

A decorative horizontal bar with a dark grey, slightly wavy, and asymmetrical shape.

Contact the BSA Data Protection Impact Assessment

Document Information	
Document Title	Contact the BSA Protection Impact Assessment
Customer	NHSBSA
Author	[REDACTED]
Date	26 th September 2018

Document Control					
PM	Ref	Information Asset Owner	Version No	Issue Date	Amendments
	1.0	[REDACTED] and Dan Britton		Oct 2018	First Version

Identify the need for a DPIA

The DPIA identifies and assesses privacy implications where information (data) about individuals is collected, stored, transferred, shared, and managed. It should be process rather than output orientated.

The purpose is to have the potential to detect and mitigate information risks, as well as to modify plans accordingly.

More specifically this means:

- consider the types of personal data it is processing;
- reduce the risk of harm to individuals through the misuse of their personal information;
- design more efficient and effective processes for handling personal data; and
- question whether it is necessary to process personal data to provide a service or deliver a project.
- Meeting our legal obligations under GDPR


The recommendations column in the following tables is to document the outcome of discussing the question responses with Information Governance.

1. Project Details

Project name/title	<i>Contact the NHSBSA</i>
<p>Description and purpose of the initiative –</p> <p>The initial aim of the project will be to explore the technology market to help inform and shape the future of how we receive and manage customer contact into the NHSBSA. The project will then aim to implement new digital technology that supports our customers to self-serve and reduce the volume of transactional contact handled by advisors. This will deliver an enhanced customer experience while allowing staff to be reallocated to handle more complex customer contact.</p> <p>In order to explore different opportunities a number of trials are proposed. The existing call centre system will be changed to pass a percentage of calls to the Amazon Connect System (via a telephone number re-direct)</p> <p>Through voice automation the caller will be asked questions to ascertain what they would like to do after which they will either be pointed towards online available literature, offered information through SMS links or passed to a waiting agent to help them further.</p> <p>Prior to being passed to the agent attempts will be made to capture information from the customer which can be displayed to the agent prior to the call being answered in the form of a pop up screen thus giving them a heads up.</p> <p>Following the end of the process the caller can be pushed to CSAT if they so wish.</p> <p>As this will ultimately be delivered as a generic service to many business streams much of the detail security protection detail will be contained within the Protection Impact Assessment that is applicable for each business stream.</p> <p>This service can also update notes on a CRM so that customer notes for calls handled automatically are in line with those handled by agents.</p> <p>If a different solution is adopted in the future then this DPIA should be updated to reflect how that process differs to the pilot assessed.</p>	
Details of any link to any wider initiative (if applicable)	Detail any NHS or other Initiatives this project supports
Stakeholder Analysis List those who may be affected, e.g. Service Users, Clients, Staff-managers and practitioners, Trade Unions, Visitors, Professional organisations, IT providers, Regulators and inspectorial bodies, MPs, Councillors, Partner organisations, Strategic Sourcing, Communications	Internal: Staff and Contact Centre Agents Managers IT Service providers Capita (network and data storage) Information Governance Information Security Strategic Sourcing

	<p>External:</p> <p>Clients Partner Organisations Regulators and auditors Public Arcus Global KCOM</p>
<p>How will you seek stakeholder's views about the proposed processing?</p> <p>If you do not intend to do so then state why?</p> <p>For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable</p>	<p>If the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), you should design a consultation process to seek the views of those particular individuals, or their representatives.</p> <p>If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research. This could take the form of carrying out market research with a certain demographic or contacting relevant campaign or consumer groups for their views</p>
<p>What is already available?</p> <p>Has a PIA/DPIA been undertaken previously by any organisation using this system? Has any research been conducted? Any consultations with stakeholders?</p>	<p>PIA will exist that have been documented by the individual business streams that have been selected to be part of any trials of the service.</p>

