Trading Parties as Data Controllers in Common was another point that some respondents disagreed on as they felt that Trading Parties could be considered separate Data Controllers for their own market data. Linked to the previous point around Data Controllers in Common, some Trading Parties also disagreed with the clause on liabilities and claims which indicated that parties would be joint and severally liable.

There were some points of collective agreement which should be implemented in the redrafted version of the provisions, such as:

- The codes should not require Trading Parties to comply with all guidance provided by the ICO;
- The codes should not reference existing industry standards and certifications within the suggested data security requirements;
- There will need to be a secure platform to facilitate the transfer of data subject requests and process forms;
- There should be additional protections in place for special categories of Personal Data (sensitive personal data);
- There will need to be at least a month of implementation time for Trading Parties to align with the Privacy Notice of the Market Operator, prior to GDPR's introduction; and
- Existing market processes should be used in place of newly proposed processes, where they are duplicated, and changes should be made to those processes to meet the requirements of GDPR.

Following the Committee's review of the consultation, it will be agreed by the Committee what items will need to be changed or included in the final version of the legal drafting. This will then be recommended to the Panel in the form of a Change Proposal, which will be proposed by the Chair of the Committee. This Change Proposal will be put forward with the intention of being implemented into the codes and system before the introduction of GDPR in April 2018.

2. Table of Issues

A table of issues has been provided which outlines all the key issues respondents to the consultation identified that will require a decision from the Committee. These include the specific questions raised in relation to these issues and a recommendation from MOSL with how to proceed on the given issue.

Issue	Questions	Discussion	Recommendation
Data Controllers in Common	• Is it appropriate for Trading Parties to be joint data controllers, or data controllers in common?	This is an issue that DACB previously advised on in their Privacy Impact Assessment/ DMP.	**No change is required**, as Data Controllers in Common is an agreed market structure and sufficient arguments aren't provided to question that.
Joint Liability/Allocation of liability	• Is it appropriate for Trading Parties to share liability? • Is it possible to allocate liability more specifically?	It may be possible to allocate liability more specifically, however, DLA would suggest that this be done in a separate document as this would not be straightforward and would likely not be suitable for a Schedule to the MAC. The key question here is the extent to which members wish to consider the granular detail of the various scenarios that could arise giving rise to liability and the extent to which it is desirable/ possible to prescribe how liability is to be allocated in such scenarios.	**Separate piece to be undertaken.** Based on the responses the preference of the industry is to identify and determine these liabilities. However, doing so would severely extend the timescales of the change so this should be addressed as a separate piece of work once this is completed.
Use of data outside of compliance with the codes	• How will the market remain competitive without marketing?	The query that was previously put to DLA in this context was whether the definition of "Purpose" i.e. the purpose for which personal data may be used (presently defined as use for compliance with the Codes) could be widened to arguably cover direct marketing without expressly mentioning it. Their clear view is that the widening of "Purpose" in such a way would not be compliant with GDPR since one of the key principles of GDPR is the need to be clear and specific about what data is being used for (and for those purposes to be very clearly and explicitly reflected in the privacy notices issued to data subjects).	**Minor amendment required.** The recommendation would be to clarify that it mandates the use of data for the purpose and current required operations of the market that do not conflict with the requirements of GDPR. Also note that the drafting does not mandate the use of data the Trading Party has collected within their own systems, as it only refers to data in CMOS and data shared bilaterally.

		Note also the additional safeguards that come into force re direct marketing with the EPrivacy Directive in 2018 (mentioned in previous advice from DLA).	
Double Jeopardy of charges	• Is there a risk of Trading Parties being charged twice for breaches of GDPR? • Will MOSL enforce compliance with the codes?	As a general observation, it should be noted that more than one form for liability for GDPR breaches could arise e.g. a fine imposed by the ICO and a civil claim by affected data subjects.	**No change required.** This is a l legal concern and not within MOSL's remit. Just as the ICO may sanction alongside a subject suing for damages, any other party to the MAC may also recover losses in addition to these charges.
Content of data subject request process forms contain personal data	• Are there potential impacts of increased time and effort required to fill in the forms? • Are there issues with circulating forms containing personal data not held in CMOS? • Is the requirement to communicate with relevant Trading Parties in actioning a request proportionate.	Such forms would include *Market Personal Data* despite not being on CMOS. As regards increased time and effort, as a general observation, DLA expect that all industries and sectors will experience an increase in the time and effort involved in dealing with data subject requests under GDPR therefore that is to be expected as a result of the change of the law. As regards proportionality, the shared dataset and complex relationships between the many parties in the market does create a complex context here. DLA have set out in more detail, some of the practical and legal issues that were taken account of in framing the processes for dealing with requests from data subjects. In summary, key considerations include: • The fact that a request will be addressed to a specific entity (most likely the retailer who deals with the customer with whom the data subject is associated) and it is **that** entity will be legally obliged under GDPR to deal with/respond to the request • The other parties, as joint data controllers, will, however, have a (potential) interest in or be affected by the request	**Minor amendments required.** The process, as identified by DLA, is likely to become more onerous for everyone based on the introduction of GDPR which cannot be avoided. However, the content of the forms can be revised to contain the minimum amount of required information to identify the customer. Response from Anglian Water Business suggest that it only require SPID, customer name and address to identify the customer.

