MOSL
MARKET OPERATOR SERVICES LTD

Data Protection Impact Assessment—DPIA—Bilaterals

C1 Process - Verification of Meter Details

Version History

Version Number	Date of Issue	Reason for Change	Sections Affected
V2.0	23 December 2020	Reviewing internal feedback and making any relevant changes to the document	Section 2 – page 4 Appendix B
V3.0	05 January 2021	Version for sign-off	
V4.0	25 January 2021	Final amendments before sign off	Section 2, page 3 Appendix A
V5.0	1 March 2021	Addition of C1.W process flow	Section 2 – page 4
V6.0	16 March 2021	Addition of actions under DPO sign-off	Section 7.2

1 Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves
The Bilaterals programme will create a new Bilaterals Hub to allow Retailers and Wholesalers to raise Service Requests with each other, bilaterally. It will provide a common interface for these bilateral transactions and will link to the data in CMOS. The pilot, which this DPIA addresses, will be for a single process, C1, which is to create a new service request for meter verification and supply arrangement checks. This will be raised by either the retailer or wholesaler and submitted to the Bilaterals Hub. The wholesaler will be able to access the Bilaterals Hub and view the service requests raised against it and respond, including arranging a site visit.

2 Describe the processing

Describe the nature of the processing
The Bilaterals Hub ("Hub") is expected to store data on non-household ("NHH") customers, with Wholesalers and Retailers able to use the Hub to check progress on Service Requests or site visits, when these are arranged. Users require individual accounts to log into the hub, which will be configured in MOSL's Azure Active Directory ("AD") instance. Trading Parties will have the option to federate with their own Active Directory instance. In order to do this, business users will need to provide their name and contact details to register on to the Hub. The data is therefore collected when the retailers complete the fields provided on the Hub and records that they have informed the customer that they may be contacted by the wholesaler. The collected data is then stored on the Bilaterals Hub. The customer data is not expected to be shared with anyone other than the wholesaler (and future retailers, should the customer switch). NHH customers will usually be companies, rather than natural persons, but in some instances, they will be sole traders or unincorporated partnerships, and their name, and contact details will constitute personal data. In addition, as the customer contact details are likely to be an individual and their contact number, this will often be personal data. In the event where premises switch retailers, the onus rests with the outgoing/incoming retailer to inform the customer that their personal data shall be shared with the new retailer. There should be no doubt with the customer as to who will have visibility of its data. The Code is currently silent on this specific point but caters for this within the generality of data protection obligations i.e. privacy notices. Given the greater level of personal data, the Bilaterals Code should clarify the requirement to have informed the customer contact via an appropriate privacy notice/declaration. Other parties will be able to comment on Service Requests and be able to see customer personal data too, for example, where SPIDs are jointly owned and Other Wholesalers or Other Retailers will see this data. As these other parties do not need to see this data, as they will not be dealing with the customer directly, it is recommended that this information is

redacted (automatically by the Bilaterals system) so that other parties are not able to access it so that the risk associated with this is therefore managed and reduced.

The security authentication for the Bilaterals Hub includes Trading Parties providing a client certificate and IP whitelist as per CMOS. Trading Parties will be responsible for providing organisational certificates. The proposed approach for the Bilaterals Hub is to use the CMOS certificates. User authentication will be against Azure AD and user roles will be mapped to privileges within the Bilaterals Hub.

