Service or Business Process

Data Protection Impact Assessment (DPIA)

Use this form to assess a service or business process, or where Delt is the controller.

*Data processing includes **anything** that might be done to data during its lifecycle, from creation through storage, use, maintenance, sharing etc. to archive and destruction.*

The Information Commissioner's Office guidance is here and contains guidance about basis for processing personal data, the rights of individuals and other GDPR and DPIA 2018 information.

Service or Process	
Owner	
Owner's job title	

The owner will usually be the member of SLT with overall responsibility for the service.

Completed by	
Date completed	

Overview

Briefly explain what the service or process aims to achieve or deliver.

Delt's role	
Check all that apply	
☐	Delt staff are the primary users of the data. Either in the course of providing a service or in running our own organisation.
☐	Delt's IT function will maintain or make changes to the data (e.g. automated batch processes, uploading, creating/maintaining interfaces…)
☐	Delt will make the data available to a supplier to enable them to operate a data service on our behalf

Section 1

Describe the Information Flows

How will data be collected?	
Who will provide it? Where will it come from (its source)?	
Is the data secure by design?	
Will pseudonymisation be used on personal data?	
How will data be received?	
Will the individual add the data themselves? Will we manually add it? Is it being imported or is there an interface to another system, what system?	
Where is it stored?	
Geographically where does the data reside when it is 'at rest'. Do we host it? If a third party supplier holds the data, where are their data centres?	
How will data be used?	
e.g. What will it be used to do? How will it be manipulated?	
What is the context of the processing?	
What is the nature of our relationship with the individuals? How much control will they have? 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 you should factor in?	
Is any of the processing likely to be high risk?	
e.g. Systematic monitoring of a publicly accessible area on a large scale; automated processing producing legal or significant effects on the individual; large scale processing of personally sensitive or criminal convictions or offences.	
If the processing is large scale, how many records do you estimate will be processed, to the nearest 100,000?	
A rough estimate will help in assessing the impact and context of risks.	

Identify the Privacy Risks

Principle 1: Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

1.1	**What personal data will be collected?**	
A general description of the types of information included in the data, particularly data about individuals e.g. names, addresses, date of birth, details of services requested, reports made…		
1.2	**Does the data include children or other vulnerable groups?**	
If so, which groups and what personal data relates specifically to them?		
1.3	**Are Delt sharing, or enabling the sharing of any of the personal data? If so how and with whom?**	
e.g. it is reportable to a third party, there is a contract to share it, a third party hosts the data or has access to where it is stored in order to perform upgrades, issue investigation etc.		
1.4	**How will individuals be told about the use of their personal data?**	
Best practice is that this is a layered approach. Explain all methods that will be used, e.g. point of collection, fully documented in our Privacy Notices etc.		

1.5	**Conditions for Delt's activities, or activities that we contract a sub-processor to carry out on our behalf, as part of the service.**
*For **all** data processing carried out, in providing services or running our own organisation. Check all that apply*	
☐	The processing is necessary for the performance of a contract with a customer organisation. (Contract) *E.g. we have a contract with PCC to provide IT support and Payroll services, it is therefore necessary for us to process information about their staff who receive those services.*
☐	The processing is necessary for the performance of a contract directly with the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. (Contract) *E.g. would include Delt job applicants or data processing that required as part of the contractual relationship with a Delt employee, could include suppliers or suppliers involved in a tender process.*

☐	The processing is necessary for compliance with a legal obligation to which Delt is subject. (Legal Obligation)
☐	The processing is necessary to pursue legitimate interests of Delt or a third party, except where those interests are overridden by the interests, rights or freedoms of the data subject. (Legitimate Interests)
☐	The processing is necessary in order to protect the life of the data subject or another person. (Vital Interest)
☐	The data subject has given consent to the processing for one or more specific purposes. (Consent) Consent needs to be freely given (so isn't a good idea where the organisation has power over the data subject e.g. employees), needs to be evidenced and can be withdrawn by the data subject.

