

# **Terrabase Ltd Framework Code of Practice for Sharing Personal Information**

**Framework and Agreement for the Sharing of  
Data between Terrabase Ltd and 3<sup>rd</sup> parties**



## Contents

Document History .....	6
Document Location.....	6
Document History .....	6
Distribution .....	6
1. Introduction and Overview.....	7
1.1. Introduction .....	7
1.1.1. Framework Aims and Scope.....	7
1.1.2. Framework Principles.....	7
1.2. Correspondence Concerning this Framework .....	8
2. Data Controllers and Data Processors .....	9
2.1. What are data controllers and processors?.....	9
2.2. Joint Data Controllers .....	9
3. Management of Terrabase Ltd Data Sharing.....	10
3.1. Monitoring and Management of Agreements.....	10
3.2. Considerations and Justification for Sharing Data.....	10
3.2.1. Conditions of sharing data .....	11
3.3. Charging for Data .....	12
3.4. Data Costs .....	12
3.5. Commercial Sharing of Data .....	12
3.6. Cross Border Sharing.....	13
3.6.1. UK Boundaries.....	13
3.6.2. International Boundaries .....	13
3.7. Terrabase Ltd Data Sharing Methods .....	14
3.8. Frequency of Data Transfers.....	15
4. Types of Data .....	16
4.1. Personal Data.....	16
4.2. Sensitive Personal Data.....	16
4.3. De-Personalised Data.....	17
4.4. Anonymised Data.....	17
4.5. Aggregated Data .....	17
5. Permissions for Processing and Consent .....	19
5.1. Rights of Individuals .....	19
5.2. Consent .....	19

5.3.	Fair Processing Notices .....	20
5.3.1.	Consent to Process Ordinary Personal Data .....	21
5.3.2.	Opt In or Opt Out .....	21
5.3.3.	Consent to Process Sensitive Personal Data .....	22
5.3.4.	Consent and De-personalised/Aggregated Data .....	22
5.3.5.	Consent and Anonymised/Personal Data .....	22
5.3.6.	Consent and Sensitive Personal Data.....	23
5.4.	New Uses for Personal Data .....	23
5.5.	Confidentiality of Information & Third Party Sharing .....	23
6.	Use of Legal Powers .....	25
7.	Data Quality .....	26
7.1.	Data Challenge and Correction .....	26
8.	Information & Data Security .....	27
8.1.	Terrabase Ltd’s Information Security.....	27
8.2.	Staff Training .....	28
8.3.	External Consultants/Contractors.....	28
9.	Retention & Disposal of Data.....	29
9.1.	Retention of Data.....	29
9.2.	Destruction of Data .....	29
9.3.	Audit Control.....	29
9.4.	Exceptions to the Data Protection Act.....	30
10.	Data Sharing Process and Agreement.....	31
Appendix A –Relevant Legislation & Useful Contacts.....		32
	Data Protection Act 1998.....	32
	Human Rights Act 1998.....	32
	Disability Discrimination Act 1995 .....	32
	Freedom of Information Act 2000 .....	32
	Other Useful Contacts.....	32
Appendix B – Key Data Sharing Texts .....		33
	Types of Published Text .....	33
	Data Protection Statement/Fair Processing Notice (FPN) .....	33
	Privacy policy/Data sharing policy .....	34
	Security and Confidentiality Policy .....	34
	Web site privacy policy – where data are collected online .....	34

Appendix C – Information Security Classification and Labelling Policy .....	35
Scope and Applicability.....	35
Policy Statement .....	35
Information Classification .....	35
Information Labelling.....	37
Information Handling.....	37
De-classification .....	38
Definitions.....	38
Responsibilities .....	38
Glossary.....	39

## Document History

### Document Location

This document will be located on the Terrabase Ltd internal network.

### Document History

Revision Date	Previous Version	Summary of Changes	New Version
13/04/2010	N/A		1.0

### Distribution

This document will be made available to 3<sup>rd</sup> parties as required.

# 1. Introduction and Overview

## 1.1. Introduction

The Terrabase Ltd data sharing framework has been developed as a common document for Terrabase Ltd and is intended to provide guidelines and principles that will enable Terrabase Ltd and associated 3<sup>rd</sup> parties to share information in a consistent and approved manner and to promote good information management practice.

The framework will be the common document for referral for data sharing issues concerning Terrabase Ltd system information and will be updated and regularly review in accordance with issues arising and changes to legislation.

This document has been written with due attention to relevant legislation, the details of which may be found in appendix A, and with reference to the Information Commissioner's "Framework code of practice for sharing personal information".

### 1.1.1. Framework Aims and Scope

This document is intended to fulfil the following functions:

- Formalise the approach to Information governance and the sharing of data between Terrabase Ltd and associated parties.
- Provide a foundation where formal sharing of data can be reviewed and enhanced with reference to a common framework
- Document data sharing guidelines, in line with relevant legislation.

As a dynamic document this framework will need period reviews. It is suggested that this document will be reviewed yearly or following legislation changes or following changes to data sharing within Terrabase Ltd.

### 1.1.2. Framework Principles

The guiding principles of this document are:

- To provide a common framework to facilitate formalised data sharing between Terrabase Ltd and associated 3<sup>rd</sup> parties.
- To act as an agreement document under which all Terrabase Ltd data sharing will take place
- To ensure that by following this framework Terrabase Ltd and associated 3<sup>rd</sup> parties share and manage personal information both legally and ethically.
- To document that:
  - Fair processing notices and/or data privacy statements must always be provided to individuals whose data are being collected.
  - Terrabase Ltd will have in place confidentiality policies appropriate to how they handle personal and sensitive personal data. More information may be found in appendix B.