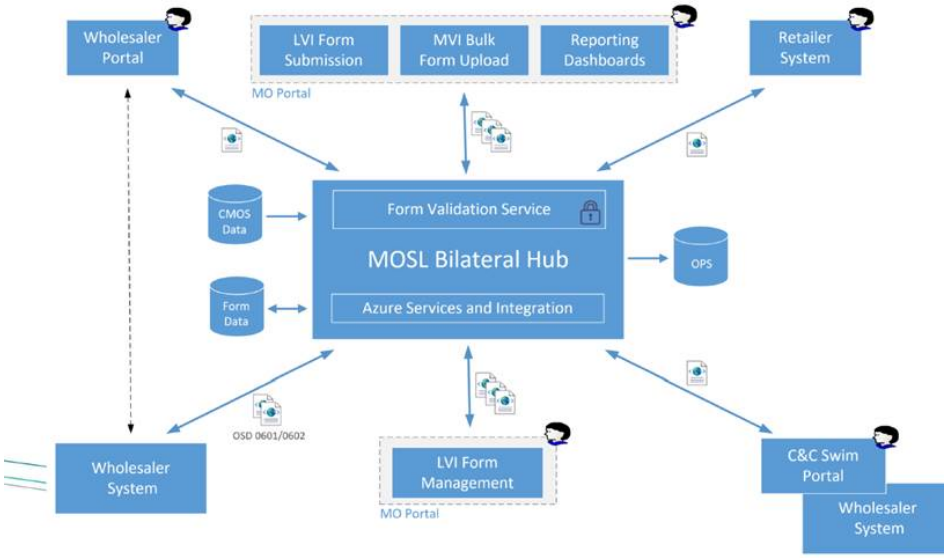
The source of the data will be fields derived from CMOS along with fields entered by the wholesaler and retailers, either through the portal, forms, or integrated systems.

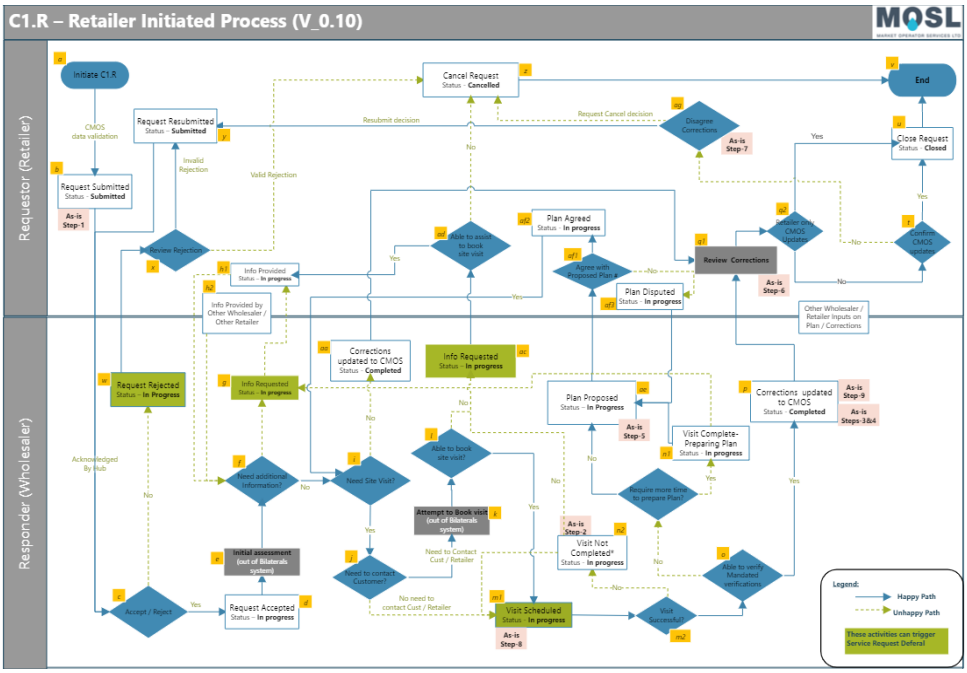
Given the additional data fields proposed by the Bilaterals programme which will record contact details for customers, the risk of personal data being processed is increased. The Appendix to this DPIA contains a list of data fields proposed for the Bilaterals programme. The proposed data field 'D8238' states that it will store additional customer information, however it is not specified what this data could be (as it is a free text field). If further personal data is entered in this field, then it may raise the level of risk further. This will typically be information about contact availability and site restrictions. Therefore, there is a high possibility of personal data being entered into these additional comment fields, with a low possibility of this data also being special category data (e.g. data relating to a customer's health). In the event that special category data is entered into these fields, then extra measures need to be in place to protect that data and ensure it is deleted as early as possible once it is no longer required i.e. retention periods may need to be shorter if there is special category data recorded.

