Smart DCC Ltd Compliance Statement

Management of Confidential Information

Version:	**V1.2**
Date:	**24 May 2018**
Author:	**Albert Sinclair**
Classification:	**DCC PUBLIC**

Document Control

Revision History

Revision Date	Summary of Changes	Author	Version Number
20/12/2013	Final published	Marc Avery	1.0
10/05/2016	Minor wording and template update	Steve Johal	1.1
10/05/2018	Minor word changing to reflect GDPR replacing DPA	Albert Sinclair	1.2

Approvals

Name	Title / Responsibility	Release Date	Version Number
Marc Avery	Chief Information Security Officer	10/05/2016	1.1
Marc Avery	Chief Information Security Officer	24/05/2018	1.2

Supporting Documents

Document Ref (if applicable)	Document Name	Location
[1]	Gas Act 1986 and Electricity Act 1989	www.ofgem.gov.uk
[2]	Smart Energy Code	www.smartenergycodecompany.co.uk
[3]	GDPR	www.eur-lex.europa.net

Table 1: Supporting Documents

Table of Contents

1 Purpose

1.1. Smart DCC Ltd ("Smart DCC") is the holder of Smart Meter Communication Licences granted by the Secretary of State under sections 7AB (2) and (4) Gas Act 1986[1] and section 6 (1A) and (1C) of the Electricity Act 1989 (together "the Licence") and having a Licence Commencement Date of 23 September 2013.

1.2. This is the Compliance Statement (the "Statement") as required by Condition 10 of the Licence setting out the managerial and operational practices, systems and procedures of the Smart DCC to ensure that it complies with the General Prohibition pertaining to the protection of Confidential Information.

1.3. This Statement sets out the practices in place to ensure that Confidential Information is only used for the purposes of the Smart DCC business and is not used for any other interest including that from other areas of Capita plc, or any other organisation or person.

1.4. It is the responsibility of the Smart DCC to ensure that any Affiliate or Related Undertaking of Smart DCC, and any agent, consultant, or contractor of Smart DCC are also governed by the conditions of this Statement.

1.5. This Statement may only be revised with the approval of the Gas and Electricity Markets Authority that is established under section 1 of the Utilities Act 2000 (the "Authority").

1.6. Smart DCC is a wholly owned subsidiary of Capita plc and is regulated by the Authority.

1.7. Smart DCC has been granted the Licence to establish and manage the smart metering communications infrastructure which is governed by the Smart Energy Code and those documents referenced therein.

1.8. Smart DCC is responsible for the establishment and enduring governance of the smart metering communications infrastructure and during its term shall collect and create information in order to provide these services. Such information consists of design documentation, business process models, audit information, service management data, service user contact details, billing data and management information.

1.9. Smart DCC takes all appropriate steps within its power to ensure compliance with the terms of this Statement.

1.10. Words or expressions that are not specifically defined in this document shall, where applicable, have the meaning given to them in the Licence.

2 Management responsibility for Confidential Information

1.11. Confidential Information is defined within the Licence as information which is provided to the Licensee (whether directly or indirectly) by any person in connection with the Authorised Business of the Licensee, including information that is provided under or pursuant to the Smart Energy Code [2] or the provisions of any External Service Provider Contract to which the Licensee is a party (and includes any personal data and special category (previously known as sensitive) personal data within the meaning of the General Data Protection Regulation[1] [3]. The Licensee being Smart DCC.

1.12. The smart metering communications infrastructure has been designed such that all consumption data sent between service users and smart meters is encrypted and is therefore not visible to Smart DCC.

1.13. A register of Confidential Information is maintained which identifies the purpose of the information being processed and formally assigns ownership of each information asset to an authorised processor (a member of the Smart DCC senior management team). The register captures all important information assets such as system documentation, database content and contracts.

1.14. Those members of the senior management team who have been assigned as the authorised processors of Confidential Information are formally included within information management processes in order that appropriate authorisation is provided for all data being accessed, disclosed or changed.

