Minutes of General Data Protection Regulation (GDPR) Issues Committee Meeting 13

16 May 2019 | 10:30 – 15:00
Etc. Venues, 8 Fenchurch Place, London EC3M 4PB

Status of the Minutes: Approved

MEMBERS PRESENT

Helyn Mensah	HM	Chair	Trevor Nelson	TN	Committee Member (Retailer)
Caroline Gould	CG	Committee Member (Wholesaler)	Emma Groves	EG	Committee Member (Retailer)
David Oliver-Sheppard	DO	Committee Member (Wholesaler)	Rachel Skelton	RS	Committee Member (Retailer)
Kulwinder Johal	KJ	Committee Member (Wholesaler)			

OTHER ATTENDEES

Hazel Moffat	HMo	Presenter (Partner at DLA Piper LLP Law Firm) (T-con)	Roland George	RG	Head of Legal (MOSL)
Huw Comerford	HC	Presenter (MOSL)	George Monea	N/A	Observer (MOSL)
Amanda Hinde	N/A	Secretariat (MOSL)			

APOLOGIES

Louise Fox	LF	Committee Member (Retailer)	Abigail Morgan	AM	Committee Member (Wholesaler)

1. Welcome and Introductions

1.1. The Committee Chair welcomed attendees to the GDPR Issues Committee meeting 13.

1.2. The attendees introduced themselves and provided some background on their experience.

2. Minutes and Outstanding Actions

2.1. The Committee agreed with the approach for the outstanding actions and to close actions: G12_A02, G12_A03, G12_A06, G12_A07, G12_A08, G12_A09, G12_A10, G12_A11 and G12_A13.

2.2. On G12_A07, the Chair noted it was preferable not to send multiple rounds of experience review questions to DPOs. As such, work would be done to improve the questions to enable a single comprehensive round, and to enable insight on the scale of personal data, whether TPs were able to identify personal data, and whether TPs were able to recognise Data Subject Rights requests. The revised questions would be circulated to Committee members for comment and approval before circulation to DPOs and designated persons. It was agreed that G12_A07 would be closed and a new action would be opened to capture G12_A07, G12_A10, G12_A11.

ACTION G13_A01

2.3. The Chair and some Committee members (Caroline Gould, Emma Groves and David Oliver-Sheppard) requested for the SharePoint link to be resent to them.

ACTION G13_A02

2.4. Some Committee members queried whether there was an easy way for Trading Parties (TPs) to update MOSL with their Data Protection Officers' (DPO) contacts, for example via an email link on the MOSL website. The Chair requested the Secretariat to explore with MOSL the feasibility of this.

ACTION G13_A03

2.5. The Chair requested the Secretariat to secure a further meeting date after the currently scheduled meeting in July to give the Committee more time to consider any Change Proposals that may be required.

ACTION G13_A04

2.6. The Committee approved minutes for GDPR Meeting 12 with no change to the draft circulated.

3. Legal Review

3.1. HMo from DLA Piper presented an overview of her legal advice to the Committee on the scope of the definition of personal under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) and whether there have been any changes to this post-implementation of the legislation. This included advice on:

(a) any ICO or regulatory guidance issued in relation to or impacting the personal data definition

(b) any case law in the UK or the EU elaborating on the definition

(c) the concept of indirect identifiers and its place and scope within the definition overall

(d) application of the personal data definition to data in the non-household (NHH) retail water market – particularly in regard to which data items within Code Subsidiary Document (CSD) 0301 are likely to be captured.

3.2. HMo commented that having conducted the legal review, she is of the view that the Central Market Operator Systems (CMOS) has a limited risk profile and is well managed.

3.3. A Committee Member queried whether DLA Piper reviewed the data in CMOS only (i.e. data items in CSD 0301) or the whole-of-market interactions including between TPs. RG advised that DLA Piper's work had comprised a review of data items in the CSD and agreed with the Chair that there had been no specific limitation but rather the focus had been on the scope of the definition of personal data to enable a determination as to how it was to be applied. The Chair noted that the original Committee had considered how widely personal data should be defined in the context of the list of data items with particular regard to 'indirect identifiers', and that the watching brief was directed at this issue and was not intended to be a wholesale review of all interactions or individual TPs compliance.