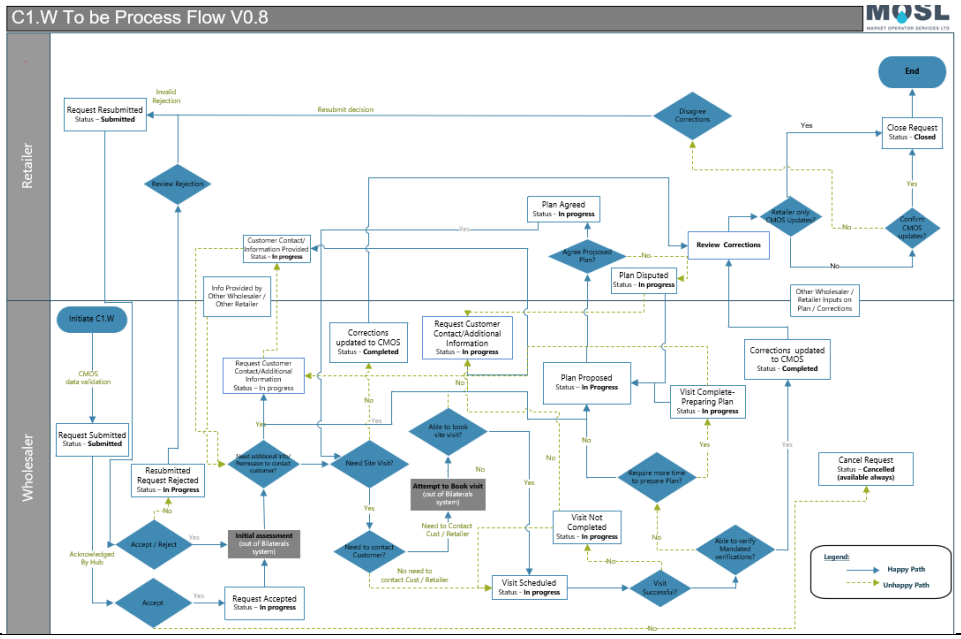
When a customer switches retailer, then it remains an active customer on the Bilaterals Hub. However, once a customer becomes inactive, for whatever reason, then steps must be taken to ensure that that customer's personal data is deleted in line with the suggested retention periods. So, for example, if a premise was a public house, which was later sold to a new owner, remaining as a public house, then the retention period will have already commenced from the point the customer contact information was originally input into the Hub. This will need to be confirmed as an appropriate business requirement.

The data is expected to be shared with retailers and wholesalers (where appropriate) and Other retailers and Other wholesalers where there are jointly owned SPIDs. The data will also be shared with the new retailer when a customer switches retailer. However, the Bilaterals Hub will also have oversight from Ofwat, and development has been outsourced primarily to CGI.

Bilaterals High-level Solution Design







Describe the scope of the processing:

The nature of the personal data proposed to be stored on the Hub includes; Customer name and contact details including address, preferred method of contact, Landlord Tenant details and Retailer contact name and contact details. Some of these data fields are new personal data that does not already exist in CMOS at present. Most data transactions look to include personal data in them. There is currently no special category data that is expected to be processed. However, if there is a need to record health data for a customer i.e. if there are any health reasons which need to be considered for continued water supply for that customer, then would be special category data. Currently, the Hub has free text fields which do not restrict what data is entered. There is a potential for special category data, such as health data, to be entered into these fields. One precaution should be that for all users, when signing up, a declaration is displayed relating to data protection.

Therefore, the sensitivity of the proposed data fields is low as there is no financial, health and ethnicity data or other special category data expected to be used.

The data will be collected during the course of all transactions, so on an ongoing basis.

With regards to the retention periods for the personal data, these will need to be clearly defined in the Bilaterals CSDs. The retention periods for data contained in CMOS are outlined in CSD400; 7 years for all transactions, authorisations and associated logs, and 2 years for interface logs which have no relationship to settlement and the 7-year requirements.

