# Data Sharing Agreement - Digital Switchover Telecare Provision

## Summary of purpose

Local authorities (LAs) sharing telephone numbers of adult social care clients who have telecare devices, to communications providers (CPs), so that suitable support can be provided to individuals during the digital switchover of analogue phone lines.

|  |
| --- |
| Parties |
| * [Insert Local authority name] |
| * [Insert CP name] |
| * Controller to Controller |

|  |
| --- |
| Part 2 processing |
| * Personal data |
| * Insert Special category data |

|  |
| --- |
| Key legislation |
| * Care Act 2014 |
| * Public Switched Telephone Network Charter |

|  |  |
| --- | --- |
| **Name of signatory** |  |
| **Date of agreement** |  |
| **Name of communications provider** |  | |
| **Date of agreement** |  | |

|  |  |
| --- | --- |
| **Name of signatory** |  |
| **Date of agreement** |  |

|  |  |
| --- | --- |
| **Name of local authority** |  |
| **Date of agreement** |  |

|  |  |
| --- | --- |
| **Publish date** |  |
| **Review date** |  |
| **Termination Date (N/A if ongoing)** | Agreement will end when the CP confirms that the digital switchover is complete. |

**Contents**

[Data Sharing Agreement - Digital Switchover Telecare Provision 1](#_Toc168982215)

[Summary of purpose 1](#_Toc168982216)

[Parties 1](#_Toc168982217)

[Part 2 processing 1](#_Toc168982218)

[Key legislation 1](#_Toc168982219)

[1. The Data Sharing Agreement 5](#_Toc168982220)

[1.1. Ownership of this agreement 5](#_Toc168982221)

[1.2. Parties to this agreement 5](#_Toc168982222)

[1.3. Responsibilities of parties involved 5](#_Toc168982223)

[1.4. Review and termination 5](#_Toc168982224)

[2. Purpose and Benefits 6](#_Toc168982225)

[2.1. Purpose 6](#_Toc168982226)

[Background 6](#_Toc168982227)

[Purpose 7](#_Toc168982228)

[2.2. Benefits 7](#_Toc168982229)

[Individuals 7](#_Toc168982230)

[Parties (name the relevant party and the benefit) 7](#_Toc168982231)

[Communications provider 7](#_Toc168982232)

[Local authority 7](#_Toc168982233)

[Society 7](#_Toc168982234)

[2.3. Data Protection Impact Assessment (DPIA) 8](#_Toc168982235)

[2.4 Lawful Basis 8](#_Toc168982236)

[2.4.1 Part 2 processing 8](#_Toc168982237)

[2.4.2 Consent 8](#_Toc168982238)

[2.4.3 Vital interests 8](#_Toc168982239)

[2.4.4 Applicable legislation 9](#_Toc168982240)

[2.5 Proportionality and necessity 9](#_Toc168982241)

[2.6 Other relevant legislation 10](#_Toc168982242)

[2.6.1 Common law duty of confidence 10](#_Toc168982243)

[Override for duty of confidentiality 11](#_Toc168982244)

[2.6.2 Freedom of information 11](#_Toc168982245)

[3 Individuals 11](#_Toc168982246)

[3.1 Data subject rights requests and complaints 11](#_Toc168982247)

[Privacy information 12](#_Toc168982248)

[Rectification, erasure or restriction 13](#_Toc168982249)

[Complaints 13](#_Toc168982250)

[3.2 Data subjects 13](#_Toc168982251)

[Types of data subjects 13](#_Toc168982252)

[Describe 13](#_Toc168982253)

[3.3 Deceased individuals 13](#_Toc168982254)

[4 Data 14](#_Toc168982255)

[4.1 Data categories 14](#_Toc168982256)

[Part 2 processing 14](#_Toc168982257)

[Describe any anonymisation or pseudonymisation of data or outputs (for pseudonymised data include details of which organisation holds the key to re-identification): 14](#_Toc168982258)

[4.2 The data to be shared 14](#_Toc168982259)

[4.2.1 Personal data 14](#_Toc168982260)

[Describe the data - are there datasets or named reports? Is there any data specifically excluded? 14](#_Toc168982261)