3.4. In regard to the Committee member's concern that all TPs are data controllers, but the review specifically looked at data items in the CSD, the Chair reminded that the watching brief review focused on clarifying the current legal scope of the definition which could then be applied to the solution; the Committee was not limited, and could consider, for example, running through case study examples to ensure fitness for purpose.

3.5. HMo advised that although there were wording changes in the GDPR/DPA 2018 versus the Data Protection Act 1998 (DPA 1998) - largely to take into consideration the evolution of technology methods - many of the underlying concepts had not changed. She further noted that the industry had not yet seen many enforcement actions or cases brought under GDPR or DPA 2018. She opined that she would expect more cases over the next year, though she did not expect the definition of personal data to change much given the slow evolution over the past ten years.

3.6. HMo said that it might be difficult and limited in value to precisely classify what amounts to 'direct' and 'indirect' identifiers. She explained that these were not new concepts, as they were embedded in the DPA 1998. In the DPA 1998, a 'direct' identifier meant one which can identify an individual from one data set, while an 'indirect' identifier represents data which must be combined with some additional information to effectively identify a person.

3.7. HMo explained that the DPA 2018 had been enacted because it was assumed the UK would have left the EU by 2019. The DPA 2018 has, as much as possible, stuck to the wording in GDPR for political reasons. The only additions in the definition of personal data are 'name', 'location data', 'online identifier' and 'genetic' because of new concepts and technology.

3.8. HMo advised that in section 3(3) of DPA 2018 direct identifiers are not restricted to the examples in section 3(3)(a), and further while section 3(3)(b) looks like an explanation of what can be an indirect identifier, neither of them is exclusive. HMo elaborated that a name would often be a direct identifier but is not always so, for example in the case of a very common name like 'John Smith' where the name

alone might not be enough to identify the person is. There is therefore no definitive classification of direct and indirect identifiers, and in many cases, it would depend on the circumstances.

3.9. On the additions to section 3(3) of DPA 2018, HMo explained that location data related to any technological data you might give off to a network from a smart phone/tablet/computer. Online identifiers mean IP address, cookies and device fingerprints. The majority of organisations impacted are online advertising businesses which use cookies to profile individuals for target advertising. Overall, HMo did not think the additions in the personal data definition would have an impact on the retail water market.

3.10. HMo advised that they understand that ICO is encouraging organisations not to look at direct and indirect data identifiers as separate categories, because under the law both are personal data and so it is best not to treat them as requiring different levels of protection which could be difficult to manage.

3.11. The Chair clarified that there was no intention amongst the Committee to encourage different treatment where direct and indirect data identifiers are concerned. The Chair added that the purpose of conducting a legal review was to understand the parameters of the personal data definition so that the Committee can assure itself that personal data has been properly identified and the solution in place is appropriate.

3.12. On the ICO's updated guidance regarding indirect identifiability, HMo explained that the principle is that indirect identifiability goes beyond an organisation combining information within its own system to identify a natural person. Not all eventualities can be captured but organisations have to give reasonable thought to what information might reasonably be known to or obtained by a third party in order to identify a person. HMo explained that this naturally raises concerns in many industries as to whether all information will be classed as "personal data"; she was inclined to suggest that the retail water market could try to assess information likely available for combination by third parties by ringfencing obvious inter-party interactions, such as when TPs access CMOS to enter or update information. In this regard, the Chair pointed out the additional TP to TP information flow, i.e. of data outside of CMOS). HMo considered these could also possibly be ring-fenced for assessment.

3.13. However, HMo continued that in the scenario of indirect identifiability, which required one to think about what information a third party may hold, or what information may a third party reasonably acquire to identify a person, this was unlikely to be a concern for the retail water market. This was because the routine types of data flows in this market are TPs data and ringfenced CMOS data. HMo therefore suggested that the Committee could consider this scenario as an exceptional circumstance.