Given that the Hub will hold more direct personal data, a shorter retention period is advisable for customer contact data. This will be dependent on the business needs, but one suggestion is that this data is retained for one year since the closure of the service request, with the retention period being reviewed at the end of each year. The rationale for this is that we could expect within that time for all service requests and site visits to have taken

place. There should also be an obligation on TP's to review their user logins, and remove inactive accounts, after 1 week, as per CMOS obligations.
Describe the context of the processing
The parties that will use the Bilaterals hub are retailers and wholesalers, plus MOSL as administrator/owner. The nature of the relationship between these parties is therefore to use the Bilaterals Hub as a central system to communicate and work together to resolve any service requests raised and to organise any necessary site visits. The retailer will own much of the personal data provided by the customer e.g. its name and contact details, as the retailer owns the customer relationship. The retailer may only share a customer's contact details with a wholesaler if the customer has been made aware that their contact information is required to be shared with the wholesaler (and potentially other service providers). This will need to be backed by a Privacy Notice from the retailer, which will be made explicit on the Codes. In addition, a system declaration will be displayed to the user which, by proceeding, will be confirmation that they have explained to the data subject of the need to share their personal data, as required. A customer will therefore not be kept in any doubt as to how its data will be used. There are no specific concerns or security flaws with the data being processed in the way intended by the Bilaterals Hub. The Hub will be hosted on Azure and will benefit from federated AD authentication and encryption in transit and at rest. There are no concerns for children as there should be no records of individuals, other than customer's, and contact points for premises, wholesaler or retailers, in the Bilaterals portal. CMOS contains a flag for premises with specific water needs, although this is understood not to be integral to the Hub processes and will not be amended by this programme. It is not believed there are any issues of public concern to factor in. The Bilaterals programme will be governed by the Market Arrangements Code and the Wholesale Retail Code, including the CSDs.
Describe the purposes of the processing
The Bilaterals programme seeks to achieve a central system allowing retailers and wholesalers to use the same system to manage service requests. What MOSL would like to achieve is make the process of communication between the customer, retailer and wholesaler much more efficient. There may be potential benefits for customers in that the Bilaterals Hub aims to facilitate more efficient services from both retailer and wholesaler, and so, potentially deliver corresponding cost savings for Trading Parties ("TPs") that may be passed onto customers. As a result of the improved performance monitoring, there may also be improved customer outcomes. Customers may also benefit from more accurate billing; however, this is all dependent on each individual TP and its use of the Bilaterals Hub. The benefits for TPs may include a reduced number of contacts between the wholesaler and

retailer. It is estimated that there may be reduced number of aborted site visits, rejected requests and overall planning time. Overall, it is expected that there will also be improved efficiency for Bilateral transactions.

The benefits for MOSL are expected to be that there is reduced time and effort requirement to produce Operational Performance Standards ("OPS") reporting. It will primarily enable a move to central OPS reporting by MOSL as opposed to the current self-reporting process by TPs, reducing the reporting burden from TPs too. MOSL can drive market improvement through identifying pain points in the process. There is also expected to be improved reporting for bilateral transactions which allows for a more in-depth wholesale/retailer comparison by area.

The Bilaterals programme in general should therefore make the process of raising Service Requests more efficient for all users.

3 Consultation process

Consider how to consult with relevant stakeholders:
Given the relatively limited extent of personal data that is expected to be processed by the Bilaterals Hub, where the majority of customers will not be natural persons, and where the personal data will primarily be basic contact details for customer owners and employees, it is unlikely that MOSL should require consultation from information security experts or NHH customers. A thorough programme is in place and several members of MOSL (TP's) are involved in developing the framework for this Hub. There are a number of consultation groups supporting the programme, from across the industry. MOSL's legal team has been engaged to assess the risks associated with the personal data that is expected to be processed by the portal. Trading Parties are already closely involved in the development of the Hub, and the MOSL legal team will engage with Trading Party DPO's, as necessary, with regard to the access to the Hub, updated privacy notices, and customer's understanding of the privacy notice to be contacted. The Pathfinder Group (formed of TP's) will also be consulted on the specific conclusions of this DPIA.