- Terrabase Ltd will have in place privacy and data protection policies appropriate to how they handle personal and sensitive personal data.
- Terrabase Ltd will manage and process data in accordance with all relevant legislation and with due regard for the rights and freedoms of the individuals to whom the data pertains.
- In accordance with the fifth data protection principle, data shall only be stored for the purposes for which the request has been made, and must be deleted once this purpose has been fulfilled.
- In accordance with principle 7 of the Data Protection Act 1998, formal agreements must be in place for the transfer of data between organisations as a requirement for the “appropriate technical and organisational measures” mentioned in the principle. Whilst organisations sharing data should work towards signed written agreements, so long as formal arrangements have been agreed, and obligations from both parties to the Data Protection Act 1998 are fully understood data sharing may take place before signature approval.
- Personal and sensitive personal data may only be passed on to commercial organisations with suitable data processing agreements in place.
- Personal and sensitive personal data will not be passed to commercial organisations for sales and marketing purposes except where that purpose has been explicitly agreed to by the data subjects.
- For the managing and processing of personal and sensitive personal data there must be in place password controlled and secure computer systems, and there must be secure areas for the filing of non-electronic records.

## **1.2. Correspondence Concerning this Framework**

Any views about the content of this framework and associated documentation may be sent to the following person:

Data Manager  
Terrabase Ltd  
Chantry Court  
Sovereign Way  
Chester  
CH1 4QN

## **2. Data Controllers and Data Processors**

### **2.1. What are data controllers and processors?**

The Data Protection Act 1998 states that any organisation that “determines the purposes for which and manner in which any personal data are, or are to be, processed” is a data controller.

Data controllers are required to comply with the Data Protection Act 1998 whenever they process personal data (in this context “processing” includes collecting, storing, amending and disclosing data).

### **2.2. Joint Data Controllers**

When the data is being controlled by Terrabase Ltd and one or more PPL(s) it is their duty to ensure that information process and shared from the Terrabase Ltd systems is done so in accordance with legislation and recognised guidelines.

### **3. Management of Terrabase Ltd Data Sharing**

Terrabase Ltd will manage the sharing of data through the use of this framework as a common point of reference for agreements and contracts between parties.

Where data sharing does not sit comfortably within the framework and/or relates to specific requirements or exceptions/constraints, it may be necessary for Terrabase Ltd to develop Data Sharing Agreements, Operational Level Agreements or seek legal guidance to facilitate data sharing.

#### **3.1. Monitoring and Management of Agreements**

Terrabase Ltd will manage and maintain a central repository of Information governance documentation to include Data Sharing Agreements, Data Sharing Protocols and Fair Processing Agreements. These documents will be altered under internal Terrabase Ltd change control procedures.

#### **3.2. Considerations and Justification for Sharing Data**

Terrabase Ltd will govern requests for data sharing through a set of controls as described in specific Data Sharing agreements established with each 3<sup>rd</sup> party.

On receiving a request for access to personal or sensitive personal data the points listed below should be considered. Organisations looking to share data should consider their answers to these questions to support the Terrabase Ltd data sharing process.

The Requesting Organisation

- Is the requester a legitimate organisation?
  - Are they known to the data controller?
  - Do they have a valid entry in the Data Protection Register?
  - Is that entry correct for the data they are requesting?
  - Are there any legal gateways for access to the data?
    - If a legal gateway exists, it does not necessarily mean that data must be provided.
    - If statute exists, then data can be shared with the requesting organisation, however this does not negate the proper recording and management of the movement of such data.
- What data are they requesting?
  - Are the data aggregated data, or other non-personal data?
    - If so then the DPA 1998 may not apply.
  - Are the data anonymised or personal data?
    - DPA 1998 applies.
    - Consider if the individual data that are held can be shared – is consent necessary, or are other conditions with the DPA 1998 fulfilled?
  - Does the requested information contain sensitive personal data?

- DPA 1998 Applies.
  - Check that the data held is shareable in terms of explicit consent or another relevant condition within the DPA 1998.
- For what purposes are the data to be used?
  - Have the purposes for which the data are to be used by the requesting organisation been stated, or otherwise recorded?
  - If the data are to be linked, does the requesting organisation have processes in place to ensure accurate linking of datasets?
- Data Agreements
  - Does the requesting organisation have similar data protection processes in place to ensure any personal or sensitive personal data are secure?
  - Have both organisations signed a formal agreement detailing their roles and responsibilities toward the data they are processing and sharing?

**In terms of deciding whether data should or should not be provided, the final decision must always lie with the organisation that is considered to be the data controller.**

The Terrabase Ltd Third Party Data Sharing Protocol will articulate these considerations as questions to enhance the controls around data sharing.

### **3.2.1. Conditions of sharing data**

Personal and sensitive personal data shared amongst Terrabase Ltd and associated 3<sup>rd</sup> parties must only be supplied subject to the following conditions

- Shared data must not be released or sold for commercial purposes, unless specifically agreed to by the data subject and data controller.
- Personal and sensitive personal data shared within the group must only be provided to third parties for the purposes of helping to fulfil obligations, once the third party has agreed with the data controller the purposes to which the data are to be processed and satisfied the data controller that they have an up-to-date and accurate entry in the “Register of Data Controllers”. Such an agreement is a requirement under the seventh data protection principle.
- Data from individual institutions or providers, other than data relating only to total numbers, must not be released without the prior permission of those institutions or providers.
- In the analysis of data, groups identified as having less than six individuals should not be published, without the permission of the data controller to do so.
- In accordance with the fifth data protection principle, data shall only be stored for the purpose(s) for which the request has been made, and must be deleted once this purpose has been fulfilled.
- In the event of sharing personal or sensitive personal data, the data controller must satisfy themselves that the relevant conditions for data sharing, under the DPA 1998, are met.

- The sharing of data for commercial purposes must only be performed in agreement with the data controller providing the data. Some organisations are restricted by statutory provisions.
- Data that are shared may not be used for the following purposes unless explicit consent has been given:
  - Commercial activity
  - Third party sales and marketing.

Terrabase Ltd will be expected to be notified of all future data sharing arrangements between partner organisations.

### **3.3. Charging for Data**

In certain circumstances, and where there are no legal requirements for data to be shared, organisations may have to place a charge for access to the requested data.

Whilst this is not seen as a normal activity, it is understood that some requested data may be resource hungry, or be otherwise difficult to produce thereby putting added pressure on staff, budgets and other resources.

### **3.4. Data Costs**

The data receiver is responsible for any associated costs which become necessary as a result of receiving data from Terrabase Ltd. The receiver of the data in each case would therefore absorb any changes to systems or paperwork. The receiver will assess whether the data requested is important enough to warrant any associated costs.

