Information Security Strategy (Undertakings)

Version 2.0

Publication Date: 2 July 2024

Table of Contents

1. Introduction

On 8 August 2007, the Office of Fair Trading, in exercise of its duty under section 22 Enterprise Act 2002, referred the completed acquisition by Macquarie UK Broadcast Ventures Limited, a subsidiary of Macquarie UK Broadcast Holdings Limited, of National Grid Telecoms Investment Limited, Lattice Telecommunications Asset Development Company Limited and National Grid Wireless No. 2 Limited (together the "National Grid Wireless Group") to the Competition Commission ("**CC**").

The CC published its report entitled Macquarie UK Broadcast Ventures Limited / National Grid Wireless Group: Completed Acquisition on 11 March 2008 (the "**Report**"). In the Report, the CC concluded that:

- the acquisition had resulted in the creation of a relevant merger situation and that the creation of that situation may be expected to result in a substantial lessening of competition ("**SLC**") in relation to the markets for the provision of Managed Transmission Services ("**MTS**") and Network Access ("**NA**") to television broadcasters and certain radio broadcasters within the UK and that the SLC may be expected to result in the adverse effects specified in paragraph 9.2 of the Report;
- the CC should take action to remedy, mitigate or prevent the SLC and any adverse effects flowing from it and to that end Undertakings should be given to give effect to the CC's decision on remedies specified in the Report.

After formal and informal consultation by the CC with Arqiva, its customers and other stakeholders, the CC accepted Undertakings from Arqiva on 1 September 2008 (http://webarchive.nationalarchives.gov.uk/20140402141250/http:/www.competition-commission.org.uk/inquiries/ref2007/macquarie/pdf/notice_undertakings.pdf).

Paragraph 16 of the Undertakings contains provisions related to confidentiality of information, including the requirement for Arqiva to publish an Information Security Strategy (at paragraph 16.2 of the Undertakings). Paragraphs 16.1 and 16.2 of the Undertakings are set out below.

"16.1 Where Arqiva holds confidential information from:

16.1.1 a Customer in relation to an Existing Transmission Agreement;

16.1.2 a prospective customer or Customer before, during or after the process of negotiating a New Transmission Agreement pursuant to paragraph 9 and 10 or a renewal pursuant to paragraph 8.1.1; or

16.1.3 an MTS Provider before, during or after the process of negotiating an agreement for Network Access pursuant to paragraph 11.1,

Arqiva shall use that confidential information solely for the purpose for which it was supplied and shall respect at all times the confidentiality of that information. The confidential information referred to in this paragraph 16.1 shall not be passed on to any other business units, departments, subsidiaries or partners of Arqiva for whom such confidential information could provide a competitive advantage. Nothing in this paragraph 16 shall prevent Arqiva from providing confidential information to the Adjudicator, the DSO Auditor, Ofcom or the Office of Fair Trading."

16.2 Within one (1) month of the Commencement Date, Arqiva shall publish an Information Security Strategy which shall set out the principles for access and use of the confidential information referred to in paragraph 16.1 in the form of a protocol which identifies the different categories of information held by Arqiva and how these will be treated to ensure compliance with paragraph 16.1. The Information Security Strategy shall also require Arqiva to implement appropriate measures:

16.2.1 to ensure the security of Arqiva's information storage systems and data systems (including data collection, storage and archiving), particularly where confidential information referred to in paragraph 16.1 is stored in systems shared between business units;

16.2.2 to ensure the physical security of confidential information referred to in paragraph 16.1;

16.2.3 to ensure that an employee of one business unit does not disclose or use the confidential information referred to in paragraph 16.1 of which the employee had become aware whilst working for another business unit;

16.2.4 to ensure the security of the confidential information referred to in paragraph 16.1 in the event that Arqiva is a bidder in a spectrum auction in competition with a Customer or prospective customer; and

16.2.5 to ensure that staff receive adequate training in relation to the Information Security Strategy as part of the education programme pursuant to paragraph 18.5.4."

By publishing this document Arqiva sets out its Information Security Strategy in line with the requirements of the Undertakings for its treatment of confidential information referred to in paragraph 16.1 of the Undertakings ("**Confidential Information**").