2. Legal Basis of processing (lawfulness, fairness and transparency principle)

Item	Question	Response	Recommendation
2.1	What type of personal data are you processing?	<ul style="list-style-type: none"> • Personal Identifiers to confirm ID • Employment history • Health • Offences • Personal Opinions e.g. references and recruiting staff • Equality and Diversify declaration data • Other: UK Residency status • Short listing evaluation scores 	
2.2	What categories of sensitive personal data (Special Categories) are you will be processing?	<ul style="list-style-type: none"> • data concerning health and disability - Occupation health • offences – DBS check • Other –UK Residency status • Equality and Diversify data 	
2.3	What is the source of the information?	Customer/caller	
2.4	Is the NHSBSA processing this information on behalf of another organisation other than DHSC? If so please name them	NHS England	
2.5	In which countries is the information being processed in?	Processing is in Ireland, Frankfurt and UK but data storage is in UK. In case of a hard Brexit Cloud hosting can be UK based.	
2.6	What is the legal basis for processing this information – consent, public interest, Contract, Directions, regulations, legitimate interests?	<p>Employment contract, NHS Terms and Conditions, employment law For all other call streams – Legitimate Interest</p>  <p>Call AI Legitimate Interests Assessment</p>	<p>GDPR Article 6(1)(b) necessary in order to take steps at the request of the data subject prior to entering into a contract;</p> <p>GDPR Article 9(2)(a) and DPA 2018 Section 10(1)(a) necessary for UK employment and social security and social protection law;</p>
2.7	Are you relying on different legal grounds for different categories of personal data?	Yes GDPR Article 9 for Special Category information	
2.8	Are sensitive personal data being differentiated / separated from other forms of personal data?	No <10 staff have access as they all manage recruitment on behalf of clients – for the trail. Full roll out ~60 for HRSS – hundreds for other call streams	
2.9	Is the processing intrusive to	Yes but only used if role requires	



	privacy? If so what public benefit does it provide and how does this outweigh the privacy intrusion? Explain any possibility of disparate treatment of individuals or groups	DBS checks or the health history of the candidate justifies an Occ Health referral. Reference, ID and residency checks follow <u>NHS Employment Check Standards</u> Loss recovery – wrong doing	
2.10	Is there a duty of confidence for any of the data being processed?	Yes for occupational health evidence the HRSS and client will only receive a summary report rather than detailed medical specifics. For DBS report the decision and report would be made by the HR client.	
2.11	How will that confidentiality be maintained?	HR Recruitment only - Occupational Health Provider uses medical professionals subject to an ethical code of conduct. Breaches can result in severe consequences to their career. DBS checks are not processed but instead the recruitment manager liaises with the candidate. There is nothing in ESR that would indicate a candidate was recruited on restricted duties due to offences disclosed in a DBS check. HRSS Administrators do not have access to this information on TRAC without specialist additional permissions which are tightly managed by 2 administrators	
2.12	For third party sourced information what is the legal basis for their obtaining that information before providing it to the NHSBSA?	N/A	<i>[IG – detail the specific legal basis]</i>

3. Processing Purposes (Purpose Limitation Principle)

Item	Question	Response	Recommendation
3.1	What are the purposes of processing the personal data?	<ul style="list-style-type: none"> To allow contact for the customer and to record notes of the call Reducing call times Record of previous contact Improved MI Reduced hand-offs 	
3.2	What are the effects on the individuals whose information you are processing?	<p>Asked privacy intrusive related health questions about absence or disability for occupational health referrals</p> <p>Allegations under Grievance and disciplinary will be affect the wellbeing of the staff affected by the actions/behaviour being investigated</p> <p>Restructures will result in data subjects needing to make important decisions about their future</p>	

		Loss recovery – distress of caller	
3.3	What are the specific as well as wider benefits of this processing?	Shorter call handling times Improved MI	
3.4	Does the project involve the use of existing personal data for new purposes?	No	
3.5	What checks are being made to ensure that further processing is not incompatible with the original purposes for which it was obtained /captured?	Feeding back office processes	
3.6	Are we changing how the information is captured or sourced? If so please provide details	Yes we are changing how some information will be captured when individuals contact the BSA	
3.7	Are we changing the technology we use and if so how are we mitigating the privacy affects?	Yes the technology is changing, currently piloting to assess the benefits and risks	
3.8	Are we accelerated information processing and decision making and if so how?	Automated voice recognition is being introduced to aid customer decision making and the efficiency of handling the customer's needs.	
3.9	Are we Consolidation and linking files and systems and if so how?	Yes we are linking some of the new technology being introduced to some of the existing NHSBSA systems.	
3.10	Are we deriving / inferring data on individuals and if so how?	No	
3.11	Are we building a profile of individuals?	No	
3.12	Does the system analyse data to assist in identifying previously unknown areas of note, concern, or pattern?	Yes – in order to maximise benefits	