3.14. A Committee member queried why certain data items such as the Unique Property Reference Number (UPRN) were not marked with a possible personal data flag in the legal advice circulated. It was noted that there was an updated legal advice which had flagged the UPRN data item and which should have been circulated by the Secretariat when it became available the day prior, as per the Chair's request. The Chair instructed the updated advice be circulated out to Committee members immediately in-meeting and confirmed the Committee would be reviewing the revised data items list in the updated advice in detail.

ACTION G13_A05

3.15. A Committee member raised concerns that where TPs were required to do work outside the market code, such as trace work for Gap sites, they had to combine data in CMOS with other sources to identify the property occupier. The Chair observed that it was open to the Committee to workshop examples of routine and extreme data flows to determine whether there was a case for raising Code change.

ACTION G13_A06

3.16. HMo continued that the ICO had taken the view that individual identification numbers such as passport numbers, National Insurance numbers, vehicle registration numbers are indirect identifiers, as this information has to be linked to another dataset to identify an individual. HMo noted that what might be a direct identifier to one person might not be direct to another under a different set of circumstances, for example you may know your neighbour's vehicle registration number by heart and not need to combine it with a database, making it direct in that instance. Therefore, even if one tried to categorise a data as direct or indirect identifier, exceptions can always be created.

3.17. HMo considered that the market data set fell into two main categories. The first category was direct data items that relate to individuals, such as account managers, individual contact details and work capacities. The other category, which is larger and more difficult to comprehend, were data items that relate to property, account details and financial background which belonged to sole traders, limited partnerships or micro companies which in turn could be linked to an individual. This would include meter reads which could be related to billing histories, and SPIDs which relate to property locations.

3.18. Therefore, HMo had taken a principled, cautious, approach to identifying whether a data item was an identifier in the retail water market. The first principle applied was "Does this data tell me anything about the property or the owner of the property?" Examples of data items that would meet these criteria were UPRN, Standard Industrial Classification Code, Rateable Value, Occupancy Status, Meter Coordinates, Meter Read Dates. The basis for this principle, was that a property could be related to an individual. As long as a picture and narrative could be built up from the data set - even if it had to be combined with other third-party data, and even if only 20% of data flows in the water market would result in this situation - HMo had taken the cautious approach of categorising such data as an identifiers. The rationale for the cautious approach was to help structure data protection in systems.

3.19. The other specific category HMo identified as personal data was any data item that allowed a free descriptor. The reason for this was it is often difficult to regulate what people may put into the free text field which could then result in identification of individuals. An obvious example of such data item would be meter locations. It was also noted that the ICO discouraged the use of free descriptor fields where possible.

3.20. The Chair commented that by design of the NHH retail water market, the majority of customers were not individuals. However, new customers come in and out of the market so at any given point in time, there could be ten or a thousand sole traders. The Committee had to be satisfied it had designed a solution that covered personal data, even if there were only a handful of individuals in the market. On one view, any data could be combined with a number of other data items to identify an individual, rendering the definition unfeasibly wide if followed through. The Chair queried if the case law or guidance indicated whether a line could be drawn, for example by a reasonableness or foreseeability test. HMo answered that to date the courts had not actively had to consider reasonableness. Most of her clients dealt with using a risk-based approach. This approach usually came down to a combination of

two tests. The first was the question of whether there was any intrinsic value in this data, both to a third party or the data subject themselves. Examples of intrinsic value in data could be health or financial information (such as payments, account details, disconnections) which could affect the financial standing of an individual, or very specific property data that may affect the security of the property. The second test was what was the combination of data sets that they would routinely use or send out again to assess what the total value of that data set could be.

3.21. The concept of the intrinsic value of the data in terms of what it reveals about the data subject chimes with sanctions in the legislation for breach which are related to the damage to the individual arising from breach. To this point, a Committee Member said that everything in CMOS could be linked back to the individual. But if one applied the test of intrinsic value, all customers in the NHH water market were commercial entities which had a natural inclination to advertise themselves to more people, so it was unlikely to cause damage if people found out about the locations of commercial entities. A Committee member highlighted that in their trace work to identify gap sites occupiers, they had the challenge of answering the occupiers' challenge that they had not consented to the collection of their contact details. To this, the Chair reminded the Committee that in its previous work consent had not been identified as the primary basis for data processing.