4 Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:
The lawful basis for processing the data includes legitimate interests (provision of water and sewerage services) and operation of the market; performance of a contract (between retailer and NHH customer, and wholesaler and retailer) and to comply with a relevant legal or regulatory obligations (Ofwat, Defra, ICO). NHH customers whose data will be recorded on the Hub shall be made aware of how their data will be processed and the fact that it shall only be shared with the wholesaler as required and where their understanding

of this has been obtained. This will be through the retailer's privacy notice and made explicit.

By processing the data, retailers and wholesalers will be able to meet the objectives of the Bilaterals programme which is to allow retailers and wholesalers to raise Service Requests with each other bilaterally. Currently, CMOS does not allow this function which is why the Bilaterals programme has been developed. Having a centralised solution will provide a clear standard for the bilateral data transfer and reduce the use of bespoke solutions, and so should reduce the risk of data loss.

With regard to data quality and data minimisation, having conducted a review of the proposed data fields for C1 process, it appears that only data relevant to the purpose of the Bilaterals hub is collated from customers and retailers. There is a data field named 'D8238' which asks for Customer Additional Information will be a free text field but is intended to record customer contact details such as time of availability of access restrictions. Personal data may be entered into that field. If further personal data is entered, or if any attachments are uploaded containing personal data then it must be made clear to the system user that MOSL takes no liability for any extra confidential/sensitive data that is entered in this field or any other 'free text' field. This will be catered for in the system declaration visible to users. The Trading Party obligations will be set out in the Codes, and so this will also be a contractual requirement on the Trading Parties and will be subject to the market audit regime.

Data retention periods will need to be clearly stated in the Code, in order to ensure data minimisation and that data is not kept for any longer than necessary. This will include not only data that is entered into data fields, but also any personal data that may be provided in attachments.

MOSL will need to ensure that it reviews the DPIA each time the Bilaterals programme introduces a new process, as this will introduce new data types. It will be important to assess the risk of any new personal data at each stage of the process. Reviewing its practices may also involve updating privacy notices, confirming that data security is in place, testing and checking if we need to update any data sharing agreements or the MAC or Market Privacy Notice/system declarations.

To ensure processors comply with the data protection measures, they will be aware of their obligations under the Code, towards confidentiality and security of personal data, and their duties in this regard. Additionally, MOSL will, where there is possibility that special category data/extra personal data may be provided in free texts fields, with the Codes and system declarations require that such information is deleted as soon as its purpose is fulfilled by the Trading Parties. Retention periods will also be highlighted to TPs so that processors are aware that they have obligations to delete the personal data within specific timescales.

There will not be any international transfers involved, provided the assumption that the Hub is hosted in the UK, although the Trading Party systems will likely also host the data,

but will be outside of the scope of this DPIA. If international transfers become required then the appropriate additional legal safeguards (such as standard contractual terms) will be implemented with the relevant suppliers, alongside updates to privacy notices.

5 Identify and assess risks (See Annexe B below for explanation of the risk scores)

Describe source of risk and nature of potential impact on individuals	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Risk of customer's data being shared with wholesalers without their understanding/consent	☐ Remote ■ Possible ☐ Probable	■ Minimal ☐ Significant ☐ Severe	☐ Low ■ Medium ☐ High
Risk of retaining personal data beyond retention period – could result in complaints from data subjects that personal data is held unnecessarily long and so at risk of loss of privacy	☐ Remote ■ Possible ☐ Probable	■ Minimal ☐ Significant ☐ Severe	■ Low ☐ Medium ☐ High
Risk of receiving extra personal data in free text fields or attachments, which may be sensitive or not relevant to purpose	☐Remote ■ Possible ☐ Probable	■ Minimal ☐ Significant ☐ Severe	■ Low ☐ Medium ☐ High
Risk of personal data being compromised through cyber-attack on the Hub	☐ Remote ■ Possible ☐ Probable	☐ Minimal ■ Significant ☐ Severe	☐ Low ■ Medium ☐ High
Risk of NHH customers not being made aware of the use of their data	☐ Remote ■ Possible ☐ Probable	☐ Minimal ■ Significant ☐ Severe	☐ Low ■ Medium ☐ High

6 Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium- or high-risk in section 5.