[Frequency 14](#_Toc168982262)

[4.3 Storing and handling information securely 14](#_Toc168982263)

[Describe 15](#_Toc168982264)

[4.4 Outside UK processing 15](#_Toc168982265)

[Describe any outside UK processing 15](#_Toc168982266)

[4.5 Data quality 15](#_Toc168982267)

[Describe how data quality and accuracy will be checked and assured - will you use standardised formats, how will you check the accuracy of data matching, which party is responsible? 15](#_Toc168982268)

[4.6 Data breaches/incidents 16](#_Toc168982269)

[Describe how incidents will be handled - which party is responsible (if not all individually), is one party responsible for a system or database? 16](#_Toc168982270)

[4.7 Retention and Disposal 16](#_Toc168982271)

[4.7.1 Retention periods 17](#_Toc168982272)

[4.7.2 When sharing ends 17](#_Toc168982273)

[Describe 17](#_Toc168982274)

[5 Appendices 18](#_Toc168982275)

[5.1 Appendix A: Parties to this agreement 18](#_Toc168982276)

[5.2 Appendix B: Applicable legislation 19](#_Toc168982277)

[5.3 Appendix C: Defence for sharing data 20](#_Toc168982278)

[5.4 Appendix D: Security of data 21](#_Toc168982279)

[Electronic records 21](#_Toc168982280)

[Phone/virtual meetings/face-to-face meetings 21](#_Toc168982281)

[Paper records 22](#_Toc168982282)

[5.5 Appendix E: Public Switched Telephone Network charter 22](#_Toc168982283)

[List of signatories 23](#_Toc168982284)

# The Data Sharing Agreement

## Ownership of this agreement

This agreement was drafted under the Pan-London Data Sharing Project, facilitated by LOTI at London Councils. It is made available for local authorities and communications providers to document data sharing between the named parties.

## Parties to this agreement

The parties are registered Data Controllers under data protection legislation and are listed in **Appendix A**. This agreement covers data sharing that is:

* Controller to Controller

## Responsibilities of parties involved

All parties will

* comply with data protection legislation and the responsibilities within this DSA, according to their statutory and professional duties.
* choose a suitable signatory, who has the authority to commit to the responsibilities.
* suitably vet staff through any necessary employee checks.
* have appropriate written contracts or agreements with employees, agency staff, volunteers, and anyone with access to the personal data. These must include requirements for compliance with policies which include confidentiality and secure handling of personal data.
* communicate this DSA to staff and instruct them to contact their organisation’s Data Protection Officer/Lead if they are unsure at any point about the sharing of personal data.
* help staff to understand their responsibilities, for example by directing them to the:
  + [ICO Data Sharing Checklist](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/annex-a-data-sharing-checklist/#:~:text=Check%20whether%20the%20sharing%20is%20justified&text=%E2%98%90%20What%20is%20the%20sharing,the%20issue%20you%20are%20addressing%3F)
  + [ICO 10 step guide to sharing information to safeguard children](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/a-10-step-guide-to-sharing-information-to-safeguard-children/)

## Review and termination

|  |  |
| --- | --- |
| **Publish/agreed date:** |  |
| **Review date** |  |
| **Termination Date (N/A if ongoing)** | Agreement will end when the CP confirms that the digital switchover is complete. |

The Agreement shall take effect on the date agreed and will last until [Insert communications provider] confirms to the [Insert local authority] in writing that the Digital Switchover has been completed ie that the CP has migrated all numbers.

# Purpose and Benefits

## Purpose

The purposes of the data sharing may differ between the parties.

**Describe purposes and their origin** - Insert full description of purposes for each party or type of party, including description of specific legislation or statutory guidance requirements. Explain why you cannot achieve these aims without sharing the personal data.

### Background

Communications providers operate Public Switch Telephone Networks (PSTN) to provide individuals in the United Kingdom with a fixed voice telephony service. Companies are migrating the existing PSTN to a new digital approach called Voice over IP Network (VOIP). This activity is known as the Digital Switchover.