4. Uses of the Personal Data (Data Minimisation Principle)

Item	Question	Response	Recommendation
4.1	Summarise how the individuals data will be used	 HRSS trial info.xlsx  Microsoft Excel 97-2003 Worksheet	
4.2	Will this system/process provide the capability to identify, locate, and monitor individuals?	Yes – allows to identify an individual No – tracking and location	
4.3	How have you ensured that only the minimum data is used to meet the purpose of processing it. e.g. each data item is justified and periodically reviewed?	Policies clearly state retention periods and the commencement of pre-employment checks needs client Recruitment manager to approval as only undertaken when a job offer is accepted. Depending on what information is divulged voluntarily by the caller.	
4.4	What consideration has been given to making the identity of the individuals so that their identity is only accessed when needed?	Only asking questions to support the back end processes of the area.	
4.5	Are items of personal data held in every case which is only relevant to some customers?	Yes. We will be capturing information relevant to the call stream	
4.6	Are users compelled to provide the information to us and if so why?	No they can refuse and be passed to a Call Centre Agent. However the agent may be unable to proceed with the call if the person is not willing for information to be stored. Example being job applicants not wanting information stored in Sales Force. Other contacts mechanisms remain in place	
4.7	How many individuals processed through this system in a given time period?	Trial will be small – post roll out volumes could be UK wide	
4.8	Is the source of that data identified in the customer record?	Yes	
4.9	How often will the information be used?	Frequently first and follow up contacts and analysis of data.	

5. Data Quality (Accuracy Principle)

Item	Question	Response	Recommendation
5.1	What is the impact on the individual and the NHSBSA of the information being inaccurate or out of date?	Call could be longer than necessary as well as repeat calls. Inconvenient business decisions being made further downstream – i.e. benefit delay, wrong business decisions (recruitment)	
5.2	How are personal data checked for accuracy?	On-going monitoring of the new technology to check for accuracy	
5.3	How frequently is the personal data updated or what would trigger the information being updated?	Updated during contact.	
5.4	What action would be taken to correct inaccurate personal data?	Change record and agree with customer in the process	
5.5	Under what circumstances would we check the accuracy of the data with the Data Subject?	eDBS check report, Occupational Health report, recruitment interview, candidate advises of an error, exemptions, benefits – other business critical decisions	
5.6	Are the sources of the personal data recorded in the record?	Yes	
5.7	Are there procedures to monitor the factual relevance, accuracy and timeliness of free text/comments about individuals?	Inaccuracy monitored through the process of data use.	
5.8	Is the quality of the information good enough for the proposed purpose(s)?	Yes – assured in an on-going process	
5.9	Are procedures in place for maintaining a comprehensive and up-to-date record of use of personal data?	Yes - call flows and process flows	
5.10	How often is this record of personal data use checked?	As required by back end review processes More often as part of pilot analysis	

6. Personal Data Retention (Storage Limitation Principle)

Item	Question	Response	Recommendation
6.1	How long are we holding the information for?	See embedded file in 4.1	
6.2	What is the business justification for holding the information for this length of time? Is this based on established guidelines?	Data analysis Quality monitoring	
6.3	Are there exceptional circumstances for retaining the data for longer than the normal period? If so please give the justification for this	Legal case	
6.4	How often is this retention period reviewed?	Annually	
6.5	Is the retention period reflected in the NHSBSA retention schedule on the NHSBSA website?	Yes https://www.nhsbsa.nhs.uk/sites/default/files/2017-	

