# Data Protection Impact Assessment

|  |  |
| --- | --- |
| **Project Name** | DSA between each local authority and communication provider(s) |
| **Pre-Assessment Completed By** | Sarah Laws, Data Protection Manager London Borough of Camden  Victoria Blyth, Pan-London Information Governance Lead (LOTI) London Councils |
| **Project Go Live Date (anticipated/planned)** | Early April 2024 |

## Description of the Project:

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. This means there will be some vulnerable users of such devices who are unaware of the switchover and the need to take action, who risk having their devices becoming inoperable putting them at risk.

It is proposed to have a set of Data Sharing Agreements (DSAs) with the communication providers to share telephone numbers of those who councils know have these devices, so the providers can undertake appropriate checks to ensure they are made aware of the issues and can take necessary steps to ensure the devices continue to be operable. Data sharing between Adult Social Care 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.

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. More information can be found on the [website of the Local Government Association (LGA)](https://www.local.gov.uk/publications/digital-switchover-telecare-checklist).

Communications providers have a duty under the Communications Act 2003 to give sufficient consideration to the particular needs of people with disabilities and people whose circumstances may make them vulnerable. Providers therefore have a duty to understand the impact of how the digital shift will impact clients who use telecare services and minimise any potential adverse effect on them. More information can be found on the [website of the Local Government Association (LGA)](https://www.local.gov.uk/publications/digital-switchover-telecare-checklist).

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 communications 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.

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 companies 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.

It is proposed that councils will securely send their whole lists to the six main providers. These providers will carry out the necessary checks. They will then securely send returns to each council to show which numbers were and were not those that had an account with the provider. The councils will then produce a smaller list of numbers which do not have accounts with the main providers. This will then be securely shared with the ‘second tier’ providers who have smaller market share/user numbers. This is to ensure data minimisation and lower volumes of data are shared with the larger number of smaller providers. Those smaller providers will do the same as the main ones.

|  |  |
| --- | --- |
| **Whose Personal data or Special Category Data are you using e.g.***,* children, vulnerable adults, residents, users of a service, employees | Adult social care users who are known to have telecare services. |
| **List the Personal Data** (eg names, addresses, MOSAIC refs) **and Special Category Data** (race /religion/sexuality/health etc) **and Criminal Offence Data** (includes allegations of offences not just convictions) **being used** | Personal data: telephone number, and by context that they have a telecare device. The communication provider who the client has the account with will therefore identify this user.  No special category data is being shared directly, but the fact the telephone number means someone has a telecare device shows they are vulnerable in some way, which would imply health or disability status.  No criminal offence data is being processed. |
| **Why are you collecting this data and what will you do with it? Give details.** | See project description above. It will be shared securely under DSAs with the main communication providers. They will check their records and where the number aligns to their account they will 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.  All providers will provide information back to the relevant council to confirm the numbers that they do have accounts for.  The councils will then produce a smaller list of numbers which do not have accounts with the main providers. This will then be securely shared with the ‘second tier’ providers who have smaller market share/user numbers. This is to ensure data minimisation and lower volumes of data are shared with the larger number of smaller providers. Those smaller providers will do the same as the main ones. |
| **Is there a piece of law that says you must, should, or may do this? If yes, set it out. If there’s no such law explain the basis for doing this processing** | The legal basis for councils for personal data is Article 6(1)(e) processing is necessary for performance of a task carried out in the public interest.  Although no special category data is being explicitly shared, if councils consider that it is shared by implication as telecare users have a vulnerability which implies there would be a health condition or disability, then the lawful basis would be article 9(2)(g) Reasons of substantial public interest (with a basis in law) with the Data Protection Act 2018 Schedule 1 Part 2 condition being para 6 Statutory and government purposes, and para 18. Safeguarding of children and individuals at risk.  Councils may also consider it may be Art 9(2) (h) Health or social care (with a basis in law) with the Data Protection Act 2018 Schedule 1 Part 1 condition being para 2 Health or social care purposes.  The underpinning law for all would be 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 tasks for the wellbeing of the borough and its residents.  For the communications providers the lawful basis for personal data would be art 6(1)(f) their legitimate interests.  Although no special category data is being explicitly shared, if councils consider that it is shared by implication as telecare users have a vulnerability which implies there would be a health condition or disability, then the lawful basis for this for the communications providers would be article 9(2)(g) Reasons of substantial public interest (with a basis in law) with the Data Protection Act 2018 Schedule 1 Part 2 condition being para 6 Statutory and government purposes, and para 18. Safeguarding of children and individuals at risk.  Communications providers have a duty under the Communications Act 2003 to give sufficient consideration to the particular needs of people with disabilities and people whose circumstances may make them vulnerable. Providers therefore have a duty to understand the impact of how the digital shift will impact clients who use telecare services and minimise any potential adverse effect on them. |
| **Are you using a new system or new IT kit? Has the security been approved** | N/a. Data will be shared securely in a manner agreed for each provider. This is expected to be SFTP, Microsoft Teams, encrypted email or similar secure manner. |
| **Are you are using a contractor or sub- contractor?** | No. The communications providers are data controllers and a DSA will be in place. |