Ancillary services traditionally connected to the telephone network (telecare), such as analogue telehealth care pendants, auto diallers and assistive technology, may require upgrading and/or additional equipment to ensure that the service continues to work.

Communications providers are unable to directly identify users of telecare services within their customer base and have to rely on customers or their representatives self-identifying. Not all customers do this.

Communications providers have a duty to understand the impact of how the digital shift will impact clients who use these services and minimise any potential adverse effect on them.

Telecare (device) Service Providers are working on solutions to notify and upgrade their services to ensure continuity of their services but due to the particularly vulnerable nature of the users and the speed of the national change it is necessary to identify these customers as a matter of priority to ensure their safety (and avoid any loss of Telecare Services).

The switchover process has begun and has left some vulnerable customers unable to access emergency services and use their telecare devices. The Technology Secretary met with the UK’s leading telecoms providers in December 2023, including Sky, BT, VMO2 and TalkTalk, to discuss urgent mitigations to reduce the likelihood of further incidents and protect vulnerable individuals, including the elderly.

These communications providers signed a Charter committing to concrete measures to protect vulnerable households, particularly those using personal alarms, known as telecare, which offer remote support to elderly, disabled, and vulnerable people – with many located in rural and isolated areas.

Providers will be required to work to provide back-up solutions that go beyond regulator Ofcom’s minimum of one hour of continued, uninterrupted access to emergency services in the event of a power outage.

They will collectively work with Ofcom and the UK government to agree a shared definition of ‘vulnerable people’ for this transition, so it is no longer dependent on the company and establishes an industry wide standard. Government will also continue to work with the telecare sector to reduce risk for users during the digital transition.

### Purpose

Where an individual is receiving support from a local authority adult social care (ASC) department, the authority is usually aware of the use of telecare devices or similar. One way for communications providers to identify individuals using telecare devices is to receive a list of users from the local authority. Data sharing between ASC departments and communications providers will also allow the provider to conduct additional checks on customers who have already been forcibly migrated to ensure they do not have telecare devices the provider was unaware of, and if they do, to ensure suitable support is provided.

No telecare users will be migrated to digital landline services without the provider, customer, or telecare company confirming they have a compatible and functioning telecare solution in place.

Communications providers are asking local authorities to share the phone numbers of ASC service users to match against the numbers the company manages. The company will then approach these clients to offer support and undertake actions and to make the necessary system and account changes to ensure the telecare service continues to operate when the Voice Service is provided over the VOIP network.

## Benefits

### Individuals

The data sharing will allow communications providers to better identify those individuals who use telecare devices and may be at risk from the digital switchover. Individuals benefit from personalised support to reduce potential harm from telecare devices not working after the digital switchover.

### Parties (name the relevant party and the benefit)

#### Communications provider

The sharing allows the communications companies to support vulnerable clients and comply with Ofcom guidance on Treating Vulnerable Customers Fairly (2022).

#### Local authority

The sharing allows local authorities to meet their duties under the Care Act 2014 to protect vulnerable individuals and promote their wellbeing.

#### Society

The protection of vulnerable individuals.

## Data Protection Impact Assessment (DPIA)

A DPIA has been undertaken by [Insert organisation name].

A DPIA has not been completed by [Insert organisation name] for this DSA as the criteria are not met.

## Lawful Basis

Each party must have a suitable lawful basis for processing personal data that has been agreed by that organisation’s Data Protection Officer/Information Governance Manager. All parties agree that they have an appropriate policy document in place when processing special category or criminal data.

### 2.4.1 Part 2 processing

For processing personal data the UK GDPR lists lawful basis conditions in Article 6 (personal data) and Article 9 (special category data) that must be identified to cover the processing. Part 2 of the Data Protection Act 2018 (DPA 2018) covers general processing. When processing special category data, a condition from Schedule 1 Part 1, or Schedule 1 Part 2 of the DPA 2018 must be identified.

Article 10 of the UK GDPR applies when processing data relating to criminal convictions and offences, and a condition from the DPA 2018 Schedule 1 Part 3 must be identified.

