PSPS
Public Sector Partnership Services Ltd

Delivering services for East Lindsey District Council, South Holland District Council

Data Protection Impact Assessment (DPIA)

Name of Project/Activity: PSPS Contact Centre Telephony Solution

Project lead officer: [redacted junior officer name s.40(3)]

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

PSPS Customer Contact requires a modern, supported and hybrid telephony solution to provide aligned services for Customer Contact with the capability to upscale to include additional clients in future. The new cloud-hosted Telephony solution will provide us with the ability to;

- Manage call flows
- Schedule a variety of reports
- Respond to Social Media and email enquiries via the telephony platform
- Work in an agile way
- Build resilience across sites
- Work in a much more intuiative and efficient way across all clients

This telephony solution provides a wide range of opportunities to improve our Customer's experience with additional services, such as online web chat, SMS facilities and automation of customer satisfaction surveys being introduced. However, it also ensures we can provide essential services to our vulnerable customers that may not be able to access digital platforms.

The new platform is capable of providing SMS, webchat and social media/email responses that will not be implementated at Phase 1 of this project, however will need to be assessed and evaluated at the point we choose to use them.

This project has a timeline of 12-14 weeks implementation from the signing of the contracts, therefore we intend for the system to go-live towards mid/end of August.

The Telephony platform will replace the existing un-supported Avaya phone system for the whole of PSPS employees and also for those employed by South Holland District Council and East Lindsey District Council. This DPIA relates to the call-recording aspect of this project and the data captured in the recordings as there will not be any migration of data from the legacy system to the new platform. The information recorded will be analysed primarily for quality assessments,customer satisfaction surveys, complaints or allegations, client clarification and GDPR purposes e.g. to ensure we are capturing accurate data from the customer and customer satisfaction surveys.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

All data will be collected via a call recording system on the telephony platform and therefore the source of this data will be our customers.

From the second the call is answered by the Contact Centre, the call recording will begin. The files will be stored in a “cloud-based storage” system held and governed by Ring Central and retained for 30 days at which point they will be automatically deleted from the system. This information can be accessed by any user that has “super admin” access granted, these people include:

- Head of Service
- Customer Operations and Delivery Manager
- Team Leaders
- Supervisors
- Resource and Performance Team

The only circumstances in which this information will be shared further than this group of people would be if requested, from Client services for complaints, allegations or investigations.This includes if a customer was to submit a Subject Access Request or a Freedom of Information request, depending on the circumstances, recorded information may be released to support these applications subject to any exemptions within legislation. There is a full audit history of any changes made within the system, therefore we can track who has what permission and when permissions are changed and only users with the full permissions, limited to the HOS, CODM and Team Leaders can amend these permissions.

The highest risk area for this new platform is that there is the capability that any call kept within the Ring Central network can be recorded from the point the call is answered, transferred and terminated. Therefore, if a customer calls the Contact Centre, their conversation with them is recorded, if the advisor transfers the call through to ELDC or SHDC back office, to a colleague or a supervisor, the whole call could recorded. This could be considered as a benefit for Customer Contact and our clients, as mentioned, if customers were to make allegations or log a complaint they can hear the whole conversation. As part of the planning and development phase of this project, Ring Central have now confirmed that this does not need to be standard practice and that they can design the system to stop recording after the call has been transferred out of the contact centre, therefore mitigating this risk.

The exception to automated call recording is when, if at any point in the call, the member of staff clicks on the payment link, the call recording will be temporarily paused whilst payment details are taken and will reactive upon closure of the payment system.

Another risk assosciated with this is that if a customer was to submit a subject access request then we would be required to provide the recordings of any conversation they have had with us. Depending on the conversation, this has the potential to disclose information relating to a third party to the customer, breaching GDPR. For example, if the back office were to disclose information relating to family member/other claimaint to the Contact Centre staff and the customer requested this information, we would breach the act as they would hear the conversation. We are unsure at this point whether there is the ability to re-dact/mask parts of the conversation before we provide the information back to customers. However, if we are unable to this is a risk. A potential mitigation would be a transcript being provided rather than the verbal recording and any unnecessary information would be redacted. We are hopeful this is possible with the new system but if we are unable to this will remain a risk.

Whilst this is beneficial when investigating complaints or any allegations made, it is not necessary for the purpose of the Contact Centre call recording. As mentioned above, the main purpose for recording the calls is to complete quality assessments on staff and to refer back to information shared when investigating data breaches and complaints. In order for us to do this, we do not need the whole call, including back office conversations, to be recorded.

