

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.



DP283 'Data Breach Reporting'

Modification Report

Version 0.1

11 February 2025



About this document

This document is a Modification Report. It sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions.

Contents

1.	Summary	3
2.	Issue	3
3.	Solution	4
4.	Impacts	4
5.	Costs	5
6.	Implementation approach.....	6
7.	Assessment of the proposal	6
8.	Case for change	7
	Appendix 1: Progression timetable	9
	Appendix 2: Glossary	9

This document also has one annex:

- **Annex A** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.

Contact

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

Georgiana Severin

020 7770 6921

Georgiana.Severin@gemserv.com

1. Summary

This proposal has been raised by Sharon Armitage from E.ON. The Proposer is also a member of the Privacy Sub-Committee (PSC).

The PSC currently has no visibility of Data breaches which may occur and there is no SEC obligation on Data Communications Company (DCC) Other Users to report Data breaches to the PSC. DCC Users – such as Suppliers, Network Parties and Registered Supplier Agents – will have appropriate permission from the consumer to access Data. DCC Other Users must obtain Unambiguous Consent from the consumer in order to access the same Data. As the reporting of a Data breach is not currently a SEC obligation it is not covered within the scope of the annual Privacy Assessment and cannot be considered in relation to a DCC Other User's compliance with SEC Section I 'Data Privacy'.

Data loss or compromise has a negative impact on consumers (both where their personal Data is involved or not) and can lead to reduced confidence in Smart Metering and the governance in place to protect consumers and their personal Data.

The Proposed Solution would therefore include changes to SEC Section I 'Data Privacy' for DCC Other Users to report Data breaches to the PSC. The Privacy Controls Framework (PCF) will outline the process for Data breach reporting. The modification costs would be limited to Smart Energy Code Administrator and Secretariat (SECAS) time and effort. This is a Self-Governance Modification and, if approved, is targeting implementation as part of the June 2025 SEC Release.

2. Issue

What are the current arrangements?

SEC Section I 'Data Privacy' sets out requirements for SEC Parties to comply with in relation to Data and Data protection. This includes requirements on DCC Other Users relating to accessing and protecting consumer data.

The PSC is tasked with ensuring that Data Privacy is protected across the Smart Metering System by all SEC Parties that have access to consumer data. It does this by carrying out an annual Privacy Assessment. The annual Privacy Assessment will identify patterns and issues that may require mitigating against.

The PCF is a document developed and maintained by the SEC Panel by which requirements are set out in relation to the Privacy Assessment. This is so that reasonable assurance is provided that DCC Other Users are complying and capable of complying with the Data Privacy obligations set out in Section I1.2 to I1.5.

What is the issue?

At present, when a Data loss or compromise takes place, there are no SEC Obligations that would require DCC Other Users to notify the PSC of any Data breach. DCC Other Users have an obligation to report any breaches to the Information Commissioner's Office (ICO) in accordance with General Data Protection Regulation (GDPR) and the 2018 Data Protection Act.

Without obligations in the SEC that would require DCC Other Users to report the Data breach to the PSC as well as the ICO, the PSC is unable to include this information in the annual Privacy

Assessment. This also means that it cannot be considered in relation to a DCC Other User's compliance with Section I 'Data Privacy'.

What is the impact this is having?

As Data loss or compromise is not currently included as part of the SEC Obligations and therefore not assessed as part of the annual Privacy Assessment, there is a risk that the PSC will not have full visibility of the DCC Other User's compliance with SEC Section I 'Data Privacy'.

Impact on consumers

Data loss or compromise has a negative impact on consumers and can lead to reduced confidence in Smart Metering and the governance in place to protect Data.

3. Solution

Proposed Solution

The Proposed Solution will include requirements for DCC Other Users to report Data breaches to the PSC. The changes in the legal text align with the reporting of Material Security Vulnerabilities by Users included in Section G 'Security' and the Security Controls Framework document.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
	Large Suppliers		Small Suppliers
	Electricity Network Operators		Gas Network Operators
✓	Other SEC Parties		DCC

Breakdown of Other SEC Party types impacted			
	Shared Resource Providers		Meter Installers
	Device Manufacturers		Flexibility Providers
✓	DCC Other Users		MAPs/ MAMs

DCC Other Users would be impacted by this modification as the obligations will require them to report on Data breaches. However, as this is already a requirement under GDPR, it is presumed that the information to report will be similar if not identical to what is reported to the ICO.

DCC Systems

DCC System changes

This modification will not require DCC System changes.

DCC System traffic

This modification will not impact DCC System traffic.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section I 'Data Privacy'
- 'Privacy Controls Framework' document

The changes to the SEC required to deliver the Proposed Solution can be found in Annex A.

Devices

This modification will not impact Devices.

Consumers

This modification will not directly impact consumers. However, consumers may indirectly benefit from the Proposed Solution as the PSC will have visibility of any Data loss or compromise and ensure appropriate action is taken to remediate and prevent future incidents.

Other industry Codes

This modification will not impact other industry Codes.

Greenhouse gas emissions

This modification will not impact greenhouse gas emissions.

5. Costs

DCC costs

There are no DCC costs associated with this modification.

SECAS costs

The estimated SECAS implementation cost to implement this as a stand-alone modification is one day of effort, amounting to approximately £600. This cost will be reassessed when combining this modification in a scheduled SEC Release. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

There are no SEC Party costs associated with this modification.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **26 June 2025** (June 2025 SEC Release) if a decision to approve is received on or before 11 June 2025; or
- **6 November 2025** (November 2025 SEC Release) if a decision to approve is received after 11 June 2025 but on or before 23 October 2025.