The conditions relevant to this DSA are:

|  |  |
| --- | --- |
| **Article 6 lawful basis conditions** | **Applicable party** |
| e) performance of a task carried out in the public interest | Local authority |
| f) purposes of the legitimate interests | Communications provider |

|  |  |
| --- | --- |
| **Article 9 lawful basis conditions** | **Applicable party** |
| h) provision of health and social care | Local authority |
| g) substantial public interest | Communications provider |

### 2.4.2 Consent

The parties will often work collaboratively with data subjects and aim for agreement with them on the actions to be taken. However, it is recognised that this is different to using consent (Article 6 (a)), explicit consent (Article 9 (a)), or consent for law enforcement processing (DPA 2018 Pt 3 Ch2 s35 2(a)) as the lawful basis conditions.

Consent is not the lawful basis for this sharing.

### 2.4.3 Vital interests

The vital interest conditions available for personal and special category data (Article 6 (d) and Article 9 (c)) allow for sharing where there is immediate risk to life. This is not applicable as sharing under this DSA occurs to reduce risk to individuals, rather than respond to an immediate threat.

### 2.4.4 Applicable legislation

Parties will have legislation, statutory guidance, and public duties for processing personal data. The applicable legislation for each party, that justifies the lawful basis conditions identified above, is listed in **Appendix B***.*

## Proportionality and necessity

Proportionality, data minimisation and necessity decisions were made when creating this DSA.

**Describe how proportionality and necessity have been and will be considered when sharing under this DSA.**

The data sharing is considered necessary to allow communications providers to better identify which of their customers use telecare devices. The data sharing is unlikely to guarantee all users are identified, but it will increase the percentage of those who are.

The need for the communications provider to identify the affected customers is a legitimate purpose so that any additional needs can be met (purpose test).

Only the minimal data required (telephone number and type of device) is being shared and matched and other avenues of identifying these customers have not provided sufficient certainty; (necessity test).

Data about customers who are not matched will not be retained beyond the initial matching exercise, the impact to individuals’ privacy rights is minimal and the need to protect the matched customers who have the additional needs is outweighed by the privacy rights of the affected individuals.

There are more than 600 communications providers. In the absence of a national data matching system that would check local authority data to identify which communications providers manage a telephone number/account, local authority ASC departments do not have the resources to individually identify which of their clients’ telephone numbers belong to which provider. In aiming to reduce incidents of vulnerable individuals losing access to emergency services and support, it is considered proportionate for local authorities to provide one list to all providers that request it.

A provider will match the list of numbers from the local authority to their client database to identify which clients they serve. The list will be deleted after matching.

The communications companies shall not retain or use the shared data for marketing purposes, the procurement of prospective customers or promoting supplementary products.

In addition, it is the responsibility of the individual making the decision to share specific data to weigh up what might happen as a result of data being shared against what might happen if it is not, and apply their professional judgement. There are legal safeguards which support a defence for sharing data listed in **Appendix C**, which the parties will communicate to their staff to support them to be confident when sharing data.

To enable the Data Controller to account for decisions made, staff sharing data must record:

* the decision to share or not to share.
* the lawful basis for sharing.
* with whom the information was shared.

## Other relevant legislation

The disclosure of any personal data to achieve the objectives listed in this DSA must consider the Human Rights Act 1998 (HRA) and the Common Law Duty of Confidence.

### 2.6.1 Common law duty of confidence

The word ’confidential’ can mean different things to different people.

* Personal and special category data as defined by data protection legislation.
* Patient Identifiable Information (PII) or ‘personal confidential information’; both terms most commonly used in health settings.
* Information which is not lawfully in the public domain or readily available from another public source.
* Where the person giving the information could reasonably expect that it would not be shared with others.

A duty of confidence arises where it is reasonable for a data subject to expect that the information will be kept confidential. This duty is often used in health settings, but applies outside of health. The duty can be overridden by legislation or justifiable necessity, or where consent has been provided by the data subject.

While much of the personal data processed under the DSA is considered confidential, it is legitimately assumed that data subjects will understand that the parties will share personal data for the purposes of safeguarding and wellbeing, preventing harm, and the prevention and detection of crime.

