This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

Paper Reference:	**SECP_78_1303_21**
Action:	**For Decision**

DP113 progression

1. Purpose

Draft Proposal DP113 'Unintended Data Disclosure when using SR8.2' is ready to be converted to a Modification Proposal. We are recommending that this modification be progressed to the Refinement Process. This paper sets out our proposed approach for progressing this modification for the Panel's approval.

The draft Modification Report setting out the detail of the modification can be found in Appendix A.

2. Summary of the issue

This proposal was raised by Ian Speller from the Data Communications Company (DCC).

DCC Service Users routinely query the DCC System to discover or validate various customer, property or meter data as part of their business processes. Queries can be generated using various identifiers, including the Meter Point Administration/Reference Number (MPxN), address and postcode, which are all treated as personal data under the General Data Protection Regulation (GDPR).

A behaviour of the current design of the DCC System has been discovered to cause a potential breach in GDPR. If a DCC Service User submits a query to the DCC Systems with a house name/number and postcode, but without a unique reference, the results may return data of an unintended property at a matching postcode.

The Proposer believes that the risk with the current arrangements is that the DCC could return data that could include unintended personal data, which would be a breach of GDPR and the System should be changed to prevent this.

3. Proposed progression

We believe that this modification should be progressed to the Refinement Process to allow for the development and assessment of a solution to the agreed issue. The proposed solution will likely impact Service Requests and consequently the DCC User Interface Specification (DUIS). This would require a DCC Preliminary Assessment.

Work package and timetable

Firstly, we will work with the DCC to develop the business requirements for a strawman solution. These will be reviewed by the Security Sub-Committee (SSC) and once agreed, will be sent for a DCC Preliminary Assessment.

Activity	Date
Prepare business requirements with the DCC	16 Mar 20 – 27 Mar 20
Discuss business requirements with the SSC	22 Apr 20
Request Preliminary Assessment	May 20
Update Panel	Jun 20

Areas of assessment

We do not believe there are any further questions that need to be considered in addition to the standard assessment areas.

4. Recommendations

The Panel is requested to:

- **AGREE** that DP113 should be converted to a Modification Proposal;
- **AGREE** that MP113 should be progressed to the Refinement Process; and
- **AGREE** the first package of work and the timetable as set out in this paper.

Joe Hehir

SECAS Team

6 March 2020

Attachments:

- **Appendix A:** DP113 draft Modification Report

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

DP113

‘Unintended Data Disclosure when using SR8.2’

Modification Report

Version 0.3

About this document

This document is a draft Modification Report. It currently sets out the background, issue, and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

1. Summary 3
2. Issue 4
3. Assessment of the proposal 5

Appendix 1: Progression timetable 6

Appendix 2: Glossary 7

Contact

If you have any questions on this modification, please contact:

Joe Hehir

020 7770 6874

joe.hehir@gemserv.com

1. Summary

This proposal was raised by Ian Speller from the Data Communications Company (DCC).

DCC Service Users routinely query the DCC System to discover or validate various customer, property or meter data as part of their business processes. Queries can be generated using various identifiers, including the Meter Point Administration/Reference Number (MPxN), address and postcode, which are all treated as personal data under the General Data Protection Regulation (GDPR).

A behaviour of the current design of the DCC System has been discovered to cause a potential breach in GDPR. If a DCC Service User submits a query to the DCC Systems with a house name/number and postcode, but without a unique reference, the results may return data of an unintended property at a matching postcode.

The Proposer believes that the risk with the current arrangements is that the DCC could return data that could include unintended personal data, which would be a breach of GDPR, and the System should be changed to prevent this.

The Change Sub-Committee (CSC) has agreed that the issue is clear and this Draft Proposal should be converted to a Modification Proposal and proceed to the Refinement Process.

2. Issue

What are the current arrangements?

DCC Service Users routinely query the DCC System to discover or validate various customer, property or meter data as part of their business processes using Service Request (SR) 8.2 'Read Inventory'. Queries can be generated using various identifiers, including the MPxN, address and postcode, which are all treated as personal data under GDPR.

The SEC defines the rules and parameters for use of the query functionality by DCC Users. Suppliers commonly use the query functionality in order to discover the data related to the MPxN including Devices, following a consumer Change of Supplier (CoS) request.

What is the issue?

Investigation into a complaint raised by a Supplier (via a severity Category 1 Incident) has highlighted a known and as-designed behaviour of the DCC System. It is possible for a DCC Service User to submit a query to the DCC System with a house name and postcode, but without a unique reference (e.g. MPxN). This may in certain circumstances return the details of an unintended property at the same postcode.

The Service Request (SR) is detailed in SEC Appendix AD 'DCC User Interface Specification' (DUIS). To allow compliance with SEC Section L 'Smart Metering Key Infrastructure and DCC Key Infrastructure', an amendment to the DUIS is required. This would facilitate additional commands and parameters in the DCC System to allow safe queries to be applied when submitted without MPxN or Device specific details.

What is the impact this is having?

The Proposer believes that the risk with the current arrangements is that the DCC could return data that could include unintended personal data. This is a breach of GDPR, and the SEC Panel and the Security Sub-Committee (SSC) have agreed that this needs to be addressed.

The Proposer believes a change to the current arrangements is required. This should provide a method by which these queries can be carried out, but only return the necessary data and avoid any exposure of Personal Data as defined by GDPR. DCC Users should be able to send these queries without using a unique reference relating to equipment on site i.e. an MPxN or Globally Unique Identifier (GUID).

3. Assessment of the proposal

Observations on the issue

Change Sub-Committee

The CSC unanimously agreed that the issue has been clearly defined and understood. It recommended that the Panel should covert this Draft Proposal into a Modification Proposal and that it should enter the Refinement Process.

One member recommended that once in refinement, the solution could be based on other Application Programming Interface (API) solutions such as the Electricity Central Online Enquiry Service (ECOES). This would be in the context of how these APIs ensure searches do not breach GDPR.

SMKI PMA

The Smart Metering Key Infrastructure (SMKI) Policy Management Authority (PMA) advised that it did not need to be kept updated with the progress of this proposal. However, a member noted that it believed it would not be a GDPR breach if a DCC User discarded any data it should not have received, including as a result from using SR8.2. It advised that a User would be in breach of GDPR if it stored or used the erroneously received data.

SSC

The SSC agreed with the issue outlined in this proposal and advised that it was already aware due to the Supplier raised incident mentioned in this document.

Appendix 1: Progression timetable

On 13 March 2020, the Panel will consider the CSC's recommendation to convert this Draft Proposal into a Modification Proposal and for it to proceed to the Refinement Process.

Timetable	
Action	**Date**
CSC recommendation that Panel convert into a Modification Proposal	25 Feb 20
Panel consider the CSC's recommendation	13 Mar 20
Prepare business requirements with the DCC	16 Mar – 27 Mar 20
Discuss business requirements with the SSC	22 Apr 20
Request Preliminary Assessment	May 20
Update Panel	Jun 20

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	**Full term**
API	Application Programming Interface
CoS	Change of Supplier
DCC	Data Communications Company
DUIS	DCC User Interface Specification
ECOES	Electricity Central Online Enquiry Service
GDPR	General Data Protection Regulation
GUID	Globally Unique Identifier
MPAN	Meter Point Administration Number
MPRN	Meter Point Reference Number
PMA	Policy Management Authority
SMKI	Smart Metering Key Infrastructure
SSC	Security Sub-Committee