3.22. HMo suggested that one approach to designing the compliance solution would be for the Committee to conduct a workshop to work out the intrinsic value of the market data set and where the boundaries lie. The Committee could consider the high-level damages that could be caused by somebody misusing that data or a third party accessing the data unlawfully, and review whether there had been complaints about the use of data and identify where problems might arise. HMo further explained that regulatory intervention usually took place when there was a data breach or numerous civil complaints from a group of individuals.

3.23. HMo continued explaining that from a compliance perspective, it was good for the majority of information to sit as indirect identifiers. This was because if information was accidentally leaked, there would be less potential damage in that the individual would not be immediately and/or obviously identifiable. In fact, a lot of her clients were actively attempting to move data from the direct to the indirect identifier category to limit what people might be able to interpret. HMo noted that the vast majority of data in the retail water market is in the indirect identifier category, which was good news from the perspective of ensuring data security by data minimization. She cautioned that an ill-informed risk-based approach would be if the organisations did not understand the entirety of their data set and what data could be combined.

3.24. The Chair queried whether the fact an organisation had undergone a process of risk assessment and mitigation would help their standing in a breach situation. HMo replied affirmatively that it would show that the organisation had actively assessed their dataset and even if an error was made, the act of conducting the risk exercise would be good mitigation.

3.25. There was a discussion as to whether there is a material need to separately identify direct and indirect identifiers. In this regard, it was pointed out that what is fundamentally important is the ability to understand the definition and scope of personal data, regardless of whether it is direct or indirect. HMo noted that it is better to use a simple and broad-based approach in identifying what is personal data so that all organisations understood the necessary approach to and treatment of personal data.

3.26. HMo concluded that the definition of personal data had been evolving slowly and there was no real categorisation of direct and indirect identifiers, as much of that depended on the circumstances. Because of this vagueness, her clients had taken an informed risk-based approach for their data compliance solution, based on general interactions between parties, the intrinsic value of the data sets and where they thought the risks might lie. From what HMo saw in the market data set, she was of the view the regime set up covered the purpose and types of data held on CMOS, who was responsible for its accuracy and keeping it up to date, and regular reviews of making sure the data was retained for as long as it was necessary. Finally, HMo advised parties to keep a record of risks assessments and to keep a watching brief on how the personal data protection regime might change.

3.27. A Committee member raised a concern as to how to handle personal data if UK crashes out of the European Economic Area (EEA) was not covered. For example, should the privacy notice be updated with regard to the transfer of data to EEA. HMo noted that after Brexit, the UK would be considered a third country insofar as the EU was concerned under the GDPR. The UK would thus have to be recognised as having an equivalent legal regime before certain allowances would be made in relation to the free flow of information across borders, which is currently the case. However, the EU had not formally given its acceptance of UK's legal regime on personal data protection, not because UK's regime was fundamentally flawed, but because it had simply not come around to it yet. Furthermore, the ICO had said reasonably publicly that if that were to happen, they would take a very supportive and pragmatic view in relation to UK-based entities sending data to EU. The difficulty for organisations would then be if they had parties in EU sending data to UK as the EU regulators had not made clear their policy position.

3.28. The Chair queried whether the simple answer would be to continue to apply the existing laws in UK, and to wait for clarification from the relevant authorities. To this point, HMo noted clients who had tried to plan for Brexit scenarios had found their work to be wasted because firstly there was no certain timeline on Brexit and secondly, there were so many variables that even the government found it difficult to pin down. HMo opined that it would be unlikely for organisations to be brought to court during a period where the law is so uncertain. HMo also said that ICO had published its position that there would be no additional measures placed on companies for transferring data to the EEA, and that this would be circulated to the Committee for information.

ACTION G13_A07

3.29. In response to a Committee member's question on whether the MO or TPs needed to do anything to show that risks of personal data breach are low, HMo said that one mitigating factor ICO liked to see is organisations running exception reports or ad-hoc testing on databases or spot-checking to see if data is accurate. HMo advised that these reports should be documented.