		e.g. a request to erase data will require action by more than one party to be effective • MOSL will also need to maintain oversight of CMOS/ the dataset and to that extent will require to oversee/co-ordinate such requests. However, in terms of dealing with such requests, in many cases MOSL may only be able to partially deal with this and there may other, separate exercises that will require to be carried out to ensure the request is properly dealt with - each request needs to be looked at in its own terms Each request needs to be looked at on its own terms.	
Additional definitions which are missing (Data Subject, Data Controller, etc.)	• Define data owner • Define Personal Data and Market Personal Data • Define Data Controller • Define Notes • Define Implementing Party • Use of Parties • Use of Market Participants	*Data Owner* - already defined in the MAC *Personal Data, Market Personal Data* and *Data Controller* - all included in the list of proposed new definitions *Parties* and *Market Participants* – These terms are referenced to be in the drafting but neither are defined and should not be used to ensure clarity. Both should be Trading Parties. *Notes* - DLA don't see a reference to this in the draft schedule - is this being picked up from MAC clause 15.1.1(b) ("*any notes published by the [ICO] or Codes of Conduct issued under Article 40 of GDPR*")? If so, DLA don't see any need to define "notes" as DLA consider the meaning is clear, however, this could be changed back to "guidance notes" if preferred (although DLA would suggest that the separate reference to Article 40 codes be retained).	**Minor amendments required.** Most of the definitions have been provided in the new definitions list or in the MAC. The only required change would be to remove references to Market Participants and Parties.
SPIDS should be personal data	• Why are SPIDS not included as a personal data item?	Recommendation would be to disagree with this point, as the PIA contends it is not Personal Data. The SPID field is just a number without any meaning and cannot be used to identify anyone.	**No change required.** The SPID data field was identified as indirect personal data in the PIA, which the GDPR does not define or legislate. Based on this it was not identified as

		DACB have given further advice on the issue of SPIDs and whether these fall within personal data - see their advice note of 120917 at paragraphs 6-7.	personal data field in the PIA and the recommendation would be to remain this way.
Should identify the conditions for processing we expect the industry to cite in their privacy notices	• Are we required to do this? • What conditions are we identifying	DACB have given advice on this previously - see their advice note of 120917 at paragraph 14 (and previous advice note of 120817). The conditions for processing will require to be considered by all trading parties in the context of considering the lawfulness of their own processing of data including any sensitive data - this will be relevant to drafting privacy notices etc. From the perspective of market-wide compliance, the parties have a shared interest in ensuring a degree of uniformity/alignment as regards the processing conditions relied upon.	**No change is required**, as captured in the legal advice, MOSL cannot prescribe processing conditions for all Trading Parties. MOSL will be publishing a Privacy Notice containing conditions it relies upon, which should be useful guidance for Trading Party consideration.
DPO requirement for 24hr contact details	• Is this requirement in excess of the requirements of GDPR? • Are the impacts on Trading Parties substantial? As one response would suggest.	There are no express/specific requirements for 24-hour contact details in GDPR. This approach was suggested on the basis that other obligations under GDPR may require swift action by trading parties e.g. the requirement to notify relevant data breaches within 72 hours of becoming aware of the breach. Were such a breach to occur, e.g. on a Friday evening, the lack of 24-hour contact details could be problematic. It may be that additional drafting could be added to make clear that out of hours contacts are for exceptional/ urgent situations.	**Minor amendments required.** It should be made clear that DPO's should only be contacted outside of working hours in strictly emergency situations i.e. there will be severe costs to the issue not being addressed immediately.
Requirement to align Privacy Notices with MO	• Will Retailers have to align many privacy notices based on multiple services?	As presently drafted, the schedule would allow individual parties to develop their own styles to fit their businesses, having considered the market operator approach. However, the parties have a shared interest in ensuring a degree of uniformity/ alignment as regards the terms of notices given the dataset is shared. It may helpful for MOSL to circulate an early draft of the privacy notice in order that parties may identify any points that prove to be sticking points.	**No change required.** The way this is drafted allows flexibility in the drafting of each Trading Party. The intention is not for Trading Parties to exactly mimic the privacy notice of the MO, but take the privacy notice into consideration and align it were is appropriate.