When overriding the duty of confidentiality, the parties may seek the views of the organisation who hold the duty of confidentiality and consider their views in relation to breaching confidentiality. The organisation may wish to seek legal advice if time permits.

### Override for duty of confidentiality

**Overriding public interest** (eg to prevent or detect a serious crime or to prevent serious harm to another person, balanced against the public interest in maintaining public confidence in public sector organisations.

There have been incidents during the switchover of vulnerable customers losing access to emergency services. Telecare devices are used by the elderly or those with significant disabilities and some of these individuals are less likely to understand the impact of the digital switchover and to proactively check with the provider. The local authority duty of care is met by helping increase the likelihood that a provider will know that a customer uses a telecare device or has needs for immediate access to the emergency services.

### 2.6.2 Freedom of information

The Freedom of Information Act 2000 gives the right to access official information held by a public authority. (For ease of drafting, FOI is used to also cover the Environmental Information Regulations 2004.) All parties subject to FOI have recognised procedures in place for managing such requests.

All requests for FOI will be directed through the relevant organisation’s FOI processes. Each party will seek advice/opinion from the other parties where there is concern about that information being released and any impact it is likely to have. The final decision to disclose or not will lie with the party who received the request as the legal duty lies with them.

It is encouraged that all parties proactively publish this document. It may also be disclosed by any party to the public under FOI.

# 3. Individuals

Organisations processing personal data are required to begin with the ethos of Data Protection by Design and Default (also known as Privacy by Design). We must consider and uphold the privacy of an individual’s data before we begin and throughout the processing taking place.

## Data subject rights requests and complaints

Each party has appropriate policies and processes for meeting individual rights and handling complaints.

The parties should describe below how they meet their duties for individual rights, including where one or more parties is responsible for meeting a right on behalf of other parties. For example, one party may be solely responsible for responding to subject access requests or ensuring suitable security for a shared system.

|  |  |
| --- | --- |
| **Individual right** | **How the Parties will comply** (or state not applicable if the right does not apply) |
| **The right to be informed** about the collection and use of personal data. | Privacy notice(s) for all relevant organisations  Local authority privacy notices already describe a council’s wellbeing duties under the Care Act 2014.  There are also multiple campaigns to notify the public about the digital switchover and the need to inform the CP if the customer uses a telecare device.  Information leaflets   * Posters * Letters * Emails * Texts * Social media campaign * Other [please state] * Not applicable |
| **The right of access** to details of data use and to receive a copy of their personal data, commonly called a subject access request. | The parties have existing processes for handling data subject requests. |
| **The right to rectification** to have inaccurate personal data rectified or completed if it is incomplete. | The parties have existing processes. The parties must establish ways to communicate, to share when data is rectified, to ensure it can be rectified in the other party’s system. |
| **The right to erasure**  (Does not apply when using the lawful basis conditions of Article 6: legal obligation, public task or legal claims, or Article 9: health and care services, public health or archiving, research or statistical purposes.) | N/A |
| **The right to restrict processing**  and limit how their data is used. | Does not apply to this DSA. |
| **The right to data portability** to obtain and re-use their personal data. | Does not apply to this DSA. |
| **The right to object** to the use and sharing of personal data where the parties are using the public interest or legitimate interests conditions It is unlikely that an objection would be upheld but each request must be considered on a case-by-case basis. | It is unlikely that a request would be upheld, but the parties have existing processes for handling subject rights. |

### Privacy information

Where personal data is created or received by one of the parties, they are responsible for making the data subject(s) aware (within a reasonable time frame) that the organisation holds the data, what they do with it, how long they keep it, and who they share it with (such as under this DSA). This is normally done through a privacy notice, whether written or verbal.

Local authority privacy notices already describe a council’s wellbeing duties under the Care Act 2014.

There are also multiple campaigns to notify the public about the digital switchover and the need to inform the CP if the customer uses a telecare device. Each party should document what privacy information has been provided to individuals.

### Rectification, erasure or restriction

If an individual successfully requests the erasure or limitation of use of their data, the relevant party will communicate this to the other parties where appropriate. Each party is responsible for securely disposing of such information or limiting its processing.