1.6	**Does processing include any of the following data (known as special category)?**
Check all that apply, or are likely to apply	
☐	Data revealing racial or ethnic origin
☐	Political opinions
☐	Religious or philosophical beliefs
☐	Trade-union membership
☐	Genetic or biometric data for the purpose of uniquely identifying a data subject
☐	Data concerning health
☐	Data concerning the sex life or sexual orientation of a data subject.
If our processing includes these special category data types, which of the following legal basis applies?	
If the data processed contains any of the data types above a second basis for processing is required. Check all that apply	
☐	The data subject has given **explicit** consent to Delt to process their data for this purpose. (Explicit Consent) Consent needs to be freely given (so isn't a good idea where the organisation has power over the data subject e.g. employees), needs to be evidenced and can be withdrawn by the data subject.
☐	The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of Delt or of the data subject in the field of employment and social security and social protection law. (Employment / Social Protection)
☐	The processing is necessary for the establishment, exercise, or defence of legal claims, or whenever courts are acting in their judicial capacity. (Legal Claims)

☐	The processing is necessary for the purposes of 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. (Medical Purposes)
☐	The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (Historic Archiving)
☐	The processing is necessary for reasons of substantial public interest. (Substantial Public Interest)
☐	The 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. (Public Health)

1.7	**If we are relying on consent to process personal data (1.5 or 1.6), how will this be collected and recorded?**

What will you do if consent is withheld or withdrawn? How will this be recorded?

Can an alternative condition for processing be used instead of consent? If yes, please provide details.
Remember that if the data being processed is special category you need to use the special category basis for processing!

1.8	**How will individuals be informed at the point of collection about how their personal data will be used?**

1.9	**Will any personal data be published on the Internet or in other media? If yes, please provide details.**

1.10	**Will a third party contractor be processing the personal data on our behalf, or involved at any stage in the data processing process? If yes, describe the scope of their processing.**

Does someone who isn't Delt or the customer host the data? Do they have access to the application to perform maintenance or fault find? This all counts!
If a third party contractor is involved, what measures will you take to ensure processors comply with Data Protection legislation?
e.g. Contract terms/Data Sharing Agreement, check, penetration testing, supplier information security and compliance questionnaire…

Principle 2: Purpose Limitation

Personal data shall be collected for specified, explicit, and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.

Do you envisage using the personal data for any purpose not already listed on this form in the future? If so, please provide details.

Principle 3: Data Minimisation

Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

3.1	**Are you satisfied that the personal data processed is of good enough quality for the purposes proposed? If not, why not?**
3.2	**Is there any personal data that you could do without, without compromising the needs of the project or service? If yes, please provide details.**
3.3	**How will you ensure that only personal data that is adequate, relevant, and not excessive in relation to the purpose for which it is processed?**
i.e. Only collecting what is needed, not what might be useful one day or isn't required for the current purpose at all.	
3.4	**If the service processes personal data for a customer organisation, does the customer have any requirements for Delt's processing? If yes, please describe and explain how you will meet them.**
e.g. Contract terms/Data Sharing Agreement, check, penetration testing, supplier information security and compliance questionnaire…	

Principle 4: Accuracy

Personal data shall be accurate and, where necessary, kept up to date.

4.1	**Are you able to update and amend personal data when necessary, after it has been collected and recorded? Please provide details.**
4.2	**How will you ensure that personal data obtained from individuals or other organisations is accurate?**
4.3	**If the service processes personal data for a customer organisation, does the customer have any requirements to ensure data is accurate? If yes, please describe and explain how you will meet them.**
e.g. data matching/validation checks, interfaces that update information from a master data set, report configuration relating to data changes or conflicts	

Principle 5: Storage Limitation

Personal data shall be 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.

5.1	**What retention periods are suitable for the personal data you will be processing?**
What is the corporate retention period of the information the system holds? If the data is temporarily held, how long does Delt and any IT systems retain what it records for?	
5.2	**How will you ensure the personal data is deleted in line with your retention periods?**
5.3	**What processes will be put in place for the destruction of the personal data?**
5.4	**Data storage arrangements. The Service/Technical Design achieves all of the following:**
☐	Includes details of how long data will be retained in the system.
☐	Includes details of any data backup arrangements.

☐	Includes details of Delt activities required relating to retention and disposition of the live or backup data.
5.5	**If data is deleted from the live system, does it also get deleted from the backups?**
5.6	**Can data held in backups be flagged as not for restore to the live service?**
For example, if a data subject has exercised their right to erasure and data is deleted from the live system, but there is a later problem with the system and Delt needs to use the backups to bulk restore data the data subject's data will not be returned to the live system.	

Principle 6: Integrity and confidentiality (security)

Personal data shall be 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.

