Business Growth Service (Advice) Data Sharing Protocol

Last updated 24 February 2015

Contents

1 Preface

The Secretary The Secretary of State for Business, Innovation and Skills ("BIS") has implemented a strategy to support businesses with the greatest potential to contribute most to UK economic growth through an integrated approach across various services known as Business Growth Service including what is known as the advice offer (incorporating the Manufacturing Advisory Service ("MAS") and GrowthAccelerator as well as Design Mentoring and Intellectual Property Office Audits in England.

This high level document has been developed by Grant Thornton UK LLP ("Service Provider") to facilitate the sharing of Business Growth Service data and information between the Service Provider and/or its subcontractors ("Suppliers") and any relevant third parties including but not limited to Department of Business, Innovation and Skills ("BIS"), UK Trade and Investment ("UKTI"), Innovate UK and the growth hubs.

2 Introduction

2.1 This document is a Data Sharing Protocol ("DSP"). The aim of this document is to facilitate the sharing of all relevant personal, sensitive and non-personal data between the public, private and voluntary sectors as appropriate, so that participants of Business Growth Service (Advice Offer) receive appropriate services.

2.2 Organisations and/or companies that comply with this DSP should ensure that all of their staff and Suppliers or other relevant third parties who are affected by it are:

- aware of its contents; and
- the obligations contained within it and/or any data sharing agreements ("DSAs") which are created.

2.3 Organisations and/or companies should also ensure that revisions to the DSP are managed in a controlled way with the latest version available on the Business Growth Service websites.

3 Scope

3.1 This DSP sets out the principles that must be followed when using and sharing information and data.

3.2 This DSP applies to all information and data shared by organisations and/or companies as appropriate. Sharing is NOT restricted solely to information and data classified as Personal Data by the Data Protection Act 1998 as amended. This includes the following information and data:

- All information processed by the organisations and or companies including electronically (e.g. computer systems, Audio etc), or in manual records;
- Anonymised, including aggregated data. The considerations, though less stringent, must take into account factors such as commercial or business, sensitive data, and the effect of many data sets being applied.

3.3 Where personal or sensitive data is held, it is likely to only include the contact listed on any forms, qualifications of individuals applying for Leadership and Management grants and possibly demographic data where provided by the participant companies.

3.4 This DSP is further extended to include other public sector, private and voluntary organisations where appropriate.

3.5 The specific purpose for use and sharing information will be defined in the DSAs that will be specific to the organisations and/ or companies sharing information.

4 Aims and Objectives

4.1 The aim of this DSP is to provide a framework for the organisations and/ or companies directly involved in and aligned to the delivery of the Business Growth Service to regulate working practices relating to the treatment and use of data and information. The DSP also provides guidance to ensure the secure transfer of information, and that information shared is for justifiable legal purposes.

4.2 These aims include:

- To guide organisations and/or companies on how to share personal and non - personal information lawfully.
- To explain the security and confidentiality laws and principles of information sharing.
- To increase awareness and understanding of the key issues.
- To emphasise the need to develop and use Business Growth Service (Advice Offer) DSA's.
- To support a process that will monitor and review all information flows.
- To encourage flows of information.
- To protect the organisations and/or companies from accusations of wrongful use of non-personal data.
- To identify the legal basis for information sharing.

4.3 Organisations and/or companies adhering to this DSP are expressly making a commitment to:

- Apply the Information Commissioner's Code of Practice's 'Fair Processing' and 'Best Practices' standards where relevant
- Adhere to/or demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act 1998
- Develop local DSA's that specify transaction details using standard Business Growth Service (Advice Offer) DSA which must be approved by the Service Provider.

4.4 Organisations and/or companies are expected to promote staff awareness of the major requirements of data sharing. This will be supported by the production of appropriate guidelines/training material where required that will be made available to all staff/contractors via the relevant intranet sites and/or via other communication media.

5 The Legal Framework

5.1 The principal legislation concerning the protection and use of personal and non-personal information is listed below and further explained in:

- Human Rights Act 1998 (Article 8)
- The Freedom of Information Act 2000
- Data Protection Act 1998
- The Common Law Duty of Confidence
- Computer Misuse Act
- Civil Contingencies Act 2004

5.2 Other legislation may be relevant when sharing specific information.

5.3 As part of each Data Sharing Agreement, organisations and/ or companies should identify how they will meet their legal obligations and the legal basis (legislation and appropriate section(s)) under which information may be shared.