**Risk Assessment**

In assessing risk we need to consider the nature, scope, context and purposes of the processing, and carry out an assessment of the impact of the proposed processing on the protection of personal data. **These are questions to help you and us assess the risk levels,**so it is essential that this table is completed accurately. **If you answer Yes or Unsure, please add detail to the Risk Explanation Table that follows this table.**

|  |  |  |
| --- | --- | --- |
| **No.** | **Risk Type** | **Yes/No/ Unsure** |
| 1 | Will you use profiling or automated decision-making eg AI (where computers do the thinking and a human isn’t involved at all) to make **significant** decisions about people (eg to help make decisions on someone’s access to a service, opportunity or benefit?) **or** on a large scale (like a large area of the borough)? | No |
| 2 | Will you use special category data (race/religion/sexuality/health etc) to help make decisions on someone’s access to a service, opportunity or benefit?) **or** on a large scale (like a large area of the council area) or for a lot of vulnerable people? | No but see note |
| 3 | Will there be large scale systematic monitoring in a publicly accessible place – like a new CCTV system? | No |
| 4 | Is the project using new technologies? Like face recognition software or a system we don’t currently use? | No |
| 5 | Will you be using criminal offence data (this includes allegations of offences not just convictions)? | No |
| 6 | Will you process biometric (fingerprint /facial recognition) or genetic data? | No |
| 7 | Will data be combined, compared or matched from multiple sources? | No |
| 8 | Will personal data be processed without providing a privacy notice directly to the individual? In other words will this processing be kept secret? | No- councils will need to add this processing to the appropriate Privacy Notices |
| 9 | Will personal data be processed in a way which involves tracking individuals’ online or offline location or behaviour? | No |
| 10 | Will children’s personal data be processed for profiling or automated decision-making or for marketing purposes, or offering online services directly to them? | No |
| 11 | Will any of the data be processed (this includes being stored and accessed by sub-contractors or IT support) outside the UK and outside the EU? | No |
| 12 | Will personal data be processed which could result in a risk of physical harm in case of a security breach? | No |

|  |  |
| --- | --- |
| **Details of specific risks and mitigations** | Acceptable risk? |
| There is no special category data being shared. However, where councils consider that the combination of a phone number and the fact that a telecare service is provided means that this becomes special category data as it implies a health condition or disability, then this would be a risk factor. However, the data is minimal and being shared in a secure non-intrusive way. Data minimisation is in place and there is a DSA with providers to cover the safe storage of the data. Purpose limitation is covered in that providers cannot, under the DSA, use the numbers for other purposes such as marketing. | Yes. Given the risks to people from their telecare being negatively affected, it is considered that the intrusion such as it is, is commensurate with the benefits of the processing |

## CONCLUSION Risk Assessment

|  |  |
| --- | --- |
| WHAT IS THE LEVEL OF RISK? | LOW |
| REASONS FOR THIS LEVEL | Although a large volume of data for some councils, very minimal re each data subject, low intrusion, unlikely will cause any harm, positive outcomes for processing, purpose specific and time limited, good controls and DSA in place. |
| Date cleared | 29th Feb 2024 |
| Cleared by | Sarah Laws, Data Protection Manager, London Borough of Camden |