It is recommended that this modification is targeted for implementation in the earliest available SEC Release. The inclusion of obligations on Users to notify the Privacy Sub-Committee of Data loss or compromise would ensure that appropriate action can be taken if needed. It would also ensure that the requirements are included in the Privacy Sub-Committee's annual assessments for Parties so the Sub-Committee can assess Data Protection in relation to Data losses or compromises.

7. Assessment of the proposal

Areas for assessment

Sub-Committee input

SECAS has engaged with the Chairs from the Operations Group (OPSG), the Privacy Sub-Committee (PSC), the Smart Metering Device Assurance Sub-Committee (SMDASC), the Technical Architecture and Business Architecture Sub-Committee (TABASC), the Security Sub-Committee (SSC), the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) and the Testing Advisory Group (TAG) to confirm what input is required from these forums. The following Sub-Committees provided the following input to this modification:

Sub-Committee input	
Sub-Committee	Input sought
OPSG	No input required
PSC	Input on proposed solution and legal text.

Sub-Committee input	
SMDASC	No input required
SMKI PMA	No input required
SSC	No input required
TABASC	No input required
TAG	No input required

Observations on the issue

This modification was presented at the SEC Change Issues Group in February 2025.

A member of the Issues Group queried what the intention of the PSC would be with the information provided on Data breaches. The Proposer clarified that it would be dependent on the circumstances, and the PSC would reach out to the DCC Other User to discuss next steps and any actions that may need to be implemented. However, the aim of the modification would be to provide transparency, as currently there is no obligation on DCC Other Users to notify the PSC of Data Breaches.

Another member of the Issues Group questioned how the Proposed Solution would extend to Third Parties employed by DCC Other Users. They expressed that while the SEC could place an obligation on DCC Other Users, this may not apply to Third Parties. The Proposer clarified that DCC Other Users employing Third Parties would have agreements in place whereby Data Privacy compliance would follow the requirements set out in the SEC.

The Issues Group member questioned whether agreements that are not currently in place would have to be included retrospectively. The Proposer agreed that this would be the intention, and in turn this would bridge the visibility gap that raised the issue in the first place.

The Issues Group member expressed that there is a risk that the SEC would not have the same governance as GDPR when imposing obligations on an indefinite amount of Third Parties. The Proposer acknowledged the concerns but clarified that the obligations would go as far as DCC Other Users Third Parties, which would have agreements in place with the relevant DCC Other Users. Therefore, the Proposed Solution obligations would be included in those agreements.

8. Case for change

Business case

The Proposer has highlighted the need for DCC Other User data breach reporting as a solution to the lack of transparency relating to Data loss or compromise. The Proposed solution would ensure that DCC Other Users are compliant and able to comply with obligations within SEC Section I 'Data Privacy'. This aligns with the obligations on SEC Parties to comply with reporting on Material Security Vulnerabilities set out in SEC Section G 'Security' and the 'Security Controls Framework' document.

Views against the General SEC Objectives

Proposer's views

The Proposer believes the modification will better facilitate SEC Objective (f)¹ as the inclusion of Data breach reporting requirements will ensure that appropriate action is taken where an incident has occurred. It would also facilitate proactive action where similar issues are identified to avoid future incidents.

Views against the consumer areas

Improved safety and reliability

The inclusion of requirements for Other Users to report Data breaches would improve safety and reliability of Data protection measures by ensuring appropriate action is taken to mitigate and prevent incidents.

Lower bills than would otherwise be the case

This modification will have a neutral impact on this consumer area.

Reduced environmental damage

This modification will have a neutral impact on this consumer area.

Improved quality of service

This modification would indirectly benefit quality of service by ensuring that Data protection is reliable, and compromises are mitigated where needed.

Benefits for society as a whole

This modification would benefit society as a whole as it would improve confidence in Smart Metering and the governance in place to protect consumers and their personal Data.

Final conclusions

The highlighted issue was identified by the PSC and the need for data breach reporting would improve the current arrangements, including the annual Privacy Assessment. The reporting model follows the requirements set out in SEC Section G 'Security', where DCC Users are required to report Security risks and vulnerabilities to the SSC.

The Proposed Solution would have a beneficial impact on consumers and lead to improved confidence in Smart Metering and the governance in place to protect consumers and their Data.

¹ ensure the protection of Data and the security of Data and Systems in the operation of this Code

Appendix 1: Progression timetable

Timetable	
Event/Action	Date
Draft Proposal raised	11 Feb 2025
<i>CSC converts Draft Proposal to Modification Proposal</i>	<i>18 Feb 2025</i>
<i>Modification Report approved by CSC</i>	<i>18 Feb 2025</i>
<i>Modification Report Consultation</i>	<i>19 Feb – 12 Mar 2025</i>
<i>Change Board Vote</i>	<i>26 Mar 2025</i>

Italics denote planned events that could be subject to change

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
CSC	Change-Sub-Committee
DCC	Data Communications Company
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
OPSG	Operations Group
MAP	Meter Asset Provider
MAM	Meter Asset Manager
PCF	Privacy Controls Framework
PSC	Privacy Sub-Committee
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMDASC	Smart Metering Device Assurance Sub-Committee
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
TAG	Testing Advisory Group