6 Information covered by this DSP

6.1 All information, including personal data and sensitive personal data as defined in the Data Protection Act 1998. In order to reduce the risk of DPA compliance and security breaches where possible anonymised data should be used. It is likely that personal and sensitive data will only include the contact listed on any forms or correspondence with the Service Provider, and demographic data provided by the participant companies.

Personal Data

6.2 The term 'personal data' refers to any data held as either manual or electronic records, or records held by means of audio and/or visual technology, about an individual who can be personally identified from that data. The term is further defined in the DPA as:

a Data relating to a living individual who can be identified from those data or
b Any other information which is in the possession of, or is likely to come into the possession of the data controller (person or organisation/company collecting that information).

6.3 The DPA also defines certain classes of personal information as 'sensitive data' where additional conditions must be met for that information to be used and disclosed lawfully.

6.4 An individual may consider certain information about themselves to be particularly private and may request other data items to be kept especially confidential e.g. any use of a pseudonym where their true identity needs to be withheld to protect them.

Anonymised Data

6.5 Organisations and/or companies should ensure anonymised data, especially when combined with other information from different agencies and or companies, **does not** identify an individual, either directly or by summation.

6.6 Anonymised data about an individual can be shared without consent (subject to certain restrictions regarding health/social care records), in a form where the identity of the individual cannot be recognised i.e. when:

- Reference to any data item that could lead to an individual being identified has been removed;
- The data cannot be combined with any data sources held by a signatory to produce personal identifiable data.

7 Responsibilities when sharing information

7.1 General

i Each organisation and/or company is responsible for ensuring that their organisational and security measures protect the lawful use of information shared under this DSP.

ii Each organisation and/or company will ensure a reasonable level of security for supplied information which is non-personal, and process the information accordingly.

iii Each organisation and/or company accepts responsibility for independently or jointly auditing compliance in which they are involved within reasonable time-scales.

iv Every organisation and/or company should consider making it a condition of employment that employees will abide by their rules and policies in relation to the protection and use of confidential information. This condition should be written into employment contracts and any failure by an individual or company to follow the policy should be dealt with in accordance with that organisation's/ and or company's disciplinary procedures.

v Every organisation and /or company should ensure that their contracts with external service providers include a condition that they abide by their rules and policies, including but not limited to the Business Growth Service Security Policy in relation to the protection and use of confidential information.

vi The organisation and/or company originally supplying the information should be notified of any breach of confidentiality or incident involving a risk or breach of the security of information.

vii Organisations and/or companies should have a written policy for retention and disposal of information.

viii Organisations and/ or companies must be aware that a data subject may withdraw consent to processing (i.e. section 10 DPA) of their personal information. In this case, processing can only continue where an applicable DPA Purpose applies (Schedule 2 and 3 if relevant)

ix Where the organisations and/or companies rely on consent as the condition for processing data then withdrawal means that the condition for processing will no longer apply. Withdrawal of consent should be communicated to other organisations and/or companies to ensure processing ceases as soon as possible.

7.2 Non-Personal Data

i Organisations and/or companies should not assume the non-personal information is not sensitive and can be freely shared. This may not be the case and the organisations and/or companies from whom the information originated from should be contacted before any further sharing takes place.

ii Organisations and/or companies must comply with the Fair Processing Notice or any other relevant consent prior to sharing data.

iii In addition to the Service Provider and its Supplier's obligations, all the employees, agents and subcontractors of the Service Provider and the third parties are subject to contractually binding obligations which forbid the unauthorised disclosure of confidential information. The Service Provider, its Suppliers and agents will keep

confidential all information supplied by the participant companies which is defined or designated as confidential in writing at the time of its supply. The Service Provider shall effect and maintain adequate security measures to safeguard confidential information from unauthorised access, use, copying or dissemination.

8 Restrictions on use of Information/Data Shared

8.1 All shared information, must only be used for the purpose(s) specified at the time of disclosure(s) as defined in the relevant DSA unless obliged under statute or regulation, or under the instructions of a court or as agreed elsewhere. Therefore any further uses made of this data will not be lawful or covered by the DSA.

8.2 Restrictions may also apply to any further use of non-personal information, such as commercial sensitivity or prejudice to others caused by the information's release, and this should be considered when considering secondary user for non-personal information. If in doubt the information's original owner should be consulted.

9 Consent – Applies to Personal Data only

9.1 Consent is not the only means by which personal data can be disclosed. Under the DPA in order to disclose personal data at least one condition in schedule two must be met. In order to disclose sensitive personal data at least one condition in both Schedules 2 and 3 of DPA must be met.