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Retention	Ensure retention periods are clearly set out in CSDs and retailers are aware of this and include in their privacy notices and MOSL makes regular checks and data cleanses. Bilaterals Hub should delete the personal data once a customer leaves the market, following an appropriate retention period.	☐ Eliminated ■ Reduced ☐ Accepted	■ Low ☐ Medium ☐ High	■ Yes ☐ No
Consent	Codify the requirements that customer contact understands and accepts the privacy notice/declaration and monitor, including via market audit	☐ Eliminated ■ Reduced ☐ Accepted	■ Low ☐ Medium ☐ High	☐ Yes ☐ No
Additional Personal Data	Codify the requirements and provide guidance for TP's, coupled with monitoring, including via market audit	☐ Eliminated ■ Reduced ☐ Accepted	■ Low ☐ Medium ☐ High	■ Yes ☐ No
Cyber-attack	Technical security mechanism, including authentication of users, encryption of data in transit and at rest, and perimeter security of the Hub, such as firewalls	☐ Eliminated ■ Reduced ☐ Accepted	■ Low ☐ Medium ☐ High	☐ Yes ☐ No

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Customer awareness	Codify requirements of TPs. Monitor compliance and privacy statements.	☐ Eliminated ■ Reduced ☐ Accepted	■ Low ☐ Medium ☐ High	■ Yes ☐ No

7 Sign off and record outcomes

7.1 Sign off

Item	Name/date	Notes
Measures approved by	Andrew Johnson David Garner Ricardo Wissmann-Alves John Gilbert	Integrate actions back into project plan, with date and responsibility for completion
Residual risk approved by	Andrew Johnson David Garner Ricardo Wissmann-Alves John Gilbert	Residual risks are not deemed high or unacceptable, but this DPIA will remain under review as the programme advances

7.2 DPO advice

DPO advice provided on compliance, section 6 measures and whether processing can proceed	■ Yes ☐ No

Name of DPO	Andrew Johnson
Date of advice	16 March 2021
Summary of DPO advice	This initial phase of the Bilaterals Hub introduces additional personal to that held in CMOS, as well as a new architecture, database and integration with Trading Parties. The extent of the personal data remains limited and is not expected to include sensitive personal data. The actions below outline the key recommendations from the DPIA, which will be taken forward by the programme team, including for the changes to the Codes, the development of the solution, and the Trading Party guidance, training and assurance process. These actions will be revised as the programme completes additional phases.
Comments	1. User access will be by individual accounts, configured using AD, with option to federate. The Codes will need to stipulate responsibility on Trading Parties to manage the accounts and, in line with CMOS, remove inactive accounts after 1 week; 2. Further security will include data encryption, (including at rest) and Hub access controlled by client certificate and IP whitelist; 3. The Hub will include a declaration* to retailers that they have informed the customers that their personal data will be shared with the wholesalers for contact purposes. This will also be a Code obligation for inclusion in TP's Privacy Notices; 4. The Hub will redact customer personal data from the 'Other Wholesalers/Retailers'; 5. Data retention needs to be considered and a retention period agreed and then implemented. It has been proposed that this is linked to when a customer becomes 'inactive' and that data is deleted one year after this point; and 6. The Bilaterals assurance for TP's will include GDPR compliance, and this will be included in ongoing assurance work by MOSL and the Market Auditors, following a risk based approach; *Suggested wording - You have made your customer aware that this information may be shared with other Trading Party organisations as necessary during the completion of this request,

	which allows such Trading Parties to contact your customer while they process this service request.