1.15. Requests for the disclosure of, or access to, Confidential Information are validated, recorded and made available for audit purposes. The internal Smart DCC compliance function shall ensure that the process is effective and independent external audits shall provide additional assurance.

1.16. Confidential information is managed in accordance with the following principles:

a. Data is only retained for the purposes of its use
b. Data is stored in as few places possible and for as short a time as possible
c. Data is distributed only to those who need to have access
d. Physical data is:
    i. stored in fixed lockable containers
    ii. transferred using secure methods (e.g. a secure courier)
    iii. shredded when no longer required
e. Electronic data is:
    i. protected using authentication and access control
    ii. encrypted when being transmitted over non-dedicated communications channels
    iii. securely deleted when no longer required

1.17. All Smart DCC employees have specific obligations towards the protection of information within their terms and conditions of employment and disciplinary processes shall be used should those conditions not be met.

[1] The General Data Protection Regulation has direct effect across all EU member states and has already been passed. This means organisations will have to comply with this regulation and will look to the GDPR for most legal obligations.

1.18. All Smart DCC employees are provided with mandatory annual security awareness training on topics including information security, fraud and data protection. For those Smart DCC employees who are provided access to Confidential Information, additional guidance is provided on their responsibilities towards the correct handling (aligned to those principles stated within section 1.6).

3 Information Management Systems

1.19. The smart metering communications infrastructure provides the interface between service users and consumer smart meters. The infrastructure is presented to service users as a number of interfaces through which communications data may be sent. Message data sent by service users is validated and transformed before being sent to the smart meters. A similar process is followed for the return path. Additional interfaces provide service management and security certificate authority capabilities.

1.20. All Confidential Information is processed under the principle of “least privilege” whereby access is only granted to those users with an approved justification, i.e. where such access is necessary to fulfil their role. By default, logical and physical controls prevent access to information unless such access is explicitly granted.

1.21. All Smart DCC systems have been procured for the sole use of smart metering. The Smart DCC IT systems are separated from other systems used by other divisions of Capita plc. or their customers. Logical access controls are in place to ensure that only authorised and authenticated users have access and that data remains segregated.

1.22. Communications and data systems are provided to the Smart DCC by external service providers who are governed (by Smart DCC) in terms of their compliance to the International Standard for Information Security – ISO/IEC 27001:2013.

1.23. Smart DCC are responsible for ensuring that all information, assets, processes or information systems that provide and/or support Smart DCC systems are certified to ISO/IEC 27001:2013. This is supported by the Smart DCC Information Security Management system (ISMS) which ensures ongoing compliance to all security obligations through internal reviews and working groups.

1.24. Privileged IT system administrators who support Smart DCC systems (which includes those employed by our external service providers) are tasked with maintaining the appropriate system security and segregation. All such privileged users have a greater level of access to system configuration and in some cases Smart DCC data and are therefore cleared to HM Government National Security Vetting; Security Check (SC) level.

1.25. Confidential Information is protected in storage and transfer using appropriate controls such as authentication and encryption.

1.26. The Smart DCC office environments are separated from those of other Capita plc business units in order to maintain the principle of least privilege. Access control systems ensure that no unauthorised staff or visitors are allowed into the Smart DCC office environments.

1.27. Security related activity such as authentication and access events within information systems are recorded and monitored in order to detect any weaknesses in the system that may result in breaches of confidentiality. This monitoring is part of the overall Smart DCC service management function and is carried out by the Smart DCC information security

teams who have received appropriate training to be able to detect and manage incidents appropriately.

1.28. Any suspected breach of information systems or unauthorised disclosure is recorded as a security incident and investigated by the Smart DCC information security team. If an investigation identifies any unauthorised disclosure or access to Confidential Information, appropriate remedial action is taken which includes notification or escalation to key stakeholders.

1.29. All Confidential Information processed by Smart DCC is included within the scope of the Smart DCC information security management system which is used as the framework for the management of all information systems. As required by the Smart Energy Code, the Smart DCC information security management system shall be assured through both internal and external review and also certified to ISO 27001:2013 by an independent UKAS accredited body.