In addition, there is the possibility that the Contact Centre could unintentially capture special category data from the customer because the advisor may not have any prior warning as to what information the customer will disclose. For example, a customer may ring regarding their own or a third party's Housing Benefit or Housing claim and disclose medical information and possibily information their sexual orientation or racial or ethnic origin if they feel relevant. To mitigate against this risk, detailed training material will be provided to staff including desk aids and standard operating procedures for the new platform to make it clear that if they need to ask any questions that will prompt the customer to disclose special category data or they feel the customer may give out this information then they must mask the recording.

In order to mitigate and lower this risk, Customer Contact will ensure that the process to stop the call-recording and at what times this is required will be built into all of the telephony training provided, contact centre staff will need to sign to confirm they understand how and when they need to do this before being able to answer any calls. We will also provide staff with clear and consise Standard Operating Procedures and desk aids that they can easily accesss at any time whilst answering calls.

If this was to happen, it is clear in the desk aid's and training guides, that staff are to contact the duty supervisor to delete the recording immediately so that we are confident the special category data isn't being stored on our system for 30 days. The supervisor involved will make a brief note of the conversation, without capturing the special category data, so there is an audit trail if the customer was to complain or we needed to refer back to the conversation for quality and assurance purposes.

Another potential risk we is that the telephony platform could record payment details from customers. We have been advised by Ring Central, that there is the ability to input the website link into the system and when the advisor is live on a call and they click into the link, the call recording will automatically pause. As soon as they close the application, the recording will continue.

Alex Tuplin - Technical Security:

ISO27001 – The system and the support staff are fully accredited. [redacted statement s.31 : prevention of crime]

All handsets comply with 802.1x eap/peap connection as a minimum and data is encrypted in transit.

Data at rest is encrypted. This prevents loss of data from compromise of back end databases, if they are directly exfiltrated.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The data collected will include a lot of personal and potentially special category data for residents of both Boston Borough Council, East Lindsey District Council and South Holland District Council. The data collected will be dependent upon what information is provided to us from customers and what information is requested from the contact centre to assist with their enquiry.

As mentioned above, although we may not ask for special category or criminal offence data, we cannot control what information is given to us by our customers. We will ensure that processes are in place to avoid recording special category data, however there is still the risk that this may be recorded.

All calls coming through the Contact Centre will be recorded from when phone lines open at 8:45 for BBC, 9 for ELDC and SHDC until close of business at 5:15 for BBC and 5 for ELDC/SHDC. Call recordings will be kept in the cloud-hosted platform for 30 days.

For 2021/22 we have received 367,539 calls into the service across all three clients and although we expect a reduction in demand due to digital transformation there will still be a high volume of calls being recorded through the new platform.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The individuals involved are East Lindsey, South Holland and Boston Borough Council's customers and any supporting third parties such as landlords, DWP, Citizens Advice etc who contact Customer Contact to provide them with first contact resolution or transfer their enquiry to a client service area or.

As standard, a message is played on all three Council's phone lines to advise customers that: "Your call will be recorded for training and quality purposes." The customer then has the choice if they would like to continue with the call and their information being recorded or to contact us via another channel.

Call recording is a standard practice for many private and public companies and therefore customers have been exposed to this method and will likely expect their call to be recorded. The calls recording may be from or include details regarding children or vulnerable groups of people as we do, on occasion, have children call on behalf of their parents (possibily to translate) for help and we do have a high volume of vulnerable groups of people contact us for support. There is also the possibility that information realting to children, will be recorded when discussing areas such as Housing and Homelessness, if the relevant department fails to mask the recording.

The legacy system [redacted s.31 : prevention of crime]and does not have many features that the new system will provide, including call recording. The system is not fit for purpose as it no longer meets the needs of the business providing services to three client councils and will soon become incompatible due to the upcoming removal of ISDN lines.

The main security risk we have relating to the new telephony platform is the unlikely possibility that Ring Central's data base was compromised. All of the call recording's and our information is held within Ring Central's Cloud-based platform, therefore if this was to happen, all of our staff's full names, email addresses and all of the information held in the call recording system would be accessible.

Prior to the system being implemented we will ensure that the Customer Contact privacy statement is updated to include details of the call recording function.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

As mentioned above, the aim of the new telephony platform is for Customer Contact to deliver aligned services to all three client councils. Currently, due to security issues with the Avaya phone system and the RAP's required, all of Customer Contact need to be on site in order to answer any phone calls, this has been and continues to be an ongoing risk for us if we were to have a COVID outbreak amongst staff then we would not be able to provide services as staff are unable to work from home. As mentioned previously, there are also many other functions such as web chat, SMS, automation of satisfaction surveys, that the system is capable of that will provide a wide range of benefits to our customers and clinets. However, at the point these are introduced the DPIA will be revised to include this information.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

IT Project Technical Lead DPIA – Review and Approval – Phil Davies
Telephony Project Manager DPIA – Review and Approval – Phil Davies
Telephony Project Board DPIA– Review and Approval – Mark Elsom
Head of Service DPIA – Review and Approval – Mark Elsom
Data Protection Officer DPO DPIA – Review and Approval – Mark Elsom
Security DPO DPIA – Review and Approval – Alex Tuplin
Information Security Analyist – Alex Tuplin

PSPS Transformation Board – Engagement with SLT & CEO of company
Communication Strategy lead by Head of ICT & Digital – Jackie Wright
Member updates as needed by Head of ICT & Digital

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

What is your lawful basis for processing?
The lawful basis for processing this information is the majority of our services are statutory services within the company and the client.