Costs associated with Terrabase Ltd's decisions, with aim of standardising processes or providing common wordings for documents etc., will be borne by each organisation individually.

### **3.5. Commercial Sharing of Data**

Commercial use of data is mainly interpreted to involve marketing; however marketing need not necessarily be for commercial purposes. As defined by the Data Protection Act 1998; "[marketing is] the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals".

The concern with regard to commercial sharing is not with the data being received by a commercial organisation, but the processes and controls in place to ensure that data residing with a commercial enterprise cannot use that data for purposes other than those agreed.

As the potential to use personal data gathered by Terrabase Ltd for commercial purposes continues to increase, careful consideration must be given to the security and understanding of commercial enterprises and how sharing may affect the individuals concerned.

Terrabase Ltd must ensure that have the right to share data with commercial organisations where there is any intention to do so. Any data gathered that may be transferred to a commercial organisation via such an agreement must be checked that they are allowed to transfer this data. This falls within the areas of consent and foreseeability covered elsewhere in this framework.

Any agreements made between Terrabase Ltd and commercial organisations must have in place a robust and fully agreed data sharing agreement that is signed and actionable by all parties. There must also be suitable clauses built into any contracts between such parties.

### **3.6. Cross Border Sharing**

#### **3.6.1. UK Boundaries**

There are four nations within the UK; England, Scotland, Wales and Northern Ireland. Terrabase Ltd is based in England.

From a Data Protection Act point of view, the legislation is a UK wide act, and so the movement of data across such boundaries is not considered to be an issue, in that the data may move through these regions and be covered unceasingly by the Act.

Note that the Isle of Man, Channel Islands and some other territories of Great Britain, are not part of the UK and may not be part of the EU. In these cases agreements made with government departments of these areas, may need to refer to legislation other than the Data Protection Act 1998.

#### **3.6.2. International Boundaries**

*Principle 8 of the Data Protection Act 1998 states that “Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data”*

In agreeing to share data any possibility of transfer to non EU member states must be agreed to and documented in data sharing agreements.

It is important that the data controller understands the implications of international sharing to any countries concerned, as to allow data to move to a country not sanctioned as having adequate protection of personal data s a breach of Principle 8 of the Data Protection Act.

Personal data may be transferred to a non-authorised country under the following conditions:

- a. The individual explicitly consents to the data being transferred or
- b. The data must be passed in order to fulfil a contract or obligation with the individual

### 3.7. Terrabase Ltd Data Sharing Methods

Terrabase Ltd's data transfer methods continue to be developed towards the Government's own Electronic Government Interoperability Framework (e-GIF). Where possible data sharing should take place within this framework through Secure File Transfer Protocol (SFTP).

Other methods of sharing data may be employed upon agreement between the parties concerned. Terrabase Ltd currently defines data transfer methods either through the Functional Specification or through Operational Level Agreements between Terrabase Ltd and associated 3<sup>rd</sup> parties.

The storage and transmission of any information classified as PROTECT will be handled in accordance with the Information Encryption policy. The PROTECT status is described in the Electronic Information processing Security Notice S(E)N 2007/04 contained in the Appendix.

For a definition of data classified as PROTECT see Appendix.

Methods of data transfer must be made as secure as possible. Terrabase Ltd insists that all data sharing between Terrabase and 3rd party organisations are undertaken through the following methods and furthermore subject to encryption:

- Transfer by **Web Based System (portal etc)**

This must be a secure system such as SFTP and include an accepted encryption and password system. When transferring information classified as PROTECT, Terrabase Ltd will encrypt all information using SSL/VPN technologies

- Transfer by **Mail Systems**

Any Information classified as PROTECT and sent by email must be encrypted in accordance with the procedure the encryption before being transferred out of the Terrabase Ltd local network.

Terrabase Ltd recommend the use of the Advanced Encryption Standard (AES) with minimum bit strength of 256 bit encryption. Where encryption is implemented the password/pass phrase should be a minimum of 15 characters and include 2 or more of:

Multiple words

Mixed case

Numbers

Special characters (e.g. £\$%^)

- **Postal Systems**

All information sent by postal systems should be pass/phrase encrypted and sent special delivery. Pass phrases should be communicated separately from the encrypted data files.

Special delivery tracks the “journey” of your item and a receipt is signed for, so you will always know where the data is.

### **3.8. Frequency of Data Transfers**

The frequency of the data sharing that takes place must be agreed between the parties arranging to share data. Any sharing of data that is deemed as ‘frequent’ should be defined in an Operational Level Agreement.

## 4. Types of Data

It is important that personnel using this framework understand fully the key data types that are covered by the DPA, and how the data may be handled. The following section describes the data types and how they should be handled across Terrabase Ltd.

### 4.1. Personal Data

In the Data Protection Act 1998 personal data are defined as:

“...data which relate to a living individual who can be identified

- a. From those data, or
- b. From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual”

Such personal data might include, but not be limited to:

- Name
- Address
- Telephone Number
- Data of Birth
- Qualifications
- Education and employment history
- A unique reference number, if that number can be linked to other data that identifies the data subject.

The Data Protection Act imposes obligations and restrictions on the way an organisation and its partners process personal data (in this context processing includes collecting, sorting, amending, using, deleting and disclosing data), and the individual who is the subject of the data (the “data subject”) has the right to know who holds their data and how such data are or will be processed, including how such data are to be shared.

Organisations providing data to Terrabase Ltd will be responsible for the ongoing data sharing through the allocation of fair processing agreements (FPNs). See section Data Sharing Process and Agreement.

### 4.2. Sensitive Personal Data

In the DPA, certain types of data are referred to as “sensitive personal data”. These are data that relate to the data subject’s private life:

- Racial or ethnic origin
- Political opinions
- Religious beliefs, or other beliefs of a similar nature

- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any office
- Any proceedings for any offence committed, or alleged to have been committed.

The data that are being shared of this type are not only sensitive personal data, but also in the many cases, the data of young people. It is important therefore that any organisation agreeing to this framework understands the sensitivity of the data being shared and attaches importance to its own internal procedures accordingly.

#### **4.3. De-Personalised Data**

De-personalised data are individual data records from which personally identifiable fields have been removed. Where an organisation removes name and address information, fields such as date-of-birth, postcode and qualifications may not be removed, due to the nature of research undertaken.