		09/NHSBSARM012%20Records%20management%20retention%20schedule.xls	
6.6	Who has approved the retention period?	BSA Corporate team in consultation with GDPR forum members which included HRSS representatives. Contact Centre team	
6.7	What format and controls exist for the archiving of the information?	Within Salesforce various tools are provided to enable archiving or deletion of records for more specific data management purposes in line with retention policy etc	
6.8	If the data is held electronically, is the deletion process automated or manual?	The deletion process can either be carried out manually using the mass deletion tools or automatically using macros or workflow rules defined.	
6.9	How are we destroying the information?	The information is logically destroyed it is not physically destroyed according to ISO27001 https://trust.salesforce.com/en/compliance/	
6.10	Are there different procedures for destroying sensitive personal data?	Salesforce have assured their services to be GDPR compliant and details can be found here: https://www.salesforce.com/gdpr/platform/	
6.11	Do we receive certificates of destruction?	Data stored on the physical servers within the Salesforce data centres is held for 30 days after the end of contract and then permanently deleted. We will not certificate data deletion as a rule - according to ISO27001 https://trust.salesforce.com/en/compliance/	
6.12	Where are the records management procedures documented?	Hub and HRSS Network drive	

7. Fair & Transparent Processing (Lawfulness, Fairness and Transparency Principle)

Item	Question	Response	Recommendation
7.1	What does the privacy notice state? Please include any variations for paper, perhaps due to space limitations	Yes – covered by existing privacy notice on the website.	
7.2	When are individuals made aware of how their personal data is being used?	privacy notice issued on KCOM and website Will be added for clients privacy notice for recruitment purposes	Recruiters could be made aware through a link to the privacy notice in email footers that include the telephone number to ring for HRSS.
7.3	Does the privacy notice include ALL of the following: <ul style="list-style-type: none"> the purpose of processing the legal basis of the 	Yes. Clients given example of NHSBSA GDPR privacy notice and have provided their own notices	

	<p>processing consent, contractual obligation, public interest grounds or details of the statutory basis,</p> <ul style="list-style-type: none"> • who we share the information with • Details of any automatic decision making • how long we retain the information or the criteria for retaining the information, who it is may be shared with, • which if any country outside the EEA the information is processed in, • IG contact details • Make individuals aware of their information rights <p>Right to lodge a complaint with the ICO?</p>		
7.4	Is the privacy notice concise, easily accessible, easy to understand and uses clear and plain language?	Yes	
7.5	Do we tell individuals about the use of cookies and other tracking technologies and are these changing?	NA	
7.6	Do you receive information about individuals from third parties?	Yes, someone acting on behalf of the customer, or an external client	
7.7	Do we state the consequences to the individual of not providing certain information?	NA – as caller will be passed to call agent	
7.8	Are there any current issues of public concern that you should factor into how you process this information?	N	

8. Data Sharing and Disclosure (Integrity and Confidentiality Principle)

Internal

Item	Question	Response	Recommendation
8.1	Name the organisation involved in this process/system working on behalf of the NHSBSA	Arcus Global Ltd	
8.2	How do you plan to ensure the processor complies with privacy requirements about the information shared with them?	Arcus do not retain ANY client data outside of the system itself. Any data used for migration testing purposes is securely destroyed and/or returned with a guarantee that no information has been retained or stored. We have a procedure for ensuring that all possible sources of non-system client data have been purged at the end of project implementation and again at the end of contract on off-boarding.	