### Complaints

Each party has clear, fair and objective complaint procedures.

**Describe how complaints will be handled -** by individual parties or where one or more parties have responsibility on behalf of others

Parties have their own processes for handling complaints. Where the individual complaint warrants it, one party may share the complaint with the other to ensure the individual receives a suitable response.

## Data subjects

Parties to this agreement are in positions of power over data subjects and data subjects have little or no control over why and how their data is processed. Many of the data subjects are vulnerable.

### Types of data subjects

* Customers, service users, clients or residents
* Carers/Guardians/Family/Support network/Next of Kin – where the account holder is not the vulnerable individual.

### Describe

The data shared is of Adult Social Care (ASC) clients who are also communications provider (CP) customers. It is possible that the data is considered that of a carers or next of kin, where the ASC client has an advocate or lives with a carer or family member who ‘owns’ the telephone account and is the listed customer of the CP.

## Deceased individuals

The sharing may involve data of deceased persons which will not be covered by data protection legislation, but will still require due regard to the common law duty of confidentiality and the Human Rights Act.

# 4. Data

## 4.1 Data categories

(Tick pseudonymised or anonymised if any part of the data or outputs will be non-identifiable.)

### Part 2 processing

* Personal data
* Special category data

### Describe any anonymisation or pseudonymisation of data or outputs (for pseudonymised data include details of which organisation holds the key to re-identification):

Names will not be included.

## 4.2 The data to be shared

### 4.2.1 Personal data

* Contact details - phone number
* Social care information – the individual is a client of the social care team and, which telecare device they use.
* Family / relationship information incl next of kin

### Describe the data - are there datasets or named reports? Is there any data specifically excluded?

The local authority will send a file containing the landline telephone numbers and the Telecare alarm type (i.e. analogue, IP, GSM or Hybrid) of the ASC client upon which a Telecare alarm device is deemed to be operating.

The file should only contain a single column of landline telephone numbers, all with a leading zero, no spaces or any other formatting. The LA should distinguish whether phone numbers are residential, or business lines for sheltered housing schemes and similar.

The communications provider will match the number against its customer records and add this to the client file. The provider will share any matched numbers with the local authority, so the authority knows which CP supplies that client.

### Frequency

[Frequency to be stated] The frequency may differ by provider and by authority. The local authority to state the frequency expected between the named parties to this agreement.

## 4.3 Storing and handling information securely

All parties will ensure that they have appropriate technical and organisational security measures in place to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. All parties will store and share data securely.

Further information on general security standards are in **Appendix D**.

Using the DPIA, describe as relevant, the following:

* Data format
* Location
* Data flows (attach images if available)
* Roles and access and access controls

### Describe

The parties agree that they have suitable technical and operational security measures. The data is held in systems controlled by the relevant party.

Data will be shared by secure email.

## 4.4 Outside UK processing

Parties are responsible for ensuring that if information is processed or shared outside the UK, that appropriate safeguards are in place and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. For example, a legally binding and enforceable instrument between public authorities or bodies, binding corporate rules, and/or standard data protection contractual clauses.

### Describe any outside UK processing

|  |  |
| --- | --- |
| **Applicable party** | **Describe** |
| None | N/A |

## 4.5 Data quality

Each partner is responsible for ensuring the accuracy and relevance of the personal data that it processes and shares and must have clear processes in place for managing data quality.

Any party learning of the inaccuracy of personal data is responsible for promptly informing the parties with whom that data has been shared.

### Describe how data quality and accuracy will be checked and assured - will you use standardised formats, how will you check the accuracy of data matching, which party is responsible?

* Councils will provide current information they hold on social care clients who have telecare devices, at a frequency that is most appropriate for that authority, as agreed with the CP.
* CPs will provide back confirmation matches based on their current customer base.
* Both sides acknowledge that the status of a client or customer may change for example, if a client dies or a customer changes provider.

## 4.6 Data breaches/incidents

All parties must have a clear policy and procedure regarding the reporting and handling of data protection breaches or data loss incidents. This includes assessing the level of risk to the data subject(s) and deciding whether the ICO must be notified within the statutory time frame of 72 hours. This complies with Articles 33 and 34 of UK GDPR, and Section 67 and 68 of the DPA 2018 for personal data processed for law enforcement purposes.