Data subject rights processes are onerous and place a disproportionate burden on Retailers	• Should the processes be streamlined further? • Can onus be moved away from mostly Retailers? • Should MOSL be the central point of the requests process?	DLA are not sure what degree of streamlining of processes/forms is being contemplated. Ultimately, if it was considered desirable, these processes could be revised right down to e.g. one single process to be followed for all types of request/ exercise of different types of rights by data subjects. However, since the various processes are all slightly different, this would require considerable care with redrafting to create a process that operated compliantly for all the relevant types of processes. The major reservations with such an approach are: • The Schedule as currently drafted makes it explicit and obvious that there are a variety of different rights/requests available and that it is important to identify the correct one to ensure the correct process is followed - DLA fear that an understanding of the complexity of the full matrix of rights could be lost to some extent by creating a single 'one size fits all' process. However, some of these concerns could be mitigated by preparing a detailed Data Subject form which would cover all possible processes and which would lead the person completing the form through the various possibilities to ensure the correct process is identified and followed; • From a GDPR audit perspective, the Schedule as presently drafted indicates a better understanding of the GDPR framework on data subject rights than a simplified version would • The Schedule as currently drafted also follows a general drafting style within the wider Codes to spell out processes individually With reference to the comment regarding the burden on retailers and MOSL's role in dealing with requests, the	**No change required.** The process, as identified by DLA, is likely to become more onerous for everyone based on the introduction of GDPR which cannot be avoided. The drafting is written with the intention that Trading Parties will undertake this process in the most efficient manner. If that means they do not require the interaction with the Market Operator we see no reason why they should not complete the request themselves. As is highlighted in the discussion, we would expect Trading Parties to consider on its own terms and dealt with as efficiently as possible.

		following points should be noted from a pragmatic perspective: • DLA suspect that a data subject seeking to exercise their rights is most likely, in the first instance, to contact the retailer as the entity that issues bills to the customer to which the data subject is connected. However, it is possible that MOSL may receive contact directly. **Whoever the request is addressed to is the entity obliged to comply.** • The processes as presently drafted were designed to ensure that regardless of which entity receives a request (a) MOSL is informed and (b) the (most appropriate) Data Owner deals with the substance of the request to ensure MOSL has an overview of any issues that arise and can consider the integrity of CMOS a whole • The entity that receives the request cannot simply transfer their obligation to deal with a request addressed to them to MOSL - albeit arrangements can be put in place (given the shared dataset) between the parties to ensure requests are dealt with expediently. The entity that received the request would, however, be responsible for any perceived failure to properly deal with it Further, depending on the terms of the request received, MOSL may not be able to deal with it fully. There may be a need for a retailer to conduct a separate non-CMOS related exercise internally. For example, data subject access requests are often received in the context of a broader customer complaint or dispute and may seek all records held in relation to that individual. In such a situation, there may be relevant records in CMOS as well as other information (e.g. telephone notes) that only the retailer will have. Whilst it may be prudent to have MOSL overseeing and managing such issues there will require to be flexibility built into the process to	

		ensure each request is considered on its own terms and dealt with properly.	
MAC disputes vs. Panel governance of data protection disputes	• Is the current process for MAC disputes sufficient? • What new process or changes to the current ones be made? • How should the Panel govern disputes? Should there be a new Committee?	The question of disputes under the Codes is a broader issue that may, in due course, be the subject of a separate and wider review. It may be most appropriate for this issue to be revisited in the context of any such future review. If, however, there was a wish to design an amended process specifically for data protection disputes now, that could certainly be done. In that event, some Committee direction (for the purposes of drafting) would be required as to the desired scope of the process (in terms of subject matter), the preferred decision-maker and preferred length of the process. The consensus of the consultation is that this should be amended as a separate Change Proposal so that it wouldn't slow down the process, which would be the recommendation from MOSL.	**Separate piece of work to be undertaken.** It is agreed that the MAC disputes process would be the preferred method, but also agreement that it will not operate in sufficient timescales. Therefore, the MAC disputes process needs to either be amended or have a new process developed specifically to manage interpretation of data protection provisions. This has the potential to severely delay the change and should be addressed separately.
Controls required for protection of special categories of personal data (sensitive data)	• Should there be further controls? • Are the current security requirements already sufficient?	Majority agreement is for stricter controls. However, we will need to consider what system impact these stricter controls might have and what system changes might be required with the change or as a separate change to ensure the process isn't delayed. Legal advice on these issues has previously been provided by DACB in their advice note of 290817 at page 7.	**Substantial change required.** Given that this has been identified as a majority agreement from the industry a system solution will need to be developed and prescribed within this Change Proposal. This would require the ability to restrict access to the sensitive customer flag, and for CMOS to produce MDS reports without sensitive customer flags included.
We aren't sufficiently covered for Automated Decision Making	• Should we future proof for automated processes that are developed?	There is scope for consideration of automated processes that may occur in the future. However, this will further widen the scope of the Change Proposal and delay the process further.	**No change required.** Following industry consultation Trading Parties have not identified any processes that will require manual intervention to be put in place.