Does the processing actually achieve your purpose?
Yes, as outlined above in this DPIA, the new system will allow for hybrid working, resilience amongst our services, provides additional functions to benefit the customer and also mitigate security risks of staff illness due to COVID.

Is there another way to achieve the same outcome?
No, implementing a new Telephony platform is the only way in which we can achieve the same outcome that is required to provide resilience across the sites and a safer, more secure way to deliver statutory service.

How will you prevent function creep?
The tender specification outlines exactly what is expected to be delivered by Ring Central. Creep potential is limited as it is a full system replacement. However, there will be additional phases to this project where the DPIA will be reviewed at each stage.

How will you ensure data quality and data minimisation?
Applied thresholds in relations to record management and destruction. What has been set out in the project specification and delivery.

What information will you give individuals?
If a customer was to submit a subject access request, we would provide them with their recorded call if it was within the specified retention period of 30 days. We will also provide them with a clear privacy statement. A risk associated to this is that if a subject access request was submitted to Customer Contact for example, 28 days after the call had taken place, if this isn't actioned as a priority then the information will be automatically deleted after 30 days. To mitigate against this, clear communication will be given to PSPS and our clients to ensure we are communicated with immediately to prevent this happening.

How will you help to support their rights?
Ensure there is a clear privacy statement accessible for customers. The system allows for easy retrieval of data in relation to subjet access requests, call recording, call logging, trace by location and call history.

What measures do you take to ensure processors comply?
ICT control of the system to ensure parameters are in place. Restricted access permissions access based on user requirements limiting control of full user access to those needed.

How do you safeguard any international transfers?

N/A

Steps 5 and 6: Identify & assess risks; identify measures to reduce risk

5. Identify and assess risks	6. Reduce Risk *(only required for those with a risk score >8)*

Source of risk and nature of potential impact on individuals. Include associated operational and corporate risks as necessary.	**Pentana Reference** *(required for medium/high risks)*	**Likelihood of harm**	**Severity of harm**	**Overall risk** *Low: 1-8* *Med: 9–14* *High: 14+*	**Options to reduce or eliminate risk**	**Effect**	**Residual Risk** *Low: 1-8* *Med:9–14* *High: 14+*	**Measure Approved?**
Call Recordings – risk that special category data could be recorded and stored on the cloud system for 30 days		2 - Unlikely	4 - Very Signfiicant	8	Staff training, desk aids and crib sheets on how and when to mask recordings and process if special category data is recorded.	Reduce		Choose an item.
Supplier misuse of data – Risk that the company will use customer data captured in call recordings.		1 - Remote	5 - Severe	5		Choose an item.		Choose an item.
Software is susceptible to cyber crime – risk that the company could be compromised and our information breached.		1 - Remote	5 - Severe	5		Choose an item.		Choose an item.
Recording of Payment Details – risk that payment details will be recorded		2 - Unlikely	5 - Severe	10	System has the ability to build in the payment link so as soon as the browser is opened the recording will mask.	Reduce		Choose an item.

Source of risk and nature of potential impact on individuals. Include associated operational and corporate risks as necessary.	**Pentana Reference** *(required for medium/high risks)*	**Likelihood of harm**	**Severity of harm**	**Overall risk** *Low: 1-8* *Med: 9–14* *High: 14+*	**Options to reduce or eliminate risk**	**Effect**	**Residual Risk** *Low: 1-8* *Med:9–14* *High: 14+*	**Measure Approved?**
Alex Tuplin- Data is compromised from source systems		3 - Possible	4 - Very Signfiicant	12	**Encryption in transit and at rest, vendor is ISO27001 accredited.**	Reduce	4	Choose an item.
		Choose an item.	Choose an item.	Multiply likelihood and severity.		Choose an item.		Choose an item.
		Choose an item.	Choose an item.	Multiply likelihood and severity.		Choose an item.		Choose an item.
		Choose an item.	Choose an item.	Multiply likelihood and severity.		Choose an item.		Choose an item.
		Choose an item.	Choose an item.	Multiply likelihood and severity.		Choose an item.		Choose an item.
		Choose an item.	Choose an item.	Multiply likelihood and severity.		Choose an item.		Choose an item.