2. Principles for Access and Use of Confidential Information

The following overriding principles will guide the treatment of Confidential Information by Arqiva:

a) **Use only for agreed purposes:** Arqiva shall use Confidential Information solely for the purpose for which it was supplied and shall respect at all times the confidentiality of that information.

b) **No supply of Confidential Information to any party for whom information could provide a competitive advantage:** Confidential Information shall not be passed on to any other business units, departments, subsidiaries or partners of Arqiva for whom such Confidential Information could provide a competitive advantage.

c) **Separation of competing business activities:** The working groups within Arqiva who are required to access and use Confidential Information will be distinct from those for whom such Confidential Information could provide a competitive advantage as set out in c) (i) below. In this sense distinct means that colleagues who are required access and use Confidential Information will not also work in groups for whom such Confidential Information could provide a competitive advantage and the colleagues in these different groups will have separate line management who will ensure that the arrangements set out in the Information Security Strategy are understood and adhered to. In particular:

   (i) the following business activities will be kept separate from the personnel within Arqiva that are required to access and use Confidential Information:

      - day-to-day management of Arqiva owned DTT multiplex operations (DTT multiplexes C&D);
      - day-to-day management of any bid that Arqiva might consider for a spectrum auction in competition with a Customer or prospective customer (as defined in the Undertakings);
      - requesting and specifying self provision of MTS and/or NA.

   (ii) Contact points into Arqiva for any Customer or prospective customer (as defined in the Undertakings) will be managed through two controlled channels and colleagues responsible for these controlled channels will be distinct from colleagues responsible for business activities for whom such confidential information could provide a competitive

advantage as set out in c)(i) above. The controlled channels are:

- a nominated account manager to manage MTS or bundled MTS/NA requirements for transmission services;
- an identified contact point to manage NA only requirements from prospective MTS providers.

(iii) Sharing of Confidential Information outside a business unit may be necessary in order to carry out Customer instructions. In this case, sharing is subject to express authorization by the Executive Director, Media & Broadcast, Head of Regulated Business or the Chief Legal Officer and additional measures may be required to limit dissemination only to those necessary purposes.

d) **Use of appropriate security measures:** Appropriate measures as set out in section 3 will be implemented and maintained to ensure the security of Confidential Information received and held by working groups that are required to access and use Confidential Information. Additional security measures may be required for more sensitive information (see e) below).

e) **Identify Very High Risk Confidential Information and implement additional measures:** some Confidential Information may require identification as Very High Risk Confidential Information and additional measures shall be implemented in respect of such information as set out in section 4.

3. Measures to Ensure the Security of Confidential Information

Paragraph 16.2 of the Undertakings requires that the Information Security Strategy sets out appropriate measures as set out in sub-paragraphs 16.2.1 to 16.2.5 (see section 1). This section 3 deals with each of paragraphs 16.2.1 to 16.2.5 of the Undertakings in turn.

3.1 Security of Information Storage and Systems (Paragraph 16.2.1)

The following measures will be implemented to ensure the security of Arqiva's information storage systems and data systems particularly where Confidential Information is stored in systems shared between business units:

- **Restricted access**: access to information systems / electronic storage space that is used to receive and hold Confidential Information shall be restricted to working groups within Arqiva that are required to access and use Confidential Information (in line with the separation principles as described in section 2). Access restriction may be by means of username based profile control, password protection or other electronic access controls as appropriate. Such restricted access will ensure that Confidential Information stored in systems shared between business units is protected from unauthorised access.

- **Up to date records of access requirements:** Up to date records to be maintained of colleagues within working groups that are required to access and use Confidential Information to ensure the effective administration of restricted access controls.

- **Disposal of Confidential Information**: disposal of electronic copy Confidential Information shall be managed securely in line with relevant contracts (if applicable) and Arqiva digital information disposal policies (which includes sanitisation in accordance with current NCSC destruction and disposal guidelines).

3.2 Physical Security of Confidential Information (Paragraph 16.2.2)

The following measures will be implemented to ensure the physical security of Confidential

Information:

- **Clear desk and locked screen policy**: Arqiva has a Clear Desk Policy and no Confidential Information should be left out in the open. Confidential Information will be stored in securely locked storage units when not in use.
- **Controlled disposal of Confidential Information:** Disposal of hard copy Confidential Information by means of shredding or other controlled waste disposal.
- **Physical separation enhanced measures:** Physical separation is an enhanced measure put in place in certain higher risk scenarios (for example, where Arqiva is acting as transmission or network access provider and also has a bid team for licence or spectrum). In such higher risk scenarios, there will, where reasonably possible, be physical separation for different teams of colleagues (in particular, those working in areas that could gain competitive advantage from access to Confidential Information such as those responsible for the day-to-day management of Arqiva owned DTT multiplex operations) which will be controlled by means of restricted door access to separate office spaces or distinct geographic locations.
- **Up to date records of physical access requirements:** Where physical separation enhanced measures are in place, up to date record to be maintained of colleagues within working groups that are required to access and use Confidential Information to ensure the effective administration of restricted physical access controls.