#### **4.4. Anonymised Data**

Because data that has been anonymised might still be used to identify the individual if matched with other data, anonymised data has been defined as data that has all identifying information stripped and regardless of other data that may be matched with it, will not provide data elements that will allow an individual to be identified.

These types of data are harder to create in terms of knowing that all possible identifying fields have been removed, but if done correctly these data types may be used without reference to privacy legislation.

Organisations requesting data from Terrabase Ltd in a de-personalised format will have to fill out the Terrabase Ltd Third Party Data Sharing Protocol. Terrabase Ltd will validate the data request protocol form to ensure that any intended future use of the data will not allow the identity of the individual to be derived.

#### **4.5. Aggregated Data**

Aggregated data represents data which is processed to produce a generalised result, and from which individuals cannot be identified. This might include data brought together to give a broad understanding of e.g., ethnicity distribution.

There is sometimes a slight risk that aggregated data might still allow an individual to be identified, for example by the results producing a very small group of results, from which other data may be used in identifying an individual, even though personal data has been removed. To safeguard data subjects and to manage the risk, it is generally accepted that aggregation of data leading to a result containing less than six individuals should not be used or disclosed (they should be destroyed), unless such aggregated data can in no way be

matched to identify individual data subjects. A decision on whether or not such results might be used, must be taken by a senior person within the organisation deemed (under the DPA 1998) to be the data controller.

Whilst management of results produced from work performed on aggregated data is needed, essentially the Data Protection Act does not apply to this form of data.

Requests for Aggregated data from Terrabase Ltd must come through the Third Party Data Sharing Protocol.

## 5. Permissions for Processing and Consent

The processing of personal and sensitive personal data is controlled by the DPA and there are several conditions under which these types of data may be processed.

Generally, the most powerful of these is the 'consent' of the individual concerned (see below).

Data relating to an individual is considered to be "owned" by that individual and the rights and freedoms of the individual must always be taken into account.

### 5.1. Rights of Individuals

*Principle one of the Data Protection Act states, "Personal data shall be processed fairly and lawfully..."*

*Principle six of the Data Protection Act states, "Personal data shall be processed in accordance with the rights of data subjects under this Act"*

Some Terrabase Ltd systems allow individuals a level of control over the data held by the system. Inaccuracies that are not able to be changed at this level may be reported to Terrabase Ltd so that changes can be made.

An individual also has the right to make a "Subject Access Request" as defined in the DPA, and this may be made to any organisation that an individual believes holds their data.

A request to Terrabase Ltd (as the legal data controller) will contain, if relevant, the names of the organisations with which personal data has been shared. 3<sup>rd</sup> parties must therefore be aware that requests for data may come directly to them, and not via Terrabase Ltd.

### 5.2. Consent

Consent is the primary tool in facilitating data sharing, but it is not the only tool. It is the main mechanism whereby individuals can have a level of control over the sharing of their personal information.

The Data Protection Act 1998 defines consent as "...any freely given and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". This definition is taken from the EU directive upon which the Act is based.

Interpretation of when consent is given, implied or explicitly required has been based on organisational needs and the views of legal teams. The Information Commissioner's Office (ICO) has issued guidelines about the methods of collecting consent "opt in" and "opt out". This is covered below, and it is important that any organisation collecting consent be aware

of the guidance issued by the ICO, and address the relative risks of using either method in the context of their business needs and prevailing legislation.

It is essential to know that whilst consent is by far the most powerful and preferable way to enable the sharing of data, it is not the only way. Schedule two and three of the DPA 1998 cover other means of enabling data sharing including through legislation, legitimate interests and so forth. It is worth the data controller considering if such conditions allow data to be shared without consent, and also if it is prudent to do so for a specific organisation or purpose.

### **5.3. Fair Processing Notices**

Fair Processing Notices are the primary vehicle for informing people how information is shared and to what uses the data will be put.

Terrabase Ltd takes a layered approach to Fair Processing Notices to establish the right balance between presenting too much information to an individual and not providing enough information.

The development of FPNs must be considerate of providing too much information or confusing people resulting in FPNs not being read. Terrabase Ltd must be mindful of the question “did the person fully understand to what they were agreeing?”.

A lack of information may not adequately cover the Terrabase Ltd uses of the information therefore an individual may feel misled if their data is used in a system to which they had no knowledge or to which they could not foresee.

It is important that people; young people, their parents and adults understand what they are agreeing to, the benefits of sharing their data and the consequences of not agreeing to data sharing.

Layered FPNs address this issue meaning that a “first layer” notice can be brief and to the point, providing only high level information, but enough that most people can make an informed decision that their information is being used correctly. The first layer will then point to a “second layer” notice that is quite often a web page.

The second layer will go into more detail about how and why personal information may be processed. It will contain specific information on third party organisations that will have access to data and why it is required. It will also provide further information for the individual to make contact with the data controller so that they may opt-out, should they wish to do so.

A third layer can then be provided which can provide detailed information pertaining to legislation, regulations, policies and protocols. The third layer will also have direct links to third parties involved so that individuals can find out more from those partners directly.

### **5.3.1. Consent to Process Ordinary Personal Data**

In general the way consent is collected by most organisations is via a “fair processing notice” or “Data Protection Statement”. These provide the individual with information as to how, when and where their personal data will be used. In cases where the individual has a legitimate right to object to processing taking place, a mechanism must exist to allow these objections to be recorded and managed correctly.

According to the DPA 1998, there are several conditions, of which one or many need to be fulfilled in order that data may be shared. Whilst consent is one of these conditions, it may be that under certain circumstances other conditions fulfil the requirements to allow certain data to be shared. If Terrabase Ltd believes that such conditions have been covered, then it is up to the data controller to decide on whether or not data might be shared under these conditions. The data controller needs to consider the relevance of the conditions, and any ramifications of sharing the data with “unusual” conditions fulfilled, some or all of which may not be understood by the individuals to whom the data relates. If a condition other than consent is to be, or is likely to be used, then this should be stated in the fair processing notice so that individuals are made aware.