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Amie Househam – Head of Customer Contact – 31/10/2022	Click here to enter text. Integrate actions back into the project plan, with date and responsibility for completion.
Residual risks approved by:	Click here to enter text.	Click here to enter text. Note that if accepting any residual high risk you need to consult the ICO before going ahead.
ICT Security advice provided:	Alex Tuplin – Information Security Analyst	Click here to enter text.
DPO advice provided:	Mark Elsom, 12/10/22 I am satisfied that the processes assess in this DPIA are lawful, subject to consideration of the points outlined below.	Click here to enter text. DPO should advise on compliance, step 6 measures and whether processing can proceed.

Summary of DPO advice:

This is a comprehensive DPIA, which defines a particular use of data that requires assessing, and in some detail outlines legitimacy, risks and how we manage a data subject's rights. I am satisfied the proposed use of data through recording is legitimate and lawful, as a fundamental step taken to support each shareholing council in meeting their legal duty to serve and support their residents. However, I ask the department implementing this change to consider and address the following queries and recommendations to maximise compliance and reduce the risks to data subject (DS), company and councils. Any supplementary comments can be included in the comments section later in this form.

- I have noted that wider functionality, such as web chat and SMS, is available but not going live immediately. This assessment commits to further assessment should that be the case, and I want to reaffirm the importance of a DPIA ahead of any such changes.
- I note that data will be hosted in the cloud but details around location of storage and technical security measures are limited, and I suggest we build in supplementary commentary in the comments below confirming details and, if appropriate, seeking clarity from our ICT colleagues.
- I support the 30 days retention approach. I suggest consideration be given to whether this can be overridden on a case-by-case basis if ever needed. For example, can we retain for longer if dealing with a SAR or a complaint, or could we delete earlier if we felt that was appropriate in response to a DS request.
- Limited access controls are noted and supported as good practice. I also note the intention to share only in very limited circumstances. It might be advisable to document an internal policy/procedure for how this will be managed, including when you might refer to other colleagues/departments for input. For example, I would expect the relevant DPO to be consulted before releasing any data to a DS, and

documented clarity helps set out responsibility and expectations and reduces the risk of incorrect practice. I note also the later comments about transcript options, which might be helpful although it should be noted we're obligated to share data and this does not necessarily require full sharing of recordings or transcripts, although it may still be appropriate to share these in some circumstances.

- The reference to the automated call recording continuing after handing calls to other council colleagues was clear on risks and options but not clear on decisions and outputs. Can you please confirm that recording will cease at hand-off, or define how the associated risks will be managed.
- SAR risk and transcript. Noted. Welcome attempts to establish transcript ability. Note also data not documents (or recordings) so depending upon the cirucmstances we may choose not to share, especially if it breaches other individual's rights and freedoms.
- Efforts to reduce the risk around capture of special category data are noted and supported. In many cases collection of this data is required, and I am satisfied that other controls in place significantly reduce the risk of failure to comply with Data Protection law.
- Clear messaging and intentions to update privacy statements are noted and supported – these are important if we're to be transparent about data use.
- For completeness I want to note that the answer 'N/A' is inaccurate in response to the question, 'Is there another way?' It is possible that we operate without call recording and I feel we should acknowledge that, although I think it's reasonable to state that we must monitor calls to ensure our staff are performing to the highest standards when fulfilling their duty to support the councils' in meeting their legal obligations to residents. The process is necessary, the 'how' is debateable but to record is an efficient way of improving performance with no real risk to the customer and very minor risks to the organisation providing we're being transparent with customers.
- Just note that although I know the ICT security officer has reviewed this DPIA there are no comments to reflect this, and I am assuming they have checked relrevant security protocols, cloud based storage and the technical elements that ensure security and protect the data being processed.

DPO advice accepted or overruled by:	Click here to enter text.	Click here to enter text. If overruled, explain reasons.

Comments:

In response to DPO comments:

- We have confirmed with Ring Central that recordings can be deleted sooner should this be needed. Users with Manager permission will have the ability to do this and staff have been advising through training and desk aids to ensure all special category data is masked and if recorded, to flag with a supervisor to delete immediately.

  The recordings are on the live system for 30 days, they then are in the "back" system for an additional 30 days before they are automatically removed, therefore if requested for a SAR or complaint, if this was after 30 days, we could request the recording from Ring Central.
- It has been confirmed and tested during this project that calls transferred through to back office will cease recording at the point of transfer, therefore significantly lowering this risk.

• I have highlighted comments made by Alex Tuplin, security analyst. in bold to make these clear. • To be clear, PSPS are the data controller for the call recordings.		
Consultation responses reviewed by:	Click here to enter text.	Click here to enter text. If your decision departs from individuals' views you must explain your reasons.
Comments: Click here to enter text.		
This DPIA will kept under review by:	Click here to enter text.	Click here to enter text. The DPO should also review ongoing compliance with DPIA.