	• Is the gap site allocation an automated process?	The recommendation would be that this is considered and reviewed as a separate Change Proposal following the completion of this proposal. Legal advice on automated decision making was provided by DACB in their advice note of 290817 at page 24.	However, we recognise the issue raised on future proofing the codes. In the event a process is identified that requires a manual work around this can be raised as a Change Proposal at that time.
Use of existing market processes to amend data	• Do existing processes need formalising? • What additional requirements are there for existing processes?	The existing process does exist for amending data, but it will need to be revisited to reflect some of the requirements of the previously drafted process. Particularly, it will need to inform parties what communications they are going to have to make to ensure all Data Owners can make the required changes. DLA agree that it would be helpful to revisit this CSD considering GDPR. You may recall that the initial advice given by DLA was that a review of certain existing (relevant) CSDs would be advisable to ensure GDPR compliance, however, the Committee's view was that it wanted a "catch all" statement rather than dealing with personal data issues in different CSDs. With specific reference to CSD0105, it may be appropriate, for example, to revisit the Purpose and Scope section (cross-referencing the new Schedule as appropriate in relation to personal data) and to flag/ possibly add additional requirements for any amendments involving changes to personal data.	**Committee decision required.** In terms of requirements met by the existing process, the only potential loss is that parties will be notified of changes but not why they have taken place. Therefore, when a data item is changed it won't be clear to parties that it was as the result of a data access request. Therefore, the Committee should come to a view on whether capability needs to be created in the system to attach a note to notifications of changes that indicate they are because of a data subject request.
What should be the role of the Market Operator be? And is this drafting widening it?	• Will the Market Operator be policing data protection? • Should the market operator act as a central liaison for	MOSL being a central liaison for Comms is resolution of the issue Trading Parties face because they won't necessarily have all the required information to circulate the request. Although they will have contact information circulated to them under these arrangements, they will not necessarily be aware of which Retailers operate in their area and which customers information they hold. However, there is an understanding	**No change required.** the drafting is written with the intention that Trading Parties will undertake this process in the most efficient manner. If that means they do not require the interaction with the Market Operator we see no reason

	Comms between parties?	from DLA that this process is flexible and there is scope for Trading Parties to resolve requests without intervention from the Market Operator.	why they should not complete the request themselves. The question on the Market Operators policing of data protection can be answered through use of the market audit, which has had a majority agreement in this consultation. The Market Audit will be the way in which the Market Operator monitors compliance with data protection.
No data mapping has taken place prior to this.	• Should data mapping take place to support the processes described?	Data mapping (suggested by a respondent to the consultation) would potentially help identify process steps that create risks for personal data more thoroughly, which may help identify further requirements of proposed new and some existing processes. This would involve monitoring the journey of specific personal data items between Trading Parties in a simulated market process. However, the time and resource constraints on the work of the Committee would not allow a piece of work like this to take place in sufficient time, and these concerns have been addressed when separately considering issues of data transmission and data subject rights processes.	**No change required.** This item was suggested by a respondent to better determine data protection issues in the proposed processes. Given that the Committee has analysed each proposed new process individually and considered this, it would seem unnecessary to complete this again more formally, especially given the potential delays it could cause.

3. Outstanding Issues prior to consultation

Prior to consultation an issue was raised which the Committee were not able to take a view on due to the time constraints involved, which has still not been solved in the legal drafting.

Currently there is nothing in place to describe the assigned liability and possible action that can be taken when the Market Operator makes an incorrect decision on whether a data subject request can be refused or not. If the Market Operator makes an incorrect judgement in this regard, the Data Subject may then legally claim based on this refusal and Trading Parties would potentially be liable.

There is currently no drafting that addresses this issue, following the amendments that allowed the Market Operator to refuse requests made to it directly if they were incurred disproportionate cost or effort.

This issue was not raised in the consultation but remains an issue which has not been resolved.

4. Next Steps

Once these issued are discussed by the GDPR Issues Committee changes will be made to the legal drafting to accommodate the issues identified in the responses and the Committee's advice on these issues. When the redraft is complete, the Committee will be consulted again for their final feedback on the proposal before it is recommended. Following this a recommendation will be provided to the Panel in the form of two new Change Proposal to both the MAC and the WRC. This Change Proposal will then be progressed by the Panel and the GDPR Issues Committee will be disbanded, providing that the Panel agrees with the Committee's recommendation.

5. Recommendation

The Committee is invited to:

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

Elliot Bird
Market Analyst