### **5.3.2. Opt In or Opt Out**

There is much debate and erroneous thinking with regard to allowing individuals to “opt in” or “opt out” of having personal data used for optional purposes. Especially in the marketing community there have been a number of policies made in organisations that effectively limit that organisation’s ability to collect legitimate consents.

At this point it is worth differentiating the two methods of obtaining consent:

Opt out, is by far the most effective way of gaining an individual’s consent and may take the form of a question such as “by agreeing to this registration form you will be indicating your consent to us sharing your personal data, unless you have indicated an objection to receiving such message by ticking the above box”. This means that the individual has to take action to opt out of having their data used. It is important to understand that the phrasing of the question is important. See the ICO guidance on this called “The Electronic Communications Guidance Part 1” published in 2003 which gives more information of structuring questions.

Opt in, is more restrictive, especially where the collection of consents is of great value to an organisation. This may take the form of a question such as “We would like to use your information for [their purposes], please tick this box if you are happy for us to do this”.

In summary opting out means that the individual objects to contact, whereas opt in means that the individual agrees to contact.

### **5.3.3. Consent to Process Sensitive Personal Data**

Explicit consent is required in order to process sensitive personal data (other conditions may also allow such processing without consent, see schedule three of the DPA 1998).

### **5.3.4. Consent and De-personalised/Aggregated Data**

Data that has had all identifying fields removed (de-personalised), or merged together (aggregated) so that individuals are no longer identifiable, does not come under the regulations of the DPA 1998.

Under the guidelines in this framework however, Terrabase Ltd and associated 3<sup>rd</sup> parties should treat these data carefully and consider that the data will not be shared with any commercial organisations or individuals, except in the case where work is being carried out by such an organisation on behalf of Terrabase Ltd or the associated 3<sup>rd</sup> party. Third party commercial organisations or individuals should be subject to the same restrictions on the use of supplied data, as the organisation to which the data were supplied in the first instance.

### **5.3.5. Consent and Anonymised/Personal Data**

As defined in section 2, personal data are the sort of data that may identify where an individual lives, their age, qualifications, education and employment history etc. Anonymised data simply means that information immediately identifying a person are removed, e.g. the name and date of birth. Other data may remain that will allow systems to identify that individual in future by matching new data to it and creating new personal data records.

Personal data requires informed consent of the individual, this type of consent may be an “opt-in” or “opt-out” consent or in certain circumstances may be part of a “contract” with the collecting organisation, i.e. it is stated that by enrolling on a course this information will be shared and processed in order to fulfil the contract with the individual and might be shared with other organisations for this purpose. The latter must be determined to be appropriate by the data controller for an individual circumstance.

Other conditions that may be fulfilled that allow the sharing of data without consent are as follows:

- The processing is necessary for the performance of a contract to which the individual is a party, or for the taking of steps at the request of the individual with a view to entering into a contract.

- The processing is necessary to comply with legal obligations to which the data controller is subject.
- The processing is necessary in order to protect the vital interests of the individual.
- The processing is necessary for Crown purposes, administration of justice etc.
- The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted.

#### **5.3.6. Consent and Sensitive Personal Data**

Sensitive personal data, which includes data such as ethnicity, religious beliefs, sexual life, has tighter controls governing their processing.

If sensitive personal data are to be shared, then from a consent point of view, explicit consent is a requirement under the data protection act. It must be noted however, that other conditions exist within the DPA that allow the processing and sharing of sensitive personal data, that might mean that consent is not required. For example, Schedule 3, point 7 in the DPA, makes provision for processing of sensitive personal data “for the exercise of any functions conferred on any person by or under enactment, or for the exercise of any functions of the Crown, a Minister of the Crown or a government department”.

At the time of writing, very little, if any, case law exists in support of schedule 3 point 7 and this should not be relied on without consultation with legal counsel.

#### **5.4. New Uses for Personal Data**

Regardless of whether an individual gives consent directly, or their consent to certain processing is built into the terms and conditions of a contract, the issue of foreseeing new uses of the data originally collected needs to be considered.

Data are collected and processed for specific purposes that should be documented or implied. New uses for data may be different enough to not be covered by the documentation when individuals agreed to have their data used.

#### **5.5. Confidentiality of Information & Third Party Sharing**

Confidentiality of Terrabase Ltd information and data is expected at all times.

The sharing of personal and sensitive personal data with third party organisations should only be performed if that organisation is doing specific work on behalf of Terrabase Ltd, and will not be used for any other purpose. This will define the third party as a data processor under the DPA. If Terrabase Ltd wishes to share personal and sensitive personal data with a third party, then they must be aware of any permissions given or refused by the individual

concerned, and if necessary obtain consent from individuals as to the new purposes to which the data are to be put.

## 6. Use of Legal Powers

There are several pieces of legislation that have a day to day impact on the sharing of personal data, the main one of these being the DPA. However, other Acts exist that may have provision for the sharing of data with other organisations, irrespective of the DPA. One of these Acts is the Finance Act and parts of this legislation provide for, for example, HMRC to access some personal data.

Due to the number of Acts under which provision might be given for access to shared data, it is not practical to try and identify all such legal gateways in this framework.

Terrabase Ltd should always be fully aware of the Acts under which it operates both in terms of acquiring personal information and providing personal information. Considering access to personal information should be part of a process where requirements are considered in their own merits and an audit trail of information flows recorded, to support the sharing decisions made.

## 7. Data Quality

*The fourth principle of the Data Protection Act 1998 states that “Personal data shall be accurate and, where necessary, kept up to date”.*

Terrabase Ltd has a Data Quality Strategy. The strategy will ensure Terrabase Ltd’s approach to data quality is both defined and pro-active.

Terrabase Ltd will influence data quality through:

- Data Standards
- Business/Validation Rules – Implementing business/validation rules at the system level will constrain the data loaded into Terrabase Ltd’s systems allowing Terrabase Ltd to validate records and reject non-conforming ones.
- Data Quality Reporting – Terrabase Ltd will offer a suite of pre-defined reports to assess the quality of the data in Terrabase Ltd’s systems. This extensible list of reports will form part of the Data Quality Strategy.
- Data Quality Audits – Periodic Data Quality Audits to assess Terrabase Ltd’s approach to data quality and to review derived metrics around data quality.