6.1	**Where, and in what format/s, will the personal data be kept?**
6.2	**Will an IT system/s or application/s be used to process the personal data? Please provide details.**
6.3	**How will this system provide protection against security risks to the personal data?**
6.4	**What training and instructions are necessary to ensure that staff know how to operate the system securely?**
6.5	**Will staff ever process the personal data away from the office (e.g. via paper files, on laptops, tablets, or smart phones)? If so, please provide details.**
6.6	**How will access to the personal data be controlled?**
For example, end users or types of end users with different access levels, controls used for admin functions, authorised elevated permissions for short periods of time.	
6.8	**Are there any business continuity arrangements for this service?**

7: Transfer of data

7.1	**Will Delt transfer any data**
This includes where the storage it resides on is geographically located, and those of any known sub-processors used by suppliers; any 24 hour 'follow the sun' support services (so the data can be accessed from outside the EEA). It doesn't include anything the customer organisation itself choses to do which Delt will not have visibility or an active part in.	
☐	To the European Economic Area (EEA)
☐	Outside of the UK or EEA

7.2	**If you will be making transfers out of the UK, how will you ensure that the personal data is adequately protected?**

7.3	**If a contractor is being used to process the personal data, where are they (and their data stores) based?**
This includes where the storage it resides on is geographically located (including backups), and those of any known sub-processors used by suppliers; any 24 hour 'follow the sun' support services (so the data can be accessed from outside the UK or EEA). It doesn't include anything the customer organisation itself choses to do which Delt will not have visibility or an active part in.	

8: Right of Access and Marketing

Personal data shall be processed in accordance with the rights of data subjects under this Act.

8.1	**If an individual requested a copy of the personal data held about them, detail how this would be provided to them.**
What is the processing for extracting it? Is it readable/clear at that point, or does it need to be changed so that it is an easily understandable format for the data subject (this is required by law)? Can they 'self serve'?	

8.2	**If the service involves marketing, have you got a procedure for individuals to opt out of their personal data being used for that purpose?**

In Summary

Are you satisfied that the Delt's processing of data is/will be legally compliant?	
☐	Delt's use of personal data is legally defensible.
☐	You can evidence that Delt's responsibilities and activities are documented (for example in a Service or Technical Design which has passed review).
☐	You can evidence that Delt has documented processes for any ongoing data processing activities that will be carried out.
☐	You can evidence we have clearly defined the role and responsibilities of any additional data processers we will use.
Where Delt is a supplier who processes data for a customer organisation	
☐	To the best of your knowledge, the data Delt has been instructed to process has been obtained legally.
☐	You can evidence that Delt's role and responsibilities in the data processing are documented and authorised by the customer.
☐	You can evidence that there is a process to identify and immediately notify the controller of any personal data breaches or data protection infringements relating to this service (or change to an existing service).

Section 2

Risk Register

Ref	Describe the source of risk and nature of potential impact on individuals.	Probability	Impact	Overall risk	Mitigation	Probability	Impact	Residual risk rating	Measure approved
	Include associated compliance and corporate risks as necessary.	*1-5*	*1-5*	*Probability x Impact*		*1-5*	*1-5*	*Probability x Impact*	*Back office only*

See table below for guide to assessing risk

Probability	Rating	Impact	Rating
1 - Rare	1	1 - Insignificant (Low - no business impact)	1
2 - Unlikely	2	2 - Minor (low - minor business impact, some loss of confidence)	2
3 - Moderate	3	3 - Moderate (medium - business is interrupted, loss of confidence)	3
4 - Likely	4	4 - Major (high, business is disrupted, major loss of confidence)	4
5 - Almost Certain	5	5 - Catastrophic (high - business cannot continue)	5

Calculating Overall Risk and Risk Rating

Score	Rating	Action
15-25	High	Immediate action required to mitigate the risk or decide not to proceed
5-14	Medium	Action should be taken to compensate for the risk
1-4	Low	Risk should be monitored and tolerated

Don’t forget that risks may also need to be added to the project, change or corporate risk registers!

Section 3 - Back Office Completion

Sign off and review & record outcomes

Risk Acceptance to pass gateway for DPO/SIRO review	
Integrate actions back into project plan, with date and responsibility for completion	
Name	
Date	

Name of customer or responsible data asset owner informed to update their IAR/ROPA

DPO/SIRO advice provided
DPO/SIRO will advise on compliance, step 6 measures and whether processing can proceed