3.30. Lastly, HMo suggested that interested organisations could register with ICO to get direct updates.

3.31. With no further questions around the table, the Chair thanked HMo for her presentation.

4. Approach to Review

4.1. The Chair reminded that the previous Committee had sought to ensure that the solution was fit for purpose whilst not being overly prescriptive, in response concerns expressed in relation to the previous

arrangements and the DMP. This led them to come up with the six guiding principles. Part of the review piece for the current Committee was to sense-check the guiding principles and ensure that the solution in place was still relevant.

4.2. The Committee members had no comments on the six principles or approach to review.

4.3. The Chair posed if it was sensible to use a risk-based approach to review the compliance solution, and whether determining the scale of personal data was necessary. HC pointed out that no Trading Party had come back to him on the scale of personal data in their database because they are not able to pull out that level of detail from their database easily or it is not held. The Chair said whilst sampling methods such as surveys could help estimate the scale of personal data, the question for the Committee was how much value this would achieve given that all data which was personal data was required to be protected. A Committee member observed that whilst the scale of personal data would help inform the size of risk, the reality was that the market-wide solution would still apply even if there were only a small number of sole traders or micro companies in the market dataset.

4.4. There was a discussion as to whether there should be an annual assurance piece for TPs, to facilitate whole-of-market compliance, or if TPs should be mandated to collect the number of NHH customers that were sole traders or non-corporates. It was noted that whilst it would be useful to know the number of sole trade and similar customers in the market, this had to be weighed against the costs and resource of doing so. It was also noted that even if TPs can work out the percentage of unique sole traders in their databases, this figure would constantly change due to change of retailer and companies both entering and leaving the market. Committee members also added that relying on the name of a business entity to identify whether it was a sole trader (or similar) might not be accurate, for example "Joe Trading" may or may not refer to a sole trader.

4.5. A further discussion ensued as to whether the ICO tended to take a broad stance and treat data about small limited companies as personal information, despite the legal person status. A Committee member explained that the ICO's response tended to vary depending on which case worker was handling it, and a junior case worker might take on an overly conservative approach whereas another more senior member would not.

4.6. The committee asked for the definition, if any, of 'natural person' in the legislation (likely to be in the definitions and interpretation section) to be checked. Of particular interest was whether there was an express exclusion for companies, ie 'legal persons' in the provisions. A list of the categories of entities which might be regarded as 'natural persons' within this market (such as sole traders, micro-companies, non-limited partnerships etc) was to be produced in light of the definition, if any. The Committee would then determine whether and, if so, how any guidance on this could be delivered.

ACTION G13_A08

5. Review of CSD 0301

5.1. HC presented on the data items in CSD 0301 n light of DLA's advice.

5.2. Members observed that there were differences between the data items listed in the DLA advice circulated on paper day and the data items listed in the slide presentation. The Chair 1) reiterated (as

noted under Section 3; Legal Review above) that data items listed in the DLA legal advice circulated on paper day had been revised in an updated legal advice from DLA in light of its further analysis with MOSL, and 2) explained that the revised list in the updated legal advice was fully reflected in the presentation slides, which also clearly identified the changes for the assistance of the Committee. The Chair again apologised on behalf of the Secretariat for the confusion caused by the updated advice not being circulated.

5.3. The Committee proceeded to review the data items in detail:

5.3.1. On the NO CHANGE category – ie those data items already flagged in the CSD as containing or potentially containing personal data – the Committee agreed that those flagged should remain flagged and none should be removed;

5.3.2. On the NEW category – ie data items which are not already flagged in the CSD as containing or potentially containing personal data, but which fell for further consideration following review – the Committee:

5.3.2.1. disagreed that 'Wholesaler ID (D4025)' and 'Other wholesaler ID (D4018)' should be flagged in the CSD because it did not consider there was a link between these two data items and the 'individual' for the purposes of data protection : these IDs revealed the wholesaler; wholesalers were large corporate entities in themselves; further, wholesalers supplied so many retail and individual businesses that the same wholesaler ID would come up in numerous cases and therefore would not lead to the identity of any particular individual(s).