The Terrabase Ltd Data Quality Plan will be embedded into relevant Terrabase Ltd business units ensuring data quality is embedded in Terrabase Ltd business as usual (service and data management) with data quality analysis management information reports created and available to senior management as required.

### 7.1. Data Challenge and Correction

Terrabase Ltd will offer users and organisations a process and system for challenging and correcting data held in their systems.

The Terrabase Ltd data challenge process is the process which allows an individual/organisation to address problems with record details.

The ‘record’ is composed of the individual’s details and relevant associated records.

The basic stages of the data challenge (DC) process are:

1. Raising a data challenge (online or via the helpdesk)
2. Processing a data challenge
3. Closing the data challenge

Data challenges are raised and must be routed to the appropriate authorising source. An authorising source is the organisation who is responsible for deciding if the data challenge is correct (or not) and deciding who will authorise any necessary changes.

## 8. Information & Data Security

*The seventh principle of the DPA states that “Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”*

The personal and sensitive personal data held about individual should be controlled carefully as part of a comprehensive Information Governance framework.

The International Standards Organisation ISO27001: “The International Standard for an Information Security Management System”, is a practical way for many organisations to ensure that their processes, policies, security and management of information are as robust as possible.

### 8.1. Terrabase Ltd’s Information Security

Terrabase Ltd is actively committed to ensuring that the appropriate security, integrity, availability and confidentiality of our users’ information are preserved.

Terrabase Ltd has implemented a Security Policy to protect Terrabase Ltd’s assets from all threats whether internal or external, deliberate or accidental.

It is a policy to ensure that:

- **Confidentiality** of information is assured
- **Integrity** of information is preserved
- **Availability** of IT systems is maintained
- **Regulatory** and **legislative** requirements are met
- **Business Continuity Plans** are produced, maintained and exercised.
- **All breaches of security**, actual or suspected are reported up the management chain, and investigated by the **Security Manager**.
- **Advice and Guidance** on Information Security is available to all staff.

Terrabase Ltd has implemented standards and processes where necessary to support the implementation of this policy.

The Terrabase Ltd Security Policy complies with the requirements of ISO27001: The International Standard for an Information Security Management System and has been developed as a Summary of Controls (SoC) in accordance with the ISO standard and it incorporates ISO Standard requirement.

The Terrabase Ltd Security Manager has direct responsibility for maintaining this policy, and is further responsible for providing advice and guidance on its implementation.

## **8.2. Staff Training**

Any organisation dealing with personal and sensitive data has a duty to ensure that all relevant personnel are advised of, and understand the implications of the Data Protection Act 1998, and any other legislation which the organisation might be affected by.

It is considered that it is the individual organisation's responsibility to ensure that all relevant staff are correctly trained and informed in the handling of personal and sensitive personal data.

Terrabase Ltd also have a person responsible for ensuring that data sharing and data protection issues are addressed within their organisation promptly and correctly, and represents where applicable the organisation with regard to data sharing issues.

## **8.3. External Consultants/Contractors**

Terrabase Ltd may use contractors or consultants who may in turn have access to any personal or sensitive personal data held by Terrabase Ltd. If a consultant/contractor is expected to, or actually does, transfer data from Terrabase Ltd, to their own computer system for processing or storage, it is expected, under the terms of this framework and under the regulations of the Data Protection Act 1998, that the consultant/contractor will have a suitable agreement in place that determines the consultant/contractor as a data processor, or an individual accessing data under the controllership of their client.

Such an agreement must be explicit in stating the requirements placed on the consultant/contractor in terms of the use of the data, security of data that they may take off-site and the fact that they will use the data according to the principles of the DPA.

It is strongly recommended that the contractor/consultant becomes data protection registered with the ICO for the purposes of handling Terrabase Ltd's information.

## **9. Retention & Disposal of Data**

*The fifth data protection principle states that “Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes”.*

Terrabase Ltd has in place a retention and disposal schedule forming part of a comprehensive records management strategy. This schedule identifies the types of data held and used by Terrabase Ltd and list the retention and destruction requirements for these data.

### **9.1. Retention of Data**

Shared data will be used for differing purposes in Terrabase Ltd and consequently retention times for these data will vary. It is important however, that any retention requirements either via guidelines or published in law are adhered to.

Data sharing between Terrabase Ltd and associated 3<sup>rd</sup> parties will have to have a retention period defined depending on the use to which the data will be put.

### **9.2. Destruction of Data**

Once shared data are finished with and the purposes that the data have been shared for has been fulfilled, the Terrabase Ltd will convert the data to aggregated form for long term statistical storage if required, and/or delete the now redundant individualised data from their systems.

The deletion of data includes non-magnetic forms also. All records of any format should be regarded as confidential waste and be discarded appropriately.

The destruction of data stored on removable media will be monitored through the Terrabase Ltd Data Destruction register. Terrabase Ltd will destroy all data transferred by CD/DVD media through the use of a purpose built CD destruction mechanism.

### **9.3. Audit Control**

Terrabase Ltd has in place processes that ensure that any data processed, moved or deleted can be retrospectively tracked in the form of audit trails. Database systems often provide transaction and audit logs and it is important that these processes are in place for if an instance arises that the movement of data needs to be audited in future.

Another area of audit control is to ensure that version control is in place.

#### **9.4. Exceptions to the Data Protection Act**

On occasion it may be necessary for Terrabase Ltd to disclose personal and sensitive personal data without the consent of the individual.

These instances may be for crime prevention or detection or when required by law.

## **10. Data Sharing Process and Agreement**

As a document under periodic review, this framework may be subject to change either as an agreement between Terrabase Ltd and 3<sup>rd</sup> party associates, or through changes in legislation.

If changes are required a new version of this document will be issued and published in accordance with the publishing scheme agreed by Terrabase Ltd and the 3<sup>rd</sup> party associate(s). This framework agreement provides the document that will put in place the requirements on Terrabase Ltd and 3<sup>rd</sup> party associates when data are being shared between them and data are being received from Terrabase Ltd's systems.