If the incident may impact the processing of another party to this DSA, all relevant parties should be informed and appropriate coordination of the incident must take place. The decision to report the incident will lie with the data controller(s) of the information. The parties agree to provide all reasonable assistance to each other, at their own expense, to facilitate the handling of any personal data incident.

Each party has internal disciplinary procedures that cover security breaches (including misuse or unauthorised disclosure). If misuse is found, each party has a mechanism to facilitate an investigation, including initiating criminal proceedings where necessary.

### Describe how incidents will be handled - which party is responsible (if not all individually), is one party responsible for a system or database?

Each party has processes for handling data protection complaints. The party shall notify the other party where it is relevant to the data that has been shared and to the complaint.

## 4.7 Retention and Disposal

The parties may have different retention periods, potentially with a different period for combined data.

Each party will state a retention period and securely dispose of or delete personal data once it is no longer required.

### 4.7.1 Retention periods

The following retention periods apply to the data shared under this DSA. These may be for the data each party is sharing and/or for the combined data being shared.

|  |  |  |
| --- | --- | --- |
| **Data/Organisation** | **Retention period** | **Automated or manual deletion? What processes ensure that disposal happens at the allotted time?** |
| Communications provider | Unmatched data – deleted after matching exercise  Matched data – retained on the client file for the normal retention period of [insert retention period of CP] | Unmatched data – manual deletion  Matched data – deletion as part of process for whole client file. |
| Local authority | [LA to state] | [LA to state] |

### 4.7.2 When sharing ends

The parties must agree what happens to the shared data once the data sharing activity ends.

### Describe

The CP will incorporate the information that a client has telecare devices into their client file as part of their normal processes for supporting vulnerable clients. The data will be retained for the periods stated above.

The LA will delete the data matches from a CP once the switchover is complete.

# 5. Appendices

## 5.1 Appendix A: Parties to this agreement

**Local Partners**

As described in 1.2, local partners are not specifically named on the DSA when it is published. However, it may be accepted that a type of organisation will be a local partner. For example, multiple London Boroughs are expected to employ NHS Trusts to deliver substance misuse services. Where this is expected, below you should list the type of organisation expected to be a local partner.

| **Organisation name or type** | **Duties** |
| --- | --- |
| [Insert CP name] | * Delivery of telephony services to customers. * Duty to protect vulnerable clients during the national digital switchover. |
| [Insert Local authority name] | * Duties under the Care Act 2014 to deliver adult social care services to vulnerable clients. * Duties under the Local Government Act 2000 and the Localism Act 2011 to undertake duties for the wellbeing of the borough and its residents. |

## 5.2 Appendix B: Applicable legislation

State the relevant sections and describe the duties and how the legislation applies to the listed party.

| **Legislation/Statutory guidance** | **Party to which it applies** | **Main purpose of Legislation** | **How it applies to this data sharing** |
| --- | --- | --- | --- |
| Care Act 2014 | Local authority | * Promoting individual wellbeing * Preventing needs for care and support * Promoting integration of care and support with health services * Providing information and advice * Promoting diversity and quality in provision of services * Co-operating * Safeguarding adults at risk of abuse or neglect | Sharing data of vulnerable adults to prevent them losing access to telecare devices and emergency services (preventing needs and promoting wellbeing and independence).. |
| Localism Act 2011 | Local authority | * General powers of competence for local authorities | Taking action (data sharing) to promote the wellbeing of vulnerable individuals. |
| Public Switched Telephone Network charter | Communications provider | Voluntary charter to ensure proper care is given during the digital switchover to protecting vulnerable individuals using telecare devices. | Data needed to better identify customers using telecare devices |
| Ofcom guidance on Treating Vulnerable Customers Fairly (2022). | Communications provider | Guidance on how CPs are expected to support vulnerable clients. | Data needed to identify vulnerable customers so support can be provided. |

## 5.3 Appendix C: Defence for sharing data

There are legal safeguards which support a defence for sharing data, where the Data Controller believed it was:

* necessary for the purposes of preventing or detecting crime
* required or authorised by an enactment, by a rule of law or by the order of a court or tribunal
* in the particular circumstances, was justified as being in the public interest.