7.3 Consultation

Consultation responses reviewed by	The DPIA will be kept under review and published on the MOSL website for any feedback.
Reasons for departing from individuals' views (if applicable)	N/A
Comments	

7.4 Ongoing review

This DPIA will be kept under review by	Andrew Johnson, MOSL DPO *The DPO will review ongoing compliance with DPIA as the Bilaterals project proceeds*

Appendix A - Bilaterals GDPR – CSD0601 Transactions Data Fields

Data item no.	Data Item name	Data owner	Data Origin
D2050	Customer Banner Name	Retailer	Autopopulated from CMOS
D2027	Customer Name	Retailer	Autopopulated from CMOS
D8020	Customer Contact Name	Retailer	Populated by Retailer in the HUB
D8021	Customer Contact Number 1	Retailer	Populated by Retailer in the HUB
D8233	Customer Extension 1	Retailer	Populated by Retailer in the HUB
D8239	Customer Contact Name 2	Retailer	Populated by Retailer in the HUB
D8145	Customer Contact Number 2	Retailer	Populated by Retailer in the HUB
D8234	Customer Extension 2	Retailer	Populated by Retailer in the HUB
D8146	Customer Contact Email	Retailer	Populated by Retailer in the HUB
D8235	Customer Aware of Service Request	Retailer	Populated by Retailer in the HUB
D8236	Customer Preferred Method of Contact	Retailer	Populated by Retailer in the HUB
D8237	Customer Preferred Contact Time	Retailer	Populated by Retailer in the HUB
D8238	Customer Additional Information	Retailer	Populated by Retailer in the HUB
D8240	Landlord Tenant Details	Retailer	Populated by Retailer in the HUB
D8019	Consent to Contact Customer	Retailer	Populated by Retailer in the HUB
D8252	Customer Contact Required	Retailer	Populated by Retailer in the HUB
D2005	Customer Classification - Sensitive Customer	Retailer	Autopopulated from CMOS
D4011	Retailer ID	Retailer	Autopopulated from CMOS
D8269	Retailer Contact Name	Retailer	Populated by Retailer in the HUB
D8270	Retailer Contact Number 1	Retailer	Populated by Retailer in the HUB
D8271	Retailer Extension 1	Retailer	Populated by Retailer in the HUB
D8272	Retailer Contact Number 2	Retailer	Populated by Retailer in the HUB
D8273	Retailer Extension 2	Retailer	Populated by Retailer in the HUB
D8274	Retailer Contact Email	Retailer	Populated by Retailer in the HUB

Appendix B – Risk scores explained

Likelihood of harm	
Remote	Only expected to occur in exceptional circumstances and not expected to happen within the next year in normal circumstances.
Possible	May happen within the next year in normal circumstances.
Probable	More likely than not to happen within the next year in normal circumstances.
Severity of harm	
Minimal	Impact is minimal or negligible. Minor problem, easily handled by normal day to day processes, within the MOSL team. E.g. minor data breach reported to the DPO (but with no loss/harm to data subjects and no sanction) or minor system error. Value of interruption/rectification does not exceed £1000.
Significant	Impacts on day-to-day operations of a significant part of the overall business. Significant time and resources required. E.g. A major data breach incident may lead to sanctions being issued by the ICO and reputational damage. Value of interruption/rectification exceeds £1000 but does not exceed £10,000.
Severe	Impact is severe with operations severely damaged. E.g. Bilateral system breakdown and personal data compromised, significant sanctions issued by ICO, severe actions taken by Ofwat and considerable reputational damage. Value of interruption/ rectification exceeds £10,000.
Overall risk	
Low	We believe that the overall risk of any harm occurring is very unlikely. Only expected to occur in exceptional circumstances.
Medium	We believe that there is a possible risk of this incident occurring. May happen within the next year in normal circumstances.
High	More likely than not to happen within the next year in normal circumstances.
Effect on risk	
Eliminated	There is no longer any threat of this risk.
Reduced	The risk is present albeit this is reduced by the method suggested.

Accepted	It is accepted that this risk is present.
Residual risk	
Low	Only expected to occur in exceptional circumstances
Medium	May happen within the next year in normal circumstances.
High	More likely than not to happen within the next year in normal circumstances.