Any future review of the Terrabase Data Sharing framework and Information Governance implementation should be considerate of the following:

1. The sharing of information is having the desired effect.
2. Fair processing notices still provide an accurate explanation of the information sharing activity.
3. Procedures for ensuring the quality of information are being adhered to and are working in practice.
4. Organisations sharing information are meeting agreed quality standards.
5. Retention periods are being adhered to and continue to reflect business needs.
6. Security remains adequate, and if not, whether any security breaches have been investigated and acted upon.
7. Individuals are being given access to all the information they are entitled to, and that they are finding it easy to exercise their rights.

## **Appendix A – Relevant Legislation & Useful Contacts**

As summarised in the introduction to this document, the following pieces of legislation have been considered when creating this data-sharing framework. Links to on-line texts of the legislation have been provided, where applicable.

### **Data Protection Act 1998**

This is the key piece of legislation that affects any data sharing that may take place.

[www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm](http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm)

### **Human Rights Act 1998**

Available from [www.legislation.hmso.gov.uk/acts/acts1998/19980042.htm](http://www.legislation.hmso.gov.uk/acts/acts1998/19980042.htm)

### **Disability Discrimination Act 1995**

as amended by the Special Educational needs and Disability Act 2001

Available from

[www.legislation.hmso.gov.uk/acts/acts1995/Ukpga\\_19950050\\_en\\_1.htm](http://www.legislation.hmso.gov.uk/acts/acts1995/Ukpga_19950050_en_1.htm)

### **Freedom of Information Act 2000**

Available from [www.legislation.hmso.gov.uk/acts/acts2000/00036--a.htm](http://www.legislation.hmso.gov.uk/acts/acts2000/00036--a.htm)

### **Other Useful Contacts**

Information Commissioner's Office including register of data controllers –

[www.ico.gov.uk](http://www.ico.gov.uk)

British Standards (BS7799/ISO27001) – [www.bsi-global.com](http://www.bsi-global.com)

## **Appendix B – Key Data Sharing Texts**

The following section provides a list of documents that are in place to be able to demonstrate good management of confidential information and to ensure that individuals who may be affected by the sharing of such information can be made aware of how their information may be managed.

This list is not to be considered exhaustive, and is provided to give guidance as to the sorts of policies and information expected in good information management.

No samples are provided as these can go out-of-date and become misleading. Instead, web-links have been supplied to documents that may be useful and will more likely remain up-to-date.

### **Types of Published Text**

The following are the types of published text that Terrabase Ltd needs to ensure are in place and in the public domain.

#### **Data Protection Statement/Fair Processing Notice (FPN)**

This is an essential document and is the document that will be presented to individuals whose data are being collected. There are a number of elements essential in the notice:

- Clear and concise language, easy to understand
- A statement regarding the Data Protection Act 1998
- For what purposes the data are collected
- Any sharing that might take place – statutory and not
- Contact details for queries
- Where consent is required for processing – tick boxes for agreement or refusal

It is very important to balance the length of such a notice with the possibility of it being too long for people to comfortably read; it must be kept as short as possible so that individuals can read, digest and understand it quickly and easily.

It is recommended, where possible, that a layered FPN is used. This format allows a short summary notice to be placed where an individual may see it, for example on enrolment forms or application forms. It will also provide a link in some way to another layer of the FPN that will provide greater detail for those individuals who would like more information as to how their personal data may be used.

This method ensures that all people will see the first layer of the FPN and this will provide all the information that most will require. The second layer, available on a web page or via a request line will go into more detail as to how personal information will be managed, shared

and used, and if necessary provide direct links to third parties that may have access to the information.

### **Privacy policy/Data sharing policy**

This is a document that can be either internal, external or both depending on the requirements. Often the privacy policy is related to the FPN, but can also be an internal policy document informing staff on how to treat and process data responsibly.

### **Security and Confidentiality Policy**

Often linked to an internal privacy policy this document serves as an internal set of guidelines for staff on handling information. Depending on the format of this document it may also take the place of an internal privacy policy and vice versa.

Such items to include in such a document might be:

- Data Protection Act overview for the casual reader
- Set of principles under which data are treated by Terrabase Ltd
- Guidelines on the processes for releasing personal and sensitive personal data
  - How requests will be dealt with
  - Release of data under statute, e.g. crime prevention
- Reference to acceptable use policies for equipment and processes, e.g. email acceptable use.

### **Web site privacy policy – where data are collected online**

When personal data are collected using online methods it is imperative that a privacy policy is published on the relevant websites used.

This policy needs to cover much the same things as a fair processing notice as well as:

- Why and how data are collected online
- Purposes to which the data are to be put
- IT Security around the collection of personal data
- Any methods used to track web usage e.g. cookies
- Contact details for queries

## **Appendix C – Information Security Classification and Labelling Policy**

### **Scope and Applicability**

This policy states how information should be classified and labelled according to its sensitivity. It is intended to help employees determine what information can be readily disclosed to the public without further authorisation and where access to highly sensitive information needs to be restricted for legal, financial or reputation reasons e.g. compliance with the Data Protection Act (DPA). It is based on the compliance with the international and e-Government security standards.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing)

It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that can be taken to protect information. The impact of these guidelines on the majority of Terrabase Ltd's daily activity should be minimal. Questions about the proper classification of a specific piece of information should be addressed to your line manager.

This policy is to be applied to all new information created and held by Terrabase Ltd including that with information technology (IT) systems. The security of IT systems shall be designed in accordance with this classification and labelling policy. Existing information need not be labelled retrospectively unless it is being updated or published for public access.

All information held by Terrabase Ltd, regardless of its security classification and label, can be requested under statute. Data subjects have the right to request data held about themselves under the Data Protection Act 1998. Under the Freedom of Information Act 2000 (and other regulations in the case of environmental information), information must be considered for disclosure upon receiving a request by a Freedom of Information request-handler.

### **Policy Statement**

#### **Information Classification**

All Terrabase Ltd information shall be categorised as one of three sensitivity types:

- Public
- Unclassified
- Protect

**PUBLIC** – Information that has been declared public knowledge by someone with the authority to do so, or is already within the public domain and can freely be given to anyone without any possible damage to Terrabase Ltd or its 3<sup>rd</sup> party associates.