9.2 Where an organisation and/or company has a statutory obligation to disclose personal data then the consent of the data subject is not required; but the data subject should be informed that such an obligation exists.

9.3 If an organisation and/or company decides not to disclose some or all of their personal data, the receiving organisation or company must be informed. For example, there may be an exemption from disclosure or failure to secure consent.

9.4 Consent has to be signified by some communication between the organisation and Data Subject. If the Data Subject does not respond this cannot be assumed as implied consent. When using sensitive data, explicit consent must be obtained subject to any existing exemptions. In such cases the data subject's consent must be clear and cover items such as the specific details of processing, the data to be processed and the purpose for processing.

9.5 If consent is used as a form of justification for disclosure, the Data Subject must have the right to withdraw consent at any time.

9.6 Specific procedures will apply where the Data Subject is either not considered able to give informed consent itself because:

i the Data Subject's age (Gillick Competency); or

ii the Data Subject does not have the capacity to give informed consent. In these circumstances the relevant policy should be consulted.

10 Security

10.1 It is assumed that each organisation and/or company complies with relevant compatible security and data is managed with the European Economic Area.

10.2 Each organisation and/or company shall comply with this DSP and agree standards of security as defined by the Service Provider. If there is a security breach in which information received from under a DSA has resulted in a breach, the originator will be notified at the earliest opportunity.

10.3 Where an organisation and/or company has regular, specific security requirements, for example a corporate policy such as the Business Growth Service (Advice Offer) Security Policy, a hypertext link to the DSP should be included. This should help to avoid reviewing standards agreed previously when each new DSA is set up.

11 Information Quality

11.1 Information quality needs to be of a standard fit for the purpose information is to be used for, including being complete, accurate and as up to date as required for the purposes for which it is being shared. Without this any decision made on the information may be flawed and inappropriate actions may result.

11.2 Where organisations and/or companies share information under this DSP it is expected that they will either have an Information Quality Strategy and the supporting processes and procedures in place, or be formally working towards this.

11.3 All organisations and/or companies are expected to give undertakings that information meets a reasonable quality level for the proposed purposes for which it is being shared and be able to evidence this.

11.4 It is expected that all organisations and/or companies will have or be working towards an organisational Information Quality Strategy. In generating and maintaining this policy due regard should be paid to the Information Quality Strategy.

11.5 Obligations and responsibilities should be identified in the contract, or DSA relevant to the sharing of particular information.

11.6 Organisations and/or companies that adhere to this DSP agree to provide all relevant information for input to FOI requests that may be made in or in connection with the Business Growth Service (Advice Offer).

12 Training

12.1 All organisations and/or companies' staff processing information shared under this DSP and its related DSA are expected to be trained to a level that enables them to undertake their duties confidently, efficiently and lawfully. This is an obligation on each organisation and/or company and responsibility for it cannot be assigned to another organisation and/or company, although delivery of training can occur with that third party's consent.

12.2 To minimise the costs associated with training and to ensure that all staff participating in activities based on information shared under a specific DSA , it is strongly advised that collaboration should occur in the development and delivery of training. Obligations and costs arising out of such collaborative working should be clearly identified in the DSA.

12.3 For the avoidance of doubt, where collaborative training is not adopted this should be stated in the DSA.

13 Individual Responsibilities

13.1 Every individual working for the organisations and/ or companies related to the Business Growth Service (Advice Offer) are personally responsible for the safekeeping of any information they obtain, handle, use and disclose.

13.2 Every individual should know how to obtain, use and share information they legitimately need to do their job.

13.3 Every individual has an obligation to request proof of identity, or takes steps to validate the authorisation of another before disclosing any information requested under this DSP and associated DSA's.

13.4 Every individual should uphold the general principles of confidentiality, follow the guide-lines set out in this DSP and seek advice when necessary.

13.5 Every individual should be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could result in dismissal due to gross misconduct. .

14 General Principles

14.1 The principles outlined in this DSP are recommended good standards of practice or legal requirements that should be adhered to by all organisations and/or companies.

14.2 This DSP sets the core standards which are applicable and should form the basis of all DSA's established to secure the flow of information and data.

14.3 This DSP should be used in conjunction with agreements, contracts or any other formal agreements that exist between the organisations and/or companies.

14.4 All signatories to this DSP are responsible for ensuring that organisational measures are in place to protect the security and integrity of information and data and that their staff are properly trained to understand their responsibilities and comply with the law.

15 Review

15.1 This agreement will be formally reviewed annually to ensure that it is 'fit for purpose'.