3.3 Employee Disclosure (Paragraph 16.2.3)

The following measures are maintained to prevent an employee of one business unit disclosing or using Confidential Information of which the employee had become aware whilst working for another business unit:

- **Internal Code of Conduct and confidentiality obligations:** The Arqiva internal Code of Conduct (which all Arqiva employees are required to comply with) refers to and requires compliance with the Undertakings and to this Information Security Strategy and the Code of Conduct includes a summary of confidentiality obligations under this Information Security Strategy. Relevant colleagues will be briefed to ensure they understand and comply with these obligations. Failure to comply with the Code of Conduct may result in disciplinary action up to and including dismissal.

- **Employees who change roles or projects:** if any colleague were to change role or project from a working group within Arqiva that is required to access and use Confidential Information to one where this information could be of competitive advantage (see section 2c) i) above), they must identify the information which might provide the competitive information and register this with the Head of Regulated Business and not disclose or exploit any such Confidential Information. The Head of Regulated Business will monitor compliance with this on an ongoing basis.

- **Awareness and Training:** All relevant colleagues will be made aware of their obligations under the Undertakings and this Information Security Strategy on joining Arqiva and will be required to complete mandatory training on their obligations under the Undertakings and the Information Security Strategy at least annually (see section 3.5 for more detail).

- **Line manager reinforcement:** Line managers will also be responsible for ensuring that at all times colleagues understand and accept their obligations and complete mandatory training. This is part of Arqiva's line manager expectations framework and is reinforced through all line manager touchpoints and the line manager induction.

3.4 In the Event that Arqiva is a Bidder in a Competitive Spectrum Auction (Paragraph 16.2.4)

The following measures will be implemented to ensure the security of Confidential Information in the event that Arqiva is a bidder in a spectrum auction in competition with a Customer or prospective customer (as defined in the Undertakings):

- **Separation of personnel:** Colleagues responsible for the day-to-day management of any bid that Arqiva might consider for a spectrum auction in competition with a Customer or prospective customer (as defined in the Undertakings), will be distinct from those that are required to access and use Confidential Information in line with the separation principles as described in section 2.
- **Very High Risk Confidential Information:** This scenario is likely to require the identification and treatment of Very High Risk Confidential Information as described in section 4.

3.5 Training and Awareness (Paragraph 16.2.5)

The following measures will be implemented to ensure that colleagues receive adequate training in relation to the Information Security Strategy:

- **New joiner training:** All new joiners are made aware of the requirement to comply with the Code of Conduct and are required to confirm they have read the Code of Conduct as part of mandatory training modules. All relevant colleagues are also required to complete mandatory training on the Undertakings and Information Security Strategy on joining.

- **Refresher training and materials:** Relevant colleagues are required to complete mandatory training on the Undertakings and Information Security at least annually. Additional briefings are carried out or communications issued as and when required. The Code of Conduct and other materials relating to compliance with the Undertakings (including this Information Security Strategy) are available to all Arqiva employees via the intranet. The Code of Conduct is also reviewed on a regular basis and any updates are publicised internally.

- **Line manager materials, training and performance reviews:** line manager responsibilities and the performance review process includes ensuring relevant colleagues understand their obligations in relation to the security of Confidential Information.

- **Compliance Statements:** relevant line managers are required to provide monthly statements on the handling of any Confidential Information in their business area to the Compliance Director.

4. Protocol for the Identification and Treatment of Different Categories of Confidential Information

Arqiva consider that any Confidential Information should be treated in accordance with the principles described in section 2 and be protected through the measures described in section 3.

However, it may be appropriate to identify "***Very High Risk***" Confidential Information for which confidentiality security is exceptionally important for the Customer or prospective customer (as defined in the Undertakings) and put in place additional measures for the protection of such Very High Risk Confidential Information.

Identifying Very High Risk Confidential Information: Very High Risk Confidential Information would include:

- information which indicates the intention of a Customer or prospective customer (as defined in the Undertakings) to bid or consider a bid for any spectrum auction that could be in competition with Arqiva;
- information which indicates the intention of a Customer or prospective customer (as defined in the Undertakings) to launch a new service where that service launch is not in the public domain.

Additional Measures for Very High Risk Confidential Information: For Very High Risk Confidential Information, measures in addition those described in section 3 would be implemented and would include:

- dissemination on a strictly need to know basis within the working groups that are required to access and use Confidential Information;
- extra protection around the storage systems and data systems used to hold Confidential Information, such as storage of electronic material in systems with highly restricted access;
- where appropriate, code names to be used to describe the work relating to the Very High Risk Confidential Information.

5. Review of the Information Security Strategy

This Information Security Strategy will be subject to regular review and may be updated from time to time as appropriate including and in the event of any changes to its business which may impact this strategy.

In accordance with Paragraph 16.4 of the Undertakings Arqiva shall also, if required, make modifications to the Information Security Strategy as the Adjudicator or Ofcom may direct from time to time.

Any modifications to the Information Security Strategy made by Arqiva must be notified to the Adjudicator and published.