**UNCLASSIFIED** – Information relates to the majority of information produced or used by Terrabase Ltd for the purposes of executing its internal business processes. Unclassified information shall normally be open access to all Terrabase Ltd employees, however the ability to change this information may be restricted to those authorised to do so in order to preserve its integrity. It should only be disclosed outside of Terrabase Ltd with the permission of the data owner in line with relevant legislation.

**PROTECT** – sensitive information that should only be accessible to those with explicit permission to access it. Information shall only be classified as PROTECT where there are specific and legitimate business reasons for doing so.

The accidental disclose of sensitive information marked PROTECT would be likely to:

- Cause substantial distress to individuals
- Breach statutory restrictions on the disclosure of information (e.g. DPA)
- Breach proper undertakings to maintain the confidence of information provided by third parties
- Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies.
- Prejudice the investigation of facilitate the commission of crime
- Disadvantage Terrabase Ltd in commercial or policy negotiations with others.

Information must only be marked as PROTECT where it is deemed essential for sensitivity reasons such as those described above. The following descriptors should accompany a PROTECT marking to specify the type of sensitive information to be protected:

- PERSONAL\* - intended only for the addressee e.g. payslip
- PRIVATE\* - collected through electronic Government services and relating to one or more individuals
- STAFF - intended for Terrabase Ltd staff only
- DEPARTMENTAL - related to the working of a group e.g. audit
- MANGEMENT - intended for named senior management only
- COMMERCIAL - related to commercial dealings e.g. suppliers
- CONTRACTS - related to contractual dealings e.g. clients
- INVESTIGATION - relating to a sensitive investigation e.g. fraud
- LOCSEN - location sensitive
- HONOURS - related to honours e.g. nominations
- REGULATORY - with a regulatory requirement restricting access

\*Note: The DPA defines “personal data” as data which “relate to a living individual who can be identified from those data”. Terrabase Ltd will classify any such data as PROTECT (PERSONAL) or PROTECT (PRIVATE) as appropriate based on the definitions above taken from the HMG Manual of Protective Security (MPS).

### **Information Labelling**

Information that is disclosed to the public shall be marked as PUBLIC through metadata attached to the document (e.g. using the document properties).

Information that is not explicitly labelled shall be considered UNCLASSIFIED.

Information with a classification of PROTECT (with appropriate descriptor) must be clearly labelled as such e.g. in the header or footer of a document (e.g. MS Word, Crystal, PowerPoint etc) and marked through metadata attached to the document.

Metadata will be applied in accordance with any published Terrabase Ltd metadata standards.

### **Information Handling**

Information classified as PUBLIC can be disclosed or transmitted outside of Terrabase Ltd without the need for any specific security controls.

Information classified as UNCLASSIFIED (or not labelled) should not be disclosed beyond those with a need to know (i.e. Terrabase Ltd staff and 3<sup>rd</sup> parties to whom it concerns) without reference to the Terrabase Ltd Records and Openness Manager. UNCLASSIFIED information may be sent over the Internet (e.g. via email) without encryption.

Information classified as PROTECT should be treated as UNCLASSIFIED with the following additional measures:

- Do not leave unattended (e.g. table, desk or printer) and store in locked cabinet when not in use
- Do not email or transmit via the Internet without the use of encryption (reference 3)
- Apply any defined data sharing protocols (e.g. reference 4)
- Dispose of sensibly by destroying in a manner to make retrieval unlikely

In all cases access to information classified as UNCLASSIFIED or PROTECT and residing on Terrabase Ltd systems shall require a user to be identified and authorised to access and if appropriate, to modify the information.

## De-classification

Where information is classified as UNCLASSIFIED or PROTECT, the data owner of the information is responsible for agreeing to lower the classification.

## Definitions

For the purposes of this policy the following definitions are used:

- None specific to this policy

## Responsibilities

The **Enterprise Architecture Board** (EAB) is responsible for:

- Updating this policy in line with Terrabase Ltd objectives
- Advising projects on and monitoring compliance with this policy

**Programme and project managers** are responsible for delivering project and systems that are compliant with Terrabase Ltd standards and policies and managing exceptions as project risks.

**Supplier solution architects** are responsible for designing systems in line with Terrabase Ltd policies and standards and identifying compliance within high level design documentation.

**Terrabase Ltd records and openness manager** is responsible for assessing requests for disclosure of information labelled as unclassified or protect under the freedom of information act and defining procedures for disposal of information.

**Staff (Data Owners)** are responsible for:

- Familiarising themselves with this policy
- Classifying information they create or are the custodian i.e. they are the **Data Owner**
- Handling information in accordance with any protocols/handling procedures
- Considering requests for declassification of information e.g. PROTECT to PUBLIC
- Agreeing processes for managing access to their sensitive information e.g. where the information is held within a specific application

## Glossary

Consultant	External company or individual working for an organisation
Contractor	External company or individual working for an organisation on a long term basis
Data controller	A person who alone or jointly or in common with other persons determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data processor	In relation to personal data, means any person other than an employee of the data controller who processes the data on behalf of the data controller. This might include consultants and contractors.
Data Protection Act 1998	The legislation governing the processing and management of personal and sensitive personal data.
Data subject	An individual who is the subject of personal data
Freedom of Information Act 2000	Legislation providing a right of access to information held by all public bodies, subject to certain exemptions.
Individual	In the context of this framework is the data subject
Legal Gateway	A term used to describe changes to legislation to allow sharing data through a specific Act.
Personal data	Data that relate to a living individual who can be identified from those data or from those data and other information that is in the possession of the data controller.
Processing	Means obtaining, recording or holding personal information or carrying out operations on the information of data including adaptation of the data, retrieval or consultation, disclosure by transmission, dissemination or otherwise making available, unlocking, erasure or destruction.
Sensitive Personal Data	Data that is personal data and consists of information as to such things as racial or ethnic origin, political opinions, religious beliefs, trade union membership, sexual life, health (physical and mental), criminal offences, criminal proceedings.
Sharing	In the context of this document is the processing of data to supply to another

	organisation directly outside the data controller's organisation.
Third party organisation	An organisation other than Terrabase Ltd.

Terrabase Ltd  
Chantry Court  
Sovereign Way  
Chester  
CH1 4QN

t 0845 644 1643

f 0870 460 1074

w [www.terrabase.co.uk](http://www.terrabase.co.uk)