5.3.2.2. agreed that the following data items contain or potentially contain personal data and should therefore be flagged in the CSD as such. This decision as these items could lead to the identification of an individual, and keeping in mind the previous risk-based approach:

- D2085 – Community Concession Charge
- D3016 – Datalogger (Non-Wholesaler)
- D3015 – Datalogger (Wholesaler)
- D6009 – Domestic Allowance
- D2015 – Occupancy Status
- D2011 – Rateable Value
- D4011 – Retailer ID
- D7601 – Section 154A Payment Value
- D4012 – Sewerage Retailer ID
- D4001 – Trading Party ID
- D4013 – Trading Party Name

5.4. The Chair noted that the data item "Total outstanding amount on account (D4020)" was included in the last GDPR Committee's recommendation to Panel and should have been flagged in the CSD accordingly but appeared not to have been. HC noted the request to check and ensure that D4020 was included.

5.5. In light of the discussions in the meeting, the Committee agreed that a Change Proposal would need to be raised to update the CSD to flag the following items:

- D2085 – Community Concession Charge

- D3016 – Datalogger (Non-Wholesaler)
- D3015 – Datalogger (Wholesaler)
- D6009 – Domestic Allowance
- D2015 – Occupancy Status
- D2011 – Rateable Value
- D4011 – Retailer ID
- D7601 – Section 154A Payment Value
- D4012 – Sewerage Retailer ID
- D4001 – Trading Party ID
- D4013 – Trading Party Name
- [and D4020 – Total outstanding amount on account, if not already included]

ACTION G13_A09

5.6. The Chair noted that as this change arose out of a legal review and update a consultation may not be necessary, but the Committee would have to take an overall view and make a decision once the review process was complete and it had a clearer idea on the 'suite' of changes.

5.7. Finally, considering HMo's advice that she would expect more legal developments over the next year, the Committee agreed that there should be a watching brief recommended to the Panel for a further review of the position 12 months from the last meeting of the Committee in this current round of work.

6. Any Other Business (AOB)

6.1. A Committee member advised that the GDPR section on MOSL's website mentioned that the summary of arrangements would be updated yearly prior to financial year commencement and that if MOSL has not fulfilled this obligation it could cause problems. RG replied that he would check on this.

ACTION G13_A10

6.2. The Committee member also asked if MOSL had shared data on meter reading with wholesalers that were not in line with the terms of its privacy policy. RG clarified that it was discussed at board level, but it did not get further. RG said that he would double check.

ACTION G13_A11

6.3. There was no further business and the Chair closed the meeting.

Actions:

G13_A01	Refine the consultation questions for Experience Review. To include whether a TP is able to work out the number of sole traders/partnerships etc. in their portfolio and to provide a number/percentage. A question should be added to see if they are aware of what a SAR is. To be done in consultation with the Chair.
G13_A02	Resend SharePoint link to Caroline, Helyn, Emma and David.

G13_A03	Explore an easy way for TPs to update MOSL their DPO contacts, potentially an email link on the MOSL website.
G13_A04	Secure a further contingency meeting date to give the Committee more time to consider any Change Proposals that may be required.
G13_A05	Circulate DLA's updated advice.
G13_A06	Committee to consider whether to workshop examples of routine and extreme data flows to determine whether there was a case for raising Code change.
G13_A07	Circulate a link to the ICO's guidance on Brexit.
G13_A08	Check the definition of 'natural person' in the legislation, in particular whether there is an express exclusion for companies/legal persons. A list of the categories of entities which might be regarded as 'natural persons' within the market (such as sole traders, micro-companies, non-limited partnerships etc) was to be produced in light of the definition, if any. The Committee would then determine whether and, if so, how any guidance on this could be delivered.
G13_A09	Raise Change Proposal to update CSD 0301.
G13_A10	Review/Update the MOSL website summary of arrangements.
G13_A11	To check if MOSL had shared any data with other wholesalers that were not in line with the terms of its privacy policy.