8.3	Which team(s) and roles have access to the information? Please include contractors working on our behalf	Limited access during the trail. Post trail – all BSA call agents could be using the technology	
8.4	How many people is this? (Not WTE/FTE)	<10 for pilot. Hundreds of trained staff post pilot	
8.5	How are system users maintained and what is the frequency of this being audited for leavers / joiners / movers / escalated access?	<p>The Arcus Solution allows for security to be applied [REDACTED] [REDACTED] Page layouts may be configured against roles or individual users to display information which the user has access to on a field by field basis.</p> <p>Together with other settings, the profile determines what tasks users can perform, what data they see, and what they can do with the data. User permissions and access settings are [REDACTED]</p>	<p>Section 31</p> <p>Section 31</p>
8.6	Which records/functions are restricted so that users only access the information they need to access for their role?	Systems have role based access controls HRSS have a restricted LAN folder due to the sensitive nature of the work they deal with	
8.6	Is unauthorised browsing of this information restricted and staff trained for awareness of this?	Systems provides details of who edits records and when. Connect provides details of who answered the call, when, how long the call lasted and other statistics; it also keeps a recording of the Agent part of the call.	
8.7	Describe what privacy training is provided to users specifically relevant to this process or system?	Built into existing processes within the team	
8.8	Are reports provided to staff outside the above teams? If so who receives them?	Yes – recruiting managers from HRSS client(s) Senior management, CCS.	
8.9	How are internal reports distributed?	Email to named individuals involved who have a business need to know	
8.10	Are the internal reports appropriately labelled as "sensitive" if they contain sensitive information?	No – statistics only	
8.11	How are any international transfers of personal data safeguarded?	<p>Salesforce have assured their services to be GDPR compliant and details can be found here: https://www.salesforce.com/gdpr/platform/</p> <p>The Salesforce platform provides built in tools to support GDPR requirements including right to be forgotten, consent, data security, restriction of processing and data portability. Our solution is built around these controls to assure the NHSBSA that all personally identifiable information is managed in a GDPR compliant manner. Consolidating onto</p>	

		the platform and actually removing back office legacy systems will make GDPR much as easier to manage for SDC in the future and is unique to our solution.	
--	--	--	--

External

8.12	How do internal and external auditors access information in the system?	They would need to ask for specific details to be provided by back end service and agree a secure way of delivering the information.	
8.13	What interfaces are there to other systems?	In this instance the only integrations are to Amazon Connect and Symbee. Symbee is used as a pass-thru mechanism and no data is retained within it. Amazon Connect is used to handle the calls and call recordings. The only personal data stored is the call recording itself and details of the customer contact along with information provided during the call. In both instances this is stored encrypted within the UK and is automatically deleted after 6 months.	
8.14	Are there any requests for information held in this system you would not refer to IG?	No	
8.15	Have Data Sharing agreements been authorised by IG?	Yes – part of existing MOU	
8.16	Is any of the data likely to be exempt from disclosure under FOI and if so why?	Yes. Either as confidential (section 41) or personal data (section 40)	

Summary Data Flow:



AI Call Centre - data flow - drawio (1).jpg

9. Technical Access and Security (Integrity and Confidentiality Principle)

Item	Question	Response	Recommendation
9.1	Have you completed a Security Assurance Triage on this process/system?	Yes. Assured by Information Security. No concerns raised.	

10. Information Rights

Item	Question	Response	Recommendation
10.1	How would you locate all personal data relevant to an individual?	All data indexed and filed by individual on Salesforce	

		Other teams (CCS) would have access to required information	
10.2	How would we handle requests from vulnerable adults or those you require reasonable adjustments under equality and diversity legislation?	Refer to client IG	
10.3	Do you have a documented explanation of any codes or other information likely to be hard for the customer to understand?	No – Staff would be familiar with ESR and HR terms used.	
10.4	Are any decisions affecting individuals made solely on processing by automatic means? If so where are these documented and are they in plain language and readily accessible?	No	
10.5	How are individuals notified of the procedures for correcting their information?	Yes – through privacy notice on website	
10.6	Would we note the records if a discrepancy was pointed out by the customer/patient or amend/delete as appropriate?	Yes. Given the short periods for which information is held the likelihood that data would need correcting is low. The application confirmation email directs people to contact us if they have an enquiry about their application. Once the application is picked up the applicant (data subject) would have contact details for the administrator leading the recruitment campaign.	
10.7	What is the procedure for this system to responding to data subject's request to be forgotten	Refer to client IG	
10.8	What is the procedure for this system for responding to data subject's notice requiring that they be adding to a stop/suspend filter list to prevent processing?	If candidate asked to withdraw then client HR would be notified but records would be retained according to retention rules	
10.9	Do individuals have the right to restrict processing for other purposes and if so how and when are they offered this?	Refer to client IG	

11. Privacy issues identified and risk analysis

Any privacy issues which have been identified during the DPIA process (for example: no legal basis for collecting and using the information; lack of security of the information in transit, etc.) should be documented in the risk register template embedded below. This risk register will enable you to analyse the risks in terms of impact and likelihood and document required action(s) and outcomes.