Or that they acted in the reasonable belief that:

* the person had a legal right to do the obtaining, disclosing, procuring or retaining
* the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it, or
* the person acted—

(i) for the special purposes,

(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and

(iii) in the reasonable belief that in the particular circumstances the obtaining, disclosing, procuring or retaining was justified as being in the public interest

To enable the Data Controller to account for decisions made, professionals sharing data must record:

* the decision to share or not to share
* the lawful basis for sharing
* with whom the information was shared

## 5.4 Appendix D: Security of data

The following are standards for security of data.

### Electronic records

All personal data held electronically will be stored in a secure area with password protected entry, audit records, and appropriate back-up functionality. All laptops, computers, and any other portable devices will be encrypted. Access will immediately be removed where an individual no longer needs it. Parties must ensure the chosen transfer method is suitably secure and that access is only provided to those who need it. Unencrypted email (i.e. sent in plain text over the public internet) must not be used to share information under this DSA. Sharing methods that may be appropriate include:

* Email encryption tools where the email and attachments are encrypted from named sender to named recipient.
* Encryption via Transport Layer Security (TLS) where the email and attachments are encrypted in transit over the internet. Both the sender and recipient email domains must have TLS enabled. This can be checked using [the CheckTLS website](https://www.checktls.com/)
* Secure corporately managed data repository and sharing platforms (e.g. MS Teams; Google Docs)
* Secure group email services (eg [Criminal Justice Secure eMail](https://cjsm.justice.gov.uk/))
* Secure File Transfer Protocols
* Virtual Private Networks

The above are examples, get advice from your organisation’s information security or IT teams on secure methods of sharing available at your organisation and document these in the organisation’s process documents.

### Phone/virtual meetings/face-to-face meetings

Information may be shared over the phone, in a virtual meeting, or at face to face meetings. Meeting attendance and distribution of content, eg meeting minutes or recordings, must be limited to those with a need to know. Sharing by telephone should be avoided unless the requirement is urgent and email is not practicable.

Individuals should be aware of their surroundings and the presence of other individuals or voice recognition or ‘Internet of Things’ devices (eg virtual assistant apps like Alexa, Cortana, SIRI) to ensure they aren’t overheard by those that should not have access to the information discussed.

### Paper records

Paper records must be minimised and kept secure whether in the office, home or during transit. Organisations must adopt an appropriate policy for the use, transfer and disposal of paper records.

## 5.5 Appendix E: Public Switched Telephone Network charter

The government met with communications companies in December 2023 to [address some incidents affecting vulnerable customers during the digital switchover](https://www.gov.uk/government/news/new-measures-to-better-protect-vulnerable-customers-agreed-with-telecoms-firms).

Leading telecoms providers agreed to a [charter to protect vulnerable clients](https://www.gov.uk/government/publications/public-switched-telephone-network-charter/public-switched-telephone-network-charter).

We, as Communications Providers, commit to the following:

1. We will not undertake any non-voluntary migrations to digital landlines, until we have full confidence that we are taking all possible steps to protect vulnerable people through the migration process.

2. No telecare users will be migrated to digital landline services without us, the customer, or the telecare company confirming that they have a compatible and functioning telecare solution in place.

3. Where battery back-up solutions are provided, we will work to provide solutions that go beyond the Ofcom minimum of 1 hour of continued, uninterrupted access to emergency services in the event of a power outage.

4. We will collectively work with Ofcom and Government to create a shared definition of ‘vulnerable’ customer groups that require greater support, specific to the digital landline migration.

5. We will conduct additional checks on customers who have already been non-voluntarily migrated to ensure they do not have telecare devices we were unaware of, and if they do, ensure suitable support is provided.

### List of signatories

* BT (incl EE Ltd and Plusnet Plc)
* Virgin Media O2
* Sky
* TalkTalk
* Vodafone
* Shell Energy
* KCOM