Note that where it is proposed that a privacy risk is to be 'accepted', approval for such acceptance should be sought from the Caldicott Guardian where patient data is concerned and the SIRO for all strategic information risks.


Where the mitigated risk remains high then this must be referred to the ICO via the IG Team. This is a legal requirement of the GDPR.

There are no risks that require further mitigation action in the embedded spreadsheet.



DPIA Risk
Template.xlsx

12. Data Protection Principles Compliance and Authorisation

CCS Information Asset Owner / Administrator	Name: Dan Britton Date: Signature:
Reasoning behind the decision to accept or reject the identified privacy risks and any decision to disregard the views of anyone consulted on the proposed processing	
HRSS Information Asset Owner / Administrator	Name: [REDACTED] Date: Signature:
Reasoning behind the decision to accept or reject the identified privacy risks and any decision to disregard the views of anyone consulted on the proposed processing	
Information Governance Lead (Mandatory in all cases to comply with GDPR legal requirements)	Name: Chris Gooday Date: 18/10/2018  Signature:
IG advise on how whether: <ul style="list-style-type: none"> • you've done the DPIA correctly; • if the processing achieves its purpose and in a proportionate way, • the outcome of the DPIA • adequacy of progress towards planned mitigations and • whether the processing can go ahead 	
The Privacy controls for this pilot are well established with: <ul style="list-style-type: none"> • Clearly defined reasons for collecting data • very limited personal data retention • a clear legal purpose • Privacy notices published for transparency • Callers able to opt out easily 	

- Accuracy being actively assessed
- Security assessed and assured
- No compromise of data subject rights

This should be reviewed annually or when changes are made to how personal data is processed.

Appendix 1 -Personal Data

A thorough assessment of privacy risks is only possible if we fully understand how information is being used. The table below lists and describes all the personal data processed and stored. It also includes a justification of the requirement for its use.

Please ensure you include all the personal data and not just the data items that allow an individual to be identified. GDPR defines personal data to be:

“any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”. This can therefore include cookies, Wi-Fi identifier and location of any personal mobile devices.

We need to consider which personal data we will not use, without compromising the aims of the project/process

See spreadsheet embedded in answer to question 4.1

Appendix 2

Glossary of Terms

Definitions

Delete and add to the following table as necessary. This may need to be completed once the Agreement has been completed in as much detail as possible to ensure all definitions are included.

In this Agreement the following words have the following meanings:

Controller	This is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;.
Data Protection Legislation	the Data Protection Act 2018 (DPA), the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to Processing of Personal Data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.
Processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; (other than an employee of the controller). This means that the person processes data for a purpose and according to a manner determined by the controller, and makes no independent determination of such matters.
Data Protection Principles	These are set out in Appendix 3 attached to this Agreement and are required to be followed to ensure compliance with GDPR.
Data Subject	Data subject means an individual who is the subject of personal data.
'Fair' processing	All controllers must have a Fair Processing Notice (otherwise known as a Privacy Notice), which is available to data subjects. A Fair Processing Notice is intended to make sure that data subjects are aware of how data is collected and used by the data controller. It aims to ensure that data controllers process personal data fairly and lawfully. Fair Processing Notices may be in oral or written form. The DPA sets out that, at a minimum, Fair Processing Notices should contain the following information - who the data controller is, what the data controller intends to do with their information and any other relevant information e.g. in the context of data sharing who the data will be shared with. Fair Processing Notices may also be used to provide additional information such as informing people about their subject access rights or the data controller's security arrangements.
General Data Protection Regulation (GDPR)	The new Data Protection Law known as the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council)
Joint Controller	1.Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation

	<p>[GDPR], in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects</p> <p>2.The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controller's <i>vis-à-vis</i> the data subjects. The essence of the arrangement shall be made available to the data subject.</p> <p>3.Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.</p>
Personal data	<p>'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as:</p> <p>a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person</p>
Data Protection impact assessment (DPIA)	<p>the controller shall, prior to the processing,[commencing] carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where it is likely to result in a high risk to the rights and freedoms of individuals. A single assessment may address a set of similar processing operations that present similar high risks.</p>
Processing	<p>any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction</p>
Special Categories	<p>GDPR defines this as Processing of personal data:: -</p> <ul style="list-style-type: none"> • revealing racial or ethnic origin, political opinions, • revealing religious or philosophical beliefs, • revealing trade union membership, • processing genetic data, • biometric data for the purpose of uniquely identifying a natural person, • data concerning health or • data concerning a natural person's sex life or sexual orientation <p>This does not include actual or alleged offences.</p>

Appendix 3

Associated Legislation

Data Protection Principles

The seven GDPR principles

All uses of personal need to comply with the following:

<u>Principle</u>	<u>Definition</u>
<u>1st</u>	Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
<u>2nd</u>	Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
<u>3rd</u>	Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
<u>4th</u>	Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
<u>5th</u>	kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
<u>6th</u>	processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
<u>7th</u>	The controller shall be responsible for, and be able to demonstrate compliance with the above principles ("accountability")

GDPR Conditions for processing: -

Article 6	Article 9
<p>Personal Data</p> <ul style="list-style-type: none"> • (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; • (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; • (c) processing is necessary for compliance with a legal obligation to which the controller is subject; • (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; • (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; • (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. • Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks. 	<p>Special Categories of Personal Data</p> <p>1.Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.</p> <p>2.Paragraph 1 shall not apply if one of the following applies:</p> <ul style="list-style-type: none"> • (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; • (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; • (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; • (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; • (e) processing relates to personal data which are manifestly made public by the data subject; • (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; • (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; [It is likely the ICO would need to approve this first] • (h) processing is necessary for the purposes of

	<p>preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;</p> <ul style="list-style-type: none"> • (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; • (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. <p>3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.</p> <p>The UK have provided for these in the Data Protection Act 2018 schedule 1 as outlined on the next page.</p>
--	---

Data Protection Act 2018 Conditions for processing: -*Those on red below are the most likely to apply*

Schedule 1 paragraph	Processing covered
1	Employment, social security and social protection
2	Health or social care purposes
3	Public health
4	Research etc
5	Requirement for an appropriate policy document when relying on conditions in Part 2 as follows
6 and 7	Parliamentary, statutory and government purposes
8 and 9	Equality of opportunity or treatment
10	Preventing or detecting unlawful acts
11 and 12	Protecting the public against dishonesty etc
13	Journalism etc in connection with unlawful acts and dishonesty etc
14	Preventing fraud
15	Counter terrorism and money laundering
16	Support individuals with disability or medical condition
17	Counselling etc
18	Safeguarding children and vulnerable adults
19	Safeguarding economic well-being of certain individuals
20	Insurance
21	Occupational pensions
22	Political parties
23	Elected representatives responding to requests
24	Disclosure to elected representatives
25	Informing elected representatives about prisoners
26	Publication of legal judgments
27	Anti-doping in sport
28	Standards of behaviour in sport
29	Consent
30	Protecting individual's vital interests
31	Processing by not-for-profit bodies
32	Personal data in the public domain
33	Legal Claims
34	Judicial acts
35	Administration of accounts used in commission of indecency offences involving children
36	Substantial public interest
35	Extension of Insurance conditions

Human Rights Act 1998 and the European Convention on Human Rights

Data sharing by public authorities must comply with the European Convention of Human Rights (now part of the UK domestic law as a result of the Human Rights Act 1998), and in particular Article 8, which provides:

“Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

Processing personal data (including sharing it) will often constitute an ‘interference’ with the right to respect for private and family life within the meaning of Article 8. However, interference will be compatible with Article 8 if it meets the requirements of Article 8(2).

The interference must be ‘in accordance with the law: it must have a proper basis in national law and that law must be adequately accessible and foreseeable.

If a public body has a lawful basis for sharing data, as set out in section 3 above, then it is likely that this requirement will be met.

The interference must answer a ‘pressing social need’, which will be the case if it pursues a legitimate aim in a proportionate manner and is accompanied by appropriate safeguards.